RSF

REVUE DE LA STABILITÉ FINANCIÈRE

AVRIL 2016

LA STABILITÉ FINANCIÈRE À L'ÈRE NUMÉRIQUE

20

BANQUE DE FRANCE
EUROSYSTÈME

111–020

Sommaire

Études

Introduction

Les nouveaux risques pour la stabilité financière

La réglementation et l'action des autorités face à ces nouveaux risques

La transformation numérique du secteur financier : illustrations

Introduction

Construire le triangle de compatibilité de la finance numérique : innovations, stabilité, régulation

François VILLEROY DE GALHAU
Gouverneur
Banque de France

Les innovations rythment l'évolution du système financier et jouent un rôle crucial pour le développement économique. Cependant, elles peuvent avoir une contribution plus contestable comme lors de la crise financière de 2008. Au regard de leurs conséquences potentiellement systémiques, les autorités (banques centrales, superviseurs, régulateurs) y sont très attentives. Elles s'attachent à comprendre les transformations profondes qui en résultent, comme à détecter et évaluer les bénéfices et les risques correspondants pour le système financier.

Au cours des dernières années, nous avons assisté à l'irruption massive des technologies numériques dans le monde industriel (les télécommunications, l'automobile, la robotique, etc.). La numérisation gagne aujourd'hui fortement le secteur des services financiers [1]. Les cas concrets d'application se multiplient : paiements mobiles, sans contact ou instantanés ; agrégation de l'information relative aux comptes bancaires ; services d'initiation de paiement ; gestion d'actifs ; conseil en matière de placements financiers ; gestion et stockage de l'information, etc.

Dans cette nouvelle ère numérique, le centre de gravité du processus d'innovation financière paraît s'être déplacé vers de nouveaux acteurs, en partie extérieurs au système financier. Les innovations financières technologiques ne résultent plus uniquement de pressions concurrentielles s'exerçant au sein du système financier lui-même, mais de l'apparition d'acteurs externes maîtrisant les nouvelles technologies. Ceux-ci viennent concurrencer les acteurs traditionnels et remettre en cause les modalités de fourniture de certains services financiers.

Cette vague numérique s'appuie également sur une offre nouvelle, moins orientée vers la vente de produits innovants, plus centrée sur le client, lui procurant un accès instantané à une très vaste gamme de services intégrés et de toutes natures, où qu'il soit et à très faible coût. Le changement de paradigme, qui place le client au centre des préoccupations, s'est imposé sous l'influence de nombreux facteurs, principalement :

- une appétence croissante pour les solutions numériques qui a modifié de manière drastique les modes de consommation, à travers l'essor de la banque en ligne et l'exploitation de données permettant aux fournisseurs d'accès à internet d'acquérir une connaissance détaillée des préférences et du profil des consommateurs ;

- une défiance certaine du public vis-à-vis du monde bancaire au sortir de la crise financière ;

- les changements réglementaires intervenus depuis 2008, qui visent à davantage de standardisation et de transparence des transactions financières, et poussent également à la numérisation croissante des échanges (par exemple en imposant des obligations d'enregistrement, ou des obligations de compensation centrale). Le renforcement de la réglementation implique également une hausse

1 *Cf.* Revue d'économie financière, *« Innovation, technologie et finance : menaces et opportunités », n°120, décembre 2015.*

du coût de l'intermédiation, rendant possible l'entrée de nouveaux acteurs ;

• les évolutions substantielles intervenues dans le domaine du stockage et de la gestion des données. La généralisation de l'*open data* [2], qui permet d'exploiter les informations multiples collectées sur les clients, joue un rôle potentiellement important dans le développement d'outils permettant de stocker et traiter de très gros volumes de données (le *big data*). L'exploitation des flux de données à grande échelle nécessite des traitements informatiques adéquats. Le *cloud*, en offrant un système d'information étendu, potentiellement activable dans toutes les régions du monde, permet de gagner en agilité et en rapidité et de répartir ainsi les coûts sur d'autres segments d'activités.

Ainsi émerge une offre inventive et multiforme, qui tend à faire évoluer le paysage bancaire et financier vers un écosystème caractérisé par une grande hétérogénéité des acteurs : acteurs traditionnels telles les institutions financières ; grandes enseignes internationales de la sphère numérique (Google, Apple, IBM, Microsoft, Amazon, Facebook, etc.) ; opérateurs de télécommunications qui disposent d'une base de consommateurs très large et d'une forte capacité d'innovation *via* les téléphones mobiles ; mais tout autant, entreprises innovantes spécialisées dans les technologies financières, souvent de petite taille, les fameuses fintechs.

Cette transformation du secteur financier, par laquelle des entités non financières s'engagent dans des activités financières réglementées, affecte les modèles bancaires traditionnels et les conditions de fonctionnement du système financier. Le propos de cet article est d'en éclairer les différentes facettes [3] : (1) l'élargissement de l'offre grâce aux innovations numériques ; (2) les risques potentiels et les défis nouveaux pour la stabilité financière ; (3) les réponses que les autorités, banques centrales, régulateurs ou superviseurs du système financier, peuvent y apporter. Nous devons ainsi, en dynamique, construire le triangle de compatibilité entre innovations, stabilité et régulation.

1| Les innovations numériques élargissent l'offre de l'ensemble des activités bancaires, à des degrés divers

Le centre de gravité du processus d'innovation financière s'est déplacé du secteur bancaire vers de nouveaux acteurs historiquement étrangers au système financier utilisant des technologies numériques.

1|1 Les services de paiement

La banque de détail est caractérisée par une grande standardisation des opérations et des coûts fixes importants. Ces aspects structurels constituent un terrain favorable à l'apparition d'une concurrence portée par des acteurs numériques agiles disposant d'une structure de coûts moins pénalisante. Ainsi, l'essor des innovations numériques dans le domaine des paiements de détail a permis de développer une palette de solutions de paiement diversifiées, pour un coût limité, dans un contexte de forte croissance du commerce en ligne. Dès 2007, la première directive européenne des services de paiement (directive 2007/64/CE dénommée DSP1) créait une nouvelle catégorie de prestataires de services de paiement, « les établissements de paiement », afin d'encadrer les conditions de cette nouvelle concurrence [4].

À la fin de 2015, on comptabilisait 24 établissements de paiement agréés en France contre 3 à la fin de 2010. Bien que ces nouveaux acteurs s'appuient fortement sur des moyens de paiement existants émis ou gérés par les banques (essentiellement les cartes de paiement et les virements et, dans une moindre mesure, les prélèvements), ils parviennent à capter des parts de marché au détriment de ces dernières. Cependant, les flux de paiement traités par l'ensemble des prestataires disposant d'un agrément d'établissement de paiement représentent

2 *Le mouvement d'*open data *a été initié par la directive informations du secteur public (PSI) datant de 2003 portant sur la réutilisation des données publiques (directive 2003/98/CE).*
3 *Le présent article se concentre sur les mutations des prestations à la clientèle et n'aborde pas directement les apports des fintechs sous forme de services aux banques, en particulier sous forme d'analyse du risque de crédit et d'évaluation des débiteurs.*
4 *Un régime juridique spécifique pour les établissements de monnaie électronique a été créé par la deuxième directive « monnaie électronique » en 2009 (2009/110/CE).*

un montant (25 milliards d'euros en 2014) encore marginal comparé à l'ensemble des flux gérés par le système de paiements de détail français CORE [5] (plus de 5 000 milliards d'euros en 2014).

Le processus de numérisation des services de paiement prend aussi d'autres formes, de nature plus disruptive. Par exemple, de nouveaux prestataires interviennent pour faire le lien entre le consommateur et le commerçant (les tiers prestataires de services de paiement) ou pour permettre aux titulaires de plusieurs comptes d'en avoir une vue agrégée (les agrégateurs), sans pour autant être couverts par la DSP1. Les monnaies virtuelles, et en particulier la principale d'entre elles le *bitcoin*, mettent en jeu un mécanisme de création monétaire parallèle, même si leur développement demeure sensiblement plus limité que les commentaires et les analyses qui l'ont accompagné. En cherchant à concurrencer les monnaies légales, les monnaies virtuelles semblent introduire une rupture forte car elles ont pour ambition de contester le monopole d'émission des banques centrales. Mais leur usage est encore très faible : les montants échangés sont inférieurs à 100 millions d'euros par jour pour une volumétrie de moins de 200 000 opérations, à comparer aux 70 milliards d'euros de paiements correspondant à 250 millions d'opérations réalisés quotidiennement dans l'Union européenne.

1|2 Les services de financement

En matière de financement des entreprises également, la numérisation crée des opportunités d'innovation, qui dans un contexte de durcissement de la réglementation bancaire et de taux d'intérêt durablement bas, participe au mouvement de diversification de l'offre en dehors du secteur bancaire. Parallèlement, les entreprises (notamment les très petites entreprises, les petites et moyennes entreprises et les entreprises de taille intermédiaire) ont manifesté un besoin de sources de financement alternatives et mieux adaptées à leurs besoins.

C'est dans ce contexte que s'inscrit le développement des plates-formes de financement participatif ou *crowdfunding* qui permettent de répondre à de petits besoins en fonds propres ou en dettes – *crowdlending* – et constituent un complément aux modes de financement existants. En France, on compte 86 plates-formes de financement participatif en mars 2016, dont 55 intermédiaires en financement participatif sous forme de prêts, 27 conseillers en investissements participatifs [6] et 4 plates-formes ayant les deux statuts [7]. Les montants collectés ont doublé en 2015 par rapport à l'année précédente pour atteindre 297 millions d'euros, dont 197 millions en prêts, 50 millions en achats de titres et 50 millions en dons [8]. Mais ils sont encore limités au regard des besoins de financement des entreprises [9].

1|3 Les services d'investissement

En matière d'opérations sur les marchés financiers, les innovations technologiques emportent des conséquences autrement significatives, en particulier sur les modes de négociation. Les firmes de négociation à haute fréquence (NHF) constituent aujourd'hui des acteurs incontournables des marchés d'actions [10]. En Europe, elles représentent 24 % des volumes traités sur les marchés d'actions. La NHF présente deux caractéristiques qui permettent la réalisation d'un nombre très important d'opérations de taille modeste à échéance très courte, souvent infra-journalière : (i) un accès très rapide, de l'ordre de quelques millisecondes, aux plates-formes de transactions et à l'information de marché ; et (ii) le fonctionnement des algorithmes de transaction sans intervention humaine durant la période d'ouverture des marchés. Même si leur utilité économique et sociale est douteuse, l'essor rapide des firmes de NHF profite aujourd'hui de faibles barrières à l'entrée. En effet, ce sont des entités non bancaires, au capital très faible voire négligeable par rapport à celui des teneurs de marché traditionnels, les banques, dont les exigences en fonds propres réglementaires au titre du portefeuille de négociation ont augmenté.

5 *CORE (*COmpensation REtail*) (FR) est le système de paiement de détail français conçu, développé et géré par la société STET, dont le capital est détenu par cinq grandes banques françaises (BNP Paribas, BPCE, Crédit Agricole, Banque fédérative du Crédit Mutuel et Société Générale).*

6 *Il s'agit de plates-formes de financement participatif par souscription de titres financiers.*

7 *Selon l'Organisme pour le registre des intermédiaires en assurance (ORIAS).*

8 *Source : Financement participatif France (association des professionnels du* crowdfunding*).*

9 *Cependant, le développement du* crowdfunding *est plus marqué aux États-Unis qu'en Europe en général, en raison d'une plus grande maturité du marché et d'un modèle de financement de l'économie structurellement plus désintermédié.*

10 https://www.banque-france.fr/publications/evaluation-des-risques-du-systeme-financier-francais.html

2| La numérisation des services financiers est cependant porteuse de risques nouveaux pour la stabilité financière

Le développement d'instruments et de services numérisés dans la sphère bancaire et financière doit être accueilli favorablement, dès lors que ceux-ci répondent efficacement aux besoins des consommateurs et des investisseurs, permettent des gains de productivité et favorisent la compétitivité de l'économie française. Néanmoins, ce développement pourrait non seulement réduire la sécurité des opérations ou faciliter le blanchiment des capitaux et le financement du terrorisme, mais aussi accroître deux risques classiques du système financier (risques de crédit et de liquidité).

2|1 La sécurité des transactions

La numérisation des services financiers présente un défi pour les banques centrales dans l'exercice de leur mission de sécurité des opérations de paiement, de compensation et de règlement-livraison.

En matière de paiements par exemple, les sources de risques ont évolué avec l'apparition de nouveaux acteurs et modes de paiement. L'essor du commerce en ligne au début des années deux mille s'est ainsi accompagné d'un usage du paiement à distance, non seulement par carte mais aussi en utilisant d'autres instruments innovants : portefeuilles électroniques, solutions de paiement reposant sur le virement depuis un compte bancaire, ou encore paiements directement intégrés au sein d'applications mobiles permettant des achats plus rapides sur *smartphones*.

Plus largement, un développement significatif des systèmes d'échange décentralisés, par exemple sous l'influence de la technologie de la *blockchain* sous-jacente au *bitcoin* [11], modifierait les conditions d'exercice de la mission de sécurité des banques centrales. De tels modèles d'échanges pourraient se substituer au mode de fonctionnement traditionnel des chambres de compensation fondé sur l'agrégation et la compensation centralisées des flux, affectant ainsi les dispositifs de gestion des garanties ou les modalités d'enregistrement des actifs. Cependant, hors *bitcoin*, cette technologie est encore très largement en phase expérimentale. Pour en confirmer le potentiel de développement, un certain nombre de conditions devront être vérifiées au préalable, en termes de sécurité, de coûts, de capacité à traiter rapidement des volumes importants d'opérations, voire d'intérêt économique à se passer de tiers de confiance pour certaines activités.

2|2 La cybercriminalité

L'entrée de la finance dans le cyberespace l'expose à la cybercriminalité, c'est-à-dire à toute forme d'infraction réalisée au moyen de réseaux informatiques ou de systèmes d'information dans le but de porter atteinte aux données ou aux systèmes d'une institution.

Ce risque est d'ores et déjà intégré par les acteurs financiers traditionnels, auxquels la réglementation prudentielle impose de constituer des coussins de protection pour faire face à des chocs de toutes natures. Les régulateurs financiers veillent également à la bonne définition des politiques de sécurité informatique des institutions financières : renforcement de l'expertise et de la sensibilisation du personnel, participation à des exercices de crise réguliers, renforcement de la protection des systèmes internes avec un contrôle des accès rigoureux, chiffrement plus étendu des données, mise en place d'outils de détection des intrusions et réalisation de tests périodiques de leur efficacité.

En revanche, les fintechs sont particulièrement exposées à la cybercriminalité, compte tenu de leurs modèles d'affaires exclusivement développés sur internet. Du fait de leur taille réduite et de leur surface financière limitée, l'occurrence d'un tel risque représente pour elles un danger de continuité d'activité, bien plus important que pour les acteurs traditionnels et qui pourrait affecter ces derniers lorsqu'ils s'engagent dans des stratégies de collaboration avec les fintechs. Les fintechs doivent donc intégrer pleinement le cyber-risque et élaborer

11 *La chaîne de blocs ou* blockchain *consiste à s'appuyer sur un registre distribué des transactions (*distributed ledger*) et sur une communication entre les acteurs par un mécanisme de type* peer-to-peer. *Elle permet l'échange d'informations de manière sûre au sein d'une communauté donnée, sans que l'intervention d'un tiers de confiance soit nécessaire.*

des politiques de sécurité informatique conformes aux meilleures pratiques du marché. L'encadrement de ces risques implique une coopération efficace entre les autorités compétentes non seulement en France (Banque de France, Autorité de contrôle prudentiel et de résolution et Agence nationale de la sécurité des systèmes d'information), mais aussi au niveau international.

2|3 Le blanchiment des capitaux et le financement du terrorisme

Les nouveaux acteurs des services financiers numériques doivent en outre se voir appliquer pleinement la réglementation relative à la lutte contre le blanchiment des capitaux et le financement du terrorisme. Cela implique pour eux de s'assurer que leur dispositif de lutte contre le blanchiment des capitaux et le financement du terrorisme soit adapté non seulement à leur activité et à leur clientèle mais aussi à leur mode d'entrée en relation avec leur clientèle – en général distant – afin de se prémunir contre toute utilisation indue ou frauduleuse de leurs solutions innovantes.

2|4 Le risque de crédit : pour un développement accompagné du *crowdfunding*

Les enjeux de stabilité financière liés aux intermédiaires en financement participatif paraissent pour l'heure limités au regard des montants collectés, et le canal bancaire continuera à jouer un rôle essentiel en tant que source principale de financement des petites et moyennes entreprises et entreprises de taille intermédiaire. Cependant, une dynamique plus importante entraînant l'émergence de plates-formes de taille conséquente drainant potentiellement des montants beaucoup plus élevés est possible. Dans ce contexte, le régulateur doit veiller à ce que le développement de nouveaux modes de financement ne porte pas préjudice à la stabilité financière ni d'ailleurs à la protection légitime des investisseurs individuels.

Par exemple, le financement par des particuliers de projets *via* des plates-formes d'appel à contribution peut comporter des risques relatifs non seulement à l'évaluation de la qualité du projet et de la contrepartie financée mais aussi à la sécurité et à la pérennité de la plate-forme par laquelle les fonds transitent. En France, l'ordonnance n° 2014-559 du 30 mai 2014 relative au financement participatif impose aux plates-formes de *crowdfunding* de mettre à disposition de l'internaute un certain nombre d'informations permettant d'éclairer son jugement [12]. Au-delà d'une certaine taille, ou en cas d'activités transfrontalières, il faudra une régulation européenne harmonisée se substituant au patchwork des statuts actuels.

L'ordonnance du 30 mai 2014 permet également aux intermédiaires en financement participatif de renforcer l'analyse de leurs risques financiers en leur fournissant un accès large à l'information financière. En particulier, elle autorise la consultation du fichier bancaire des entreprises (FIBEN) géré par la Banque de France, qui constitue un outil de référence en matière d'analyse et de suivi du risque de crédit. Cette initiative participe à la fiabilisation et au développement pérenne de ce nouveau canal de financement, tout en répondant aux enjeux de stabilité financière.

2|5 Le risque de liquidité : pour une réglementation renforcée de la négociation à haute fréquence

L'expansion rapide de la négociation à haute fréquence (NHF) modifie l'organisation des marchés d'actions et le modèle économique des plates-formes d'échange. En offrant de la liquidité au marché sans subir d'exigence réglementaire à ce titre, les opérateurs de NHF peuvent évincer les teneurs de marché traditionnels. Ceux-ci sont contraints de rattraper leur retard technologique s'ils souhaitent continuer à opérer. En outre, les firmes de NHF ne sont aujourd'hui assujetties à aucune obligation vis-à-vis des bourses de valeurs ou des clients. Aussi leur offre de liquidité peut-elle se réduire subitement en cas de stress. Elles ont recours à des stratégies qui peuvent s'apparenter à de nouvelles

12 *Ces informations portent notamment sur les conditions d'éligibilité et les critères de sélection des projets et des porteurs de projets, les risques encourus par les prêteurs et les taux de défaillance enregistrés sur les projets déjà présentés par la plate-forme, la responsabilité de chaque acteur (prêteur, porteur de projet, plate-forme) en cas de défaillance du porteur de projet.*

formes d'abus ou de manipulation de marché : par exemple, l'envoi disproportionné d'ordres voués à ne pas être exécutés dans le but de ralentir le fonctionnement des plates-formes d'échanges et de profiter plus facilement d'opportunités d'arbitrage, altère l'information de marché.

La rapidité d'exploitation de l'information permise par cette technologie accroît la volatilité des marchés et la contagion entre classes d'actifs. La forte corrélation de nombreuses stratégies de NHF tend à amplifier les chocs. Les algorithmes de transaction peuvent en particulier réagir à un événement de marché de façon pro-cyclique, provoquant ainsi une sur-réaction des prix et des volumes avec un risque de spirale auto-réalisatrice déclenchée par des transactions en cascade et pouvant aller jusqu'aux phénomènes de rupture dits de *flash crash*, particulièrement en période d'aversion au risque. Si des firmes de NHF devaient subir des pertes conséquentes, l'absence de coussins de capital adéquats pourrait conduire à des défaillances qui seraient d'autant plus nombreuses que ces sociétés prennent souvent des positions similaires, et qui pourraient affecter rapidement leurs contreparties de marché.

Certes, une réglementation des conditions d'exercice des firmes de NHF va bientôt intervenir dans le cadre de la révision de la directive Marchés d'instruments financiers (MiFID 2). MiFID 2 devrait entrer en application en janvier 2018 et prévoit notamment un agrément de la NHF et une définition harmonisée du pas de cotation, en fonction des instruments et de leur liquidité. Le texte comporte également des obligations de transparence pré- et post-négociation qui devraient améliorer la compréhension des activités de NHF sur les plates-formes et la précision des indicateurs de liquidité, ainsi que des exigences de robustesse des algorithmes de transaction (à travers la mise en place de *stress tests* et la fonctionnalité d'arrêt forcé des algorithmes) de nature à augmenter la résilience des marchés. Mais plus globalement, la NHF reste un champ où les régulateurs – y compris aux États-Unis – semblent en retard persistant par rapport aux opérateurs et à la technologie. Combler ce *gap* doit être une priorité des discussions internationales.

3| Pour concilier innovations et stabilité, la Banque de France et l'ACPR doivent retenir deux principes d'action

Innovations et stabilité font rarement bon ménage. Ceci vaut en matière financière comme ailleurs. Le périmètre du nouvel écosystème financier n'est pas encore stabilisé, l'horizon de temps de déploiement des nouvelles technologies numériques est incertain, et la définition du cadre réglementaire applicable à une très grande diversité d'entreprises est complexe. La réglementation des services financiers qui apparaissent dans le sillage de la vague numérique doit être adaptée aux risques correspondants. Dans le cadre fixé par le régulateur, il s'agit pour la banque centrale et le superviseur de s'assurer que les nouveaux risques attachés à la transformation numérique du système financier n'entravent pas l'exercice efficace du mandat de stabilité financière et qu'au total les innovations renforcent bien le fonctionnement du système financier au service de l'économie. À cette fin, nous devons à mon sens retenir deux principes d'action : un impératif absolu de sécurité des paiements et opérations ; une adaptation proportionnée face au développement des fintechs.

3|1 Un impératif absolu : la sécurité des paiements et des opérations

Dans le cadre de sa mission de surveillance de la sécurité des moyens de paiement, la Banque de France veille à la promotion de solutions de paiement innovantes, efficaces et sûres. Dans cette perspective, elle s'assure que l'introduction de nouveaux acteurs et de nouvelles solutions sur le marché ne se traduit pas par un nivellement par le bas de la sécurité.

Les révisions apportées ou en cours d'adoption, en ce qui concerne les textes européens en vigueur

en matière de services de paiement et de marchés d'instruments financiers, constituent des premiers éléments de réponse. Ainsi, avec l'apparition de nouveaux prestataires qui n'étaient pas couverts par la réglementation des services de paiement (cf. *supra*), une révision a dû être engagée et vient de s'achever par l'adoption le 25 novembre 2015 de la deuxième directive européenne des services de paiement (directive 2015/2366 dénommée DSP2). La DSP2 ne soumet pas ces nouveaux prestataires à des exigences de fonds propres car ils ne prennent pas possession des fonds de leurs clients ; mais ils doivent souscrire une assurance de responsabilité civile professionnelle ou une garantie comparable.

Bien antérieurement, la création de l'Observatoire de la sécurité des cartes de paiement en 2001, adossé à la Banque de France, répondait déjà à cette exigence dans le domaine de la carte. La promotion par l'Observatoire depuis 2008 de solutions d'authentification fortes concernant les paiements par carte en ligne a ainsi contribué efficacement à une diminution des taux de fraude sur ce canal (0,248 % en 2014 contre 0,269 % en 2013). Son champ de compétence devrait être étendu à l'ensemble des moyens de paiement scripturaux, comme le ministre des Finances l'a préconisé à l'occasion des Assises nationales des paiements qui se sont tenues en juin 2015.

Nous nous attachons également à analyser et évaluer la résilience des institutions financières et des infrastructures de marché. Puisqu'il n'est pas possible de garantir à 100 % leur sécurité informatique face à une cyber-attaque, il convient de s'assurer de leur capacité à maintenir leur activité ou à la rétablir rapidement en cas de dysfonctionnement de leurs systèmes d'information. Cette réflexion s'inscrit dans un cadre international : sous l'égide du Comité des paiements et des infrastructures de marché (*Committee on Payments and Market Infrastructures* – CPMI) [13], un rapport recommandant des mesures favorisant la résilience des infrastructures de marché systémiques a été publié pour consultation en novembre 2015. Ce type de travaux doit se poursuivre dans toutes les enceintes internationales appropriées de façon à couvrir les autres entités systémiques (banques, sociétés d'assurance, fonds d'investissement).

S'agissant des monnaies virtuelles, la Banque de France a émis une alerte dès décembre 2013 soulignant qu'elles n'offraient aucune garantie de sécurité, de convertibilité et de valeur, leur caractère anonyme pouvant en outre favoriser le contournement des règles relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme. Afin de mieux prévenir ces risques, l'activité de conversion contre monnaie ayant cours légal par des plates-formes internet doit s'analyser – dans la mesure où il y a réception, virement et tenue de comptes de fonds concernant une monnaie ayant cours légal – comme un service de paiement nécessitant un agrément correspondant. L'Autorité de contrôle prudentiel et de supervision (ACPR) a publié une position en ce sens au début de 2014.

Par ailleurs, une réflexion est aujourd'hui engagée à la Banque de France, et plus largement au sein du Haut Conseil de stabilité financière, afin de suivre le développement des initiatives autour de la technologie de la *blockchain*, tant en ce qui concerne les possibilités d'application qu'elle semble offrir qu'en ce qui concerne les questions qu'elle soulève notamment en termes de sécurité.

3|2 Une adaptation proportionnée face au développement des fintechs

Adapter la réglementation pour accompagner la diffusion des innovations

Les fintechs posent des défis particuliers aux autorités de régulation. Leur développement rapide conduit les régulateurs à anticiper et à développer leur réflexion sur les méthodes les plus adaptées pour garantir la protection de la clientèle et répondre aux enjeux de stabilité financière. Il s'agit de trouver un équilibre concernant la réglementation de ces nouveaux acteurs afin de ne pas étouffer des innovations qui seraient porteuses de bénéfices directs et indirects pour le consommateur (sous la forme de nouveaux services et d'une réduction des coûts du fait de la concurrence avec les intervenants traditionnels), et de manière plus générale pour l'économie et la société (*via* de nouveaux modes de financement de l'économie).

12 https://www.bis.org/cpmi/publ/d138.htm

Bien que les nouveaux acteurs fournissent des services qui relèvent largement des activités bancaires (moyens de paiement, recherche de financement, gestion d'épargne), leur taille souvent modeste, le caractère tout à la fois original et fragile de leur *business model* (du type *start-up*) font douter de la pertinence de leur appliquer la réglementation bancaire, largement construite pour des acteurs matures. Des dispositions spécifiques permettant une certaine progressivité en termes d'intensité réglementaire pourraient être mieux adaptées pour prévenir les risques portés par les fintech. Par exemple, le régime des établissements de paiement a récemment été modifié en France afin d'intégrer la possibilité d'un agrément allégé [13] pour les acteurs dont les flux de paiement sont faibles.

Enfin, les fintechs, dont les activités s'exercent essentiellement par internet, ne connaissent pas de frontière, ce qui amène à s'interroger sur l'intérêt de réglementations de portée encore assez largement nationale ou fondées sur des critères de résidence ou de domiciliation (par exemple, en matière de règles relatives à la protection du consommateur). La dimension transfrontière du changement technologique en matière de services bancaires et financiers, constitue une incitation forte pour les autorités de réglementation à coordonner leur action au niveau international. Un statut européen pourrait être défini pour des activités bien identifiées et présentant un certain seuil de développement.

Superviser les fintechs avec souplesse et vigilance

Il n'apparaît pas toujours évident de qualifier juridiquement certaines innovations, comme en témoignent les débats sur le régime applicable aux monnaies virtuelles et à leurs plates-formes d'échange au regard des notions d'instrument de paiement et de services de paiement. Les statuts applicables aux nouvelles activités sont assez variés, ce qui reflète une certaine souplesse réglementaire pour s'adapter aux activités conduites et moduler l'intensité de la supervision. En pratique, cela peut être assez complexe pour les porteurs de projets, qui sont souvent des spécialistes de l'informatique et plus rarement des professionnels issus du domaine financier. En France par exemple, 62 % des 55 fintechs membres de l'association France Fintech sont régulées sous une dizaine de statuts différents [14]. Selon leur activité, les entités relèvent soit de la supervision de l'Autorité de contrôle prudentiel et de résolution (71 % des entités régulées), soit de l'Autorité des marchés financiers (21 % des entités régulées), soit des deux autorités (8 % des entités régulées).

Au-delà des simplifications réglementaires déjà évoquées, un traitement spécifique des fintechs dans le parcours d'agrément paraît nécessaire pour expliciter les règles applicables, évaluer dans quel cadre réglementaire le projet est susceptible de s'insérer, accompagner la constitution du dossier de demande d'agrément. Enfin, dans un certain nombre de cas, par exemple lorsque le modèle d'affaires présenté est mixte (associant par exemple des services d'investissement et des services de crédit ou de paiement), le dialogue entre les autorités nationales de supervision bancaire et de supervision des marchés devra être renforcé afin d'accompagner au mieux les porteurs de projets.

La nécessité d'adapter la supervision aux spécificités des fintechs justifie la création d'équipes dédiées dans leur parcours d'agrément et dans la perspective de leur supervision : cela va être le cas en France par la création d'un pôle commun entre l'ACPR et l'Autorité des marchés financiers. Cette initiative permettra notamment aux nouveaux acteurs d'identifier leur interlocuteur, de poser des questions et d'accéder à une banque de réponses aux questions posées. Un forum consultatif permettant un dialogue continu entre les superviseurs et les fintechs sera en outre mis en place pour une meilleure compréhension des innovations, notamment pour identifier les évolutions réglementaires nécessaires et favoriser l'échange d'informations entre les parties prenantes.

13 *Cet agrément allégé est une possibilité prévue par la DSP1.*
14 *Établissement de paiement, établissement de monnaie électronique, agents de services de paiement, distributeurs de monnaie électronique, entreprises d'investissement, intermédiaires en financement participatif, conseillers en investissement participatif, etc.*

4| Conclusion

Les apports de la numérisation aux services financiers sont indéniables, notamment en matière d'information et de qualité d'exécution. Le développement des innovations financières technologiques est à ce titre souhaitable. Elles favorisent également l'apparition de nouveaux processus et de nouveaux acteurs en matière de services financiers. Pour autant, elles s'accompagnent de risques qu'il convient de gérer. L'analyse des vulnérabilités doit être approfondie, la réglementation adaptée, la sécurité des transactions maintenue, et la supervision prudentielle à la fois souple et vigilante. À terme, une fois passée la phase expérimentale, il faudra veiller à l'application des mêmes règles aux mêmes activités quels que soient les acteurs qui les exercent. Le traitement équitable, – ou *level playing field* – c'est de réguler les acteurs financiers selon ce qu'ils font, non selon ce qu'ils sont. Cela nécessite aussi un effort de coordination internationale face à l'influence grandissante sur le système financier d'un univers technologique qui se veut sans frontière. Tels sont les défis que les autorités publiques s'apprêtent à relever.

Les nouveaux risques pour la stabilité financière

Banque numérique et désorganisation du marché : un sentiment de déjà-vu ?

Jean DERMINE
Professeur d'économie bancaire et de finance
INSEAD, Singapour

Cet article évalue la menace que représente la banque numérique dans le contexte des nombreuses innovations survenues dans le secteur bancaire : banque par téléphone, cartes de paiement, développement des marchés financiers, internet, smartphones *et* cloud computing*. Nous nous intéressons aux deux principales fonctions économiques des banques et des services bancaires, à savoir la fourniture de liquidité et l'octroi de crédit, et nous analysons dans quelle mesure les établissements bancaires sont susceptibles d'être supplantés par des plates-formes de prêts directs basées sur un système de* peer-to-peer *(P2P).*

La numérisation des services bancaires constitue l'un des principaux axes stratégiques pour les banques compte tenu des menaces qu'elle induit, mais aussi des opportunités qu'elle présente. Elle soulève également des problématiques de politique publique : conséquences sur la rentabilité et la solvabilité des banques, protection des emprunteurs et des investisseurs, et importance systémique des nouveaux acteurs, les fintechs qui englobent des start-up *spécialisées dans les services financiers.*

Même ceux qui lisent la presse occasionnellement seront forcément tombés sur un article annonçant la disparition imminente de la banque classique. Les fintechs, ces *start-up* spécialisées dans les services financiers, désorganisent les marchés bancaires. Les nouveaux systèmes de paiement se multiplient : PayPal, Venmo, M-Pesa, Apple Pay, Android Pay, Alipay ou Samsung Pay. Même les réseaux sociaux comme Facebook proposent des solutions de paiement. TransferWise et WorldRemit font concurrence à Western Union pour les envois de fonds et les virements internationaux. Sur le marché du crédit à la consommation non garanti, Lending Club et Prosper (aux États-Unis), Zopa et Funding Circle (au Royaume-Uni) et Prêt d'Union (en France) concurrencent les banques traditionnelles. L'ampleur de la menace pour le secteur bancaire peut se résumer ainsi :

« Elles veulent toutes nous retirer le pain de la bouche. Je dis bien toutes, et elles feront tout pour y parvenir » (Jamie Dimon, PDG de JP Morgan Chase, *Financial Times*, 26 février 2014). *« Leur objectif est de nous faire mourir à petit feu. Les* start-up *fintechs sont d'agiles piranhas, chacune s'attaquant à une infime partie du modèle économique des banques »* (*Financial Times*, 14 octobre 2015).

Les prévisions apocalyptiques annonçant la mort lente de la banque traditionnelle me rappellent d'autres prévisions tout aussi funestes que l'on a pu entendre au cours des trente-cinq dernières années. Dans les années quatre-vingt, lorsqu'est apparue la banque par téléphone, on craignait que les opérateurs téléphoniques pénètrent sur le secteur bancaire et évincent les acteurs en place. Or, ces craintes ne se sont pas matérialisées, car les banques elles-mêmes se sont mises à proposer des services bancaires par téléphone.

À l'époque, j'ai été consulté par un grand groupe pétrolier britannique, dont les clients utilisaient une carte émise par le groupe pour acheter du carburant, et qui envisageait d'ajouter des services financiers à cette carte et de les proposer à ses millions de clients. Ce projet n'a jamais vu le jour. De même, Standard Chartered Bank, à Hong Kong, craignait d'être concurrencée par Octopus, une carte de paiement utilisée par des millions d'usagers du métro de Hong Kong, en particulier si d'autres services financiers y étaient ajoutés. Là encore, la menace ne s'est pas concrétisée.

Lorsque, dans les années quatre-vingt-dix, les marchés d'obligations et d'actions ont été déréglementés, on pensait que la finance directe remplacerait la finance indirecte et l'intermédiation financière, qui étaient coûteuses et inefficaces. Mais cette prévision s'est révélée infondée : le ratio actifs bancaires/PIB a progressé tant dans les pays développés que dans les économies émergentes.

Au tournant du millénaire, avec la bulle internet, les banques redoutaient que Microsoft pénètre dans leur secteur et permette à ses clients de naviguer en ligne d'une banque à une autre. La transparence des tarifs et des offres de produits semblait sur le point d'éroder les revenus bancaires. À l'époque, on pensait que la fin des agences bancaires (*branch banking*) était imminente, et qu'elle entraînerait de profondes restructurations et des licenciements massifs (comme dans le secteur du charbon et de l'acier). Là non plus, la menace ne s'est pas concrétisée. Au contraire, dans plusieurs pays, les banques ont ouvert de nouvelles agences, répondant ainsi au souhait des clients d'une proximité physique.

Plus récemment, c'est le *smartphone*, véritable ordinateur de poche connecté, qui a suscité des inquiétudes : on le disait prêt à révolutionner le monde de la banque.

Après trente-cinq années de prédictions apocalyptiques, il semble justifié de se demander si la banque numérique va désorganiser le marché, ou s'il ne s'agit que d'une lubie passagère et d'un phénomène suscitant à nouveau un sentiment de déjà-vu ? Les banques sauront-elles s'adapter et maîtriser ces nouvelles technologies, ou « demain sera-t-il véritablement différent » lorsque de nouveaux acteurs auront démantelé la chaîne d'offre des services bancaires ?

Cet article cherche à analyser les sources de désorganisation du marché induites par le numérique et à identifier les questions de politique publique importantes. Il comporte quatre sections. La première examine six services de base proposés par les banques, la deuxième tente d'identifier les principales évolutions technologiques, la troisième étudie comment elles pourraient perturber l'offre de services bancaires et la dernière traite des questions de politique publique liées au *marketplace lending*.

1| Les six grandes fonctions des services bancaires

Sur les marchés financiers, les unités économiques qui détiennent des fonds excédentaires, qu'il s'agisse de ménages ou d'entreprises (ou plus rarement d'États) peuvent financer directement des unités économiques qui sont à court de fonds (entreprises, ménages ou États). Les épargnants peuvent acheter des obligations ou des actions émises directement sur les marchés financiers par des unités en manque de capitaux. C'est ce que l'on appelle la *finance directe*. Lorsqu'il y a un intermédiaire entre les unités qui disposent de fonds excédentaires et celles qui veulent en obtenir, on parle de *finance indirecte*. Une banque est un exemple d'intermédiaire financier : elle reçoit des dépôts et accorde des prêts. Mais c'est aussi le cas des compagnies d'assurance, des fonds de pension et des fonds d'investissement, comme les fonds communs de placement ou les *hedge funds*.

Même si les services proposés par les banques sur les marchés financiers sont étroitement liés les uns aux autres, nous pouvons distinguer six catégories de services dont la complexité est croissante (Dermine, 2015) : souscription et placement, gestion de portefeuilles, services de paiement (virements), services de suivi ou d'information, partage du risque et services de conseil.

Souscription et placement : le premier service proposé par les banques est la mise en relation des épargnants et des emprunteurs. La souscription et le placement de titres (obligations ou actions) permettent aux emprunteurs (entreprises ou institutions publiques) de rencontrer des unités « excédentaires », ainsi que de structurer ou de personnaliser le type de titres qui répondent au profil risque/rendement des emprunteurs et des prêteurs. Le souscripteur participe ici non seulement à la composition du titre, mais aussi à la valorisation des actifs et à la détermination du prix de sorte que les conditions de l'émission soient compétitives. Ensuite, les investisseurs peuvent souhaiter transformer leurs créances (pour obtenir des liquidités, d'autres titres, ou à des fins de consommation). Ces créances doivent donc pouvoir être échangées. Les sociétés de courtage (*broker-dealers*) ou les teneurs du marché (*market makers*) proposent ces services afin de garantir les opérations sur le marché secondaire et la liquidité. Dans un service uniquement axé sur la souscription et le placement, on suppose que le rendement et le risque des titres peuvent être correctement définis, de sorte qu'il n'y a pas de gros problème d'asymétrie de l'information (théorie de l'agence) entre prêteurs et emprunteurs. Dans ce cas, le suivi ne pose pas problème. Grâce aux services de souscription et de placement, l'investisseur final détient directement les créances des unités « déficitaires ».

Gestion de portefeuilles : les investisseurs peuvent acquérir à faible coût un portefeuille diversifié de titres émis par des unités à court de fonds. Les fonds communs de placement et les OPCVM offrent à leurs porteurs un portefeuille diversifié. Le revenu dégagé par les actifs financiers est versé aux actionnaires, une fois déduite la commission du gestionnaire du fonds. Ces fonds ont trois objectifs : réduire les coûts grâce à l'émission de nombreux titres, proposer un portefeuille diversifié aux investisseurs et déléguer la gestion d'actifs à des spécialistes capables d'évaluer les perspectives économiques.

Services de paiement : la troisième fonction des marchés financiers est la gestion des systèmes de paiement : ils facilitent et assurent la traçabilité des transferts de capitaux entre personnes. Il s'agit là de la fonction de tenue de comptes que les banques exercent lorsqu'elles débitent ou créditent les comptes de leurs clients. Même si la réglementation limite le type de dépôts (dépôts à vue) que les systèmes de paiement de masse peuvent accepter, il est possible de débiter ou de créditer n'importe quel type d'actifs liquides.

Services de suivi et d'information : l'information privée que détiennent les emprunteurs induit des problèmes contractuels, étant donné qu'il est coûteux d'évaluer la solvabilité d'un emprunteur ou de suivre l'évolution de sa situation une fois le prêt accordé (Stigliz et Weiss, 1981). Il peut s'avérer judicieux de regrouper ces créances dans un portefeuille. Les banques jouent un rôle utile car elles réduisent le coût de sélection et de suivi des emprunteurs. La délégation de la sélection et du suivi aux banques s'est révélée efficace (Diamond, 1984). Cette quatrième fonction est liée à la première (souscription et placement) mais nous la considérons ici comme un service distinct puisqu'elle correspond aux cas dans lesquels une forte asymétrie de l'information rend difficile l'émission de créances financières négociées sur les marchés des valeurs mobilières. Alors que le deuxième service

(gestion de portefeuille) concerne la gestion d'actifs liquides, la quatrième fonction concerne la gestion d'un portefeuille de prêts illiquides, qui constituent souvent la plus grande partie du bilan d'une banque.

Partage des risques : les banques remplissent une fonction de plus en plus importante, celle qui consiste à rendre le marché plus abouti en apportant une certaine forme d'assurance contre de multiples sources de risque. Premièrement, les banques non seulement proposent des actifs diversifiés, mais elles organisent également de manière efficiente la distribution du revenu généré par le panier d'actifs. Les porteurs de titres de créance reçoivent une rémunération fixe, tandis que les actionnaires se partagent le revenu résiduel. Parmi les autres services d'assurance figurent l'assurance contre le risque de taux d'intérêt (prêts à taux variable assortis d'un plafond sur le taux d'intérêt appelé *cap* ou *floor*), l'assurance contre l'inflation dans le cadre d'un contrat réel et l'assurance contre le risque de liquidité, c'est-à-dire la possibilité, pour un déposant ou pour le bénéficiaire d'une ligne de crédit, de retirer son argent rapidement, à sa valeur nominale (Diamond et Dybvig, 1983).

Services de conseil : les services de conseil aux entreprises et aux particuliers constituent une importante source de revenus (commissions). Les banques peuvent conseiller les entreprises en matière de fusions et acquisitions, de gestion du risque ou de gestion d'actifs, et les particuliers en matière de stratégie fiscale ou de planification successorale.

Dans les deux sections qui suivent, nous traitons des innovations technologiques et nous évaluons comment la technologie numérique pourrait perturber l'offre de services bancaires.

2| Un historique des technologies qui perturbent les activités bancaires

Les sections qui suivent passent en revue (avec le regard d'un néophyte) les innovations technologiques et leur incidence sur le secteur bancaire : traitement électronique des données, banque par téléphone, internet, *smartphones* et services informatiques hébergés (*cloud computing*).

Traitement électronique des données : selon Ali *et al.* (2014a), le passage de la saisie manuelle des débits et des crédits dans un registre aux lecteurs de chèques, puis aux paiements électroniques, a constitué une avancée majeure qui a eu un impact sur les systèmes de paiement. L'activité de paiement requiert la maîtrise du traitement électronique des données liées aux opérations de débit et de crédit sur les comptes. Dans ce domaine, les banques ne disposent d'aucun avantage concurrentiel par rapport aux entreprises technologiques telles que les opérateurs de téléphonie ou internet, comme le montre la multiplication des nouveaux acteurs/systèmes de paiement, et notamment ceux que nous avons déjà mentionnés : M-Pesa, PayPal, Apple Pay, Samsung Pay et Alipay, développé par Alibaba, géant chinois du commerce en ligne.

La banque par téléphone (minitel) : la banque par téléphone (minitel) avait pour principal intérêt de donner accès à des informations bancaires (comme le solde du compte) et la réalisation d'opérations bancaires depuis n'importe quel endroit situé en dehors de l'agence bancaire. Le traitement électronique des données permet le traitement automatique des transactions.

Internet : comparé à la banque par téléphone, internet a permis à des millions d'utilisateurs d'accéder plus facilement aux données à distance et a facilité la saisie des transactions. En outre, la compensation et le règlement du négoce de titres sont peu coûteux grâce au recours à des algorithmes mathématiques. Des sociétés de courtage et de gestion d'actifs en ligne ont ainsi fait leur apparition : Boursorama et Cortal en France, Banco BIC au Portugal ou Binckbank aux Pays-Bas, en Belgique et en France. Plus récemment encore, la combinaison d'internet et d'algorithmes mathématiques a rendu possible la mise en relation des investisseurs et des emprunteurs.

Le cas de Lending Club, aux États-Unis, illustre parfaitement ce phénomène. Cette société a attiré l'attention, en décembre 2014, avec la réussite de son introduction en Bourse et la présence de personnalités connues à sa tête (Larry Summers, ancien secrétaire américain au Trésor, et John Mack, ancien PDG de Morgan Stanley). Créée en 2006 à San Francisco par l'entrepreneur français Renaud Laplanche, qui en est l'actuel PDG, cette plate-forme de courtage met en relation les investisseurs et les particuliers qui empruntent. Dès son premier jour de cotation

(le 12 décembre 2014), l'action, introduite à 15 dollars, a atteint 24,75 dollars (+ 65 %).

Conçu à l'origine comme un système de prêt entre particuliers (*peer-to-peer* – P2P), grâce auquel des particuliers en financent d'autres, Lending Club s'est transformé en plate-forme de *marketplace funding* avec l'arrivée de gros investisseurs institutionnels (fonds de pension et *hedge funds*). D'après les analystes du Credit Suisse (CS, 2015), le volume de prêts (4 milliards de dollars) émis par Lending Club en 2014 est à rapprocher d'un marché total disponible (*total addressable market* – TAM) de 873 milliards de dollars de prêts à la consommation non garantis, voire de 1 171 milliards de dollars si l'on inclut les prêts non garantis aux petites et moyennes entreprises (PME). Lending Club estime qu'en ne s'encombrant pas d'un coûteux réseau d'agences physiques et d'une informatique obsolète, il peut opérer à moindre coût, proposer des rendements plus élevés aux investisseurs et des prêts moins onéreux aux particuliers. Le 11 janvier 2016, son ratio cours/valeur comptable ressortait à 3,5, mais le cours de son action n'était que de 9,24 dollars, soit bien loin des 15 dollars de son introduction en Bourse en décembre 2014. Le score FICO, qui renseigne sur la solvabilité des particuliers aux États-Unis, permet de classer le risque de crédit, que les investisseurs peuvent atténuer en scindant leurs investissements en tranches de 25 dollars et en les répartissant sur plusieurs prêts (diversification). Lending Club utilise la technologie numérique pour éviter les problèmes évoqués plus haut (asymétrie de l'information et division de l'investissement).

***Smartphones* avec capteurs :** les *smartphones* qui allient puissance de calcul et accès à internet permettent d'effectuer des opérations bancaires n'importe quand et n'importe où. De plus, des capteurs recueillent des données sur les habitudes de consommation et permettent l'analyse de données massives (*big data*).

Services informatiques hébergés (*cloud computing*) : les progrès du stockage et de la transmission de données permettent d'agréger des données et des logiciels dans des espaces dédiés sur le *cloud*. Cette évolution a des conséquences non négligeables sur la chaîne de valeur des banques. Les données et les logiciels n'ont plus besoin d'être stockés en interne, ils peuvent être hébergés par un tiers. Les entreprises les plus petites tirent parti des économies d'échelle des services d'hébergement sur le *cloud*.

3| Services bancaires et technologies numériques perturbatrices

Pour bien comprendre les impacts de la technologie numérique sur le marché bancaire, il est utile de rassembler sous trois catégories certains des services bancaires mentionnés à la section 1, selon qu'ils sont liés au traitement des données, à l'analyse des données ou à la structure du bilan bancaire (cf. tableau 1).

La première colonne du tableau dresse la liste des services bancaires qui ont essentiellement besoin d'un traitement électronique des données. On y trouve les opérations de paiement (débit et crédit), les monnaies numériques (comme les *bitcoins* [1]), le courtage de titres (y compris le *trading*

Tableau 1
Services bancaires

Traitement des données	Analyse des données	Bilan bancaire
Paiement, crypto-monnaies (*bitcoin*)	Prêts aux PME (avec évaluation du risque, garanties, suivi du risque, restructuration, recouvrement)	Dépôts : sûrs (adossés à une assurance-dépôts et à un portefeuille de prêts diversifié) et liquides (retirables à la demande)
Courtage de titres (actions et obligations), fonds d'investissement gérés passivement	Conseil (finance d'entreprise et gestion du risque)	Lignes de crédit (les emprunteurs peuvent accéder à la liquidité à la demande)
Prêts à la consommation (le risque de crédit est quantifiable, standardisé)	Gestion d'actifs (conseils en planification successorale, fonds gérés activement, produits structurés)	

Source: Jean Dermine.

1 *Cet article ne s'intéresse pas au cas des crypto-monnaies (Ali* et al.*, 2014b).*

algorithmique) et les fonds gérés passivement, mais aussi les prêts à la consommation pour lesquels le risque de crédit peut être quantifié à l'aide de facteurs externes discriminants. La facilité d'accès à des progiciels statistiques et à des données externes pour évaluer le risque de crédit indique qu'il y a standardisation du risque. Ces services requièrent une expertise en matière de traitement de données et non dans le domaine du secteur bancaire. C'est pourquoi ils attirent de nouveaux acteurs. Le nombre de nouveaux acteurs sur le segment des paiements (PayPal, Apple Pay, etc.) et sur celui des virements internationaux (TransferWise) atteste de l'importance de la menace.

Bien souvent, les banques sont en mesure de réagir. En France, elles ont uni leurs forces pour lancer le service de paiement en ligne Paylib. Sur le segment du courtage en ligne de valeurs mobilières, Boursorama et Cortal ont lutté contre la concurrence, mais leur commission par transaction a néanmoins fortement diminué. On observe aussi des cas de coopération avec des opérateurs téléphoniques (comme Apple), mais là encore au prix d'une baisse des revenus bancaires. Enfin, lorsque le recours à des données externes permet la quantification et la standardisation du risque de crédit, celui-ci s'apparente à un simple traitement de données. C'est ce qui explique pourquoi, aux États-Unis, Lending Club a réussi à pénétrer le marché des prêts à la consommation non garantis. La section 4 analyse la désorganisation que ces évolutions ont engendrée sur le marché du crédit.

La perte de l'activité paiements entraînera-t-elle aussi la perte de la relation client et des opportunités de vente croisée ? La question est posée, et d'une importance capitale pour les banques (Forum économique mondial, 2015). Il n'est pas certain que les spécialistes du traitement de données veuillent pénétrer le segment des services bancaires lié à l'analyse des données et à la structure du bilan, car il leur faudrait acquérir l'expertise des banques, ce qui leur coûterait cher. En revanche, ils pourraient l'envisager si leurs clients souhaitaient passer par un guichet unique pour acheter des services financiers (paiement et autres services bancaires). Jusqu'ici, la croissance de la solution de paiement en ligne PayPal ne semble pas encore avoir affecté les banques.

La deuxième colonne inclut des services qui nécessitent à la fois une expertise en analyse des données et une expertise bancaire spécifique. Pour proposer des prêts, il ne suffit pas de disposer des fonds, il faut également maîtriser les risques, ce qui nécessite d'évaluer les garanties et, lorsque l'économie est en crise, de restructurer et de recouvrer les prêts. Ces activités nécessitent une expertise bancaire spécifique que les spécialistes du traitement de données ne peuvent pas aisément reproduire.

La troisième colonne liste les services bancaires qui s'appuient sur la spécificité du bilan bancaire et sur la capacité des banques à gérer les décalages d'échéances. Comme nous l'avons expliqué plus haut, les banques garantissent la liquidité sur les marchés des dépôts et du crédit grâce à leur large gisement de déposants et d'emprunteurs. Les spécialistes du traitement de données ne peuvent pas facilement offrir ce type de service. Lending Club, par exemple, ne gère pas de décalages d'échéances, mais propose des investissements à moyen terme avec une symétrie des échéances.

Nous pouvons en conclure que les activités de traitement de données sont menacées par des entreprises spécialisées comme les opérateurs téléphoniques ou internet. L'Inde, par exemple, a récemment accordé un agrément bancaire à des opérateurs téléphoniques dans le but de stimuler la concurrence. Le 6 janvier 2016, l'opérateur téléphonique français Orange a annoncé son intention de racheter Groupama Banque, la filiale bancaire de l'assureur, afin de lancer une banque mobile en 2017. Ce projet sera observé de près. Les services bancaires standardisés et quantifiables à l'aide de données externes sont eux aussi exposés à la concurrence (Lending Club sur le marché du crédit à la consommation, par exemple). La question fondamentale est de savoir si les banques seront affectées par la perte de l'activité paiements et de la relation clients. Les banques réactives peuvent proposer, seules ou en partenariat, une distribution multicanaux pour répondre aux besoins de leurs clients, mais souvent au prix d'une baisse de leurs revenus, ce qui les contraindra à réduire leurs coûts d'exploitation.

L'activité de prêt bancaire est fondamentale pour l'économie. C'est pourquoi nous analysons spécifiquement, ci-après, les perturbations causées par le numérique sur le marché des prêts.

4| Perturbations causées par le numérique, prêts bancaires et politiques publiques

Nous avons vu comment les prêts directs entre particuliers (P2P) et le *marketplace funding* pouvaient perturber deux services bancaires : la résolution du problème de l'asymétrie de l'information et la division de l'investissement en petits montants, à des fins de diversification. S'il est trop tôt pour savoir si cette hypothèse va se concrétiser, les conditions économiques (taux d'intérêt très faibles et reprise aux États-Unis) sont favorables à la croissance de ce secteur.

La faiblesse des taux d'intérêt suscite l'appétit pour les actifs risqués et les primes pour risques de crédit parmi les investisseurs institutionnels en quête de rendement. La reprise économique aux États-Unis fait oublier le risque à la baisse associé à une récession et à des pertes sur prêts. Il est évident que l'activité de prêt ne se résume pas à la mise en relation d'investisseurs et d'emprunteurs. Elle s'accompagne également de la maîtrise des risques et de la gestion des actifs douteux. De ce point de vue, une entreprise internet basée à San Francisco sera en situation de désavantage concurrentiel par rapport à une banque disposant d'agences qui sont physiquement plus proches de ses clients douteux. L'exemple du *marketplace funding* nous incite à classer l'activité de prêt en fonction du type de risque de crédit et du véhicule de financement (tableau 2).

La technologie numérique permet la finance directe avec la mise en relation des emprunteurs et des investisseurs. Elle constitue un concurrent à bas coût pour le secteur bancaire. Cependant, comme nous l'avons vu plus haut, l'activité de prêt ne se résume pas à la mise en relation des emprunteurs et des investisseurs. Elle inclut le contrôle des risques après que le prêt a été contracté, le négoce des créances si les investisseurs ont besoin de liquidités, et la gestion des actifs douteux. Étant donné la complexité de ces services de prêt, il est utile de classer les actifs en fonction de leur niveau de risque de crédit (du plus élevé au moins élevé), comme présenté dans la première colonne du tableau 2.

Tableau 2
Perturbations dues au numérique et activité de prêt

Types de prêts	Véhicules de financement
Risque élevé (« sensible à l'information » : évaluation des garanties, suivi des risques, restructuration, recouvrement).	Dépôts garantis, dépôts non garantis, ou obligations, dettes subordonnées et capitaux propres Les banques portent le risque crédit.
↓	Prêts titrisés à plusieurs tranches – secteur bancaire parallèle Compte tenu de la réglementation internationale actuelle, les banques portent une partie du risque crédit.
Risque faible (« insensible à l'information », par exemple : créance hypothécaire présentant un faible ratio prêt/valeur).	P2P, *marketplace funding* Les sociétés de courtage ne portent pas le risque crédit.

Source: Jean Dermine.

Si le risque de crédit est élevé, un suivi du risque s'impose, et la probabilité d'avoir à gérer des actifs douteux s'accroît. En outre, lorsque le risque de crédit s'accompagne d'une asymétrie de l'information entre le détenteur d'un actif et un acheteur potentiel, le marché peut se montrer frileux, ce qui s'explique par la crainte classique d'acheter quelque chose qui ne vaut rien. Ces actifs « sensibles à l'information » deviennent illiquides lors d'une récession, alors même que c'est le moment où la liquidité est la plus nécessaire (Dang *et al.*, 2013). Seul un financement sur le bilan de la banque, avec un décalage des échéances, permet de rendre de tels actifs liquides. Mais cette opération dépasse les compétences d'une société de courtage, comme Lending Club, qui ne procède pas à la transformation des échéances.

À l'opposé, on trouve des actifs très sûrs (hypothèques présentant un ratio prêt/valeur très faible, par exemple), qui ne sont pas touchés par le risque de crédit : ils sont « insensibles à l'information », et par conséquent liquides. Une société de courtage est bien placée pour proposer des véhicules de financement bon marché. Si l'on classe les prêts du plus risqué au moins risqué, on peut avancer que les transactions les plus risquées resteront sur le bilan des banques, que les transactions moins risquées peuvent être titrisées et que les actifs très sûrs peuvent entrer dans le champ de compétences des sociétés de *marketplace funding*. Cette évolution ne désorganisera pas forcément le marché car les banques peuvent riposter en proposant aux investisseurs des produits analogues.

La titrisation des prêts et le secteur bancaire parallèle ont été à l'origine de la crise financière mondiale de 2007. Le problème était alors triple : un excès d'emprunts, un manque d'information

des investisseurs sur les véhicules titrisés et un profond décalage des échéances lorsque les prêts étaient financés *via* des véhicules d'investissement structurés (SIV). Pendant l'été 2007, les billets de trésorerie à court terme n'ont pas pu être renouvelés (Dermine, 2013).

Les plates-formes de prêts entre particuliers (P2P) et de *marketplace funding* se développent dans une situation particulière où les taux sont extrêmement bas et où l'économie repart, du moins aux États-Unis. Reste à voir comment le risque et les pertes se matérialiseront pendant une récession ou une période de hausse des taux. Les sociétés de courtage ne semblent pas procéder à la transformation d'échéances, mais il reste à confirmer que les investisseurs institutionnels qui achètent ces prêts ne le font pas non plus. Si nous ne voulons pas que l'histoire se répète, il est impératif que les organes de réglementation s'attachent à protéger les emprunteurs et les investisseurs et qu'elles repèrent et surveillent les acteurs du secteur bancaire parallèle susceptibles d'opérer des décalages d'échéances (Kelly, 2014).

Conclusion

Les perturbations causées par les technologies numériques sonnent-elles le glas de la banque classique, comme on a pu le croire par le passé avec l'apparition de la banque par téléphone (minitel), le développement des marchés obligataires et d'actions, l'arrivée d'internet et des *smartphones*, d'où un sentiment de déjà-vu ?

Nous avons analysé deux grandes sources de perturbation du marché. La prestation des services de paiements par de nouveaux acteurs risque de rompre la relation client des banques et la vente croisée de produits. Cependant, il n'est pas certain que ces nouveaux acteurs spécialistes du traitement de données puissent acquérir, à un prix raisonnable, une expertise bancaire dans des domaines tels que la gestion d'actifs ou le conseil aux entreprises. Les banques ont bien réussi à s'adapter dans le passé aux nouvelles technologies (développement de la distribution multicanaux), et il n'y a aucune raison qu'elles n'y parviennent pas cette fois encore.

Internet facilite les solutions de P2P et de *marketplace funding* pour le financement du risque de crédit. De plus, actuellement, l'environnement est extrêmement favorable, en raison de la faiblesse des taux d'intérêt et de l'expansion de l'activité économique, mais cette situation pourrait ne pas durer. En outre, rien n'empêche une banque de proposer un service de courtage de prêts analogue.

De même que pour la titrisation, les politiques publiques doivent garantir aux emprunteurs et aux investisseurs un niveau de transparence minimum. Elles doivent repérer et surveiller les acteurs du secteur bancaire parallèle afin de déterminer s'ils opèrent un décalage des échéances, lequel est une cause majeure de crise de la liquidité. Les banques ont un rôle unique à jouer dans l'apport de liquidité et dans le financement des actifs à risque de crédit élevé, qui se caractérisent souvent par leur opacité. Les technologies numériques ne représentent pas, à mon avis, une menace fondamentale pour ces deux services bancaires.

Bibliographie

Ali (R.), Barrdear (J.), Clews (R.) et Southgate (J.) (2014a)
« *Innovations in payment technologies and the emergence of digital currencies* », Banque d'Angleterre, *Quarterly Bulletin,* 3e trimestre, p. 262-275.

Ali (R.), Barrdear (J.), Clews (R.) et Southgate (J.) (2014b)
« *The economics of digital currencies* », Banque d'Angleterre, *Quarterly Bulletin,* 3e trimestre, p. 276-286.

Credit Suisse (2015)
« *Lending club, equity research* », 21 janvier, p. 1-22.

Dang (T. V.), Gorton (G.) et Holmström (B.) (2013)
« *Ignorance, debt and financial crises* », *mimeo*, p. 1-34.

Dermine (J.) (2013)
« *Banking regulations after the global financial crisis, good intentions and unintended evil* », *European Financial Management*, Vol. 19 (4), septembre, p. 1-17.

Dermine (J.) (2015)
Bank valuation and value-based management, 2e édition, McGrawHill, NY.

Diamond (D. W.) (1984)
« *Financial intermediation and delegated monitoring* », *Review of Financial Studies*, 51, p. 393-414.

Diamond (D. W.) et Dybvig (P.) (1983)
« *Bank runs, deposit insurance and liquidity* », *Journal of Political Economy*, 91, p. 401-419.

Forum économique mondial (2015)
« *The future of financial services* », juin, p. 1-176.

Kelly (G.) (2014)
« *The digital revolution in banking* », *Occasional Paper 89*, Groupe des Trente, Washington DC, p. 1-41.

Stiglitz (J.) et Weiss (A.) (1981)
« *Credit rationing with imperfect information* », *American Economic Review*, 71, p. 393-410.

Le risque numérique : défi stratégique et opportunité de développement pour les assureurs

Nicolas SCHIMEL
Directeur général
Aviva France

Bien avant beaucoup d'industries, l'assurance a dès son origine assis son modèle économique sur la collecte et la maîtrise des données, et dès l'apparition de l'informatique, sur le stockage, l'utilisation et le contrôle des données du passif, puis au rythme de la sophistication de la finance, de celles de l'actif. Entre actuaires et statisticiens, financiers, informaticiens, le traitement des données et la gestion des risques associés ont toujours été une zone d'investissement majeure, ce qui a valu à l'assurance d'être longtemps en pointe dans ces domaines. La digitalisation accélérée de la société fait qu'aujourd'hui l'utilisation intensive de la donnée est présente dans tous les secteurs d'activité.

Toutefois, on voit que le risque numérique auquel font face les assureurs constitue un défi en partie spécifique et certainement majeur : d'abord, dans sa dimension stratégique, de par les reconfigurations possibles de modèles économiques, ouvertes par le développement numérique ; ensuite, l'obligation de continuité d'activité dans la longue durée, traduite désormais en Europe par les normes Solvabilité II, crée un niveau d'exigence extrêmement élevé, et place l'assurance parmi les industries et services les plus sensibles, à l'instar de la banque ou de la défense. Au regard de ce niveau d'exigence, la profession a des moyens et des atouts pour s'organiser face aux risques opérationnels.

Maîtriser pour son propre compte le risque numérique sera sans doute un atout de la profession pour jouer à son tour un rôle clef vis-à-vis du risque numérique dans la société. Cette opportunité donne déjà lieu à de premières offres, en soulevant les questions classiques sur l'assurance d'un type de risque nouveau, mais elle interroge aussi, à certains égards, l'assurabilité d'organisations de grande taille ou stratégiques, et au regard de son niveau élevé de technicité, ouvre des perspectives nouvelles liées à la mise en place d'un écosystème dédié.

Le risque numérique représente de nouvelles menaces pour les assureurs, consommateurs et producteurs historiques de données.

Les données et leur exploitation mathématique sont au cœur du modèle de l'assurance moderne...

L'assurance moderne a, dès son origine, assis son modèle économique sur une évaluation des risques basée sur la collecte et la maîtrise de données fiables. Par essence, les données constituent la clé de voûte du modèle économique assurantiel. En permettant de déterminer la probabilité de réalisation d'un risque – et donc la prise de décision quant à son assurabilité – ainsi que la tarification associée au transfert du risque, le traitement mathématique des données conditionne le pilotage stratégique, le positionnement compétitif et la performance opérationnelle de toute compagnie d'assurance.

En déployant des méthodes d'évaluation des risques de plus en plus poussées, appuyées par les innovations informatiques qui ont permis de renforcer la capacité de calcul et la sophistication des modèles utilisés, les assureurs s'adaptent aux évolutions de la société.

… et trouvent une résonance nouvelle dans le contexte de la « révolution par les données »

Aujourd'hui, les sources des données permettant d'étayer la modélisation des risques sont amenées à se diversifier, comme conséquence du phénomène numérique *big data*. Les implications et enjeux pour la profession sont considérables ; l'exploitation de ces données pourrait en théorie bouleverser les modèles économiques traditionnels de l'assurance.

Se prémunir contre les risques croissants de cyber-attaques constitue un enjeu de taille

Le caractère souvent sensible et confidentiel des données conservées de manière dématérialisée par les assureurs, et plus généralement par toute organisation économique, expose ces derniers à des risques de cyber-attaques : vol et violation de données clients, espionnage, etc. Le numérique a démultiplié la force de frappe des acteurs économiques et est un facteur considérable de croissance économique lorsqu'il s'agit de transformer sa relation avec le client, d'affiner ses offres et son *pricing*, d'automatiser ses opérations administratives ou de nouer des partenariats. Mais son développement a également créé des couches de complexité et de vulnérabilité supplémentaires lorsqu'il s'agit de cyber-résilience, par exemple en renforçant la dépendance des organisations vis-à-vis d'infrastructures numériques qu'elles ne peuvent totalement contrôler (Deloitte, 2014).

Le défi numérique se décline donc pour les assureurs aussi bien en risques qu'en opportunités stratégiques : en risque opérationnel sur les données et les systèmes, qui trouve un écho particulier dans l'environnement de Solvabilité II, mais également en nouveaux risques à couvrir, avec toutes les problématiques portées par un marché en émergence.

1| Menaces et opportunités d'une reconfiguration des modèles d'assurance

Si la sécurité des données et des systèmes d'information est la première à venir à l'esprit quand est évoqué le risque numérique dans le secteur de l'assurance, un risque tout aussi fondamental de fragilisation des acteurs actuels réside dans les reconfigurations potentielles des modèles économiques.

L'intégration progressive et rapide des technologies numériques offre de nombreuses occasions de transformer les modèles économiques de l'assurance

On assiste à une explosion de la quantité et de la variété de la donnée clients (*big data*), chez de nombreux acteurs aujourd'hui loin du métier d'assureur (téléphonie, constructeurs automobiles et, d'une manière générale, tout pourvoyeur d' « objet connecté ») mais qui demain collecteront plus d'informations sur les comportements des clients que les assureurs. Or ces informations portent en elles une capacité à mieux tarifer, suivre

et prévenir le risque. Que feront-ils de ces données ? Les vendront-ils à l'assureur le plus offrant ? (C'est le modèle actuel de Google). Voudront-ils intégrer certains pans de la chaîne de valeur de l'assurance : distribution, sélection du risque, service de prévention à valeur ajoutée, laissant à l'assureur les parties les moins commercialement discriminantes et les moins génératrices de marge ? Quelles en seraient alors les conséquences pour l'assureur ? La perte du contact client initial avec toutes les conséquences pour le développement commercial ? La mise en concurrence entre assureurs pour proposer les plates-formes de gestion les moins coûteuses avec pour corollaire, une baisse de marges, voire une concentration significative sur quelques acteurs afin de réaliser les économies d'échelle nécessaires ?

Par ailleurs cette explosion de nouveaux services digitaux et de données pourra conduire à une baisse de la matière assurable classique, menant à une réduction du volume d'activité des assureurs. Les objets connectés favoriseront par exemple la détection des risques et donc la prévention, ce qui en fait un modèle vertueux. Avec la voiture connectée ou autonome, les risques d'accident vont très probablement diminuer significativement, la création de flottes de voiture verra une partie du marché B2C évoluer vers un marché B2B, l'information recueillie sur la dangerosité des routes modifiera l'évaluation du risque, etc.

L'intrusion du *big data* pourra également conduire à ajuster significativement le tarif et l'offre de chaque assuré (*segment of one*) pour optimiser le positionnement des offres auprès des « bons risques ». Le concept de mutualisation disparaîtra et les clients trop risqués se verront proposer des tarifs si élevés qu'ils ne pourraient plus s'assurer.

Autre risque, même si aujourd'hui les expériences sont peu significatives : l'assurance *peer-to-peer*, qui consiste en la mutualisation, au sein d'une communauté restreinte et cooptée, des primes et des risques à assurer en dehors de toute approche traditionnelle de gestion assurantielle et de provisionnement. À ce stade, le risque semble peu important et limité à des risques de petits montants. Néanmoins, la créativité des acteurs n'est pas encore allée jusqu'au bout des opportunités que porte la digitalisation des relations entre clients et fournisseurs.

Enfin, il existe aussi un risque collatéral sur la pérennité de la distribution traditionnelle de l'assurance, qui est encore aujourd'hui intermédiée à plus de 90 %. Le développement des modèles multi-canaux de relation, l'apparition de nouveaux concurrents avec leur propre logique de distribution, la vente en direct de produits d'assurance sur le web, l'apparition d'outils robotisés de conseil, l'augmentation du *self-service* en ligne, par exemple, sont autant de remises en cause des rôles actuels de la distribution traditionnelle en assurance. Celle-ci n'aura d'autres issues pour exister que de se transformer pour continuer à apporter une valeur ajoutée à ses clients.

L'acceptation des assurés de partager leurs données personnelles pèsera sur l'ampleur des transformations économiques

L'acceptation de partage des données individuelles n'est possible que sur la base d'un consentement éclairé dans un cadre de confiance et de transparence et suppose aussi une vision claire sur les bénéfices associés et les moyens de contrôle disponibles. Et, au-delà des craintes que peuvent avoir les particuliers sur la sécurité des données et l'utilisation frauduleuse qui peut en être faite, c'est aussi une question bien plus philosophique que soulève le numérique, celle du risque d'une société où chaque individu pourra voir son existence tracée, catégorisée, mémorisée avec toutes les dérives totalitaires que cela peut engendrer. Un débat public émerge aujourd'hui, il ne manquera pas de s'intensifier et, à terme, d'aboutir à cadrer de manière plus ou moins restrictive les opportunités ouvertes par le recueil, le traitement et l'utilisation de la donnée, ayant ainsi une influence sur la profondeur de la transformation des modèles économiques, dont celui des compagnies d'assurance.

L'intervention de nouveaux acteurs sur la chaîne de valeur de l'assurance ouvre la question de la réglementation devant s'appliquer

La dématérialisation numérique ouvre la voie à une délocalisation ou à une absence de localisation nette du recueil, du stockage, du traitement des

données et des prestations offertes. Cela pose la question complexe de la régulation des nouveaux acteurs, en liaison avec la protection des données personnelles et des consommateurs et les conditions de concurrence [1]. Si ces dimensions du risque numérique ne touchent pas que les assureurs, elles sont toutefois significatives dans un secteur où la donnée est à la base du métier [2].

Il existe donc un vrai risque de fragilisation financière des acteurs actuels

La matérialisation de ce risque profiterait à de nouveaux entrants (télécom, constructeurs automobiles et d'autres objets connectés, *peer-to-peer*, Google, Apple, Facebook, Amazon, etc.), non pas nécessairement sur l'intégralité de la chaîne de valeur de l'assurance, mais plutôt en tant qu'intervenants sur certains pans de cette dernière, où ils pourraient capitaliser sur un avantage concurrentiel apporté par le numérique, le tout étant associé à la baisse de la matière assurable.

La période est donc disruptive pour les assureurs. L'avantage est qu'ils subissent le risque stratégique numérique après d'autres secteurs et qu'ils peuvent en tirer des leçons. La prise de conscience est profonde et les initiatives très nombreuses pour s'adapter et, au-delà, utiliser la révolution numérique pour réinventer ses métiers et se rapprocher de ses clients. C'est au prix d'un très gros travail de transformation interne, pour accroître la capacité à se remettre en cause, à écouter les clients, à tester des initiatives, à savoir monter les bons écosystèmes avec des partenaires externes (fintechs notamment), que les assureurs transformeront cette époque formidable en opportunités. Et c'est dans la capacité d'exécution de cette transformation que se compteront les gagnants de demain.

2| Prise en compte du cyber-risque par les assureurs, dans le cadre de Solvabilité II

Tout acteur économique est exposé aux cyber-attaques. Ces dernières sont caractérisées par une sophistication grandissante

Dans un contexte de digitalisation accélérée, et face à des tactiques de plus en plus sophistiquées, agiles, difficilement prévisibles, la menace d'une cyber-attaque plane sur toutes les organisations économiques, de la PME à la multinationale, du secteur public aux ONG, et ce, malgré une prise de conscience collective du risque, et la mise en œuvre des investissements dédiés à la cyber-résilience (en augmentation de 24 % au niveau mondial en 2015, cf. PwC Consulting, 2016 b). 43 millions de cyber-incidents ont été relevés dans le monde en 2014 (cf. PwC Consulting, 2015).

Par ailleurs, les stratégies mises en place par les cyber-criminels évoluent, vers une plus grande sophistication. La tendance est en effet au déploiement de procédés d'intrusion passant par les salariés d'une compagnie (courriels frauduleux, etc.), avec l'objectif de s'introduire dans les systèmes d'information de l'organisation, de s'y déployer de manière graduelle, et d'y rechercher, en se basant sur des compétences pluridisciplinaires, à la fois technologiques et métiers, les données clés qui seront exfiltrées à des fins de tentatives d'extorsion, de reventes, etc.

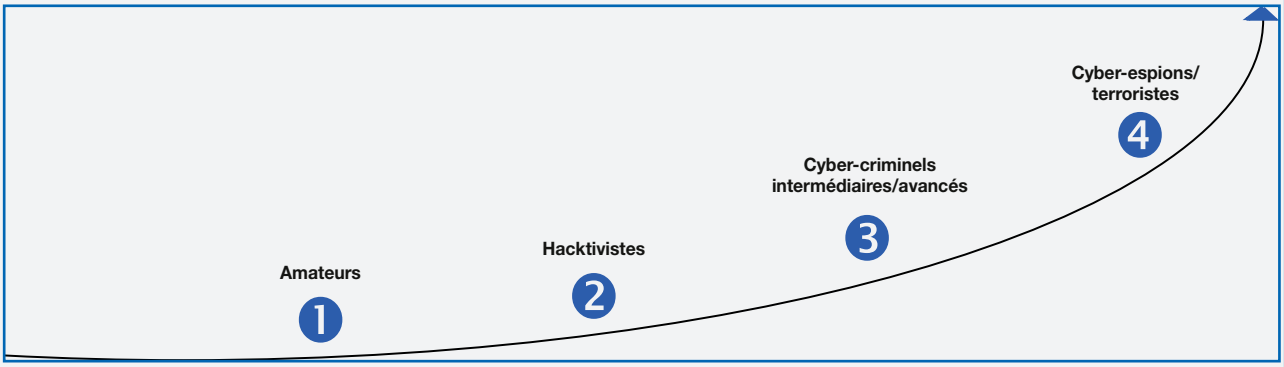
Bien entendu, la nature d'une cyber-menace apparaît comme fortement liée au secteur d'activité : espionnage du patrimoine industriel dans le secteur des nouvelles technologies, vol et violation de données personnelles et interruption de services pour le secteur des services y compris publics, etc..

1 *La palette des situations potentiellement créées est large : intervenant local ; intervenant d'un pays de l'Union européenne (UE) ; intervenant en libre prestation de service dans l'UE ; intervenant établi dans un pays ayant plus ou moins d'accords avec l'UE ; et à l'extrême, les modèles totalement disruptifs comme le* peer-to-peer, *qui échappent encore aujourd'hui à la régulation d'assurance.*

2 *Les pouvoirs publics se sont emparés de ce sujet afin de conduire à plus d'homogénéité et d'équité entre les acteurs. La directive n° 95/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, les positions des commissaires européens Margrethe Vestager (*La Tribune, *2015 a), en charge de la concurrence, ou Günther Oettinger (*La Tribune, *2015 b), en charge du numérique, montrent le chemin, mais le voyage n'est pas fini.*

Encadré 1

Les cyber-attaques voient leur nature et leur degré de sophistication évoluer



	1 Amateurs	2 Hacktivistes	3 Cyber-criminels intermédiaires/avancés	4 Cyber-espions/ terroristes
Objectifs et cibles	• Souvent sans objectif précis ; « petites » arnaques visant des particuliers, réalisation d'expériences • Cibles aléatoires (techniques standardisées)	• Revendications politiques (type *Anonymous*) ; thématiques émotionnelles • Cibles liées aux revendications	• Motivations financières (vol de données bancaires, etc.) • Ciblage opportuniste	• Vol/compromission de données dans le cadre d'attaques ciblées contre des États/organisations • *Advanced persistent threat* (APT) : attaques ciblées, de long terme
Organisation	• Pas organisés	• Organisés	• Très organisés • Très professionnalisés/ couplage compétences technologiques et métiers	• Très organisés • Très professionnalisés/ couplage compétences technologiques et métiers

Sources : CERT IST, SOPRA, Swisscom.

Encadré 2

Quelles sont les conséquences potentielles des cyber-risques auxquels une organisation est confrontée ?

- Vol de propriété intellectuelle ou de données commerciales confidentielles
- Interruption d'activité
- Pertes ou dégradation de données et de logiciels
- Pertes financières directes (extorsions, détournements de fonds, etc.)
- Responsabilité envers des tiers
- Impacts sur la réputation
- Dommages physiques
- Coûts d'investigation/de réponse

Autres parties susceptibles d'être impactées :
- Clients
- Employés
- Fournisseurs, prestataires, etc.

Source : HM Government (2015).

Avec des coûts associés aux cyber-crimes estimés à plus de 400 milliards de dollars par an en 2014 [3] et dans un contexte d'interconnexion croissante de l'économie faisant que, par un effet de « cascade », les conséquences d'une cyber-attaque peuvent s'étendre bien au-delà de la cible visée en premier ressort, l'enjeu de la cyber-résilience est plus que jamais de taille pour toutes les organisations.

Les pouvoirs publics se sont fermement saisis du sujet de la cyber-sécurité

Le fait que les pouvoirs publics aient mis en œuvre une démarche volontariste visant à renforcer la cyber-résilience, tant au niveau européen (accord sur les premières règles européennes concernant la cyber-sécurité – Parlement européen, 2015 –,

3 *Cf.* Center for Strategic and International Studies (2014). *Les auteurs estiment que les coûts annuels découlant des cyber-crimes à l'échelle mondiale sont compris entre 375 milliards de dollars (hypothèse conservatrice) et 575 milliards (hypothèse maximale), et s'accordent à dire qu'ils devraient s'élever à plus de 400 milliards de dollars par an.*

futur règlement européen sur la protection de données personnelles [4]), que national, constitue un signal fort quant à l'enjeu et aux défis liés à la cyber-criminalité. La création de l'Agence nationale de la sécurité des systèmes d'information et la promulgation de la loi de programmation militaire 2014-2019 ont déjà concrétisé la démarche volontaire de la France face aux cyber-menaces.

En tant qu'utilisateurs de données personnelles, y compris de données sensibles, les acteurs de l'assurance seront directement impactés par les futures évolutions réglementaires européennes relatives à la protection des données personnelles (cf. projet de règlement général sur la protection des données, dont l'application est prévue pour 2018). Il est attendu que ce règlement renforce les pouvoirs de sanction de la Commission nationale de l'informatique et des libertés (CNIL) et expose les assureurs ayant subi une fuite de données – comme toute autre organisation – à de fortes amendes en cas de manquements avérés (mesures techniques et organisationnelles de traitement de données non conformes, absence de notification d'une fuite de données à la CNIL/aux personnes physiques concernées, etc.). Par ailleurs, l'introduction dès 2014 des *class actions* en France et le fait que les consommateurs soient davantage sensibilisés à la protection de leurs données personnelles devraient contribuer à renforcer la pression juridique et financière pesant sur les organisations économiques lorsqu'il s'agit de traitement de données sensibles.

Le secteur de l'assurance a jusqu'à présent été relativement préservé des cyber-attaques

Ce n'est qu'en 2014 qu'a eu lieu la première cyber-attaque visant un opérateur de l'assurance, le courtier en assurance britannique Brightside (Insurance Speaker, 2014).

Cette préservation des cyber-attaques dans le secteur de l'assurance trouve racine en partie dans la digitalisation plus tardive du secteur. Néanmoins, il faut s'attendre à court ou moyen terme à une augmentation à la fois de la fréquence et de la gravité des cyber-attaques visant le secteur, qui s'explique en partie par le rattrapage de la profession sur le volet digital. À ce sujet, l'étude réalisée par le World Economic Forum (2014), montre que la moitié des dirigeants de compagnies d'assurance interrogés identifie le risque d'une cyber-attaque comme un enjeu aux implications majeures.

Le fait qu'en 2015, l'un des plus importants assureurs américains du secteur de la santé, Anthem, ait été victime d'une cyber-attaque d'envergure susceptible d'avoir abouti à un vol massif de données personnelles (Reuters France, 2015), met en avant toute l'importance du défi numérique que vit et vivra la profession.

L'exigence de professionnalisation de la gestion des cyber-risques est renforcée par Solvabilité II

Les assureurs ont depuis longtemps une profonde compréhension des risques assurantiels et financiers. La gestion des risques opérationnels franchit quant à elle une étape supplémentaire avec l'inclusion explicite de ces risques dans Solvabilité II, sous la définition d'un « *risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs* ». Aujourd'hui, Solvabilité II fait explicitement référence au risque opérationnel *via* les risques juridiques, les risques de modélisation par exemple. D'autres types de risques devront être inclus dans cette définition, par exemple ceux de fraude, de sécurité, et de non-protection des données – lesquels se rapprochent des cyber-risques.

Des typologies de risques numériques émergent, dans un environnement non stabilisé

Chaque assureur peut vouloir créer ses propres définition et typologie des risques numériques, qui comprennent au moins les cyber-attaques.

4 *Le règlement européen sur la protection des données personnelles devrait concerner toutes les organisations traitant des données à caractère personnel et imposer, en cas de compromission de données personnelles, la nécessité d'informer la CNIL et les personnes physiques concernées lorsqu'il existe un risque élevé pour leurs droits et libertés.*

Extrait de la typologie ORIC, comportant l'exposition au risque numérique

Type d'évènement (niveau 1)	Catégorie (niveau 2)	Activité (niveau 3, non exhaustif)
Fraude interne	Activité non autorisée	Transactions non déclarées ou non autorisées Falsification de données personnelles
Vol et fraude	Vol ou destruction d'actifs Divulgation d'informations confidentielles Irrégularités comptables	
Fraude externe	Systèmes de sécurité	Vol d'informations Virus
Interruption d'activités et panne des systèmes	Systèmes	*Hardware* *Software* Panne/Interruption
Gestion de la mise en œuvre, de la livraison et des *process*	*Transaction capture*, mise en œuvre et maintenance	Erreur dans la saisie de données Erreur comptable Prix unitaires ou allocation incorrects Inadéquation des *process* de documentation
Surveillance et *reporting*	Manquements aux *reporting* obligatoires Inexactitudes du *reporting* externe	
Gestion de comptes clients/consommateurs	Paiement au mauvais consommateur/client Paiement incorrect à un consommateur/client	

Une approche consiste aussi à utiliser une typologie existante couvrant tous les risques opérationnels, telle celle proposée par ORIC International (*Operational Risk Insurance Consortium*), ce qui permettra aussi d'échanger des informations avec les pairs sur les risques possibles et avérés, anonymisées *via* ORIC (*benchmarks*).

Ainsi, le risque numérique est une des causes possibles de bien des défaillances opérationnelles, dans des domaines allant de la comptabilité aux ressources humaines ou au service clients. De la même manière, les cyber-attaques à proprement parler peuvent avoir des impacts colossaux en termes de relations clients, de responsabilité juridique, d'exploitation commerciale, etc.. Plus encore, la transformation numérique exacerbe certains risques tant pour les institutions financières que pour les clients : les interactions quotidiennes se font en ligne, les rendant donc plus exposées aux vols d'identités ou aux interruptions de services. Nous sommes donc face à un paradoxe : le numérique peut aider à mieux contrôler les risques, à les rendre plus rares, mais aussi plus graves et moins visibles quand ils se réalisent.

La difficile mesure du cyber-risque

Les cyber-risques comme tous les risques opérationnels reflètent, par nature, toute la complexité de l'organisation et sont associés à des causes multiples et à des conséquences variées, qui les rendent difficiles à décrire, quantifier et analyser. En effet, les conséquences potentielles d'un incident peuvent recouvrir des impacts financiers à la fois directs (pertes d'exploitation liées à une interruption d'activités, coûts de traitement technique/remise en l'état, compensations financières de préjudices externes, frais juridiques, etc.), et indirects (dégradation de la réputation de l'entreprise, avec des répercussions négatives sur son chiffre d'affaires futur, coûts d'opportunité liés au temps passé par les équipes à la restauration informatique au détriment d'activités de croissance, etc.). Par ailleurs, l'évolution permanente de la technologie, des risques et de leurs parades complexifie le processus d'estimation des risques, en lien avec une obsolescence rapide de toute tentative d'évaluation d'un incident numérique.

Le cyber-risque estimé *via* le filtre des méthodes d'évaluation de l'impact sur le capital

Solvabilité II impose aux assureurs d'estimer leur capital comme « *le capital de solvabilité requis correspondant à la valeur en risque* (value-at-risk) *des fonds propres de base de l'entreprise d'assurance ou de réassurance, avec un niveau de confiance de 99,5 % à l'horizon d'un an* » (Art. 101 §3 de la directive Solvabilité II).

Les organismes d'assurances doivent donc estimer quel sera l'impact financier d'un risque pouvant survenir dans l'année avec une probabilité de 0,5 %.

Cela conduit donc l'assureur à évaluer le risque numérique sous l'angle de Solvabilité II.

Citons trois méthodes pour calculer cette statistique :

• **Approche par « distribution de pertes »**
Modélisation statistique du montant des pertes possibles en partant d'une base de données interne (ou de données de marché). Cette approche se heurte généralement au trop faible nombre de pertes observées pour des montants élevés – ce qui rend très difficile de calibrer le modèle statistique.

• **Estimation par analyse de scénario**
C'est l'approche la plus courante. Des experts métiers et *risk managers* développent conjointement un « narratif » décrivant le risque et la manière dont il peut se réaliser, jusqu'à son impact sur les opérations et les coûts financiers induits. On estime ensuite des probabilités d'occurrence à chaque « étape » du scénario et un montant pour chaque source de coût. Cette approche présente l'avantage d'une grande clarté dans la description du risque, d'une analyse assez fine des causes possibles et des impacts. En revanche, elle offre peu de flexibilité pour comprendre les interactions entre les risques.

• **Estimation *via* les réseaux bayésiens**
En extension de la démarche précédente, l'approche par réseaux bayésiens, part de scénarios décrivant comment un risque se manifeste, mais remplace les probabilités d'événements ou les estimations de montant « ponctuelles » par une distribution de probabilité complète, y compris les interdépendances éventuelles entre variables. Cette approche offre davantage de finesse d'analyse et une meilleure compréhension des risques – en particulier comment des valeurs extrêmes de pertes peuvent survenir. Les logiciels de modélisation permettent aussi de réaliser facilement des analyses de sensibilité.

La gestion des cyber-risques est en cours de sophistication

La gestion des risques numériques des assureurs, à l'instar de celle des autres risques, doit s'appréhender de manière robuste et professionnelle, notamment dans un contexte où la nature, les méthodes et les impacts potentiels des cyber-incidents se transforment, gagnant en sophistication et en agilité, appelant ainsi des réponses adéquates, à la mesure des enjeux rencontrés par la profession.

Conduite dans le cadre d'une approche holistique, décloisonnée et pluri-compétente, la démarche de gestion des risques numériques déployée par les assureurs recouvre les actions suivantes :

En amont :

• identification et analyse des risques : cartographie des risques numériques basée sur un recensement des actifs immatériels critiques, incluant une identification des points de vulnérabilités internes mais également externes, des logiciels utilisés, des parties prenantes, etc. ;

• développement de capacités de protection : basées sur une approche segmentée des risques, elles passent par la gestion des équipements informatiques (applicatifs pare-feu et anti-virus à jour et administrés avec rigueur, etc.), la gestion des accès et des droits dans les applications métiers et serveurs sensibles, la protection des données (chiffrement, classification, etc.), la gestion de la signature électronique, etc. ;

• détection des risques dans le cadre d'une approche pro-active et continue : une force de veille en cyber-incidents permet par exemple à l'organisation de disposer d'une vision plus fine des attaques potentielles et réelles auxquelles elle est exposée (en lien avec des organismes de recherche, Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques – CERT, etc.) ;

• mise en place d'actions de prévention (stratégie de cyber-sécurité et corpus de bonnes pratiques associés à une sensibilisation des équipes, audits de conformité, simulations d'attaques gérées en temps réel, etc.).

En aval, dans le cas où la survenance d'une attaque n'a pu être évitée, par le développement de capacités de réaction/de réparation rapides, non disruptives :

• mise en place de procédures d'intervention incluant une structure de *leadership* dédiée ;

• développement d'une capacité de réponse transversale (informatique et autres fonctions supports : communication et relations publiques, juridique, marketing, etc.) ;

• *testing* continu des capacités de réponses et retours d'expérience en cas d'application d'un plan de réponse.

Néanmoins, il est nécessaire de garder à l'esprit qu'au-delà de l'aspect purement technologique, et au regard des stratagèmes utilisés par les cyber-criminels, qui visent à s'introduire dans les systèmes en infiltrant des postes utilisateurs, la sensibilisation de tous les salariés aux risques numériques apparaît comme un point central à toute politique de cyber-résilience.

L'enjeu des cyber-risques dans le secteur de l'assurance retient toute l'attention du superviseur

L'Autorité de contrôle prudentiel et de résolution (ACPR), dans son rôle de stabilisation de la place financière et de protection de la clientèle, donne aussi un cadre à la démarche de lutte contre la cyber-criminalité, associé aux principes de Solvabilité II. Son action est organisée principalement sur quatre axes, selon les mots de son secrétaire général Édouard Fernandez-Bollo (2015) :

• *« L'incitation pour les institutions supervisées à s'organiser efficacement pour répondre à la menace des cyber-attaques ;*

• *l'amélioration de l'identification de la menace avec un recensement centralisé des attaques au niveau européen ;*

• *l'adaptation du suivi du risque opérationnel pour mieux tenir compte des spécificités du risque des attaques ;*

• *la promotion de la coopération entre tous les acteurs publics ou privés ».*

3| Le risque numérique, une opportunité pour une nouvelle offre d'assurance

Un contexte à la fois anxiogène et réglementaire a contribué à l'émergence d'un besoin de protection contre toute forme de cyber-risques

La médiatisation de récentes cyber-attaques d'envergure (JP Morgan, Sony, Target, etc.) a contribué à marquer les esprits et à alimenter une prise de conscience collective : aucun système numérique n'est aujourd'hui infaillible et les répercussions associées à une cyber-attaque peuvent être colossales.

Aux États-Unis, où le marché de la cyber-assurance est l'un des plus matures, il est à noter que celui-ci n'a véritablement pris son envol qu'à la fin des années deux mille, et cela, largement en lien avec l'instauration d'une obligation de notification de toute fuite de données à caractère personnel aux personnes concernées, associée à des charges financières élevées, et renforcée par les recours aux *class actions*.

L'entrée en vigueur attendue du futur règlement européen sur la protection des données personnelles, qui devrait se traduire, dès 2018, par un élargissement de l'obligation de notification de compromission de données à caractère personnel, concernant à ce jour uniquement les entreprises de télécommunications et fournisseurs d'accès Internet, à toutes les organisations, participera très certainement à l'ouverture du marché.

Si la cyber-assurance est, pour l'heure, principalement concentrée au sein du monde anglo-saxon, et demeure principalement l'apanage de grands groupes, œuvrant notamment dans les secteurs de la santé, des technologies et du commerce, elle devrait s'étendre en France non seulement aux grandes entreprises, mais également aux entreprises de plus petite taille, traditionnellement moins résilientes d'un point de vue numérique, et aux particuliers.

De manière générale, les enjeux en termes de cyber-sécurité, les impacts associés, les attentes des acteurs en termes de cyber-assurance ainsi que les réponses assurantielles potentielles diffèrent largement selon le type d'acteurs concernés : grandes entreprises ou grandes organisations y compris publiques ; ETI et PME ; particuliers.

Les trois catégories d'assurés structurent et conditionnent le marché de la cyber-assurance

De manière générale, une grande organisation souhaite en tout premier lieu éviter la survenance d'une cyber-attaque, laquelle serait susceptible d'engendrer des charges financières trop élevées, mais également de causer des préjudices réputationnels dont elle pourrait avoir du mal à se défaire. Par ailleurs, dans la mesure où l'existence de « risques de pointe » questionne à certains égards l'assurabilité des cyber-risques des grandes structures, comme nous le détaillerons par la suite, les attentes de ces dernières sont davantage tournées vers la prévention, dans une logique partenariale avec des tiers dont l'assureur.

Les ETI/PME, traditionnellement moins résilientes en termes de cyber-attaques, souhaitent quant à elles s'assurer, car elles ne disposent pas nécessairement de l'assise financière nécessaire à l'absorption des coûts associés à une attaque, qui dans certains cas, pourrait conduire à leur faillite. Elles sont par ailleurs enclines à souscrire une police d'assurance proposant de l'expertise et des services (cyber-experts, prévention, etc.), dont elles ne disposent généralement pas.

Enfin, les particuliers, dont les cyber-risques ne posent pas d'enjeu spécifique en termes d'assurabilité, apparaissent comme enclins à souscrire des polices d'assurance leur permettant de maîtriser, par l'apport d'un service et d'expertise, les conséquences d'une cyber-attaque (services en e-réputation, conseils juridiques, etc.).

Encadré 3

Le marché français de la cyber-assurance

Le marché français de la cyber-assurance a une capacité théorique comprise entre 405 et 570 millions d'euros [1] et repose sur une douzaine d'assureurs référencés (AIG, ACE, AGCS, ALLIANZ, XL, CAN, BEAZLAY, Munich RE, Zurich, AXA, etc.). Selon une étude réalisée par PwC en 2015, moins de 5 % des entreprises françaises et de 6 % des particuliers ont déjà souscrit une cyber-assurance.

Les polices dédiées aux cyber-risques sont généralement combinées pour les professionnels (dommages, responsabilité civile et services/expertise) et recouvrent principalement les aspects suivants :

	Recouvrements des coûts proposés par l'assureur	Services et expertise proposés par l'assureur
Entreprises	• Dommages (frais de reconstitution de données, pertes d'exploitation, frais de notification, frais de publication, extorsion, etc.) • Responsabilité civile (frais de défense dans le cadre d'une enquête ouverte par la CNIL ; e-réputation généralement peu couverte)	• Cyber-sécurité/Gestion de cyber-incidents • Prévention • Communication de crise • Juridique • *Monitoring*
Particuliers	• Remboursement des préjudices financiers liés à une usurpation d'identité • Remboursement du montant de l'achat d'un bien en cas de préjudice subi sur un site de vente *online* • Remboursement des préjudices causés par des actions de cyber-harcèlement (*cyberbullying*)	• E-réputation (nettoyage/noyage de l'information sur le web) • Juridique (informations juridiques, actions judiciaires) • Assistance psychologique

1 *Gras Savoye.*

La cyber-assurance bouscule les méthodes « traditionnelles » d'évaluation et de mutualisation des risques, et, par ricochet, la tarification associée

Le faible recul des assureurs sur la cyber-assurance et le manque d'historique relatif à la survenance de cyber-incidents, s'érigent en tout premier lieu comme un frein aux procédés d'évaluation et de mutualisation des risques traditionnellement appliqués par la profession, impactant de ce fait la tarification des cyber-polices.

En effet, en tant que risque « nouveau » du point de vue de l'assurance, disposer d'une base de données fournie sur les sinistres passés permettrait aux porteurs de risques d'affiner leurs calculs actuariels, en observant à la fois la fréquence et l'intensité de cyber-incidents survenus, et se traduirait par une vision plus fine du risque d'exposition maximal d'un assuré potentiel, conditionnant la décision de l'assureur de couvrir ce risque, la mise en place par l'assureur d'exclusions et de franchises le cas échéant, et impacterait la tarification d'une police d'assurance.

Cependant, l'existence d'une telle base de données sur les sinistres passés trouve une première limite dans l'évolution constante et très rapide des technologies, et l'agilité des cyber-criminels face à ces évolutions. En effet, cela implique pour toute tentative de catégorisation des cyber-risques à des fins d'évaluation des risques basée sur des observations passées, un risque pour les assureurs d'être rattrapés par l'obsolescence rapide de ladite catégorisation. En d'autres termes, c'est l'hypothèse de continuité, « *ce qui était vrai hier l'est encore aujourd'hui* », qui est inapplicable lorsqu'il s'agit d'assurer un cyber-risque. De plus, les conséquences de deux cyber-attaques de même type peuvent considérablement différer, notamment selon leur action sur le système d'information, la rapidité de leur découverte, le nombre d'informations détenues, rendant difficile toute évaluation des cyber-risques sur la base de leur catégorisation.

Par ailleurs, l'utilisation de données sur les sinistres passés est fragilisée par le nombre limité, à une date donnée, de la population des cyber-assurés. En effet, cette utilisation aurait pu permettre aux assureurs d'appliquer le principe de la mutualisation et de la compensation des risques en se basant sur la loi des grands nombres, mais se heurte actuellement au nombre réduit d'assurés, caractéristique d'un marché en émergence.

Une difficulté complémentaire repose aussi sur l'interdépendance des risques numériques, du fait de l'interconnexion croissante des systèmes d'information et de la propension des cyber-attaques à se propager très rapidement, au-delà de la cible visée en premier ressort et au-delà des frontières. Cela implique que le principe de diversification des risques appliqué par les assureurs est bousculé par l'existence d'un risque de corrélation marqué des risques individuels constitutifs du portefeuille d'un assureur, et que le principe de diversification géographique par la réassurance est lui-même compromis.

Comment faire reculer les frontières de l'assurable dans le cas des cyber-risques d'une grande entreprise ou organisation

Un certain degré d'analogie existe entre les cyber-risques visant une entreprise ou une organisation stratégique de grande taille et les risques terroristes ou de catastrophes naturelles, bien que la comparaison se heurte à la fréquence de plus en plus élevée des cyber-attaques, et au fait qu'elles ne recouvrent pas celles visant des particuliers, dont les impacts restent à ce jour largement moins massifs. Dans un contexte où une cyber-attaque de forte intensité visant une entreprise ou une organisation pourrait avoir des répercussions systémiques, ses répercussions financières pourraient largement dépasser les capacités d'assurance et de réassurance [5].

5 *Une étude projective publiée par le Lloyds chiffre les pertes potentielles d'une cyber-attaque sur le réseau électrique nord-américain, causant une coupure de courant au sein de quinze États américains, à un total compris entre 243 et 1 000 milliards de dollars, pour une indemnisation comprise entre 21,4 et 71,1 milliards de dollars. La violation en 2011 de données du réseau PlayStation de Sony a entraîné des coûts estimés à 170 millions de dollars. La fuite de données de l'Office of Professional Management (OPM) constatée en 2015 pourrait coûter 330 millions de dollars.*

Or, au niveau des entreprises, ce sont précisément ces « risques de pointe » qui soucient les *risks managers*, et que ces derniers souhaitent assurer.

Comment s'assurer de la viabilité économique des polices souscrites et donc de la prise en charge effective des garanties le moment venu, si survient un tel « risque de pointe » ? Se pencher sur cet enjeu nécessite de conduire des réflexions de fond, notamment sur l'opportunité :

- de regrouper les porteurs de risques, assureurs et réassureurs, en *pool* lorsqu'il s'agit d'assurer une grande entreprise et/ou une entreprise sensible ;

- de créer un écosystème de l'assurance cyber-risques, intégrant notamment, au-delà des assureurs et réassureurs, tous les prestataires de services de cyber-sécurité dédiés à une gestion professionnalisée des cyber-incidents, à la veille technologique, à la cartographie des risques, et l'État, en tant qu'assureur ou réassureur de derniers recours et vecteur de bonnes pratiques (sensibilisation de l'opinion publique, durcissement des exigences réglementaires, dans le cadre d'une coopération étroite à l'échelle internationale).

Au-delà des enjeux d'assurabilité et d'évaluation des risques, la cyber-assurance soulève des questions nouvelles, dépassant le champ de l'assurance

Utilisation de réseaux sociaux, envoi de courriels, stockage de données personnelles sur le *cloud*, utilisation de *smartphones*, achats en ligne, déclarations sur les sites web d'agences publiques, tous ces comportements réalisés dans la sphère personnelle, aujourd'hui perçus comme tout à fait anodins et communs, posent question lorsqu'il s'agit de contractualiser une police de cyber-assurance pour particuliers. Au-delà de l'évaluation du risque, ce sont des enjeux plus larges relatifs à la propriété des biens numériques et à la responsabilité associée à son traitement qui émergent.

Les attentes du marché vis-à-vis de l'assureur élargies à la prévention et aux services

Face à l'ampleur des conséquences générées par une cyber-attaque, la prévention apparaît comme essentielle, et les assureurs très bien placés pour participer activement à ce rôle de prévention, par exemple en communiquant à leurs clients, qu'ils soient particuliers ou professionnels, un corpus de bonnes pratiques, des retours d'expériences anonymes issus de leur base de clients en lien avec la cyber-sécurité, etc..

En plus de la prévention, et du fait de la technicité et complexité des risques couverts, les partenariats stratégiques entre assureurs et acteurs de la cyber-sécurité sont clés. Ils permettent à la fois, lors du processus de contractualisation, d'identifier de manière précise et personnalisée les besoins du client, les mesures déjà en place, les risques auxquels il est exposé et de réaliser des audits des systèmes d'information de manière régulière tout au long de la vie du contrat. Par exemple, des assureurs se sont associés à des acteurs de type Thalès et Cassidian (EADS), dans l'objectif de sensibiliser les entreprises aux cyber-risques et à la nécessité de mettre en place des actions de prévention concrètes et de développer des capacités d'actions en cas de cyber-attaque.

Par ailleurs, en cas de survenance d'un cyber-incident au sein d'une entreprise, certains assureurs proposent des prestations de conseil et de formation en gestion de crise.

Certains contrats de protection « e-réputation » pour particuliers proposent enfin les services d'un prestataire spécialisé en charge de l'identification des sources de mauvaise réputation et du traitement de celles-ci. Des juristes peuvent également intervenir pour accompagner les assurés en cas de besoin.

Conclusion

En quelques années, le risque numérique a pris des proportions considérables qui nécessitent une prise de conscience sans délai de la part des acteurs clés de l'économie.

Jeremy Rifkin, auteur dès 2011 de *La troisième révolution industrielle*, et penseur précurseur des impacts du numérique sur la société économique, concluait son ouvrage de 2014 *La nouvelle société du coût marginal zéro* en faisant ressortir que le parallèle entre le risque numérique et le risque climatique était frappant, comme conséquences indésirables du progrès humain, avec mondialisation des causes et des conséquences et possibilité de réaction en chaîne incontrôlable.

En réalité toutefois, là où le risque climatique pourrait échapper à tout contrôle, le risque numérique ne deviendrait catastrophique à l'échelle de l'humanité que dans des cas extrêmes de guerre terroriste (à l'instar du risque d'une attaque terroriste nucléaire par exemple), combinée à une fragilité excessive des défenses de la société, qui serait la conséquence d'une négligence extrême. L'action déjà engagée des États, dont une partie importante n'est sans doute pas visible, est un signe fort que ce risque, s'il peut devenir fort coûteux, n'est pas incontrôlable.

En ce qui concerne l'assurance, la prise de conscience et l'organisation de moyens de détection et de gestion du risque, se situent dans la moyenne de l'économie plus que sur son front avancé. On peut imaginer que dans les années à venir la réglementation imposera aux opérateurs financiers des normes de sécurité renforcées, issues par exemple de la future loi européenne ou des normes sectorielles. La prolifération de normes spécifiques n'est d'ailleurs sans doute pas nécessaire dans la mesure où le risque numérique est avant tout une réalité transversale qui nécessitera de fortes coopérations intersectorielles et qu'il ne faudrait pas trop en cloisonner l'approche.

On pourrait en conclusion dégager les trois pistes d'action suivantes face aux menaces et opportunités du risque numérique pour l'assurance :

- insister sur la qualité de la prise en compte du risque numérique dans les rapports ORSA, en dégageant avec pragmatisme des niveaux d'exigence proportionnés à la nature des activités et des risques des compagnies ou acteurs de l'assurance, et en y associant le régulateur et la profession, à même d'apporter un éclairage pédagogique et des *guidelines* méthodologiques sur ce sujet, notamment aux acteurs les plus vulnérables ;

- éclairer et si possible encadrer le risque juridique lié à la protection des données personnelles, afin de le rendre à la fois plus visible mais aussi « assurable », sans attendre l'émergence d'une jurisprudence qui cumulerait l'inconvénient du temps long et de l'incertitude juridique qui ne sont pas propices à une bonne anticipation ;

- favoriser l'émergence d'un marché de l'assurance cyber qui souffre aujourd'hui d'un déficit d'offres, alors que la triple fonction des assureurs, conseil/prévention/indemnisation, pourrait être un formidable adjuvant à une meilleure maîtrise de ces risques au sein de l'économie française et à une stabilité économique meilleure, etc. à condition bien sûr que la qualité de gestion des risques opérationnels et stratégiques (dont le risque numérique) des assureurs leur permette d'être des offreurs de confiance, eux-mêmes gages de stabilité.

Bibliographie

ANSSI (2011)
« Défense et sécurité des systèmes d'information – Stratégie de la France ».

AON (2015)
« *Global risk management survey* ».

Argus de l'Assurance (2015)
« Le cyber-espace décuple les risques ».

Center for Strategic and International Studies (2014)
« *Net losses: estimating the global cost of cyber crime* », juin.

Deloitte (2013)
« *Cyber crime fighting* ».

Deloitte (2014)
« *Changing the game on cyber risk – The imperative to be secure, vigilant, and resilient* ».

L'Expansion/L'Express (2014)
« Cyber-attaques : un nouveau marché prometteur pour les assurances ».

Fédération française des sociétés d'assurance
« Les conditions d'assurabilité des cyber-risques ».

Fernandez-Bollo (É) (2015)
« Institutions financières et cyber-criminalité », *Revue d'économie financière.*

HM Government/Marsh (2015)
« *UK cyber security – The role of insurance in managing and mitigating the risk* », mars.

IBM (2015)
« *IBM 2015 cyber security intelligence index* ».

Institut d'assurance (2015)
« Les cyber-risques : conséquences pour l'industrie de l'assurance au Canada ».

Insurance Speaker (2014)
« Brightside : un acteur du secteur de l'assurance victime d'une cyber-attaque ».

Lemarchand (H.) (2014)
« *Assurances et cybersécurité* », *Observatoire* – FIC.

Marsh (2015)
« *European 2015 cyber risk survey report* ».

Parlement européen (2015)
« Les députés concluent un accord avec le Conseil sur les toutes premières règles européennes relatives à la cyber-sécurité », communiqué de presse 8 décembre.

PwC Consulting (2015)
« *Insurance 2020 & beyond: reaping the dividends of cyber resilience* ».

Pwc Consulting (2016a)
« Le marché de la cyber-assurance : la révolution commence maintenant ».

PwC Consulting (2016b)
« *Turnaround and transformation in cyber security* ».

Reuters France (2015)
« La 2e compagnie US d'assurance santé cible d'une cyber-attaque », 5 février.

La Tribune (2015a)
« Comment l'Europe veut mettre les GAFA au pas ».

La Tribune (2015b)
« Sans Europe du numérique, ce sont Amazon, Google, Microsoft qui vont décider ».

World Economic Forum (2014)
« *Risk and responsibility in a hyperconnected world* ».

Le risque systémique dans les paiements

Georges PAUGET
Président
Institut d'éducation financière du public et de la société de conseil économie finance et stratégie

Les plates-formes de paiement, qu'elles concernent les activités de détail ou de marché, ont continué à fonctionner sans incident majeur au cours des récentes crises financières, ceci malgré des hausses brutales du volume des transactions lors de certaines journées. Ces résultats, pour satisfaisants qu'ils soient, ne doivent pas conduire à sous-estimer les risques inhérents à ces plates-formes. L'analyse du risque systémique dans les paiements ne saurait cependant se réduire à la seule problématique du risque lié aux plates-formes même si celles-ci jouent un rôle clé dans l'ensemble du système. Il y a lieu d'appréhender le problème de façon plus globale et, pour ce faire, d'appliquer au domaine des paiements les méthodes d'analyse du risque utilisées dans les domaines bancaire et financier. Ces méthodes seront appliquées, dans le cadre du présent article, aux paiements de détail, domaine qui connaît de véritables transformations structurelles et dont la vocation est d'assurer la sécurité et la traçabilité des transactions commerciales.

De manière comparable aux domaines bancaires et financiers, le déclenchement d'un risque systémique peut survenir dans les paiements avec pour origine soit la défaillance d'un acteur important, soit un choc externe qui conduit à une désorganisation brutale du système (FSB *et al.*, 2009). Le cas de la défaillance d'un acteur clé s'applique bien évidemment au domaine des paiements. Mais un choc externe peut également survenir : tel sera le cas si un événement provoque une crise de confiance à l'égard de tel ou tel moyen de paiement ou si un changement brutal des règles du jeu dans le domaine fiscal ou réglementaire provoque une fuite devant certains types de paiement. Les régulateurs ont pris conscience de cette situation, ils en ont souligné le caractère systémique et engagé le processus permettant d'identifier et de gérer le risque qu'elles présentent (FSB, 2015).

Pour mieux appréhender le risque systémique des paiements, il a paru utile d'identifier les transformations intervenues dans les systèmes de paiement (première partie), pour faire ressortir ensuite (deuxième partie) les vulnérabilités de ces systèmes qui rendent possible le déclenchement d'une crise systémique (Pauget, 2012).

1| Les transformations du secteur des paiements

Trois grandes catégories de transformations sont à l'œuvre dans les paiements. Les unes sont directement liées à l'accélération du déploiement des innovations technologiques. Les paiements sont en effet l'un des domaines de l'activité bancaire dans lequel les évolutions technologiques ont le plus d'impact. D'autres transformations viennent de la modification des usages sous l'effet de la révolution digitale. Enfin les changements réglementaires qui impactent les modèles économiques des opérateurs et les conduisent à s'adapter à cette nouvelle donne sont une troisième source de transformation.

1|1 L'accélération du déploiement des innovations technologiques

Ce phénomène peut être appréhendé sous divers aspects : développement des téléphones mobiles et extension de leurs fonctionnalités et de leurs capacités, multiplication des applications en ligne à vocation commerciale. Les conséquences du déploiement de ces innovations sur les systèmes de paiement sont majeures. L'arrivée sur ce marché d'acteurs de taille mondiale, spécialistes des nouvelles technologies, qui, soit s'allient, soit viennent concurrencer les grands réseaux de cartes témoigne du fait que les paiements sont sortis de la sphère bancaire pour être désormais, sur les plans économique et opérationnel, pleinement intégrés au secteur commercial. Conséquence : des stratégies de dimension mondiale et non plus simplement nationale ou européenne se développent même si elles se déploient progressivement pays par pays. Ceci devrait conduire à une intensification de la concurrence. Dans le même temps, l'émergence et la multiplication des fintechs témoignent de la dynamique des marchés du paiement et de leur intérêt pour des entreprises technologiques. Un tel mouvement ne peut qu'être encouragé par les premiers succès enregistrés par ces *start-up*. Comme cela s'est passé dans les autres secteurs économiques, ces jeunes entreprises innovantes seront progressivement rachetées par de plus gros opérateurs qui s'attacheront à donner une nouvelle dimension à ces innovations ou elles deviendront elles-mêmes des acteurs de référence. Ces évolutions sont de nature, d'une part, à conduire à un mouvement de concentration des grands acteurs internationaux sous l'impulsion des fournisseurs de mobiles, des opérateurs du net ou des télécommunications et, d'autre part, à permettre la survivance d'acteurs de niche qui se distinguent des autres opérateurs par leur flexibilité ou leur qualité de service.

Il est une autre transformation qui conduit à changer la structure des systèmes de paiement : les infrastructures y jouent un rôle déterminant et ont un effet modélisant sur l'ensemble du système. La concurrence que se livrent les infrastructures fait, en effet, évoluer les modèles économiques et technologiques des opérateurs. Deux types d'infrastructure sont en concurrence et celle-ci devrait également s'intensifier. Leurs évolutions respectives vont façonner progressivement le paysage des systèmes de paiement. Les systèmes cartes vont continuer à se développer. Ils occupent à ce jour une position centrale dans les économies développées (Pauget, 2016 ; Saidane et Le Noir, 2016). Le paiement sans contact, la possibilité d'utiliser la carte quel que soit le montant de la transaction, l'usage des « *wallet* », celui des cartes virtuelles pour les transactions à risque sont

autant de facteurs qui vont permettre au système carte de se maintenir même si son poids relatif devrait se réduire dans le temps du fait de l'usage de plus en plus répandu du téléphone mobile utilisé comme terminal de paiement. Précisément du fait de cette évolution, les ACH (*automated clearing house*) devraient occuper une place croissante au sein des systèmes (Edgar, Dunn & Company, 2015). Là encore un mouvement de concentration est prévisible. Les volumes traités déterminent directement les prix de revient. C'est un domaine où les économies d'échelle jouent à plein. Un troisième type d'infrastructure pourrait émerger, même si cette hypothèse apparaît peu probable aujourd'hui : on fait ici référence à la technique des « *blockchains* ». Il s'agit d'une infrastructure décentralisée par opposition aux systèmes cartes ou aux ACH qui sont des moyens de centralisation des opérations. Les *blockchains* permettent de certifier l'exécution d'une transaction. Mais cette technologie, même si elle peut paraître prometteuse à certains, souffre de réelles limitations. La première est la limite aux capacités d'exécution de cette technique en temps et en volume. La seconde est l'absence de traçabilité des opérations ou la difficulté d'assurer la transparence. Mais comme toute innovation dans une phase d'émergence, la technique des *blockchains* peut évoluer et les limitations existantes être progressivement levées.

L'accélération du déploiement des innovations technologiques n'est pas le seul facteur de transformation des systèmes de paiement. Avec les technologies nouvelles, les usages se modifient et la demande de services prend des formes différentes.

1|2 La modification des usages sous l'effet de la révolution digitale

Cette modification des usages concerne aussi bien les consommateurs que les commerçants ou les opérateurs des systèmes de paiement. La dématérialisation croissante des paiements induit en effet des changements de comportement et des attentes nouvelles. Ainsi le pouvoir de la marque va en augmentant. Dès lors que le support physique est moins présent, le consommateur a besoin d'une référence qui lui inspire confiance : c'est ce que la marque apporte. Dans le domaine des paiements, les banques disposent d'un avantage certain par rapport aux autres opérateurs. Même si ceux-ci disposent de marques connues, celles-ci ne sont pas le plus souvent un support de référence pour les paiements (Ministère des Finances, 2015). Les consommateurs sont en effet réticents à confier leur argent à des opérateurs disposant d'une faible notoriété dans le domaine bancaire. Le maintien de cet avantage en faveur des banques implique des efforts *marketing* et commerciaux importants et suppose également un très haut niveau de fiabilité dans l'exécution des transactions. L'avantage dont disposent les banques sera d'autant plus valorisé quelles continueront à coopérer avec les réseaux de cartes. Une concurrence trop directe entre ces deux types d'acteurs ne manquerait pas d'avoir un effet destructeur de valeur. Le type de stratégie choisie devrait conduire à une différenciation des systèmes de paiement suivant les pays ou les régions.

Pour les commerçants comme pour les banques, il n'est désormais plus possible de séparer l'acte de vente dans toutes ses composantes de la transaction de paiement. La connaissance du client et des caractéristiques de ses achats que permettent les données contenues dans une transaction est un élément de plus en plus déterminant. La capacité à disposer de ces informations et à les exploiter impacte en effet directement les performances du commerce. La frontière entre opérations bancaires et opérations commerciales est désormais plus floue. De ce fait, les investissements à réaliser dans le domaine du traitement des données revêtent un caractère stratégique. Ces investissements sont coûteux : ils nécessitent de mobiliser des compétences qui deviennent rares. Ils doivent être réalisés dans des délais courts, plus courts que ceux observés dans le cycle des investissements habituels des banques. Celles-ci sont, dans ce domaine, en compétition avec les grands acteurs du net qui sont de taille internationale et disposent de savoir-faire et de moyens importants. Tout retard dans les investissements et donc dans la capacité à fournir de nouveaux services se traduit par des pertes de revenus. La conséquence prévisible d'une telle évolution sur le plan du *marketing* comme du traitement des données est la poursuite du mouvement de concentration au sein de cette industrie. Même si, et cela n'est pas contradictoire, de nouveaux acteurs, les fintechs, apparaissent porteurs d'innovations qui pour certaines d'entre elles peuvent modifier l'économie du secteur.

La troisième grande transformation qui intervient dans le domaine des paiements est liée à l'évolution de la réglementation et à ses conséquences sur les formes et l'intensité de la concurrence.

1|3 Les nouvelles réglementations des paiements et leurs conséquences sur le modèle économique des opérateurs

Les nouvelles réglementations, qu'elles soient d'origine européenne ou nationale, ont pour caractéristique commune de rechercher à intensifier la concurrence pour réduire le coût des échanges et faciliter leur développement tout en garantissant un bon niveau de sécurité. La recherche du meilleur équilibre possible efficacité/sécurité peut être appréhendée différemment suivant les grandes zones économiques ou les pays et conduire à des réglementations ou des pratiques différentes qui ont pour effet de fragmenter les marchés. C'est précisément pour cela que les instances européennes sont intervenues à deux niveaux.

La première intervention a consisté à casser le monopole des banques dans le domaine des paiements. En introduisant la notion d'établissement de paiement, la première directive (DSP 1) a ouvert le marché à des opérateurs nouveaux dont les exigences en fonds propres étaient plus réduites que celles des banques en raison du caractère plus limité de leurs activités. Ces nouveaux acteurs ont abordé le marché avec un regard neuf en utilisant des technologies souvent plus récentes et moins coûteuses. À la différence des banques, ces opérateurs n'ont pas à assumer tout un historique technique et humain souvent lourd et complexe à gérer. Cette nouvelle forme d'établissement a permis aux *start-up* comme aux opérateurs de télécommunications ou du *web* d'entrer sur ce marché. Cette ouverture porte en germe une autre transformation potentiellement importante pour l'évolution du secteur. C'est la séparation entre les activités de paiement et la gestion des dépôts. Le livre blanc de la Commission européenne de 2012 va clairement en ce sens. Il est possible qu'à terme certains acteurs assurent le traitement des paiements tandis que d'autres se spécialiseront dans les services liés à la valorisation des données contenues dans les transactions. Les banques pourront aussi exercer ces mêmes activités mais, à la différence des autres acteurs, elles continueront à gérer des dépôts quelles sont seules à pouvoir garantir.

La deuxième directive (DSP 2) récemment adoptée renforce cette tendance puisqu'elle permet à de nouveaux intervenants, les intermédiaires de paiement, d'entrer sur le marché, de proposer de nouveaux services, d'initier des opérations sur les comptes tenus par les banques ou les établissements de paiement et/ou de fournir des informations consolidées à partir des comptes qu'un client détient dans différents établissements.

L'entrée de nouveaux acteurs qui s'appuient sur des expériences et des savoir-faire différents est de nature à intensifier la concurrence et à en modifier les formes. Nul doute que cette compétition va permettre l'émergence de nouveaux services, les différents acteurs cherchant à se différencier. Cette compétition a et aura aussi pour conséquence de faire baisser les prix des transactions de « base », celles-ci devenant des « *utilities* ».

Le deuxième moyen d'intervention des autorités publiques est une intervention directe ou indirecte sur le prix des services. L'intervention indirecte a concerné le taux d'interchange. En considérant que l'interchange s'apparente à une entente car il conduit dans les faits à instaurer un prix plancher du service, les autorités de la concurrence ont remis en cause ce taux et obtenu une baisse substantielle. La conséquence est certes une perte de revenus pour les banques mais aussi une modification de l'équilibre entre les banques suivant que leurs clients sont majoritairement des consommateurs ou des commerçants. L'intervention directe a été le fait de certains gouvernements qui, comme en France, ont réglementé le prix des services bancaires de base.

Au total, les innovations technologiques, l'évolution du comportement des consommateurs et des commerçants, les changements réglementaires et l'intensification de la concurrence modifient profondément l'économie des paiements. Il en résulte une modification de la cartographie des risques au sein du système. C'est cette cartographie qu'il y a lieu de décrire pour en isoler les risques qui présentent potentiellement un caractère systémique.

2| Une cartographie des risques dans les systèmes de paiement

Une crise systémique peut se déclencher pour deux raisons principales :

• une défaillance d'un acteur majeur du système qualifié alors d'acteur systémique (banque, établissement de paiement, plate-forme d'autorisation ou de compensation). Cette qualification peut être liée à sa taille et plus précisément à son poids dans le système mais aussi à la position qu'il occupe dans le réseau des échanges ou encore à la capacité que l'on peut avoir à lui substituer, immédiatement ou non, un autre opérateur en cas de défaillance ;

• une déstabilisation de l'ensemble du système consécutive à un choc externe. C'est ce qui s'est passé récemment en Grèce. La crainte d'un défaut sur la dette de l'État a fragilisé les banques et le système de paiement a vu son fonctionnement gravement perturbé.

Ces deux origines d'une défaillance du système peuvent être utilisées pour décrire la cartographie des risques d'un système de paiement.

2|1 Les risques liés aux opérateurs

Il y a lieu de distinguer ici le risque de fraude des risques qualifiés de majeurs.

Le risque de fraude est analysé, suivi, et fait l'objet d'actions correctrices dans tous les systèmes. La fraude a, en effet, un double impact. Elle conduit à des pertes pour les opérateurs, mais également, et peut-être surtout, elle peut altérer la confiance que les acteurs ont dans le système si elle est trop importante en volume et/ou trop répandue.

La fraude augmente de façon régulière et un peu plus rapidement que l'activité. En France, la fraude totale sur les cartes de paiement qui était de l'ordre de 150 millions d'euros au début des années deux mille serait d'environ 400 millions à la fin de l'année 2015. Dans ce total, la fraude réalisée à l'étranger représente environ 50 %. La nature de l'activité a aussi beaucoup évolué. Le poids de la vente à distance est trois fois plus important qu'il y a dix ans et le taux de fraude est vingt fois plus élevé que celui du paiement de proximité Europay MasterCard Visa (EMV) [1]. Cette fraude peut être contenue à la fois en développant le protocole et la technologie EMV et en intensifiant la coopération entre acteurs (commerçants, émetteurs, réseaux). À titre d'illustration, l'étude de faisabilité du projet Monet de cartes européennes avait montré que l'intégration sous égide européenne des fraudes identifiées par les réseaux Visa et MasterCard permettait une économie de plusieurs centaines de millions.

Au-delà de cette approche globale, il y a lieu de distinguer les moyens de lutte contre la fraude suivant que celle-ci est initiée par les porteurs ou les commerçants. La fraude émanant des porteurs est bien tracée par les grands réseaux. Au niveau de la vente à distance, secteur sensible, la lutte contre la fraude suppose une coopération étroite entre la banque ou l'établissement de paiement et le e-commerçant pour analyser les données et localiser ainsi le plus rapidement possible l'origine des fraudes. La fraude émanant des commerçants représente pour les acquéreurs le premier risque de fraude en importance [2]. Elle est plus complexe à analyser. Elle suppose en effet une bonne connaissance des commerçants, de leur modèle d'activité et notamment de leurs revenus, de la cinématique des paiements, du contenu de leurs sites marchands, des produits et services vendus. Cela suppose une mise à jour constante de leur profil d'activité.

Si la fraude est toujours coûteuse et potentiellement déstabilisante, il est peu probable (compte tenu des systèmes existants) qu'elle soit à elle seule à l'origine d'un épisode systémique. Elle relève plutôt de la catégorie « vulnérabilité d'un système », c'est-à-dire les fragilités d'un système qui, si elles ne sont pas à elles seules, à l'origine d'une crise systémique peuvent cependant contribuer à son développement.

Il en va différemment des risques dits « majeurs » qui peuvent déstabiliser un système de paiement voire interrompre au moins temporairement, son fonctionnement. Ces risques ont une probabilité

1 *Sources GIE Cartes bancaires.*
2 *Source Dalenys.*

de survenance faible et un impact fort. Ce sont des risques limites (*tail risks*). Pour les prévenir et les gérer, les acteurs concernés s'attachent à réduire leur probabilité de survenance en définissant des règles strictes de fonctionnement, en surveillant leur application par des audits réguliers et un suivi des actions correctrices préconisées. Dans l'hypothèse où le risque se matérialiserait, des procédures d'alerte, des mises en place de cellules de crise sont prévues et régulièrement testées soit à l'échelle des établissements, soit à un niveau plus large à l'initiative des superviseurs. Pour chaque grand risque, des plans de prévention et de secours sont ainsi définis.

Quelques cas de risque majeur méritent un examen plus détaillé.

Il s'agit, en premier lieu de la défaillance d'une plate-forme d'autorisation ou de compensation. À ce jour, ces plates-formes sont le plus souvent interbancaires. Les établissements, qu'ils soient actionnaires ou utilisateurs, doivent apporter des fonds propres ou des garanties qui sécurisent la plate-forme et lui permettent de faire face à des incidents, même s'ils sont importants. Ces plates-formes présentent d'évidence un caractère systémique et il appartient aux superviseurs de s'assurer de la qualité de leur gestion et de l'adéquation de leurs fonds propres. De ce point de vue, la procédure n'a pas vocation à être sensiblement différente de celle appliquée aux banques systémiques même si le risque est essentiellement un risque opérationnel.

Une autre source de risque majeur tient à la défaillance simultanée ou rapprochée de plusieurs établissements. La mesure du risque systémique dans le domaine bancaire a montré que la défaillance de seulement 3 % des établissements peut provoquer une crise (BCE, 2015). Ceci est d'autant plus probable que le nombre d'établissements est important. La prévention de ce type de risques repose pour une large part sur les procédures d'agrément des opérateurs. L'expérience des dirigeants comme des équipes opérationnelles, l'adéquation des moyens mis en œuvre par rapport aux volumes et à la complexité des opérations traitées, le montant comme la qualité des fonds propres destinés à couvrir des risques sont autant d'éléments à prendre en compte. Un niveau d'exigence élevé contribue de façon déterminante à la sécurité et à la stabilité du système. La difficulté tient au fait que cet agrément n'est pas délivré avec le même niveau d'exigence dans l'espace européen. Les distorsions qui en résultent sont sources de fragilité à l'intérieur du système. L'existence de maillons faibles dans un système aussi interdépendant que les paiements est un facteur de risque potentiel important. Il pourrait se trouver aggravé si, à la faveur de la mise en œuvre de DSP 2, les intermédiaires en paiement bénéficiaient de contraintes moindres que les autres acteurs notamment dans le domaine très sensibles de la protection des données. Les exigences à leur imposer devraient être proches de celles des établissements de paiement pour éviter que de nouvelles distorsions et donc de nouvelles fragilités apparaissent. En outre, la mise en œuvre de ces dispositions devrait être mieux coordonnée à l'échelle européenne qu'elle ne l'a été jusqu'ici. L'harmonisation devrait aussi concerner le suivi de ces différents établissements.

La captation ou l'altération des données peuvent aussi constituer un risque majeur. L'utilisation frauduleuse des données est de nature à altérer gravement la confiance des consommateurs, des commerçants, des établissements traitant les opérations et donc à permettre le déclenchement d'une crise systémique. La sécurité des données est un enjeu d'autant plus important que celles-ci croissent en volume et sont traitées par un plus grand nombre d'intervenants.

Une deuxième origine possible d'une crise systémique tient aux vulnérabilités qui existent dans tout système et qui autorisent le déclenchement d'une crise. Ces vulnérabilités ne sont pas en elles-mêmes des facteurs déclenchants mais leur addition rend le système plus instable. On peut alors basculer dans la crise à la faveur d'un événement qui, dans un autre environnement, n'aurait pas eu un impact aussi important. C'est pourquoi la prise en compte et la réduction de ces vulnérabilités s'intègrent dans l'analyse et la gestion du risque systémique.

2|2 Les vulnérabilités des systèmes de paiement

Deux grandes catégories de vulnérabilités peuvent être distinguées : les vulnérabilités liées aux technologies nouvelles et celles qui ressortent d'une modification rapide du modèle économique du système. Elles résultent de la transformation des systèmes de paiement.

Les vulnérabilités associées aux technologies nouvelles sont multiples et évolutives.

Il y a, en premier lieu, le fait que ces technologies se diffusent de plus en plus rapidement (Edgar, Dunn & Company, 2014). La conséquence de ce phénomène est que tous les acteurs du système, aussi bien les opérateurs que les superviseurs, doivent s'adapter dans des délais très courts. Mais tous ne le font pas ou tout au moins ne le font pas au même rythme. Il en résulte des distorsions au sein du système et donc l'apparition de maillons faibles. L'un des domaines les plus sensibles est celui de la mise à jour des protocoles de sécurité avec les moyens requis.

Un deuxième risque associé à l'évolution des technologies est le développement du temps réel « absolu » dans le traitement des opérations. Cette tendance est de nature à favoriser le développement des ACH au détriment des réseaux de cartes. Dans un tel environnement, l'autorisation préalable à toute transaction n'est plus indispensable et la notion de garantie de paiement associée à la carte perd de son sens. La transaction est en effet dénouée instantanément. Ceci peut fragiliser le « système carte », faciliter le développement du « *direct debit* » initié, par exemple, depuis un téléphone mobile.

Un troisième risque tient à la multiplication des données associées aux paiements, de leur traitement ou de leur agrégation par de nombreux acteurs. Ce risque est en effet de nature à changer de dimension. Les données contenues dans les transactions ou qui leur sont associées seront à l'origine de nouveaux services pour mieux informer le consommateur mais aussi pour le solliciter plus efficacement. Ces données seront donc plus nombreuses mais aussi plus complexes à traiter. Mais surtout elles seront conservées ou véhiculées par un plus grand nombre d'acteurs dont le niveau de maîtrise sera, notamment en termes de sécurité, par nature différent. Le risque de compromission des données devrait s'en trouver aggravé.

Un quatrième risque tient à l'émergence des monnaies virtuelles. Certes celles-ci, à commencer par la plus importante, le bitcoin, occupent une position encore très marginale. De plus, leur développement se trouve contraint par leur capacité et leur vitesse de traitement des opérations. Il n'en demeure pas moins que ces transactions sont, pour une large part, hors du champ de la régulation et de la supervision. Ce n'est en effet que lorsque ces monnaies sont converties en monnaie légale que les superviseurs ont à en connaître (ACPR, 2014). Ceci mérite d'autant plus d'attention que si la traçabilité des transactions au sein du système de monnaie virtuelle est assurée, c'est sous forme anonyme. Cette opacité explique que le bitcoin ait été utilisé comme un moyen de contournement de la réglementation sur les exportations de capitaux en Chine ou en Russie.

Aux vulnérabilités liées aux évolutions technologiques, viennent s'ajouter celles qui tiennent à la transformation du modèle économique des paiements que celle-ci ait pour origine l'arrivée de nouveaux entrants, l'évolution de la structure du marché et de la concurrence ou des réglementations nouvelles.

Les paiements sont restés pendant très longtemps un système fermé avec les banques pour seuls opérateurs. Cette activité, vécue comme le prolongement de la gestion des dépôts, n'a pas été considérée le plus souvent comme un centre de profits. Dans de nombreux systèmes bancaires européens et particulièrement en France, des mécanismes de subventions croisées ont été développés. Les pertes résultant de la gestion de la monnaie fiduciaire et des chèques étaient partiellement compensées par les résultats des activités de virement-prélèvement et d'émission et de gestion des cartes, le solde négatif venant s'imputer sur les revenus tirés des dépôts non rémunérés (Pauget et Constans, 2012).

L'arrivée de nouveaux entrants remet en cause ce modèle intégré et les subventions croisées qui lui sont associées. Il en résulte une baisse des prix, encouragée ou provoquée par les autorités publiques. De plus, pour les acteurs du commerce et notamment du e-commerce, le paiement est un accessoire de la vente. Les revenus des paiements sont sans rapport avec ceux tirés des ventes, il leur est donc possible d'accepter une faible rémunération des services de paiement. Ces baisses de prix conduisent de nombreux opérateurs à modifier l'organisation de la production des services de paiement pour rester compétitifs. Certains acteurs se spécialisent sur tel ou tel segment de la chaîne de valeur et améliorent ainsi leur efficacité. Ils deviennent les sous-traitants d'autres opérateurs qui fonctionnent alors comme des ensembliers. Un mouvement de concentration-spécialisation analogue à celui observé

dans d'autres industries se développe alors. Il en résulte une plus grande complexité du système et une plus grande interdépendance entre les acteurs. C'est potentiellement un facteur aggravant de la fragilité du système et plus précisément de sa capacité de résistance à un choc.

Les vulnérabilités associées à cette transformation du modèle peuvent se trouver augmentées par les réglementations.

Les paiements s'apparentent à une industrie lourde ; ils requièrent des investissements importants et réguliers et des compétences très spécifiques, sur des durées d'amortissement longues. Les opérateurs peuvent d'autant plus améliorer leurs performances que leur environnement réglementaire est stable. Ceci est particulièrement vrai pour les dispositions qui concernent le prix des services.

Un autre facteur d'instabilité potentielle consisterait à favoriser la séparation entre la gestion des flux et celle des dépôts, ce qui impacte les banques au premier chef. Or les exigences prudentielles appliquées aux banques ont considérablement renforcé la capacité de résistance des établissements à une situation de crise. Elles sont donc un îlot de stabilité au sein du système des paiements. Cette position particulière mérite d'être préservée à un moment où toute l'économie du système se trouve modifiée.

Enfin, les dispositions réglementaires conçues à l'échelle de l'Europe et transposées pays par pays peuvent être à l'origine d'un renforcement de la fragmentation des marchés. Force est de constater que malgré le SEPA et la directive sur les paiements, le marché européen des paiements restera très fragmenté. On peut observer qu'il n'existe pas réellement d'opérateur d'envergure européenne. Les deux seuls acteurs que l'on pourrait qualifier ainsi sont Visa et MasterCard. Mais ces deux groupes américains ne couvrent pas l'ensemble des services de paiement. Cette fragmentation ne pourra être réduite que par un double mouvement : des exigences communes en matière d'information des consommateurs et des procédures d'agrément et de contrôle des opérateurs harmonisées et coordonnées.

L'émergence d'une industrie européenne des paiements apparaît utile pour la stabilité et la sécurité du système. Cela suppose une modification de la doctrine de la direction de la concurrence de la Commission européenne dont le caractère inadapté est manifeste.

3| Conclusion

Le système des paiements de détail connaît aujourd'hui des transformations profondes. L'entrée de nouveaux acteurs inégalement régulés et contrôlés, une rentabilité plus incertaine, le déploiement rapide de technologies nouvelles augmentent sa vulnérabilité. Des maillons faibles apparaissent. Le risque systémique s'en trouve augmenté. Pour maîtriser une telle évolution, le dispositif de surveillance doit s'étendre en pratique à tous les opérateurs et s'effectuer sur une base étroitement coordonnée au niveau européen.

Bibliographie

ACPR (2014)
« Position de l'ACPR », P-01 du 29 janvier.

Banque centrale européenne (BCE) (2015)
« *Systemic risk, contagion, and financial network* », *Financial Stability Review*, novembre.

Conseil de Stabilité financière (2015)
Reports describe progress in implementing OTC derivatives market reforms, and highlight where further work is needed, communiqué de presse, 4 novembre.

Conseil de Stabilité financière, Fonds monétaire international et Banque des règlements internationaux (2009)
« *Guidance to access the systemic importance of financial institutions, markets and instruments* », « *Initial considerations* », « Rapport aux ministres des Finances et aux gouverneurs de banques centrales du G20 », octobre.

Edgar, Dunn & Company – Pôle finance innovation (2014)
« La filière des paiements, le fleuron caché de l'industrie française », avril.

Edgar, Dunn & Company (2015)
« *Paiements innovation trends and implications for the schemes* », Peter Sidenius, Mobey Forum, Varsovie, 9 décembre.

Ministère des Finances et des Comptes publics (2015)
« Assises des Paiements », juin.

Pauget (G.) (2012)
« Banques : le grand saut ? », *Éditions de la Revue Banque*, juin.

Pauget (G.) (2016)
« Europe-Afrique : les facteurs clés de succès des systèmes de paiement », Analyses et perspectives, in D. Saidane et A. Le Noir « Banque et finance en Afrique », *Éditions de la Revue Banque*, janvier.

Pauget (G.) et Constans (E.) (2012)
« L'avenir des moyens de paiement en France », Rapport au ministre de l'Économie, des Finances et de l'Industrie, mai.

Institutions financières et cybercriminalité
Entre vulnérabilité et sécurité

Quentin GAUMER, Stéphane MORTIER et Ali MOUTAIB
Club cybersécurité – École de guerre économique – Paris

Dans le monde actuel, les institutions financières, comme les entreprises, sont de plus en plus tributaires de leurs systèmes d'information, qui leur permettent à la fois de réaliser des opérations (virements, gestion de comptes, retraits, etc.) et de surveiller l'information échangée.

*L'information est de plus en plus la cible de cyber-attaques lancées par différents types de cybercriminels, qui recourent à des stratégies d'ingénierie sociale (renseignement humain, manipulation, notamment) ou à des techniques plus sophistiquées (comme l'*Advanced Persistent Threat *dans le cas de Carbanak). L'année 2015 fut essentielle pour les acteurs de la cybersécurité. Les cyber-attaques se sont révélées très instructives pour le secteur bancaire, lequel a ajusté sa tactique de défense et renforcé sa résilience.*

Les entreprises de sécurité déploient des efforts et les RSSI (responsables de la sécurité des systèmes d'information) améliorent leurs stratégies, mais les cybercriminels ne cessent de changer leurs méthodes. Les acteurs de la sécurité doivent affiner leur connaissance des techniques de cybercriminalité et améliorer la surveillance afin de répondre aux nouvelles menaces qui ciblent les entreprises, notamment les banques.

Comme nous l'avons observé l'an dernier, les hackers *ciblent désormais davantage les institutions financières que les utilisateurs finals. On recense de nombreux exemples d'attaques visant des systèmes pour points de vente et des distributeurs bancaires, dont les conséquences financières ne sont pas négligeables pour les banques. Cette tendance devrait se poursuivre dans les années qui viennent, car les* hackers *rechercheront des failles pour s'introduire sur les marchés boursiers et dans les systèmes de paiement.*

En outre, étant donné l'utilisation croissante des technologies mobiles intelligentes, les cybercriminels s'intéressent aux smartphones. Les nouvelles solutions de paiement, comme Apple Pay ou Google Pay, incitent les hackers *à monétiser des cartes de crédit volées ou falsifiées. Par ailleurs, les programmes malveillants* (malware) *transactionnels vont se multiplier sur les appareils mobiles.*

L'amélioration de la résilience constitue un aspect majeur de la stabilité financière. Elle a pour objectif d'éviter que des cyber-attaques ou des défaillances informatiques ne provoquent une crise systémique. Cependant, même les meilleures protections possibles ne réduiront jamais à néant le risque, pour les institutions financières, d'être la cible d'une cyber-attaque. Les institutions financières doivent également mettre en place les meilleures solutions permettant une reprise rapide et efficace de leurs activités après une atteinte à leurs systèmes informatiques.

Les États, les institutions, les entreprises et le grand public sont confrontés à des menaces nouvelles liées à la forte augmentation du volume, de l'importance et du champ des activités numériques :

• infractions aux traités internationaux ou à la législation nationale perpétrées dans le cyberespace ou par un système informatique (cybercriminalité) ;

• intrusion sans autorisation dans des organismes publics, des entreprises ou des fichiers personnels pouvant donner accès à des informations confidentielles. Le but est de collecter des données personnelles, économiques ou financières (cyber-espionnage) ;

• acte de terrorisme utilisant les systèmes ou les technologies informatiques comme arme ou comme cible. Le cyber-terrorisme peut avoir des motivations politiques, sociales ou religieuses. L'objectif est de susciter la peur, de provoquer une panique ou de déstabiliser une population, une institution, une entreprise, une armée, etc. ;

• risque de guerre de l'information ou de guerre informatique en lien ou non avec un conflit armé réel. Ceci caractérise un cyber-conflit avec cyber-attaque et, partant, nécessite l'instauration d'une cyber-défense.

Cyber-risque et cybercriminalité sont les termes consacrés lorsqu'on aborde ces sujets. Tous types d'activités numériques peuvent être concernés. La cybercriminalité est l'un des principaux problèmes qui se pose aux institutions financières et aux banques en particulier, mais aussi à n'importe quelle grande organisation. La direction générale et les RSSI doivent s'assurer en permanence que l'information et les données internes sont protégées et que les besoins de l'entreprise sont pleinement satisfaits.

La protection des actifs bancaires nécessite des mesures de prévention et d'anticipation, au moyen de processus qui évaluent et réagissent aux différents risques et menaces. Le secteur financier est aujourd'hui confronté à divers défis, essentiellement liés à la combinaison de menaces classiques (*carding*, *phishing*, etc.) et de menaces ciblées (APT [1], fuite de données, etc.). Les cybercriminels ciblent non plus les utilisateurs finals mais les institutions financières. Ils cherchent à voler des données précieuses ou à pirater directement les systèmes pour points de vente et les distributeurs automatiques. La campagne d'hameçonnage ciblé *(phishing)* Carbanak est l'une des plus importantes cyber-attaques jamais découverte à ce jour. Repérée par Kaspersky Lab, elle ciblait des organisations financières permettant à ses initiateurs de dérober plusieurs centaines de millions de dollars.

Par ailleurs, de plus en plus, les cybercriminels ciblent directement les places boursières en recourant à des stratégies plus subtiles. Ils visent par exemple les opérations de *trading* haute fréquence (ciblage d'algorithmes) afin de capter des gains stables et de long terme tout en réduisant la probabilité d'être appréhendés.

1| Du cyberespace à la cybersécurité

Mais tout d'abord, d'où vient le mot *« cyber »* ? En grec, *kubernan* signifie guider et gouverner. Le cyberespace est un territoire dépourvu de frontières et même si ce n'est pas totalement vrai, il semble n'être soumis à aucun contrôle ni à aucune règle. Le terme « cyberespace » a été inventé en 1984 par le romancier William Gibson, l'un des leaders du mouvement cyberpunk [2], dans son roman *Neuromancier*. Le cyberespace y est un lieu utopique et abstrait, où l'information circule librement. Parfois, la ligne de démarcation entre réalité et fiction se brouille. Dans la vraie vie, le cyberespace est le lieu de stockage et d'échange de flux dématérialisés (Chawki, 2006). Cet espace est l'objet de la *Déclaration d'indépendance du cyberespace* rédigée en février 1996 par John Perry Barlow, fondateur de l'*Electronic Frontier Foundation* : « *Gouvernements du monde industriel, vous géants fatigués de chair et d'acier, je viens du Cyberespace, le nouveau domicile de l'esprit. Au nom du futur, je vous demande à vous du passé de nous laisser tranquilles. Vous n'êtes pas les bienvenus parmi nous. Vous n'avez pas de souveraineté où nous nous rassemblons.* »

1 *APT :* Advanced Persistent Threat. *Il s'agit d'une attaque dans laquelle une personne non habilitée accède à un réseau. Sa présence demeure cachée et non détectée pendant une longue période durant laquelle elle pilote le réseau et/ou vole des données.*
2 *Cyberpunk est un genre de la science-fiction qui met en scène un futur proche dans un monde technologiquement très avancé.*

En ce sens, le cyberespace est une sorte d'utopie, dépourvu de gouvernement et de contrôles. Mais la cybercriminalité se développe dans le cyberespace, que divers criminels utilisent pour parvenir à leurs fins, et même s'il n'est pas totalement dépourvu de règles, il est extrêmement difficile de le contrôler, de traquer les criminels et de les sanctionner. L'échelon national (l'État) n'est pas toujours le mieux à même de comprendre et de traiter les problèmes liés au cyberespace.

Au cours de la dernière décennie, beaucoup de progrès ont été réalisés et nombre d'instruments internationaux ou régionaux de lutte contre la cybercriminalité ont été définis. Ces instruments sont plus ou moins contraignants, mais ils témoignent d'une sensibilisation croissante à ce fléau.

Tous ces instruments s'inspirent essentiellement de la *Convention sur la cybercriminalité* (2001). Élaborée par le Conseil de l'Europe, cette Convention est le premier traité international sur les délits commis *via* Internet et d'autres réseaux informatiques. Elle s'intéresse surtout aux infractions liées aux atteintes à la propriété intellectuelle, à la fraude informatique, à la pédopornographie et aux failles de sécurité des réseaux (ONUDC, 2013).

La plupart des politiques nationales relatives à la cybersécurité sont postérieures à la Convention. En France, la cybercriminalité est définie en ces termes : *« Actes contrevenant aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime, ou les ayant pour cible »* (Agence nationale de la sécurité des systèmes d'information – ANSSI).

Parce qu'il y a des cybercriminels, nous devons trouver des moyens de faire appliquer les règles et de fournir une protection, d'où la cybersécurité. La cybercriminalité et la cybersécurité couvrent un vaste éventail de domaines. Dans son étude, Sieber (1998) propose la typologie suivante : protection de la vie privée, droit pénal des affaires, protection de la propriété intellectuelle, lutte contre les contenus illégaux et dangereux, droit pénal procédural, droit de la sécurité.

Même si l'objectif de Sieber est de présenter une base de données des législations nationales, les quatre premiers domaines correspondent à une typologie des actes cybercriminels : actes ciblant les données personnelles, infractions informatiques à visée économique, actes ciblant les droits de propriété intellectuelle, contenu dangereux et illégal.

D'autres spécialistes, comme le professeur David L. Carter (1992) de l'Université d'État du Michigan, scindent la cybercriminalité en deux catégories :

- les actes ciblant un système informatique ;

- les actes qui se servent d'un système informatique pour commettre un délit. Le système informatique est simplement un outil pour commettre une infraction classique.

Quel que soit le type de délit, les institutions financières, comme n'importe quelle autre grande entreprise, sont vulnérables. Non seulement les institutions en elles-mêmes, mais aussi les transactions financières, les informations qu'elles stockent, les données personnelles de leurs salariés et de leurs clients, les employés manipulés qui communiquent des informations, les virements, les distributeurs automatiques, etc.

2| Panorama de la cybercriminalité dans les institutions financières

2|1 Où en sommes-nous aujourd'hui ?

De nombreuses mesures ont été prises pour assurer la sécurité des systèmes des institutions financières. Les instances de réglementation s'efforcent de mettre en place des normes de sécurité et de faire respecter les processus de sécurité internes.

Pour ces instances, la gestion du risque de cybersécurité doit passer par différentes mesures : audits, contrôles réguliers et évaluation périodique du suivi de la cybersécurité.

Le secteur financier doit lui aussi élaborer différentes mesures pour éviter d'être la cible de piratage :

- gestion des identités et des accès : prévention et contrôle de toute tentative d'accès d'une entité non habilitée au système et à ses données (accès distant, identifiants et mots de passe, protocoles des *help desks* et accès direct) ;

• prévention de la fuite de données (gestion et protection des documents sensibles et stockage dans le système) ;

• campagnes de sensibilisation et formation : des programmes de formation visant à sensibiliser les salariés à l'application des processus de sécurité internes ;

• planification des réponses aux incidents : définition de la réponse à un incident de manière à gérer correctement la réaction à une attaque majeure du système (planification, formation d'une équipe d'intervention et plans de gestion de crise) ;

• gouvernance de la sécurité : définition d'un plan de gestion clair, permettant une communication fluide entre le RSSI, le service chargé de la sécurité et la direction générale.

2|2 Quelles sont les tendances actuelles ?

Malgré les procédures de sécurité strictes qui ont été définies, les institutions financières sont conscientes qu'une protection totale est impossible et que les capacités technologiques des cybercriminels évoluent constamment, et qu'il faudra faire face, dans les années qui viennent, à différentes menaces qui auront une incidence sur leur activité. L'une des plus importantes est liée à la généralisation de la mobilité, ce qui conduira certainement à l'apparition de programmes malveillants *(malwares)* financiers ciblant les utilisateurs de smartphones.

En outre, dans les institutions financières, la plus grande menace viendra de l'intérieur : le danger réside dans la divulgation intentionnelle d'informations sensibles et stratégiques à la concurrence ou à une organisation cybercriminelle.

Les programmes malveillants mobiles

La croissance rapide du nombre d'utilisateurs de smartphones et de tablettes incite les escrocs et les cybercriminels à cibler les applis financières et à élaborer de nouvelles solutions pour monétiser leurs opérations frauduleuses. Le taux d'infection ne cessant d'augmenter, il convient de renforcer les mesures de sécurité relatives aux appareils mobiles, en particulier dans le secteur financier.

Quels sont les principaux programmes malveillants mobiles ? Les programmes malveillants transactionnels restent la principale menace pour les appareils mobiles : environ 30 % des programmes malveillants ont pour but de dérober des informations financières [3]. Ils peuvent effectuer de nombreuses opérations sur les smartphones et autres appareils mobiles : vol de données personnelles, lecture et envoi de SMS, introduction de logiciels espions et vol d'informations sensibles.

Comment ces programmes fonctionnent-ils concrètement ? Un utilisateur travaillant dans une institution financière reçoit un courrier électronique d'hameçonnage et télécharge un « cheval de Troie ». Une fois activé, ce programme récupère les autorisations de l'administrateur du système. Le *hacker* peut alors commettre tous les actes malveillants qu'il veut (modification de mots de passe, chiffrement du stockage, etc.). Il peut en effet accéder à des documents sensibles, à des informations financières ou à des données à caractère personnel et les revendre sur le marché noir.

Sur ce marché souterrain, la demande de piratage d'appareils mobiles ne cesse d'augmenter. Les *hackers* s'intéressent aux mobiles pour lancer des campagnes d'infection en introduisant des chevaux de Troie.

L'infection mobile constitue donc une menace majeure pour l'utilisateur final, mais aussi pour les institutions financières. De nombreux processus sont déployés pour assurer la sécurité des appareils mobiles dans ces entreprises. Néanmoins, le risque d'erreur humaine ne peut être évité : même si un système de gestion des données de référence (*Master Data Management* – MDM) peut contrôler l'équipement mobile de l'entreprise, de nombreux utilisateurs libèrent *(jailbreak)* ou débrident *(root)* leurs appareils pour accéder à des « *app stores* » non officiels ou pour obtenir des applications gratuites. Ce faisant, ils ouvrent la porte aux *hackers* et aux escrocs.

3 *IBM (2015).*

Fuite de données et ingénierie sociale

La diffusion de l'information constitue un enjeu crucial pour les entreprises, et en particulier pour les institutions financières. Ceux-ci ont mis en place des mesures de protection contre les menaces externes, mais des études récentes[4] montrent que les menaces internes sur la sécurité restent par ailleurs considérables. Or, étant donné le nombre croissant de dispositifs et de systèmes, leur complexité et l'évolution des utilisations, il devient plus difficile de déceler ces menaces.

L'obtention d'un avantage financier et l'espionnage industriel demeurent les deux principaux objectifs des attaques internes.

L'entreprise devrait pouvoir détecter parmi son personnel toute intention de nuire, et organiser des sessions de formation pour éviter qu'un employé ne commette une erreur involontaire. Les méthodes et le mode opératoire diffèrent d'un escroc à l'autre et ils sont susceptibles d'avoir de graves répercussions sur l'activité d'une entreprise. En voici quelques exemples :

- ingénierie sociale : différentes techniques (*phishing*, programmes malveillants, *phoning*, etc.) permettent de manipuler un employé dans une entreprise ciblée, dans le but de récupérer des données sensibles ;

- fuite de données : moyennant une forte somme, un employé d'une entreprise livre des informations sensibles.

3| Le principal risque est lié aux comportements humains

3|1 Ingénierie sociale : évolution du *modus operandi*

Au fil du temps, les cybercriminels améliorent leur *modus operandi*, leur capacité d'attaque, et leurs objectifs évoluent eux aussi. Les premiers *hackers* étaient motivés par leur égo, par le défi à relever et par la volonté de prouver leurs talents informatiques. Aujourd'hui, les motivations sont différentes. Les cybercriminels sont des groupes organisés, à l'instar de la mafia, ou, parfois, ce qui est le plus surprenant, ils se présentent comme des sociétés de services informatiques. Il est en effet possible de recourir aux services d'un ou de plusieurs *hackers* pour attaquer une ou plusieurs cibles. Organisés comme une véritable entreprise, ils peuvent même proposer un service après-vente d'un nouveau genre !

Les *hackers* mettent à profit leurs compétences techniques, mais qui ne sont pas uniquement liées à l'informatique. Ils exploitent également les fragilités humaines pour lancer des cyber-attaques (comme le *phishing*, par exemple). Ils ont développé l'ingénierie sociale pour parvenir à leurs fins. Les *hackers* n'hésitent donc pas à contacter leur cible (un individu) par courrier électronique, par téléphone ou en face à face, afin d'établir une relation de confiance et de manipuler le comportement de leur victime.

La lutte contre les attaques d'ingénierie sociale concernent deux grands aspects de l'environnement des institutions financières, et en particulier des banques. En effet, à l'instar des autres institutions financières, les banques peuvent être la cible première d'une attaque ; mais elles peuvent aussi être une cible secondaire, *via* leurs clients, surtout sur le segment de la banque de détail et des services bancaires aux entreprises. Le meilleur moyen de réduire ces risques d'attaque consiste à sensibiliser et à former l'ensemble de l'entreprise (le président, les administrateurs, l'encadrement, les secrétaires, les comptables, les réceptionnistes, etc.). Comme toutes les autres entreprises, les institutions financières ont besoin de mettre en place des programmes de sensibilisation simples :

- face au *phishing* : ne pas faire confiance aux e-mails, se montrer aussi vigilant que possible, vérifier les adresses et repérer les fautes d'orthographe, faire attention en cas d'extension *mail.com* ou *gmx (global message eXchange)*, etc.

- face au *phoning* : s'assurer de l'identité de l'appelant, ne pas communiquer d'informations sensibles (identifiant, mot de passe, numéro de téléphone personnel, informations personnelles, etc.), mettre en place un système de rappel, etc.

4 *Vormetric (2015).*

Depuis quelques années, des entreprises, notamment en France, sont touchées par une forme d'attaque appelée « escroquerie aux faux ordres de virement international (FOVI) ». Le *modus operandi* consiste en un *phishing* classique, destiné à obtenir les identifiants et les mots de passe qu'une entreprise utilise pour se connecter au site Web de sa banque. Après avoir obtenu ces données, les *hackers* peuvent effectuer des virements pour créditer leur propre compte bancaire. Le mode opératoire devient de plus en plus complexe : en général, les cybercriminels (qui sont des spécialistes du renseignement humain) entrent en contact téléphonique avec un comptable en se faisant passer pour le dirigeant de l'entreprise. Le *hacker* demande à ce comptable d'effectuer un virement destiné à une opération de fusion/acquisition confidentielle avec une société étrangère. Souvent, un faux juriste (lui aussi spécialiste du renseignement humain) passe un second appel téléphonique pour donner des détails sur l'opération. Le comptable qui a été manipulé procède au virement. Cette escroquerie exploite les fragilités humaines et non les failles de la sécurité d'un système informatique ou d'un réseau. Elle pose un très grave problème juridique à propos de la responsabilité de la banque dans l'autorisation du virement en question. En France, il peut arriver que la banque soit juridiquement responsable car elle est tenue de vérifier toutes les signatures qui apparaissent sur l'ordre de virement et d'avertir son client en cas de doute relatif à un document ou à une transaction (jurisprudence de la Cour de cassation).

Pour éviter tout problème, les institutions financières doivent mettre en place des programmes de sensibilisation à l'intention de leurs clients [5]. Ces programmes ne sont toutefois pas suffisants, et des mesures de sécurité supplémentaires sont donc nécessaires. Par exemple, de nombreuses banques n'envoient pas de courriers électroniques à leurs clients et préfèrent utiliser leur messagerie interne. Pour contrer l'ingénierie sociale, les solutions sont non seulement humaines, mais également techniques.

3|2 L'ingénierie sociale, première étape avant le lancement d'une attaque destinée à craquer un système informatique

Comme indiqué plus haut, l'ingénierie sociale est l'une des premières étapes possibles avant le lancement d'une cyber-attaque plus complexe, telle qu'une attaque APT. Ces attaques ciblées emploient toutes les techniques disponibles pour craquer un système informatique. L'ingénierie sociale qui repose sur le renseignement humain permet d'obtenir des informations techniques et technologiques sur la cible et son environnement. C'est ce mode opératoire que Carbanak a privilégié.

L'attaque Carbanak constitue un cas d'école. Nombre de spécialistes de la cybersécurité analysent les failles potentielles de plusieurs banques et autres institutions financières à travers le monde. À la fin de 2013, ces institutions ont été la cible d'une importante organisation cybercriminelle, qui n'a toujours pas été identifiée. Le préjudice financier pourrait atteindre un milliard de dollars. Kaspersky, l'un des leaders de la sécurité des systèmes informatiques, a publié un rapport détaillé sur cette affaire [6] après avoir participé à la détection de l'attaque et aidé ses clients à nettoyer leur système informatique. Selon ce rapport, une centaine de banques ont été visées, et environ la moitié d'entre elles ont subi des pertes financières. La plupart des victimes (des institutions financières) étaient situées en Russie, aux États-Unis, en Allemagne, en Chine et en Ukraine. Pour infiltrer ces banques et opérer un nouveau type de cambriolage, les *hackers* ont utilisé la technique du *spear phishing*. Premièrement, les administrateurs du système informatique ont été ciblés en personne : ils ont reçu un courrier électronique contenant un programme malveillant en pièce jointe. Deuxièmement, ce programme malveillant s'est exécuté sur des ordinateurs sensibles (ceux des administrateurs du système). Troisièmement, les *hackers* ont espionné les systèmes

5 *Exemples :* http://www.dailymotion.com/fbffrance
https://static.societegenerale.fr/ent/ENT/Repertoire_par_type_de_contenus/Types_de_contenus/01-Pages/00-perennes/espace_securite/commun_pdf/ingenierie-sociale.pdf
Différentes administrations publiques (les services de renseignement, la police, la gendarmerie, etc.) sensibilisent les entreprises.

6 http://www.kaspersky.com/about/news/virus/2015/Carbanak-cybergang-steals-1-bn-USD-from-100-financial-institutions-worldwide

informatiques de la banque pendant un certain temps (durant plusieurs mois, ils sont restés dormants à l'intérieur de ces systèmes), pour repérer les mesures de sécurité en place, et donc les vulnérabilités, les failles de la sécurité. Ils ont ainsi pu :

- se servir du système de la banque pour effectuer des virements sur leurs propres comptes ;

- créditer des comptes de clients de façon illicite pour ensuite transférer l'excédent sur leurs propres comptes ;

- prendre le contrôle des distributeurs automatiques, les reprogrammer pour qu'un complice puisse y retirer de l'argent (sans carte ni numéro d'identification personnel). C'est d'ailleurs le dysfonctionnement d'un distributeur automatique à Kiev qui a permis de détecter l'attaque Carbanak.

Ce type de cyber-attaque, une nouvelle forme de cambriolage sans armes ni violence, préfigure les futures cyber-attaques que subiront des institutions financières. Ces attaques passeront par le renseignement humain, par des opérations techniques, puis par un cyber-cambriolage, etc.

Les institutions financières ont acquis une certaine expérience dans le domaine de la cybersécurité et elles peuvent aujourd'hui mesurer elles-mêmes, ou faire mesurer par un tiers, le niveau technologique d'un programme malveillant. Cependant, la première des vulnérabilités, en particulier dans le cas de Carbanak, est la vulnérabilité humaine. La vigilance sera donc toujours nécessaire, quel que soit le niveau technologique.

4| Veiller à la stabilité financière dans un environnement de cybercriminalité

À l'échelle internationale, le CPMI *(Committee on Payments and Market Infrastructures)* se préoccupe de la cybercriminalité et a publié un premier rapport, pour consultation, en novembre 2015[7]. Les infrastructures de marché sont en effet indispensables au bon fonctionnement du système financier et, si elles sont touchées par des cyber-attaques, l'ensemble du système pourrait en pâtir.

Les travaux consacrés aux institutions financières, et aux banques en particulier, ne sont pas aussi avancés. Le Conseil de stabilité financière a élaboré et met régulièrement à jour une liste de banques d'importance systémique mondiale (G-SIB)[8], ainsi qu'une liste de compagnies d'assurance d'importance systémique (G-SII)[9]. En outre, une liste d'institutions financières d'importance systémique qui ne sont pas des compagnies d'assurance ni des banques est à l'étude. Les institutions financières considérées comme ayant une importance systémique doivent satisfaire à des exigences spécifiques, afin de prendre en compte les effets que leur défaillance potentielle produirait sur les marchés.

Concernant la stabilité financière, le scénario du pire serait une cyber-attaque ciblant des institutions financières d'importance systémique, qui seraient alors contraintes de mettre en œuvre un mécanisme de résolution. Mais une organisation criminelle du type de celle se cachant sous l'appellation Carbanak n'a aucun intérêt à lancer une attaque aussi extrême. Pour dérober des fonds, l'attaque doit être aussi discrète et aussi restreinte que possible afin d'éviter d'être détectée et les contre-mesures enclenchées. Quel est donc le risque pour une institution financière ? Deux types d'attaque sont possibles :

- une attaque lancée par un concurrent ou par un groupe de concurrents en vue d'obtenir des parts de marché et de se développer. Étant donné les conséquences si l'affaire s'ébruite, il est peu probable, mais pas impossible, qu'une institution orchestre une telle attaque. C'est un cas de guerre économique ;

- une cyber-attaque reposant sur des motivations politiques ou religieuses et destinée à faire diversion ou à provoquer des dégâts financiers considérables.

Les programmes de sensibilisation déjà mentionnés et les moyens de protection informatique dont les institutions financières se sont dotées ne suffisent pas pour garantir que ce scénario extrême ne se concrétisera jamais. Il faut par conséquent poursuivre

7 https://www.bis.org/cpmi/publ/d138.htm
8 www.fsb.org/wp-content/uploads/2015-update-of-list-of-global-systemically-important-banks-G-SIBs.pdf
9 http://www.fsb.org/2015/11/2015-update-of-list-of-global-systemically-important-insurers-g-siis/

les travaux à l'échelle internationale, non seulement pour empêcher, autant que possible, les attaques, mais aussi pour protéger la résilience si une attaque a réussi. Les institutions financières doivent pouvoir préserver leurs fonctions vitales et leurs services essentiels même si leur système informatique n'est plus opérant, et les pouvoirs publics doivent être prêts à réagir et à apporter, au besoin, une aide. Des synergies entre les deux sont plus que jamais nécessaires.

Dans ce contexte, la meilleure façon d'assurer la stabilité financière consiste à combiner de solides moyens de protection et une grande résilience.

Conclusion

Les institutions financières opèrent de plus en plus dans le cyberespace, de même que l'ensemble de la société. Aucun pays, aucune entreprise, aucune organisation, aucune institution financière, aucun individu ne peut se soustraire à ce nouvel univers. Et comme le monde qui nous entoure, le cyberespace compte aussi des criminels. De même qu'un État souverain protège son territoire et veille à la sécurité de ses citoyens, un chef d'entreprise protège son entreprise en prenant les mesures nécessaires pour permettre à son système informatique de résister à des cyber-attaques.

Les institutions financières ne font pas exception. En général, les cyber-attaques qu'elles subissent exploitent à la fois les vulnérabilités techniques et humaines. Aujourd'hui, la plupart des opérations sont dématérialisées mais ce sont des êtres humains qui les effectuent *via* des ordinateurs, des smartphones, des réseaux sociaux, etc. et le système informatique interne de leur entreprise. Au-delà de la dimension technique des cyber-attaques, il y a les fragilités humaines. L'obtention d'informations sensibles qui permettront de lancer une attaque technologique s'appuie sur le renseignement humain. Les deux sont intimement liés.

La lutte contre la cybercriminalité doit associer tous les acteurs au sein des institutions financières. Des campagnes de sensibilisation, notamment, doivent être organisées afin que les employés et l'encadrement sachent repérer les activités suspectes. La diffusion de l'information et des bonnes pratiques est cruciale pour la cybersécurité. Les pouvoirs publics ont pris un certain nombre d'initiatives qui vont dans ce sens [10], et les institutions financières ont suivi. Par exemple, des clubs comme *Luxembourg for finance* organisent des conférences qui ont pour thème le numérique, la technologie financière et la sécurité. La prise de conscience est réelle, mais il faudra toujours faire mieux, et notamment recentrer l'attention sur le facteur humain. À l'échelle internationale, il est nécessaire d'améliorer la coordination des efforts visant à renforcer la résilience.

10 *France :* http://www.ssi.gouv.fr/uploads/IMG/pdf/guide_hygiene_informatique_anssi.pdf
Belgique : http://vbo-feb.be/fr-be/Publications/Telechargeable-gratuitement-/Belgian-Cyber-Security-Guide/
Pays-Bas : http://english.nctv.nl/Images/cybersecurityassessmentnetherlands_tcm92-520108.pdf?cp=92&cs=65035

Bibliographie

Carter (D. L.) (1992)
« Computer crime categories: how techno-criminals Operate », FBI Law enforcement Bulletin.

Chawki (M.) (2006)
« Essais sur la notion de cybercriminalité », IEHEI, juillet.

De Villenfagne (F.) et Dussollier (S.) (2001)
« La Belgique sort enfin ses armes contre la cybercriminalité : à propos de la loi du 28 novembre 2000 sur la criminalité informatique », Auteur & Média, n°1.

IBM (2015)
Security Trusteer Report.

Sieber (U.) (1998)
« Legal aspects of computer-related crime in the information society – COMCRIME Study », Rapport établi pour la Commission Européenne.

UNODC (2013)
« Étude approfondie sur le phénomène de la cybercriminalité et les mesures prises par les États Membres, la communauté internationale et le secteur privé pour y faire face », UNODC/CCPCJ/EG.4/2013/2, février.

Vormetric (2015)
Vormetric insider threat report – Trends and future directions in data security.

Quels sont les risques du *trading* haute fréquence ?

Thierry FOUCAULT
Professeur de finance
HEC Paris

Les progrès des technologies de l'information et de trading *ont contribué au développement des* traders *haute fréquence (THF), c'est-à-dire des opérateurs qui déploient des stratégies mettant à profit une réaction extrêmement rapide aux événements de marché. Cet article décrit tout d'abord ces stratégies et l'importance de la vitesse pour leur mise en oeuvre. Il analyse ensuite les risques potentiels que certaines de ces stratégies peuvent induire en ce qui concerne la qualité des marchés financiers. Il souligne en particulier qu'une réaction extrêmement rapide peut entraîner des coûts de sélection adverse et saper les incitations à produire des informations, ce qui réduit la capacité des participants à répartir les risques avec efficience et diminue le contenu informationnel des prix des actifs, sur lequel repose l'allocation des ressources. En outre, cet article s'intéresse à plusieurs événements de marché extrêmes et de courte durée qui ont récemment eu un impact négatif sur les cours (c'est le cas, par exemple, du* flash crash *de 2010) et avance que ces événements sont plus probablement imputables à l'automatisation du* trading *et à la réorganisation des marchés qu'au* trading *haute fréquence lui-même. Cet article montre que la régulation du* trading *haute fréquence devrait cibler des stratégies de négociation spécifiques plutôt que le* trading *rapide en général.*

La répartition des risques entre les investisseurs figure parmi les principales fonctions des marchés financiers. À cette fin, le secteur financier innove en permanence, en créant de nouveaux instruments ou de nouvelles méthodes de *trading* (Allen et Gale, 1993), comme en témoigne l'évolution des technologies de *trading* au cours des trente dernières années. Le *trading* n'a cessé de s'automatiser, d'abord sur les marchés boursiers, et plus récemment sur les marchés des dérivés, des devises et des obligations. Les Bourses ont remplacé la corbeille ou le parquet par des systèmes d'appariement automatisés des ordres [1] et les opérateurs humains (courtiers ou tables de négociation pour compte propre) cèdent progressivement la place à des machines et à des algorithmes. Cette évolution s'est également accompagnée de changements dans le mode de diffusion de l'information aux opérateurs et a fait apparaître de nouvelles formes de négociation. En particulier, la négociation automatisée permet de réagir extrêmement rapidement aux événements, et le modèle économique de certaines sociétés de *trading* (les *traders* haute fréquence, ou THF) exploite cette possibilité.

Comme d'autres innovations financières, cette évolution ainsi que le *trading* haute fréquence soulèvent de nombreuses questions. À des fins de réglementation, il convient de comprendre quelles sont les forces économiques qui tirent la croissance du *trading* haute fréquence, ainsi que leurs effets sur la capacité des marchés financiers à remplir efficacement leurs fonctions (en particulier le partage des risques). Cet article traite ces aspects à la lumière des résultats de récents travaux d'universitaires portant sur les *traders* haute fréquence. Son objectif n'est pas de présenter un panorama complet de la littérature, de plus en plus abondante, consacrée à ce sujet, mais plutôt de repérer les sources de risques associées au *trading* haute fréquence, qui doivent retenir l'attention des autorités de réglementation [2].

1| *TRADING* ALGORITHMIQUE ET *TRADING* HAUTE FRÉQUENCE

Le *trading* algorithmique englobe un large éventail de stratégies. Par exemple, les sociétés de courtage recourent à des algorithmes pour optimiser le découpage et la répartition de leurs ordres dans le temps et entre différentes plates-formes de négociation (à l'aide de ce que l'on appelle des *smart routers*, ou routeurs intelligents) afin de réduire leur impact sur les prix, et donc les coûts d'exécution pour leurs clients. Ces stratégies requièrent souvent de soumettre et d'annuler des ordres à grande fréquence, ce qui se traduit par une forte augmentation du trafic sur les plates-formes de négociation électroniques (cf. graphique 1).

Certaines stratégies des sociétés de *trading* pour compte propre reposent sur une réaction extrêmement rapide aux événements survenant sur les marchés, définis très largement. Il peut par exemple s'agir de l'arrivée de nouvelles concernant une action, d'une mise à jour de la cotation de ce titre, ou d'une transaction sur des actifs aux rendements corrélés (par exemple une option sur l'action ou un contrat à terme sur un indice de marché). Pour agir rapidement, ces sociétés investissent dans des technologies qui les aident à minimiser leur « latence » de *trading*, c'est-à-dire le temps qu'il leur faut pour recevoir des messages des sources de données (comme les plates-formes de négociation ou les fournisseurs de données tels que Bloomberg ou Thomson-Reuters), traiter

Graphique 1
Évolution du ratio ordres/transactions
(Nombre d'ordres/nombre de transactions)

Source : Foucault, Kozhan et Tham (2015). Ce graphique présente l'évolution du ratio ordres/transactions avant et après l'introduction de la fonctionnalité Autoquote API sur Reuters D-3000 (une plate-forme de négociation sur les marchés des devises) en juillet 2003. Autoquote API permet aux ordinateurs de saisir automatiquement des ordres sur Reuters D-3000 sans intervention humaine. Son introduction marque le début du trading *algorithmique sur Reuters D-3000.*

1 *Par exemple, la Bourse de Paris est passée à la négociation électronique en 1986 et le* Chicago Mercantile Exchange *a fermé sa corbeille en juillet 2015.*
2 *Cf. Biais et Foucault (2014) et SEC (2014) pour des études plus détaillées de la littérature sur le* trading *haute fréquence.*

ces messages et prendre une décision de *trading* (c'est-à-dire la soumission d'un ordre au marché, d'un ordre à cours limité ou l'annulation d'ordres précédemment passés), et finalement exécuter cette décision. Par exemple, elles investiront dans des connexions à haut débit avec les marchés et les fournisseurs de données, notamment en achetant le droit d'implanter leurs serveurs très près des machines exécutant directement les ordres dans les centres de données des plates-formes de négociation (selon une pratique appelée *« co-location »*) ou en s'abonnant aux flux de données directs afin de recevoir les informations sur le marché une fraction de seconde avant les autres participants [3].

Ces sociétés sont généralement appelées *traders* haute fréquence (THF). Les THF sont une catégorie de *traders* algorithmiques, car ils recourent à des stratégies informatisées. Cependant, les THF présentent une autre caractéristique qui ne se retrouve pas chez tous les *traders* algorithmiques : la très grande vitesse de leurs opérations. Par exemple, en s'appuyant sur des données relatives aux ordres passés par 15 *traders* haute fréquence sur le Nasdaq OMX Stockholm, Baron *et al.* (2015) observent que la latence minimum moyenne pour la soumission des ordres par les *traders* les plus rapides de leur échantillon est inférieure à 1 milliseconde (de l'ordre d'une microseconde pour le *trader* le plus rapide). Parmi les sociétés de *trading* indépendantes bien connues qui pratiquent le *trading* haute fréquence, on peut citer KCG, Virtu, Flow traders ou Tradebot. Des sociétés de courtage pour compte propre (*broker-dealers*) et des banques (comme Goldman Sachs, Morgan Stanley ou Deutsche Bank) ou encore des *hedge funds* (par exemple Citadel ou Renaissance) sont également dotés de tables de négociation spécialisées dans le *trading* haute fréquence.

Jusqu'ici, le *trading* haute fréquence n'est défini clairement ni dans la législation ni dans la réglementation, ce qui pose problème lorsque l'on entend analyser ses effets sur les marchés financiers et sur la régulation [4]. Selon les définitions les plus courantes, le THF présente les caractéristiques suivantes (cf. SEC, 2010) : (i) le placement d'un grand volume d'ordres, (ii) le recours à une très grande vitesse et à des algorithmes pour générer et exécuter les ordres, (iii) le recours à des services de co-location et aux flux de données fournis par chaque place de marché, (iv) la prise et le dénouement de positions dans des délais très brefs, (v) un taux d'annulation élevé des ordres, et (vi) des positions restreintes en fin de séance.

Il est rare que les chercheurs aient accès à des séries de données dans lesquelles les ordres placés par les tables de négociation de *trading* haute fréquence portent une marque qui les distingue des ordres des autres acteurs du marché. Ils doivent donc souvent recourir à des méthodes indirectes afin de repérer ces ordres (cf. SEC, 2014, pour une revue des études empiriques consacrées au *trading* haute fréquence et aux séries de données utilisées dans ces études). Il convient, dès lors, de faire preuve de prudence dans l'interprétation des résultats empiriques concernant le *trading* haute fréquence. En particulier, les régularités empiriques mises au jour dans les études sur les THF pourraient en réalité s'expliquer par les stratégies de participants qui ne sont pas des THF.

Tout en gardant à l'esprit cette limite des études empiriques existantes sur le THF, on peut considérer que les *traders* haute fréquence représentent une part significative du volume de négociation sur les marchés électroniques. Par exemple, un rapport du groupe Tabb a estimé que les THF représentaient 51 % du nombre d'actions échangées sur les marchés boursiers aux États-Unis. Une étude de l'*European Securities and Markets Authority* (ESMA, 2014), portant sur douze plates-formes de négociation européennes et 100 actions, a relevé que les sociétés pratiquant exclusivement le *trading* haute fréquence (ce qui exclue les tables de négociation de *trading* haute fréquence des banques d'investissement) totalisaient 24 % de la valeur négociée. Les *traders* haute fréquence opèrent également sur les marchés des devises, sur les marchés obligataires et sur les marchés des matières premières.

3 *Par exemple, aux États-Unis, les plates-formes de négociation doivent transmettre leurs données à des systèmes centralisés d'agrégation des données* (plan processors) *(la* Consolidated Tape Association *et la* Consolidated Quote Association*), qui regroupent les données et les diffusent en continu au public. Sachant que ce processus prend quelques millisecondes, les acteurs du marché disposant d'un accès direct au flux de données des plates-formes de négociation peuvent obtenir les informations sur le marché encore plus rapidement que les participants qui se les procurent auprès des adhérents aux systèmes d'agrégation* (plan sponsors)*, (pour une analyse, cf. SEC 2010, § IV.B.2). En Europe, il n'existe pas encore de flux de données agrégées pour les actions négociées sur des plates-formes multiples.*

4 *La directive MiFID II définit le* trading *haute fréquence comme du* trading *algorithmique qui s'appuie sur des programmes informatiques afin de déterminer le moment, les prix ou les volumes des ordres en quelques fractions de seconde.*

2| Les stratégies de négociation des THF

Les effets des *traders* haute fréquence sur la qualité des marchés dépendent probablement de leurs stratégies de négociation. Avant d'analyser ces effets, il est donc utile de décrire ces stratégies, lesquelles peuvent globalement se ranger en trois catégories.

2|1 Tenue de marché à haute fréquence

Les teneurs de marché affichent des prix acheteurs et vendeurs auxquels ils sont prêts à acheter ou à vendre des parts d'un actif. Ils sont donc des intermédiaires entre les vendeurs et les acheteurs finaux de cet actif. Par exemple, un teneur de marché peut acheter une action auprès d'un investisseur à un moment donné, puis la revendre après un certain temps à un autre investisseur. Autre possibilité, quand le même actif se négocie sur plusieurs plates-formes (par exemple sur les marchés boursiers européens et des États-Unis), un teneur de marché peut acheter l'actif à un investisseur sur une plate-forme (par exemple BATS en Europe) et le revendre sur une autre (par exemple Euronext).

Les teneurs de marché sont exposés à des risques divers (cf. Foucault, Pagano et Röell, 2013) : (i) le risque de fluctuation de la valeur de leurs positions (« risque d'inventaire »), (ii) le risque de négocier avec des investisseurs mieux informés (« risque de sélection adverse ») et (iii) le risque de négocier à des prix obsolètes lorsqu'une nouvelle arrive (appelé en anglais *picking off risk*). Leur *spread* ou écart de cotation (la différence entre le prix auquel ils vendent et le prix auquel ils achètent) rémunère ces risques et augmente donc lorsque ces risques s'accroissent. Les fourchettes acheteur-vendeur servent souvent d'indicateurs de l'illiquidité du marché.

En principe, une réaction rapide aux événements de marché peut atténuer certains risques inhérents à l'activité de tenue du marché. Premièrement, en permettant aux teneurs de marché d'inverser leurs positions promptement, la rapidité peut les aider à réduire leur risque d'inventaire [5]. Deuxièmement, elle permet aussi aux teneurs de marché d'actualiser leurs prix plus vite lorsqu'une nouvelle arrive, ce qui réduit leur exposition au risque de négocier à des prix obsolètes.

Ainsi, la vitesse peut permettre aux teneurs de marché de comprimer leurs coûts, et donc d'afficher des *spreads* plus compétitifs. Dans le même ordre d'idées, Brogaard *et al.* (2015) observent que les *traders* qui souscrivent au service de co-location le plus rapide sur le Nasdaq OMX Stockholm présentent des caractéristiques de teneurs de marché, et qu'une sophistication de ce service a réduit leur exposition au risque de traiter à un prix inadéquat ainsi que leurs coûts d'inventaire.

2|2 Arbitrage à haute fréquence

Les opportunités d'arbitrage entre actifs liés abondent dans l'univers à haute fréquence. Prenons par exemple le cas d'un fonds négocié en Bourse reproduisant un indice boursier (*Exchange Traded Fund* – ETF). En théorie, le prix de l'ETF doit à tout moment être égal à la valeur de l'indice (la valeur du portefeuille de titres composant l'indice). Si, au contraire, le prix de l'ETF est supérieur (inférieur) à la valeur de l'indice, un arbitragiste peut acheter (vendre) immédiatement le portefeuille d'actions et vendre (acheter) l'ETF, en réalisant un bénéfice. Dans la pratique, ce type d'opportunité d'arbitrage est fréquent sur les marchés des ETF, pour deux raisons. Premièrement, les ordres d'achat ou de vente volumineux sur les ETF (ou sur les actions qui les composent) exercent des pressions passagères au niveau des cours, ce qui engendre une opportunité d'arbitrage. Deuxièmement, lorsqu'une information arrive, les prix affichés pour les ETF et les actions qui les composent ne sont pas actualisés simultanément (par exemple, les cours des actions sous-jacentes ont tendance à être actualisés avec un léger décalage temporel par rapport aux prix sur le marché des ETF). Cette synchronisation imparfaite dans l'ajustement des prix en fonction de l'information fait, elle aussi, apparaître des opportunités d'arbitrage. Le même type d'opportunités se présente plus généralement entre les

5 *Considérons le cas d'un teneur de marché qui a une position longue sur une action française négociée sur plusieurs marchés (par exemple Euronext et BATS). Si un prix acheteur particulièrement élevé est affiché sur un marché, un teneur de marché rapide peut saisir cette opportunité pour dénouer sa position avant que d'autres vendeurs n'en profitent.*

produits dérivés (CDS, contrats à terme, options, etc.) et leurs actifs sous-jacents, sur les marchés des devises (par exemple, l'arbitrage triangulaire), entre actions négociées sur des plates-formes différentes, etc. [6]

Ces opportunités d'arbitrage sont très éphémères : elles disparaissent dès que les teneurs de marché actualisent leurs prix ou dès qu'un arbitragiste exploite ces opportunités. Ainsi, Budish *et al.* (2015) ont observé que la durée médiane des opportunités d'arbitrage entre le SPDR S&P 500 ETF (SPY) et le contrat à terme E-mini S&P 500 entre janvier 2005 et décembre 2011 s'échelonnait entre 250 millisecondes (en 2006) et environ 10 millisecondes (en 2011). Ils ont également dénombré, en moyenne, 801 opportunités par jour, qui s'accompagnent d'un bénéfice potentiel de 98,01 dollars par opportunité. Ainsi, un *trader* ne peut exploiter ces opportunités éphémères, modestes mais nombreuses, qu'à condition d'être très rapide. Ces opportunités ont constitué une autre motivation importante pour le développement du *trading* haute fréquence (cf., par exemple, Chaboud *et al.*, 2014, pour une analyse s'inscrivant dans le contexte du marché des devises).

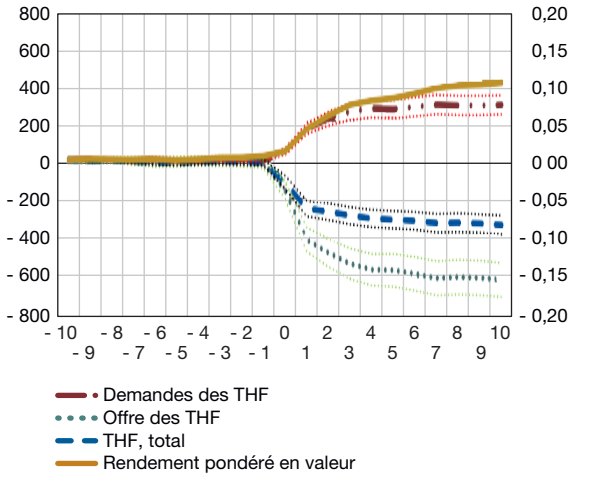
2|3 L'arbitrage directionnel à haute fréquence

Les *traders* haute fréquence peuvent également prendre une position en anticipation d'un futur mouvement des prix. Ce type de stratégie est qualifié de « directionnelle », car les *traders* prennent une position sur un actif en misant sur la direction dans laquelle ils estiment que les prix vont évoluer (par exemple, ils achètent une action s'ils anticipent une hausse de son cours). La vitesse peut se révéler utile pour ce type de stratégie, puisqu'elle permet aux *traders* de réagir plus rapidement aux informations.

Penchons-nous par exemple sur le graphique 2 (extrait de Brogaard *et al.*, 2014). La courbe pleine en gras représente la variation du cours moyen pendant les 10 secondes qui suivent l'arrivée (date 0)

Graphique 2
Nouvelles macroéconomiques positives

(Secondes avant et après l'annonce de nouvelles macroéconomiques)
Flux d'ordres des THF (en dizaines de milliers de dollars) *Rendements*



Source : Brogaard, Hendershott et Ryordan (2014), Figure 5, p. 2297.

d'une nouvelle macroéconomique « positive » (c'est-à-dire meilleure que prévu) pour un échantillon de 120 actions du Nasdaq sur la période 2008-2009. En moyenne, dans l'échantillon, les nouvelles macroéconomiques engendrent une variation des cours d'environ 10 points de base pendant les 10 secondes qui suivent l'annonce. Dès lors, un *trader* qui réagit assez vite (disons en 10 millisecondes) à l'annonce d'une nouvelle macroéconomique positive peut s'attendre à dégager un petit bénéfice, en moyenne, en achetant l'action. Brogaard *et al.* (2014) montrent que c'est ce que font certains THF. La courbe en traits et en points sur le graphique 2 représente la différence agrégée cumulée (sur la durée, par tranche de 10 000 dollars) entre les achats et les ventes « agressifs » (c'est-à-dire exécutés *via* des ordres au marché) effectués par des THF dans l'échantillon de Brogaard *et al.* (2014). De même, la courbe en pointillés représente la différence agrégée cumulée entre les achats et les ventes « passifs » (c'est-à-dire exécutés *via* des ordres à cours limité) effectués par les THF de l'échantillon [7].

6 *Cf., par exemple, Ben-David* et al. *(2015) pour des données relatives aux opportunités d'arbitrage sur les marchés des ETF ou Chaboud* et al. *(2014) et Foucault, Kozhan et Tham (2015) à propos des opportunités d'arbitrage sur les marchés des devises.*

7 *Un ordre à cours limité est un ordre d'acheter ou de vendre un nombre donné d'actions à un prix donné. De manière générale, ce prix est tel que l'ordre ne peut pas être exécuté immédiatement. Dans ce cas, l'ordre est stocké dans un carnet d'ordres à cours limité jusqu'à ce qu'un autre investisseur accepte de négocier à son prix ou jusqu'à ce que l'émetteur annule cet ordre. Les « ordres au marché » sont des ordres d'acheter ou de vendre un nombre donné d'actions à un prix tel que ces ordres puissent être exécutés instantanément face à d'autres ordres figurant dans le carnet des ordres à cours limité. Les plates-formes de négociation qualifient souvent les ordres au marché d'ordres « agressifs », dans le sens où leur soumission entraîne une transaction. Les ordres à cours limité sont dits « passifs », dans le sens où leur exécution ne peut être activée que par l'arrivée d'un ordre au marché.*

À l'évidence, certains *traders* haute fréquence accumulent rapidement une position acheteuse significative (en plaçant des ordres d'achat au marché) juste après une annonce macroéconomique positive, probablement en anticipation de la hausse du cours qui se matérialisera dans les 10 secondes qui suivent. Il est intéressant de noter que d'autres THF (ceux qui opèrent *via* des ordres à cours limité) vendent les actions juste après l'annonce, comme le montre la courbe en pointillés. La symétrie entre la courbe en traits et en points et la courbe en pointillés suggère en fait que ces derniers n'ont pas le temps de revoir leurs prix après l'annonce de la nouvelle et qu'ils sont pris de vitesse (*picked off*) par les THF qui sont suffisamment rapides pour tirer parti de cette annonce avant que les prix ne soient corrigés (cf. Dugast, 2015, pour un modèle de correction des prix après l'arrivée d'une nouvelle, qui formalise ce scénario).

Les annonces macroéconomiques ne constituent qu'une petite fraction de toutes les « nouvelles » qui arrivent pendant une journée donnée. En réalité, les avancées des technologies de l'information permettent aux *traders* de réagir à une multitude de signaux susceptibles, en principe, de faire évoluer les prix sur le marché. Par conséquent, certains fournisseurs d'informations (comme Thomson-Reuters, Bloomberg ou Dataminr) communiquent désormais des signaux d'achat et de vente extraits de l'information brute disponible sur les réseaux sociaux comme Twitter [8]. De plus, les données de marché (prix, transactions, soumission d'ordres, etc.) constituent en elles-mêmes une information sur l'évolution à venir des prix [9]. Disposer d'un accès à ces données plus rapidement constitue un autre moyen d'anticiper les mouvements des prix à court terme. Dans le même ordre d'idées, Brogaard *et al.* (2015) observent que les rendements des contrats à terme sur l'indice OMXS30 permettent de prévoir, une seconde à l'avance, la direction des ordres au marché soumis par les *traders* rapides dans leur échantillon (30 actions suédoises composant l'indice OMXS30). Ce résultat suggère que ces *traders* utilisent l'information contenue dans les variations de prix des contrats à terme pour anticiper à très court terme les variations des actions qui composent l'indice (cf. également Zhang, 2013 pour des constats similaires).

Les *traders* haute fréquence peuvent également mettre à profit leur capacité à traiter rapidement un large volume de données grâce à leurs investissements massifs dans des ordinateurs et des algorithmes efficients. Cette capacité peut en particulier se révéler utile pour mieux isoler le bruit présent dans les données de marché, et donc pour obtenir un signal plus précis afin de prévoir les évolutions des prix à venir. Foucault, Hombert et Rosu (2016) définissent la stratégie de *trading* optimale d'un investisseur qui réagit plus rapidement aux nouvelles et en soustrait le bruit plus efficacement que les autres acteurs du marché. Ils montrent que la rapidité compte : la stratégie de *trading* à l'équilibre de cet investisseur diffère significativement de celle d'un investisseur qui est simplement compétent pour traiter l'information (comme dans les modèles traditionnels de *trading* avec asymétrie de l'information).

De surcroît, la puissance de calcul des THF (et leurs techniques sophistiquées d'analyse des données) peut les aider à détecter les empreintes laissées par d'autres *traders* qui ont exécuté des ordres volumineux (cf. Hirshey, 2013, et Menkveld et van Kervel, 2015, pour des données). En effet, ces ordres volumineux sont souvent découpés en une chaîne d'ordres plus petits (appelés *child orders*), ce qui réduit leur impact sur les prix. La détection des premiers *child orders* dans cette chaîne peut permettre de prévoir l'arrivée de *child orders* ultérieurs.

Cette stratégie d'« anticipation des ordres » peut se révéler rentable pour au moins deux raisons. Premièrement, il arrive que les *traders* qui placent des ordres volumineux soient eux-mêmes informés. Ainsi, leurs achats (ventes) annoncent une augmentation (baisse) des prix à l'avenir. Dans ce cas, il est optimal pour les *traders* anticipant les ordres de répliquer ces transactions (cf. Lyang et Zhu, 2015, pour une analyse théorique). Dans ce scénario, à force de concurrence, les *traders* anticipant les ordres font disparaître les bénéfices des *traders* informés. Deuxièmement, les *traders* plaçant des ordres volumineux sont parfois contraints de liquider une position substantielle car ils ont besoin de financement (il arrive par exemple qu'un *hedge fund* doive liquider une position importante pour honorer des appels de marge). Ce type de liquidation forcée opérée par les *traders*

8 *Cf.* « Mining for tweets of gold », *7 juin 2014,* The Economist *ou* « How investors are using social medias to make money », *Fortune, 7 décembre 2015.*
9 *Cela concorde avec les théories énoncées par Grossman et Stiglitz (1980) ou par Blume, Easley et O'Hara (1994), qui affirment que les données relatives aux marchés, telles que le cours des actions ou le volume des transactions, contiennent des informations qui peuvent servir à prévoir les rendements à venir.*

en difficulté s'accompagne en général d'une décote sur les prix. Comme le montrent Brunnemeier et Pedersen (2005), les *traders* qui repèrent la présence d'un *trader* en difficulté sont incités (i) à commencer par prendre une position dans la même direction que lui pour amplifier la pression à la baisse sur les prix induite par les ordres du *trader* aux abois puis (ii) à acheter l'actif moyennant une forte décote sur le prix (Brunnermeier et Pedersen, 2005, qualifient cette stratégie de « prédatrice »).

En se fondant sur des données relatives aux ordres des THF et aux investisseurs institutionnels sur le Nasdaq OMX, Menkveld et van Kervel (2015) ne mettent en évidence aucun élément démontrant que les THF de leur échantillon se livrent à des pratiques prédatrices sur des transactions volumineuses d'investisseurs institutionnels. En fait, les THF semblent plutôt fournir de la liquidité aux *child orders* initiaux des investisseurs institutionnels et ce faisant atténuent leur impact sur les prix. Cependant, les THF finissent par finalement se positionner dans la même direction que ces *child orders*. Ce comportement peut soit dénoter une gestion optimale du risque par les THF, soit concorder avec « l'hypothèse d'anticipation des ordres » selon laquelle les THF « répliquent » les transactions informées des investisseurs institutionnels dès lors qu'ils ont repéré la présence de ces investisseurs grâce à leurs transactions passées.

Les *traders* haute fréquence sont également accusés de manipuler les prix. En particulier, deux stratégies (le « déclenchement de tendance » et le « *spoofing* ») retiennent l'attention. Le déclenchement de tendance consiste à commencer par placer des ordres d'achat (ou des ordres de vente) dans l'espoir que ce comportement poussera d'autres *traders* à faire de même. La rafale des ordres d'achat qui s'ensuit propulse ensuite les cours à la hausse, ce qui permet au *trader* à l'origine de cette opération de liquider sa position en engrangeant un bénéfice. Le *spoofing* consiste à afficher, par exemple, un grand nombre d'ordres d'achat à cours limité et à les annuler rapidement dans l'espoir d'inciter d'autres *traders* à acheter l'actif, permettant ainsi au manipulateur de réaliser des gains sur l'exécution des ordres d'achat à cours limité à prix gonflés. Cette pratique est interdite par le Dodd-Frank Act, et, récemment, plusieurs *traders* ont été accusés de *spoofing* aux États-Unis [10].

Il est difficile de définir la manipulation des prix ou du marché, que ce soit en termes juridiques ou économiques (cf. Fishel et Ross, 1991, et Kyle et Viswanathan, 2008). En particulier, comme le précisent Kyle et Viswanathan (2008), il est malaisé de faire la différence entre des stratégies de *trading* qui nuisent à la fois au pouvoir informatif des prix et à la liquidité (ce que Kyle et Viswanathan, 2008, considèrent comme une manipulation) et des stratégies de *trading* qui peuvent paraître manipulatrices mais qui consistent juste à exploiter rationnellement le pouvoir de marché et l'information privée. Plusieurs modèles montrent que le comportement optimal des investisseurs informés peut se révéler complexe et contre-intuitif et que, pourtant, leurs transactions renforcent le pouvoir informatif des prix et n'ont aucune visée manipulatrice [11]. Le même problème se pose pour l'interprétation des intentions qui se cachent derrière les schémas de soumission des ordres des THF.

La tenue de marché, l'arbitrage, le *trading* directionnel, l'anticipation des ordres et les stratégies manipulatrices existent depuis longtemps sur les marchés financiers et ont tous été analysés de manière poussée par les économistes. Ce qui est nouveau, c'est le recours intensif aux technologies de l'information pour l'exécution de ces stratégies et la façon dont elles sont mises en œuvre. À ce sujet, on ne dispose que de très peu d'informations, car les THF considèrent que cette mise en œuvre constitue précisément la source de leur avantage compétitif, et s'efforcent naturellement de protéger leur « recette secrète » [12].

Sachant que les différentes stratégies laissent des empreintes différentes dans les données, il est possible de repérer, dans une certaine mesure, les stratégies des THF. Par exemple, les teneurs de marché ont tendance à utiliser principalement des ordres à cours limité (appelés « ordres passifs »),

10 *Cf.* « Flash crash : trading terms and manipulation techniques explained », Financial Times, *22 avril 2015 et* « Regulators step up efforts to stop spoofing », Financial Times, *5 novembre 2015.*

11 *Par exemple, Back et Baruch (2004) montrent que la randomisation entre ordres d'achat et ordres de vente peut constituer un moyen de minimiser les coûts de transaction pour un investisseur informé.*

12 *Le cas d'Alexei Aleynikov constitue un bon exemple. Il a été accusé d'avoir volé le code de* trading *haute fréquence de Goldman Sachs (cf.* « Ex-Goldman Programmer Guilty of Stealing Code », New-York Times, *mai 2015).*

tandis que les *traders* directionnels cherchant à tirer parti des variations des prix à très court terme recourent en priorité à des ordres au marché (car l'exécution des ordres à cours limité prend du temps et est incertaine). Dans une revue récente de la littérature empirique, la *Securities Exchange Commission* (SEC) note :

« *Le constat peut-être le plus notable des études s'appuyant sur les ensembles de données relatifs aux THF est que le* trading *haute fréquence n'est pas un phénomène monolithique, mais qu'il englobe des stratégies diverses et variées. En particulier, le* trading *haute fréquence ne se caractérise pas uniquement, voire pas même principalement, par des stratégies de tenue passive des marchés employant des ordres pourvoyeurs de liquidité […] De plus, le niveau et la nature de l'activité de* trading *haute fréquence peuvent varier considérablement entre différentes catégories d'actions.* » (SEC, 2014)

Cette observation est importante, car les effets du *trading* haute fréquence sur la qualité des marchés dépendront plus probablement du type de stratégie que les *traders* utilisent (cf. *infra*) que de la rapidité en soi. Dans la pratique, les grandes sociétés pratiquant le *trading* haute fréquence sont probablement opportunistes et emploient une stratégie tant qu'elle est rentable (et, on peut l'espérer, licite), puis l'abandonnent lorsqu'elle cesse d'être lucrative. Les données suggèrent toutefois un certain degré de spécialisation parmi les sociétés pratiquant le *trading* haute fréquence : certaines paraissent davantage spécialisées dans la tenue de marché, tandis que d'autres privilégient l'arbitrage ou le *trading* directionnel (cf. Hagströmer et Norden, 2013).

3| Risques et avantages du *trading* haute fréquence

Les médias et les régulateurs s'intéressent de près au *trading* haute fréquence, une technique qui, selon plusieurs auteurs, pourrait nuire à l'activité d'autres opérateurs ainsi qu'à l'intégrité des marchés financiers (cf. notamment Flash Boys : *A Wall Street Revolt*, le best-seller de Michael Lewis). Une question fondamentale se pose : le *trading* haute fréquence accroît-il, ou au contraire, réduit-il (i) la liquidité des marchés, pour le partage des risques, et (ii) la « précision » des cotations, c'est-à-dire le pouvoir informatif des prix des actifs sur lequel repose l'allocation des ressources, étant donné que le partage des risques et la production d'informations constituent deux fonctions importantes des marchés financiers ? Une autre question est de savoir dans quelle mesure le *trading* haute fréquence peut mettre en péril la stabilité des marchés. Nous discutons ces points ci-dessous.

3|1 Avantages privés *versus* avantages sociaux

Comme expliqué plus haut, les *traders* haute fréquence investissent massivement dans la technologie et l'information. On peut donc penser qu'ils en tirent individuellement un certain nombre d'avantages. En revanche, l'avantage social de ces investissements est moins manifeste. Grâce à ces investissements, les THF accèdent à l'information avec une longueur d'avance et sont très réactifs, ce qui entraîne un problème de sélection adverse pour d'autres participants.

Reprenons par exemple le graphique 2. Il montre que certains THF placent des ordres d'achat juste après l'annonce de bonnes nouvelles macroéconomiques et un peu avant une hausse des cours liée à ces annonces. Le gain qu'ils réalisent sur ces opérations d'achat constitue une perte pour leurs contreparties, lesquelles sont victimes de la « sélection adverse » pratiquée par les participants mieux informés. Les données empiriques dont on dispose sur le *trading* haute fréquence (cf. par exemple Baron, Brogaard et Kirilenko, 2014, ou Brogaard, Hendershott et Riordan, 2014) laissent à penser que les ordres au marché passés par les THF mettent à profit une information (anticipent les futurs mouvements des prix), ce qui génère des coûts de sélection adverse pour leurs contreparties (y compris pour les THF spécialisés dans l'apport de liquidité). Ainsi, Brogaard, Hendershott et Riordan (2014) indiquent (p. 2268) : « *nous montrons que le* trading *haute fréquence entraîne des coûts de sélection adverse pour d'autres investisseurs.* »

On pourrait avancer que ce n'est pas un problème car le *trading* rapide informé consiste en un simple transfert monétaire entre opérateurs réactifs et opérateurs lents, c'est-à-dire un jeu à somme nulle. Cette redistribution peut être jugée inéquitable (pour les opérateurs lents), mais, globalement, il

n'y a pas de perte de bien-être. Cependant, Biais, Foucault et Moinas (2015) montrent que cet argument est incomplet, pour deux raisons. Premièrement, en présence d'une sélection adverse, tous les opérateurs supportent des coûts d'impact plus élevés. À mesure que le coût du *trading* augmente, les investisseurs dont les gains sont faibles (par rapport à ce coût) réduisent leurs opérations (par exemple, ils couvrent leurs risques avec moins d'efficience), voire se retirent du marché. Deuxièmement, les investissements des THF doivent être pris en compte dans le calcul des gains et avantages sociaux de cette activité. S'il s'agit seulement d'un jeu à somme nulle, alors, son coût social est égal aux ressources qui lui sont allouées. Or celles-ci sont significatives. Ainsi, Hibernia Networks a posé un nouveau câble sous-marin transatlantique à fibre optique, « Project Express », qui accélère de 5 millisecondes le délai d'interconnexion entre les Bourses de New York et de Londres. Cette infrastructure, d'un coût de 300 millions de dollars, sera financée par les redevances d'utilisation que les *traders* verseront pour accéder rapidement à l'information. D'après les estimations du groupe Tabb, pour la seule année 2013, les investissements dans les technologies de *trading* haute fréquence se sont chiffrés à 1,5 milliard de dollars, soit deux fois plus qu'en 2012 (cf. l'article *« High speed traders turn to laser beams »*, The Wall Street Journal, 2014).

Cependant, les THF ne pratiquent pas tous le *trading* directionnel. Comme expliqué plus haut, certains s'appuient sur leur accès rapide aux marchés et à l'information pour opérer comme teneurs de marché. Si, dans ce cas, la vitesse réduit le coût de la tenue de marché (coût d'inventaire et coût lié au risque de ne pas traiter au prix adéquat en étant devancé par les *traders* plus rapides) ou intensifie la concurrence entre teneurs de marché, les THF devraient comprimer les coûts de transaction pour les investisseurs. De plus, si la tenue de marché à haute fréquence fait baisser le coût d'intermédiation, cette baisse constitue un avantage social.

Il est à ce jour difficile de mesurer séparément les effets des différents types de stratégies employées par les THF. Les chercheurs empiriques observent souvent les activités de ces *traders* (soumissions d'ordres, transactions, etc.), directement ou indirectement, mais pas les stratégies sous-jacentes, alors que ce sont précisément les stratégies qui importent. Brogaard *et al.* (2016), par exemple, analysent l'évolution des mesures de la liquidité (notamment l'écart de cotation – ou *spread* – effectif) pour 30 titres cotés sur le Nasdaq OMX à la suite d'une amélioration des services de *co-location* proposés également par le Nasdaq OMX. Ils constatent que cette amélioration se traduit par un accroissement de la liquidité (diminution du *spread*). La décomposition de cet effet montre que l'amélioration des services a deux conséquences : (i) elle resserre le *spread* « réalisé » (qui mesure le bénéfice par transaction, hors coûts de sélection adverse pour les teneurs de marché) et (ii) elle accentue l'impact sur le prix (qui mesure les coûts de sélection supportés par les teneurs de marché). Le resserrement du *spread* réalisé reflète une intensification de la concurrence entre teneurs de marché, tandis que l'accentuation de l'impact sur le prix reflète un risque de sélection adverse accru.

Dans l'étude de Brogaard *et al.* (2016), la diminution du *spread* réalisé surcompense l'augmentation de l'impact sur le prix. Au final, un accès plus rapide au marché *via* la *co-location*) apparaît donc bénéfique. Néanmoins, cette analyse montre qu'il est important de mesurer séparément les effets des différentes stratégies (l'effet bénéfique de l'amélioration des services de *co-location* pourrait être encore plus marqué si la *co-location* ne servait pas à déployer des stratégies directionnelles).

Par conséquent, les interventions des pouvoirs publics devraient cibler des stratégies de *trading* particulières plutôt que le *trading* haute fréquence en général. La régulation ne devrait pas décourager le *trading* haute fréquence quand celui-ci permet de réduire les coûts de transaction pour les investisseurs. *A contrario*, elle devrait décourager les stratégies qui mettent à profit de légères différences dans la rapidité d'accès à l'information sur les futurs mouvements des prix.

Considérons par exemple le projet qui consiste à faire payer une taxe aux *traders* lorsque leur ratio ordres/transactions dépasse un seuil donné (défini dans la directive MiFID II). Cette taxe augmente le coût d'annulation des ordres pour les *traders* qui passent principalement des ordres à cours limité, c'est-à-dire pour ceux qui sont les plus susceptibles d'être des teneurs de marché. Ces opérateurs doivent fréquemment annuler des ordres à cours limité afin (i) d'optimiser la gestion de leur risque d'inventaire (les annulations peuvent s'inscrire dans une stratégie optimale de gestion de l'inventaire), (ii) d'être

moins exposés au risque de transaction à des prix obsolètes *(stale quotes)* et (iii) de prendre en compte l'information provenant d'autres plates-formes de négociation (cf. van Kervel, 2015). Si les annulations d'ordres deviennent plus coûteuses, les teneurs de marché à haute fréquence doivent augmenter leurs *spreads* car les coûts qu'ils supportent en qualité de teneurs de marché augmentent. En revanche, étant donné que les *traders* directionnels (informés) soumettent essentiellement des ordres au marché, leur ratio ordres/transactions est naturellement inférieur. C'est pourquoi une taxe sur ce ratio risque d'être contreproductive : elle a un effet dissuasif sur la tenue de marché à haute fréquence (qui est susceptible d'améliorer la liquidité), mais n'a *a priori* aucun impact sur le *trading* haute fréquence directionnel (qui nuit à la liquidité). Il serait plus efficace d'allonger très légèrement, de manière aléatoire, le délai d'exécution des ordres au marché. De fait, ce différé devrait réduire la capacité des THF à tirer profit des cours obsolètes, tout en laissant la possibilité aux *traders* qui soumettent des ordres à cours limité de réviser leurs cotations si nécessaire.

3|2 Information privilégiée *versus* découverte

Outre qu'ils facilitent le partage des risques et la réalisation de gains de transaction, les marchés financiers ont une autre fonction importante : la production d'informations. En effet, les prix des actifs agrègent les signaux envoyés par les investisseurs informés et transmettent ainsi des informations permettant des décisions réelles, par exemple un investissement (cf. Bond, Edmans et Goldstein, 2012) [13]. L'un des avantages potentiels du *trading* informé est qu'en rendant les prix plus informatifs, il aboutit également à des décisions plus efficientes.

Il est naturel de penser qu'en étant plus rapides, les THF directionnels accélèrent aussi la vitesse à laquelle les prix reflètent l'information. Brogaard *et al.* (2014) mettent en évidence des éléments qui étayent cette thèse. Ils montrent que les THF opèrent dans la direction inverse des erreurs de prix transitoires, et dans la même direction que les évolutions durables de la valeur des actifs. En d'autres termes, ils rapprochent les prix d'une marche aléatoire *(random walk)*, comme cela doit être le cas sur un marché où les prix reflètent toute l'information disponible. On constate par ailleurs que la croissance du *trading* algorithmique s'accompagne d'opportunités d'arbitrage de plus courte durée (cf. Budish *et al.*, 2015, à propos de l'arbitrage croisé sur les ETF, et Chaboud *et al.*, 2014, pour l'arbitrage triangulaire).

Cela ne signifie pas pour autant que le *trading* haute fréquence rend effectivement les prix plus informatifs en tant que signaux pour l'allocation des ressources [14]. Hirshleifer (1971) distingue deux types d'information : « l'information privilégiée », c'est-à-dire l'information sur un état qui, en temps voulu, sera connu de tous, et la « découverte », c'est-à-dire la production d'informations qui, sans une intervention humaine active, ne seraient pas accessibles. Cette distinction est très utile pour réfléchir à l'effet du *trading* haute fréquence sur le contenu informationnel des prix. Considérons de nouveau le cas d'une annonce macroéconomique positive (graphique 1) : en observant des annonces macroéconomiques un peu plus rapidement que d'autres *traders*, certains THF obtiennent de manière privilégiée un élément d'information qui sera connu de tous quelques secondes plus tard. En opérant sur la base de cette information, ils accélèrent la vitesse à laquelle les prix reflètent cette information, ce qui accroît l'efficience informationnelle des marchés. Mais ils ne « découvrent » pas l'information : l'annonce macroéconomique a lieu indépendamment du fait que certains *traders* l'observent, ou non, très rapidement. *A contrario*, un analyste qui combine différentes données pour évaluer la valeur d'une entreprise produit une information qui, sinon, ne serait pas disponible. En opérant sur la base de cette information, il intègre dans les prix une information qui, sinon, n'aurait pas été disponible.

À ce jour, il n'est pas avéré que les THF contribuent à intégrer dans les prix des actifs des informations qui, sinon, ne seraient pas disponibles. En fait,

13 *Par exemple, selon Fama et Miller (1972, p. 335), «* un marché efficient présente une caractéristique très intéressante. À tout moment, les prix de marché des titres envoient des signaux précis pour l'allocation des ressources, ce qui permet aux entreprises de prendre des décisions de production/d'investissement. *»*

14 *En effet, l'efficience informationnelle est définie par rapport au « stock » d'informations disponibles. Elle ne dit rien sur la quantité d'informations. Si aucune information n'est disponible, les prix des actifs ne seront pas du tout informatifs, y compris lorsqu'ils présentent une efficience informationnelle.*

dans la mesure où ils réduisent les profits liés à la découverte d'informations, il se pourrait qu'ils rendent les prix des actifs moins informatifs. Ainsi, Dugast et Foucault (2015) examinent un modèle dans lequel les investisseurs peuvent choisir d'opérer soit sur la base d'informations brutes (signaux d'achat ou de vente fondés sur le contenu de *tweets*, par exemple ; cf. l'article « *How investors are using social medias to make money* », paru dans *Fortune* le 7 décembre 2015) soit sur la base d'informations traitées (le traitement de l'information constitue une forme de découverte). L'information traitée est plus précise, mais le traitement prend du temps. Le *trading* sur la base d'informations brutes est donc une forme de *trading* rapide. Dugast et Foucault (2015) montrent qu'une diminution du coût d'accès à l'information brute peut décourager la production d'informations traitées, ce qui rend les prix moins informatifs à long terme. Cette possibilité trouve un écho dans les résultats empiriques de Weller (2016). Celui-ci montre empiriquement qu'il existe une relation négative entre le volume de *trading* algorithmique sur les actions et le contenu informationnel des prix des actions sur les annonces de résultats futurs des entreprises.

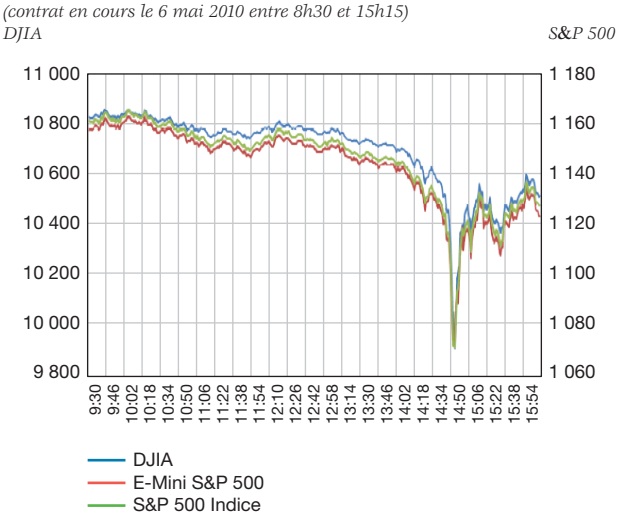
3|3 Fragilité *versus* fiabilité

Ces dernières années, les marchés financiers des États-Unis ont connu à plusieurs reprises des variations de prix de grande ampleur mais de courte durée. Trois de ces épisodes ont été particulièrement marquants.

- **Le *flash crash* du 6 mai 2010 (cf. graphique 3).** Sur un intervalle de 30 minutes, à partir de 14 heures 32 (côte Est), les indices boursiers des États-Unis, les ETF et les contrats à terme sur indices ont subi de très forts mouvements de cours, à la hausse et à la baisse. Le Dow Jones, en particulier, a reculé d'environ 6 % en cinq minutes, et les distorsions de cours ont été considérables (par exemple, le titre Accenture s'est échangé à un penny par action, et le titre Apple à 100 000 dollars par action). Ce *flash crash* a affecté les marchés d'actions, les marchés des ETF et les marchés des contrats à terme. À 15 heures, les cours étaient revenus à un niveau proche de leur niveau initial.

Graphique 3
Prix des transactions à la fin de chaque minute pour le Dow Jones Industrial Average (DJIA), le S&P 500 et le contrat à terme E-Mini S&P 500 (échu en juin 2010)

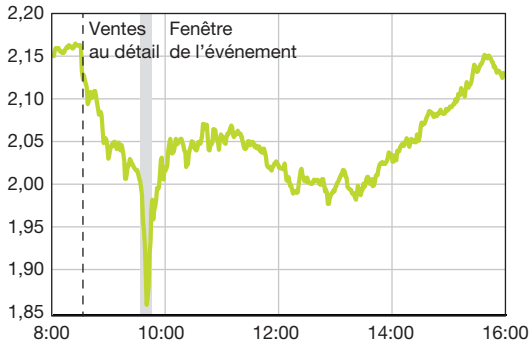
(contrat en cours le 6 mai 2010 entre 8h30 et 15h15)



Source : « Preliminary Findings Regarding the Market Events of May 6, 2010 ». *Ce graphique présente les prix de transaction à la fin de chaque minute, le 6 mai 2010, entre 8h30 et 15h15 (heure du Centre), pour le Dow Jones Industrial Average (DJIA), le S&P 500 et le contrat à terme E-Mini S&P 500 (échu en juin 2010).*

- **Le *Treasury flash crash* du 15 octobre 2014 (cf. graphique 4).** Entre 9 heures 33 et 9 heures 40, le rendement du bon du Trésor américain à 10 ans a cédé 16 points de base. L'ensemble de la courbe des rendements des bons du Trésor et des contrats à terme sur les obligations du Trésor a été touchée, ainsi que, dans une moindre mesure, les marchés des *swaps* de taux et les marchés d'actions. À 10 heures, les rendements avaient retrouvé leur niveau antérieur au *flash crash*.

Graphique 4
Rendement du bon du Trésor américain à 10 ans sur le marché au comptant, le 15 octobre



Source : Joint Staff Report *(2015), graphique 2.1.*

- **Le *flash crash* du 24 août 2015 sur les ETF.** À l'ouverture, à 9 heures 30, le cours de plusieurs ETF a baissé nettement par rapport aux indices de référence. Par exemple, le SPDR S&P 500 (SPY) affichait une décote de 5,2 % par rapport à son niveau de clôture de la veille. Cette décote a atteint 7,8 % à 9h35. Ensuite, le cours de SPY s'est rapidement redressé, dépassant le cours d'ouverture. Cette dépréciation par rapport au cours de la veille a été l'une des plus fortes de la dernière décennie (cf. SEC, 2015). Les 50 premiers ETF (environ 40 % du total) ont perdu plus de 10 % de leur valeur SEC (2015). De surcroît, entre 9h30 et 9h45, nombre de titres de grands groupes cotés sur le NYSE et sur le Nasdaq ont chuté de plus de 10 %.

Tous ces événements présentent des caractéristiques communes. Premièrement, les mouvements extrêmes observés lors de ces événements s'accompagnent d'une importante contraction de la liquidité sur les marchés concernés (cf. Joint Staff Report (2015) pour le *Treasury flash crash* et *Joint Staff Report* (2010) pour le *flash crash* de 2010). Ces *flash crashes* affectent donc les cours et la liquidité. Deuxièmement, ils se produisent sans qu'il n'y ait de changements apparents dans les fondamentaux. De fait, la rapide inversion du cours qui suit à chaque fois la forte baisse ou hausse initiale indique que ces mouvements ne sont pas imputables à une évolution des fondamentaux. Troisièmement, beaucoup d'actifs sont affectés, peut-être à cause des interactions entre des catégories d'actifs qui sont liées par des relations hors arbitrage.

En outre, les participants au marché affirment que les « *mini flash crashes* » (baisse ou hausse soudaine du cours d'un actif, suivie d'une inversion en quelques secondes) sont aujourd'hui courants [15]. On parle de *mini flash crashes* parce que ce type de *crash* n'affecte pas simultanément un grand nombre d'actifs, contrairement aux trois *flash crashes* décrits plus haut. Pourtant, ces événements posent potentiellement problème car ils pourraient provoquer des perturbations de plus grande ampleur sur les marchés.

Au lendemain du *flash crash* de 2010, plusieurs commentateurs ont avancé l'idée que le *trading* haute fréquence avait joué un rôle dans cet événement et qu'il fragilisait les marchés. Ainsi, en septembre 2010, Mary Schapiro, présidente de la *Securities and Exchange Commission*, a déclaré devant la *Security Traders Association* : « *Compte tenu de leurs capacités en terme de volume et d'intervention, les entreprises de* trading *à haute fréquence peuvent considérablement affecter la stabilité et l'intégrité des marchés d'actions. Or, à l'heure actuelle, [ils] […] n'ont quasiment pas de règles à respecter, que ce soit sur la préservation de cette stabilité […] pendant les périodes difficiles ou sur la limitation de la volatilité des cours […]. Un algorithme […] hors de contrôle peut également perturber fortement les transactions, nuisant à la stabilité des marchés et érodant la confiance des investisseurs.* »

Cependant, il n'est pas du tout certain que les THF aient contribué aux *flash crashes*, et les rapports détaillés des agences publiques ne montrent pas, et n'émettent même pas l'hypothèse, qu'ils ont eu une responsabilité directe dans la survenue de ces événements (cf., par exemple, SEC, 2015, *Joint Staff Report*, 2015, ou « *Preliminary Findings Regarding the Market Events of May 6, 2010* »). En réalité, on est encore loin de bien comprendre la ou les causes des *flash crashes* (ou des *mini flash crashes*) et les mécanismes de propagation des chocs parmi différentes catégories d'actifs. Il est probable que ces événements sont imputables à une conjonction de facteurs et que l'automatisation, plutôt que la rapidité des transactions, pourrait avoir joué un rôle [16].

Il est utile de reconnaître que l'automatisation du *trading* induit de nouveaux risques opérationnels [17]. Considérons tout d'abord la croissance du *trading* algorithmique. Plusieurs événements récents montrent que des erreurs dans l'élaboration de ces algorithmes peuvent être à l'origine de graves

15 *Par exemple, d'après un article paru dans le Huffington Post, « […]* aujourd'hui, des *mini flash crashes* se produisent tout le temps. Rien que lundi, le titre Google s'est brièvement effondré à la suite du *flash crash* qui a touché l'une des entreprises les plus importantes et les plus grandes du pays. *» (cf. Huffington Post, «* Twitter causes a flash crash, highlighting market's structural problems *», 23 avril 2013). De même, selon Nanex (un fournisseur de données financières), plus de 18 000* mini flash crashes *se sont produits entre 2006 et 2010 sur les marchés d'actions des États-Unis, soit environ 195 par mois (Nanex définit un* flash crash *comme un mouvement de baisse ou de hausse de plus de 0,8 % en moins de 1,5 seconde). Cf.* http ://www.nanex.net/FlashCrashEquities/FlashCrashAnalysisEquities.html

16 *D'autres facteurs pourraient aussi être à l'œuvre, tels que la fragmentation des marchés (cf. Madhavan, 2012) ou des changements au niveau de la source d'apport de liquidité, en particulier la disparition de teneurs de marché désignés.*

17 *Le Comité de Bâle sur le contrôle bancaire (2001) définit le « risque opérationnel » comme « le risque de pertes résultant de l'inadaptation ou de la défaillance de procédures internes, de personnes et de systèmes, ou résultant d'événements extérieurs. »*

défaillances sur les marchés financiers. Par exemple, l'introduction en Bourse de BATS Global Market, le 23 mars 2012, a échoué en raison de problèmes liés à l'algorithme utilisé pour les enchères électroniques [18]. Autre exemple : le 1er août 2012, Knight Capital (une importante société de courtage pour compte propre aux États-Unis jusqu'en 2012) a perdu 440 millions de dollars en 30 minutes à cause d'un algorithme mal conçu, ce qui a entraîné le rachat de Knight par l'un de ses concurrents (GETCO).

Les systèmes d'appariement des plates-formes de *trading* et les flux de données qui diffusent l'information sur les conditions de marché peuvent, eux aussi, connaître des défaillances techniques. Ainsi, le 9 juillet 2015, une défaillance informatique (due au déploiement d'un nouveau logiciel) a provoqué une suspension des transactions pendant deux heures sur le NYSE. L'automatisation pourrait également favoriser la manipulation des marchés, ou les tentatives délibérées de porter atteinte à leur intégrité (à des fins terroristes, par exemple). Ainsi, en avril 2015, un courtier indépendant basé à Londres (Monsieur Navinder Singh Sarao) a été accusé par les autorités américaines d'avoir directement causé un *flash crash* en recourant à une stratégie de *spoofing* (cf. section 2) [19]. Une autre stratégie, le *quote stuffing*, consiste à multiplier délibérément le nombre de messages envoyés à une plate-forme de négociation (soumission d'ordres à cours limité, puis annulation de ces ordres, par exemple), afin de ralentir d'autres *traders* (c'est-à-dire la vitesse à laquelle ils reçoivent les informations provenant du flux de données sur les places de marché [20]).

La course à l'accès rapide aux plates-formes de négociation ou aux données de marché peut aussi induire un risque opérationnel lorsqu'elle conduit des *traders* à contourner les contrôles de sécurité. Ainsi, dans le cadre de la gestion des risques, les *traders* intègrent habituellement dans leurs algorithmes des contrôles automatisés de leurs ordres, afin que l'exposition aux risques ne soit pas excessive. Néanmoins, ces contrôles prennent du temps et ne sont donc pas compatibles avec l'objectif de rapidité poursuivi par les THF. De même, en général, les courtiers imposent des limites de risque automatisées à leurs clients, mais, souvent, les THF contournent ces limites en demandant un « accès direct aux marchés » (*direct market access* – DMA), là encore dans l'objectif de soumettre leurs ordres plus rapidement.

Étant donné l'automatisation et la complexité croissante des marchés financiers, il n'est pas surprenant que des incidents technologiques surviennent parfois, comme dans d'autres secteurs (le transport par exemple). Kumiega, Sterijevski et van Vliet (2016) estiment par conséquent qu'il faudrait s'inspirer de notions venant de l'ingénierie industrielle, telles que la « fiabilité » (estimation de la probabilité d'un incident) pour évaluer le fonctionnement et la fragilité des marchés financiers et suggèrent que, de ce point de vue, ces marchés ne sont pas différents d'autres secteurs (par exemple l'industrie du transport). Il faudrait davantage de travaux empiriques pour confirmer ou infirmer cette conjecture. Concernant les États-Unis, Gao et Mizrach (2015) ont mesuré la fréquence de mouvements intrajournaliers des cours amples mais éphémères (ce qu'ils appellent des « *breakdowns* » ou des « *breakups* ») sur des actions [21]. Ils constatent que la fréquence de ces événements décroît depuis 2000. Ces dernières années, elle est tombée à moins de 1 % par jour de cotation, alors que l'on a l'impression que ces événements sont plus fréquents.

Plusieurs initiatives récentes des pouvoirs publics visent à atténuer les risques opérationnels imputables au *trading* algorithmique (y compris ceux liés au *trading* haute fréquence) et à l'automatisation. Par exemple, conformément au règlement de la SEC sur la conformité et l'intégrité des systèmes de régulation (Regulation SCI) (cf. SEC, 2013), les places de marché et les *traders* qui recourent à des systèmes de négociation informatisés sont tenus « d'élaborer des documents présentant des politiques et des procédures raisonnablement conçues pour veiller à ce que leurs systèmes affichent un niveau de capacité, d'intégrité, de résilience, de disponibilité et de sécurité permettant de préserver leur capacité opérationnelle et de promouvoir le maintien de marchés équitables et ordonnés, et à ce qu'ils

18 *Ironie du sort, BATS est l'opérateur de l'une des plus importantes plates-formes de* trading *électronique aux États-Unis et en Europe.*
19 *L'affaire est pendante. On ne sait pas encore si les ordres passés par M. Sarao correspondaient à une tentative de manipulation, ni s'ils auraient pu avoir déclenché, à eux seuls, le* flash crash *en question (cf. «* Ex-SEC economist to testify on Flash crash *», Financial Times, 22 octobre 2015).*
20 *Cf. Ye, Yao et Gai (2013) à propos du* quote stuffing.
21 *Ils définissent un «* breakdown *» (un «* breakup *») comme une baisse (une hausse) de 10 % du cours d'un titre par rapport à son niveau à 9h35, avec une inversion d'au moins 2,5 % à 15h55.*

fonctionnent comme prévu » (p. 3). Ce règlement impose également aux places et aux *traders* de tester régulièrement leurs systèmes et de mettre en place des plans de continuité de l'activité. En Europe, la directive MiFID II comporte des dispositions qualitativement analogues pour les algorithmes utilisés par les THF. Ainsi, elle imposera à ces derniers de concevoir des systèmes et des contrôles du risque efficaces, et de rendre compte de leurs stratégies algorithmiques aux autorités.

Comme indiqué plus haut, le *flash crash* de mai 2010 et le *Treasury flash crash* se sont accompagnés d'une évaporation soudaine de la liquidité, ce qui pourrait être le signe d'une fragilité due à une évolution de la nature de l'apport de liquidité sur les marchés électroniques. On se demande notamment, si, en période de tensions sur le marché, les teneurs de marché à haute fréquence peuvent apporter une liquidité suffisante, ou s'ils ne risquent pas de se retirer purement et simplement du marché. Là encore, les travaux d'universitaires qui s'intéressent à cette question sont rares, et ils n'étayent pas particulièrement la théorie selon laquelle l'apport de liquidité par les teneurs de marché à haute fréquence est nettement plus fragile que lorsque les teneurs de marché sont des humains. Ainsi, en s'appuyant sur les données du Nasdaq, Brogaard *et al.* (2015) concluent qu'en moyenne, les THF qui composent leur échantillon réalisent des transactions qui vont dans la direction inverse des mouvements de prix extrêmes, que ces mouvements soient permanents (à la suite de l'arrivée d'informations, par exemple) ou transitoires. *A contrario*, les ordres qui n'émanent pas de THF sont corrélés positivement à la direction des mouvements de prix extrêmes. Ces constats suggèrent que le *trading* haute fréquence atténue les mouvements extrêmes, au lieu de les amplifier.

Il se pourrait que la nature de l'apport de liquidité ait évolué ces dernières années. Il est notamment possible qu'il soit moins résilient aux chocs de grande ampleur. Cependant, là encore, cette évolution pourrait avoir de multiples causes et, à ce jour, rien ne prouve que les THF en soient directement responsables. En fait, les banques ont réduit le volume de capitaux qu'elles allouent aux activités de tenue de marché sur différents marchés (en raison de la crise financière et de l'adoption de nouvelles règles, comme la loi Dodd-Frank aux États-Unis). De nouveaux acteurs (tels que les THF et les *hedge funds*) pourraient se substituer aux banques pour l'apport de liquidité, mais, leur capitalisation étant probablement plus modeste, leur capacité à supporter le risque est aussi plus faible. En lui-même, ce changement est susceptible d'entraîner plus fréquemment que par le passé une évaporation soudaine de la liquidité.

Bibliographie

Allen (F.) et Gale (D.) (1994)
« *Financial innovation and risk sharing* », *MIT Press*.

Back (K.) et Baruch (V.) (2004)
« *Information in securities markets: Kyle meets Glosten-Milgrom* », *Econometrica*, n° 72, p. 433-465.

Baron (M.), Brogaard (J.), Hagströmer (B.) et Kirilenko (A.) (2015)
« *Risk and return in high frequency trading* », disponible sur : *http ://dx.doi.org/10.2139/ssrn.2433118*

Ben David (I.), Franzoni (F.) et Moussawi (R.) (2015)
« *Do ETFs increase volatility ?* », *document de travail*, Université de l'Etat de l'Ohio.

Biais (B.) et Foucault (T.) (2014)
« *HFT and Market quality* », *Bankers, Markets and Investors*, janvier-février.

Biais (B.), Foucault (T.) et Moinas (S.) (2015)
« *Equilibrium fast trading* », *Journal of Financial Economics*, n° 116, p. 292-313.

Bond (P.), Edmans (A.) et Goldstein (I.) (2012)
« *The real effects of financial markets* », *Annual Review of Financial Economics*, n° 4, p. 339-360.

Brogaard (J.), Carrion (A.), Moyaert (T.), Riordan (R.), Shkilko (A.) et Sokolov (K.) (2015)
« *Trading fast and slow: colocation and market quality* », *Review of Financial Studies*, à paraître.

Brogaard (J.), Hagströmer (B.), Norden (L.) et Riordan (R.) (2015)
« *High frequency trading and price discovery* », *Review of Financial Studies*, n° 27, p. 2267-2306.

Brogaard (J.), Hendershott (T.) et Riordan (R.) (2014)
« *High frequency trading and extreme price movements* », disponible sur : *https://www.rsm.nl/fileadmin/home/Department_of_Finance__VG5_/LQ2015/Ryan_Riordan.pdf*

Brunnermeier (M.) et Petersen (L. H.) (2005)
« *Predatory trading* », *Journal of Finance*, n° 60, p. 1825-1864.

Budish (E.), Cramton (P.) et Shim (J.) (2015)
« *The high frequency trading arms race: frequent batch auctions as a market design response* », *Quartely Journal of Economics*, n° 130, p. 1547-1621.

Chaboud (A.), Chiquoine (B.), Hjalmarsson (E.) et Vega (C.) (2014)
« *Rise of the machine: algorithmic trading in the foreign exchange market* », *Journal of Finance*, n° 65, p. 2045-2084.

Dugast (J.) (2015)
« *Unscheduled news et market dynamics* », *document de travail*, Banque de France.

Dugast (J.) et Foucault (T.) (2016)
« *Data abundance and asset price informativeness* », disponible sur : *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2398904*

ESMA (2014)
« *High frequency trading activity in EU equity markets* », *Economic Report*, n° 1, p. 1-30.

Fama (E.) et Miller (M.) (1972)
« *The theory of finance* », New York : Holt, Rinehart and Winston.

Fishel (D.) et Ross (D.) (1991)
« *Should the la prohibit manipulation* », *Harvard Law Review*, n° 503.

Foucault (T.), Hombert (J.) et Rosu (I.) (2016)
« *News trading and speed* », *Journal of Finance*, n° 71, p. 335-382.

Foucault (T.), Kozhan (R.) et Tham (W. W.) (2015)
« *Toxic arbitrage* », disponible sur : *http ://dx.doi.org/10.2139/ssrn.2409054*

Foucault (T.), Pagano (M.) et Röell (A.) (2013)
« *Market liquidity: theory, evidence and policy* », Oxford University Press.

Gao (C.) et Mizrach (B.) (2015)
« *Market quality breakdowns in equities markets* », disponible sur : *http ://dx.doi.org/10.2139/ssrn.2153909*

Hagströmer (B.) et Norden (L.) (2013)
« *The diversity of high-frequency* traders », *Journal of Financial Markets*, n° 16, p. 741-770.

Hirschey (N.) (2013)
« *Do high frequency* traders *anticipate buying et selling pressure* », *document de travail*, London Business School.

Hirshleifer (J.) (1971)
« *The private et social value of information et the reward to inventive activity* », *American Economic Review*, n° 61, p. 561-574.

Joint Staff Report (2015)
« The U.S. treasury market » le 15 octobre 2014, disponible sur : *https ://www.treasury.gov/press-center/press-releases/Documents/Joint_Staff_Report_Treasury_10-15-2015.pdf*

Joint Staff Report (2010)
« *Findings regarding the market events of May 6, 2010* », disponible sur : *https ://www.sec.gov/news/studies/2010/marketevents-report.pdf*

Kumiega (A.), Sterjevski (G.) et van Vliet (B.) (2016)
« *Beyond the flash crash: systemic risk, reliability, et high frequency financial Markets* », *document de travail*, Université de l'Illinois.

Madhavan (A.) (2012)
« *Exchange traded funds market structure et the flash crash* », disponible sur : *http ://dx.doi.org/10.2139/ssrn.1932925*

Security Exchange Commission (SEC) (2010)
« *Concept release on equity market structure* ».

SEC (2013)
« *Regulation systems compliance et integrity* ».

SEC (2014)
« *Equity market structure literature review, Part II: high frequency trading* », Staff of the Division of Trading et Markets, p. 1-37.

Van Kervel (V.) et Menkveld (A.) (2015)
« *High-frequency trading around large institutional orders* », *document de travail*, Vrije Universiteit.

Van Kervel (V.) (2015)
« *Competition for order flow with fast et slow traders* », *Review of Financial Studies*, n° 28, p. 2094-2127.

Wall Street Journal (2014)
« *How to define illegal price manipulation ?* », *American Economic Review*, n° 98, p. 274-279.

Weller (B.) (2016)
« *Efficient prices at any cost: does algorithmic trading deter information acquisition ?* », *document de travail*, Université Northwestern.

Yang (L.) et Zhu (H.) (2015)
« *Back-running: seeking et hiding fundamental information in order flows* », *document de travail*, MIT.

Ye (M.), Yao (C.) et Gai (J.) (2013)
« *The externalities of high frequency trading* », *document de travail*, Université de l'Illinois.

Zhang (S.) (2012)
« *Need for speed: an empirical analysis of hard and soft information in a high frequency world* », *document de travail*, Université de Manchester.

La réglementation et l'action des autorités face à ces nouveaux risques

Faire des infrastructures européennes de marché un bastion de la stabilité financière

Yves MERSCH
Membre du Conseil
Banque centrale européenne

*Les infrastructures européennes des marchés financiers ont démontré leur résilience lors des épisodes de volatilité observés sur les marchés, en soutenant la liquidité et la stabilité des marchés financiers en période de crise. La Banque centrale européenne et l'Eurosystème, en coordination avec les régulateurs et les participants de marché ont fait de ces infrastructures européennes de marché un bastion de la stabilité financière. Pour l'avenir, outre l'approfondissement de l'intégration, le développement des infrastructures de marché doit tenir compte des conséquences des innovations technologiques telles que les technologies de registre distribué (*distributed ledger technologies*). Pour relever les défis technologiques et stratégiques auxquels les infrastructures sont confrontées, l'Eurosystème a défini trois grands axes de travail d'ici 2020 : 1) étudier les synergies entre TARGET2 et T2S ; 2) accompagner le développement d'un système paneuropéen de paiements instantanés ; 3) examiner l'harmonisation des dispositifs et des procédures de l'Eurosystème pour la constitution de garanties.*

Les infrastructures européennes de marché, qui comprennent les systèmes de paiement d'importance systémique, les contreparties centrales (CCP) et les systèmes de règlement de titres, ont démontré leur résilience lors des épisodes de volatilité observés sur les marchés financiers, en soutenant la liquidité et la stabilité des marchés financiers en période de crise.

La dernière *Revue de stabilité financière* de la Banque centrale européenne (BCE) [1] a identifié quatre risques majeurs pour la stabilité financière : une inversion brutale des primes de risque à l'échelle mondiale ; de faibles perspectives de rentabilité pour les banques et les assurances dans un contexte de croissance nominale réduite ; des inquiétudes quant à la soutenabilité de la dette dans le secteur public et le secteur privé non financier ; enfin, un risque accru de tensions au sein du secteur bancaire parallèle (*shadow banking*) qui est en rapide expansion.

Si ces aspects sont, à juste titre, au cœur du débat sur la stabilité financière, il convient en outre de souligner qu'en coulisse, la Banque centrale européenne et l'Eurosystème, les législateurs européens et les acteurs du marché ont également contribué à la stabilité financière en faisant des infrastructures de marchés financiers européens un bastion de la stabilité financière. Cependant, malgré les avancées réalisées, les infrastructures de marché n'ont pas encore atteint leur situation d'équilibre. Il faut encore renforcer l'intégration et, en particulier, relever les défis posés par les innovations technologiques, comme les technologies de registre distribué (*distributed ledger technologies* – DLT) et leur utilisation future potentielle dans les services financiers.

Dans ce contexte, cet article traitera des enjeux de la numérisation des services financiers et de l'apparition des DLT. Il présentera également la façon dont l'Eurosystème entend répondre à ces problématiques à l'horizon 2020.

1| L'IMPACT DE LA NUMÉRISATION DES SERVICES FINANCIERS ET DES INNOVATIONS TECHNOLOGIQUES SUR LES INFRASTRUCTURES EUROPÉENNES DE MARCHÉ

Parmi les principaux sujets d'attention pour l'Eurosystème au cours des prochaines années, figureront les innovations technologiques dans les services financiers, notamment les DLT, parce qu'elles auront une influence sur l'évolution des infrastructures de marché.

La numérisation ouvre des opportunités pour des innovations de produits et de services dans le domaine des paiements de la banque de détail. L'an dernier, la création d'un système **paneuropéen** de **paiements instantanés** a occupé une place centrale. Les paiements instantanés sont des solutions électroniques de paiements de détail, disponibles 24 heures sur 24, 365 jours par an. Ce système permet une compensation interbancaire des transactions. Le compte du bénéficiaire est crédité et le payeur reçoit une confirmation dans les secondes qui suivent le paiement, et ce, indépendamment de l'instrument utilisé (virement, prélèvement ou carte de paiement), des mécanismes de compensation sous-jacents (compensation interbancaire bilatérale ou compensation *via* des infrastructures) et de règlement (assortis de garanties ou en temps réel, par exemple).

Le Conseil des paiements de détail en euros (*Euro Retail Payments Board* – ERPB), entité de haut niveau présidée par la Banque centrale européenne (BCE) et créée pour favoriser le développement d'un marché intégré, innovant et concurrentiel pour les paiements de détail en euros dans l'Union européenne (UE), a décidé de créer un **mécanisme de paiements instantanés** (c'est-à-dire un ensemble de règles et de normes techniques permettant d'exécuter des

1 Revue de stabilité financière, *novembre 2015.*

opérations de paiement instantanées). Le Conseil européen des paiements (CEP) doit élaborer, d'ici novembre 2016, un dispositif pour les paiements instantanés en euros s'appuyant sur le virement SEPA (*Single Euro Payments Area*) et le mettre en œuvre d'ici novembre 2017. Dès lors, les prestataires de services de paiement proposeront aux utilisateurs finaux des solutions de paiements instantanés en euros dans toute l'Europe.

En conséquence, d'ici novembre 2017, les infrastructures européennes des marchés financiers devront être prêtes à **compenser** et à **régler** les paiements instantanés à l'échelle de l'Europe. Conformément à l'objectif d'un marché des paiements de détail innovant, intégré et concurrentiel, le secteur de la compensation devrait adopter une approche paneuropéenne pour les paiements instantanés, en permettant aux participants du dispositif d'être en lien avec un autre participant au sein de l'UE. Lorsqu'il existe plusieurs infrastructures de compensation, il suffira que le prestataire de services de paiement participe à une infrastructure pour qu'il soit relié au niveau paneuropéen. À cet égard, les infrastructures devront impérativement adopter des politiques d'accès équitables et ouvertes vis-à-vis des prestataires de services de paiement et des autres infrastructures. Elles devront également garantir une interopérabilité technique et commerciale complète. Enfin, le secteur de la compensation devra s'assurer en mettant en place des mesures appropriées que les risques demeurent limités.

En tant qu'opérateur des infrastructures de marchés, l'Eurosystème soutiendra l'initiative des règlements de paiements instantanés paneuropéens grâce à ses services TARGET2. Les paiements instantanés sont par conséquent l'un des éléments clés de la stratégie de l'Eurosystème à l'horizon 2020, sur laquelle nous reviendrons ultérieurement.

Les **paiements de particulier à particulier (P2P) par téléphone mobile** constituent un autre service innovant qui aura une incidence sur les infrastructures de marché. En 2015, l'ERPB a approuvé l'idée de permettre à quiconque de procéder, en toute sécurité, à un paiement P2P paneuropéen par téléphone mobile. Il a indiqué que les solutions mobiles P2P locales existantes et futures devraient coopérer afin d'assurer une interopérabilité à l'échelle européenne. Les paiements mobiles P2P paneuropéens devraient s'appuyer sur un service de consultation (*standardised proxy lookup* – SPL) rattaché à une base de données capable de relier le numéro de mobile (ou d'autres équivalents, comme l'adresse e-mail) du destinataire du paiement au compte bancaire de destination (c'est-à-dire l'IBAN). Cette mise en correspondance (entre proxy et IBAN) facilitera considérablement les paiements mobiles car les utilisateurs n'auront plus besoin de connaître et d'utiliser l'IBAN du bénéficiaire.

Ce type de services existe déjà au niveau national. L'ERPB a demandé à l'industrie d'élaborer une solution à l'échelle européenne, tâche à laquelle participe actuellement le CEP. Cette solution devra, bien entendu, respecter la législation existante sur la protection des données.

La possibilité de proposer des produits et des services de paiements de détail innovants, conformément à la législation européenne sur les activités que peuvent mettre en œuvre les prestataires de services de paiements non bancaires sujets à la réglementation (les « établissements de paiement » définis dans la Directive sur les services de paiement révisée – DSP2), a permis à de **nouveaux acteurs d'entrer sur le marché**. Il s'agit souvent de *start-up* qui s'appuient sur les nouvelles technologies de l'information appliquées aux services financiers (les entreprises fintechs), ainsi que des entreprises bien établies spécialisées dans les technologies internet (réseaux sociaux ou plates-formes de commerce électronique, les GAFA [2]). Si les premières sont généralement très agiles et capables de tirer parti des nouvelles technologies dès qu'elles apparaissent, les secondes sont très attentives à l'expérience client, exploitent les données des réseaux et disposent des capitaux nécessaires pour acquérir les nouvelles solutions développées par les start-up de la fintech. Dans la plupart des cas, elles ne proposent pas d'autres services bancaires que l'initiation de paiements ou l'accès à des informations sur les comptes, et n'ont donc pas besoin d'un agrément bancaire.

Les entreprises établies proposant des plates-formes basées sur les technologies internet disposent déjà d'une vaste clientèle et considèrent les paiements comme un élément logique qui s'intègre à leur chaîne de valeur. En effet, elles estiment que les méthodes de paiement traditionnelles sont peu conviviales ou

2 *Google, Apple, Facebook, Amazon.*

trop lentes pour le commerce électronique et/ou elles disposent déjà d'un vaste réseau et de la technologie nécessaire pour leur permettre de transmettre de grandes quantités de données entre leurs clients. En outre, elles considèrent généralement leurs services de paiement comme une source secondaire de revenus et n'attendent donc pas nécessairement d'en tirer des bénéfices substantiels, ni même des bénéfices tout court. Bien souvent, elles proposent des services de paiement simplement pour rendre leur activité principale plus attractive.

Même si ces nouveaux prestataires de produits et de services pourraient représenter une menace au niveau des recettes des acteurs de marché traditionnels, ils auront moins d'incidence sur les infrastructures des marchés financiers si la compensation et le règlement des paiements et des opérations sur titres s'effectuent toujours entre les entités établies qui détiennent les comptes.

Les technologies de registre distribué (DLT) pourraient en revanche avoir un impact bien plus important sur les infrastructures de marché dans les années qui viennent. En permettant la vérification des transactions financières de manière décentralisée, elles sont susceptibles de redéfinir les mécanismes de ces transactions. Dans le cas des DLT, le règlement ne s'opère pas *via* une infrastructure centralisée (telle qu'un système de paiement, une contrepartie centrale, un système de règlement-livraison de titres, une chambre de compensation ou un conservateur). Grâce à de solides algorithmes cryptographiques et de vérification, tous les participants d'un réseau DLT disposent d'une copie du registre, lequel peut être géré et mis à jour par de multiples participants.

En sa qualité d'opérateur, de catalyseur du changement et d'autorité de surveillance des systèmes de paiement, l'Eurosystème se doit de réfléchir aux conséquences et aux utilisations éventuelles des DLT.

- Concernant les services d'infrastructure de marché gérés par l'Eurosystème, à savoir TARGET2 et TARGET2-Securities (T2S), des discussions sont en cours dans le cadre de la stratégie de l'Eurosystème à l'horizon 2020.

- Concernant le rôle de catalyseur de l'Eurosystème, des discussions ont déjà commencé avec les participants au marché dans le cadre de la gouvernance T2S (*via* le Comité de pilotage sur l'harmonisation – *Harmonisation Steering Group*). Bien que les travaux n'en soient qu'à leurs prémices, les perspectives d'amélioration en lien avec les nouvelles technologies sont importantes, allant de l'exécution d'opérations de sociétés aux appels de marge automatiques sur comptes de trésorerie.

Compte tenu de son rôle de surveillance, l'Eurosystème doit parvenir à une position commune au regard des évolutions susceptibles d'affecter la continuité des infrastructures encadrées. Il faudra déterminer si les cadres existants peuvent continuer de s'appliquer ou s'ils doivent être adaptés. Par exemple, les travaux en cours dans le domaine des régimes de redressement et de résolution des CCP doivent tenir compte des effets éventuels des DLT. Les avantages potentiels d'un registre décentralisé doivent également être analysés dans le cadre des activités en lien avec la cyber-résilience des services d'infrastructures de marché.

2| La stratégie de l'Eurosystème à l'horizon 2020

Les infrastructures européennes de marché reposent sur une approche collective, pilotée conjointement par les secteurs public et privé, et sont encadrées par une gouvernance robuste. Pour y parvenir, il a fallu à la fois mettre en œuvre une base réglementaire solide et mener des interventions techniques. On trouve à ce titre dans la dernière décennie quelques exemples de cas dans lesquels la création d'infrastructures intégrées de marché pour les paiements et les opérations sur titres a été appuyée par une action réglementaire visant à lever les obstacles et à remédier à la fragmentation européenne. La mise en place d'une gouvernance appropriée associant l'ensemble des acteurs concernés s'est révélée efficiente car elle a permis aux participants au marché de faire progresser l'intégration et l'innovation grâce à leurs réflexions stratégiques.

Dans le domaine des paiements de détail, la création du système SEPA est un exemple de la collaboration complexe aux niveaux réglementaire et technique appuyée par une gouvernance solide. Le projet T2S en est un autre exemple dans le domaine des opérations post-marché.

Tandis que la migration vers T2S se poursuit, l'Eurosystème répond aux besoins d'évolution

permanente des infrastructures de marché en Europe pour s'adapter au rythme de l'évolution des marchés et des progrès technologiques. En particulier, les problématiques posées par la numérisation des services financiers et par les DLT doivent être prises en compte. Pour relever les défis technologiques et stratégiques auxquels les infrastructures sont confrontées, l'Eurosystème a identifié trois priorités qui nécessiteront d'engager des travaux d'ici 2020 [3].

La première est d'**explorer les synergies entre TARGET2 et T2S, pour éventuellement envisager une fusion dans le futur en une plate-forme unique**, l'objectif étant de regrouper les infrastructures de marché pour les systèmes de paiements de montant élevé et le règlement de titres. Ces deux plates-formes disposent de fonctions essentielles pour la stabilité financière en Europe.

La plate-forme TARGET2, utilisée dans toute l'Europe pour le règlement des opérations de paiement de montant élevé en euros, y compris pour les opérations de politique monétaire des banques centrales, contribue à la stabilité financière dans la zone euro en permettant la circulation des capitaux de manière extrêmement rapide et efficiente sur l'ensemble des marchés. Comme les paiements sont réglés en monnaie centrale avec finalité immédiate, les bénéficiaires ne sont exposés à aucun risque de crédit. Le risque de liquidité est également attentivement géré. La plate-forme TARGET2 est régulièrement contrôlée de manière à garantir la continuité de l'activité et ses utilisateurs savent qu'ils peuvent toujours compter sur sa disponibilité, même dans des circonstances exceptionnelles (l'an dernier, sa disponibilité technique a une nouvelle fois enregistré une performance de 100 %).

La plate-forme informatique intégrée T2S, qui procède au règlement en temps réel des opérations sur titres en monnaie centrale dans toute l'Europe, contribue, elle aussi, largement à la stabilité financière en atténuant le risque de survenue d'une crise de liquidité. Elle permet aux banques de gérer plus facilement leurs besoins de collatéral et de liquidité, grâce à l'existence d'un gisement unique de collatéral dans T2S, au lieu de répartir les garanties entre plusieurs systèmes. Les banques peuvent ainsi transférer rapidement et facilement du collatéral partout où il est nécessaire en Europe, et ainsi, équilibrer les déficits sur un marché et les excédents sur un autre, opération auparavant longue et coûteuse. De plus, les normes avancées de résilience, de disponibilité, de continuité de l'activité et de sécurité de cette plate-forme permettent de renforcer la stabilité financière en Europe.

Le regroupement de certaines composantes des infrastructures techniques de TARGET2 et T2S, voire leur fusion en une plate-forme unique, permettra à TARGET2 de bénéficier de certaines caractéristiques sophistiquées de T2S, comme le respect des normes ISO 20022. TARGET2 devait à l'origine migrer vers ISO 20022 en novembre 2017, mais les banques ont demandé que la migration soit différée et intégrée à la stratégie de l'Eurosystème à l'horizon 2020, ce qui permettra de déterminer la méthode et le moment les plus appropriés.

D'un point de vue technique, les utilisateurs bénéficieront des améliorations envisagées pour les infrastructures européennes des marchés financiers, à travers un portail unique qui donnera accès à l'ensemble des services disponibles. De plus, ces améliorations permettront d'accroître encore la résilience du système, ce qui est également bénéfique pour la stabilité financière.

Les utilisateurs profiteront également des avantages découlant de l'amélioration des services proposés par TARGET2. Notamment les mécanismes d'optimisation des besoins de liquidité devraient encore être améliorés, et des outils statistiques pourraient être ajoutés, afin de faciliter le *reporting* réglementaire effectué par les banques.

La deuxième priorité stratégique de l'Eurosystème pour 2020 consiste à examiner les possibilités de nouveaux services qui résulteraient d'une intégration plus poussée de TARGET2 et de T2S. En particulier, l'Eurosystème envisage d'**ajouter les paiements instantanés à la palette de services de TARGET2**, du moins concernant le volet règlement. Nous sommes en train de collecter auprès des participants de marché leurs requêtes fonctionnelles pour le règlement des paiements instantanés et la gestion du risque de crédit sur les différents systèmes. Nous devons également évaluer dans quelle mesure l'adoption d'un modèle de règlement unique dans TARGET2 par tous les

3 *Pour plus de détails sur la vision de l'Eurosystème pour 2020, consulter le site :* https://www.ecb.europa.eu/press/key/date/2015/html/sp151014.en.html

systèmes faciliterait le règlement et la gestion du risque de crédit sur l'ensemble des systèmes.

Troisièmement, il est prévu de se pencher sur l'harmonisation des dispositifs et procédures de l'Eurosystème pour la **constitution du collatéral**. Le modèle de la banque centrale correspondante (MBCC) est un mécanisme transfrontière qui permet à toutes les contreparties de l'Eurosystème d'avoir accès au collatéral, indépendamment du lieu où elles ou leur collatéral se trouvent au sein de la zone euro. Parallèlement au MBCC, les liens entre les dépositaires centraux (*central securities depositories* – CSD) facilitent le transfert transfrontière d'actifs.

À mesure que l'intégration des marchés bancaires et financiers de la zone euro progresse, la demande de dispositifs plus efficients de gestion du collatéral s'accroît. L'Eurosystème cherchera à répondre à cette demande. Il examinera également les avantages d'un système commun de gestion du collatéral, en particulier au regard de la dépendance croissante du marché vis-à-vis du collatéral transfrontière pour les opérations de financement sécurisées et la gestion de la trésorerie.

Pour ces trois domaines d'action, l'Eurosystème continuera de travailler en étroite collaboration avec le marché afin de bénéficier de son savoir et de son expérience et de permettre aux infrastructures de marchés en Europe de répondre parfaitement aux futurs besoins de ses utilisateurs. Cela passe par une gouvernance efficiente. C'est pourquoi le système de gouvernance interne de l'Eurosystème pour les infrastructures de marchés est en cours de rationalisation. Le régime de gouvernance de T2S s'étant révélé performant, il est envisagé de créer un Conseil des infrastructures de marché, qui serait en charge des opérations et des projets concernant les infrastructures de marché de l'Eurosystème. De surcroît, il faut examiner les interactions avec les participants de marché pour s'assurer que les services de l'Eurosystème répondent bien aux besoins du marché.

Dans ses trois fonctions (opérateur, catalyseur du changement et autorité de surveillance des systèmes de paiement), l'Eurosystème contribue non seulement à renforcer l'intégration des marchés financiers, ce qui nous rapproche de l'objectif d'un véritable marché unique en Europe, mais également à renforcer la stabilité financière en mettant en place des infrastructures solides et efficientes pour les marchés européens. Pour l'avenir, l'Eurosystème reste attaché à la réalisation de ces objectifs et cherchera à exploiter les avancées technologiques et l'innovation tout en veillant à la sécurité, à la fiabilité et, *in fine*, à la confiance et à la stabilité.

Au-delà de la technologie : une réglementation et une supervision adéquates à l'ère des fintechs

Andreas R. DOMBRET
Membre du comité exécutif
Banque fédérale d'Allemagne

À l'ère du numérique, les banques ainsi que les régulateurs doivent faire face à la multiplication du nombre d'entreprises impliquées dans les technologies financières, les fintechs. Les autorités de contrôle doivent s'assurer que les règles de supervision qu'elles établissent contribuent à la stabilité financière et visent à traiter de manière équitable (level playing field) *les banques classiques et les nouveaux acteurs. En Allemagne, l'approche réglementaire, basée sur l'analyse des risques, veille à une prise en compte de l'ensemble des risques pertinents émanant des banques traditionnelles et des fintechs. Concurrencés par de nouveaux acteurs, les établissements bancaires traditionnels doivent s'assurer que leur modèle économique demeure rentable. Cet article présente la réglementation des fintechs actuellement en vigueur en Allemagne (le* statu quo*), en mettant en évidence les défis qui se posent aux institutions réglementées ainsi que les risques potentiels susceptibles de se présenter.*

Étant donné la dimension considérable prise par le numérique, la multiplication des entreprises spécialisées dans les technologies financières innovantes, communément appelées « fintechs », soulève des questions au niveau des banques traditionnelles comme au niveau des autorités de réglementation. Ces nouveaux acteurs ont introduit des solutions innovantes dans de nombreux secteurs de la banque et de la finance classiques. Par exemple, l'activité d'octroi de prêt par les banques est complétée par des plates-formes de prêt et de financement basées sur la technologie *peer-to-peer* ou *peer-to-business*. Du conseil en investissement est également proposé par des plates-formes *(social trading platform)* à travers lesquelles les utilisateurs peuvent partager leurs expériences et présenter leurs stratégies en la matière. Les services de paiement bénéficient d'un enrichissement grâce à des applications pratiques, telles que les solutions de paiement mobile ou les portemonnaies électroniques. D'autres services donnent accès à des solutions de financement sur mesure, à des données et à des analyses ainsi qu'à des logiciels financiers.

Même les infrastructures sont concurrencées : par exemple, les crypto-protocoles, qui proposent des transactions quasiment en temps réel et protégées contre la manipulation, pourront en principe être utilisés dans un environnement entièrement décentralisé, sans l'intervention des banques, grâce aux technologies de registre distribué (*distributed ledger technologies* – DLT). Une fois opérationnel, ce dispositif est susceptible de menacer l'activité des fournisseurs actuels d'infrastructures financières pour les opérations sur devises, titres, contrats ou certificats. Toutes ces innovations expliquent le dynamisme de l'évolution des fintechs, même si l'emploi de ce terme recouvre en réalité des activités variées. En 2014, d'après les estimations, les investissements dans les fintechs ont totalisé 12,2 milliards de dollars à l'échelle mondiale (Accenture, 2015). Et selon le portail de statistiques Statista, plus de 250 fintechs sont apparues en l'espace de quelques années en Allemagne.

Pour l'heure, la plupart de ces nouveaux services génèrent *a priori* peu de valeur ajoutée au niveau du secteur financier. Cependant leur taux de croissance significatif et leur caractère disruptif suscitent notre attention. Cette vague d'innovations contraint les banques à réviser leurs stratégies. Du côté des autorités, les considérations de stabilité et de réglementation vis-à-vis des fintechs se renforcent compte tenu du large éventail de risques qu'elles induisent. Ces risques ont communément trait au cyber-risque et aux technologies de l'information (TI), ainsi qu'à la protection des consommateurs, tels que la fraude, la communication d'informations trompeuses ou la vente abusive. De plus, en fonction de leur modèle économique, les fintechs – à l'instar des établissements de crédit – sont elles aussi confrontées à des risques de crédit et de liquidité (EBA, 2015). La première question à se poser est donc relativement simple : notre cadre réglementaire et prudentiel est-il adéquat et permet-il d'encadrer ces nouveaux acteurs innovants, ou bien faut-il l'améliorer, voire le repenser entièrement, à l'ère de la nouvelle vague de la finance numérique ?

Le débat actuel sur l'encadrement des fintechs est encore peu structuré, en partie en raison du flou entourant le concept même. En général, le grand public et les médias perçoivent ce secteur comme initiant des attaques concertées à l'encontre du secteur bancaire traditionnel. De plus, les activités nouvelles telles que le prêt *peer-to-peer* et le *crowfunding* (ou financement participatif), les services de paiement mobile, les conseils en investissement automatisés et les DLT sont souvent décrites comme des solutions bancaires et financières novatrices qui ne sauraient relever de la réglementation existante. La description qui est faite de ce secteur influence la perception des fintechs par le grand public. Or, cette description est trompeuse car elle présente, à tort, les fintechs comme un groupe homogène d'entités à caractère disruptif, qui viennent concurrencer les banques traditionnelles ou d'autres intermédiaires établis de longue date (gestionnaires d'actifs, assureurs, etc.). Cependant, même si, dans certains cas extrêmes, les fintechs pourraient théoriquement susciter des perturbations dans les services financiers, la plupart de ces *start-ups* ne cherchent pas à contrôler l'ensemble de la chaîne de valeur des prêts, des paiements ou des commissions bancaires, mais à améliorer des services spécifiques. Hormis leur appellation « fintech », ces sociétés financières innovantes qui s'appuient sur les TI n'ont pas de modèle économique commun ni de base économique commune. C'est pourquoi il faut adopter une approche différenciée vis-à-vis des fintechs et de leurs implications en termes de réglementation et de stabilité.

Les objectifs de politique publique sont une deuxième source de confusion en ce qui concerne la réponse à apporter sur le plan de la réglementation. Certains soulignent que le secteur des fintechs est potentiellement instable, ou que les règles du jeu ne sont pas égales pour tous les acteurs financiers. D'autres, au contraire, affirment que les fintechs pourraient avoir des effets bénéfiques considérables et qu'il faut par conséquent une réglementation propice à l'innovation et aux nouveaux opérateurs. Les pouvoirs publics se préoccupent de différents aspects, en particulier de la réglementation microprudentielle, de la supervision macroprudentielle, de la protection des consommateurs, et aussi du soutien à l'innovation. Il pourrait néanmoins en résulter une définition erronée des responsabilités en matière de réglementation et de surveillance. Afin de déterminer quels aspects du secteur financier numérique devraient être encadrés, cet article présente la réglementation actuelle des fintechs en Allemagne (le *statu quo*) comme un exemple d'approche réglementaire neutre sur un plan technologique (section 1). Il évalue ensuite les menaces qui pèsent sur les établissements réglementés (section 2), avant d'analyser les futurs risques potentiels (section 3). Enfin, la section 4 synthétise toutes ces observations.

1| Le *statu quo* : la réglementation actuelle encadre-t-elle suffisamment les fintechs ?

Étant donné que les fintechs sont présentées et se considèrent elles-mêmes comme des concurrentes des banques, on pense généralement, à tort, que leurs innovations passent le plus souvent à travers les mailles du filet réglementaire. En réalité, si l'on se penche sur le cas de l'Allemagne [1], on constate que, dans ce pays, la logique actuelle de la réglementation financière s'applique de manière équivalente à toutes les entreprises innovantes qui mettent à profit les TI. La principale raison est que la réglementation s'appuie rigoureusement sur le type de risque et sur une définition des activités financières qui permet d'appliquer une codification basée sur le principe « même activité, même risque, mêmes règles ». Les aspects techniques ne rentrent pas en ligne de compte lorsqu'il s'agit de définir les autorisations et les responsabilités. En Allemagne, les nouvelles entreprises du secteur financier sont soit considérées comme des établissements de crédit, des prestataires de services financiers ou des prestataires de services de paiement, soit ils ne sont pas encadrés. Par exemple, il se peut qu'une plate-forme de financement participatif, comme n'importe quelle autre fintech, doive obtenir une autorisation d'activité, pour diverses raisons, mais, en général, elle n'est pas considérée comme un établissement de crédit si elle n'accepte pas de dépôts de particuliers ou d'autres fonds remboursables, et si elle n'accorde pas de prêts pour compte propre. Le raisonnement est cohérent avec l'orientation du risque puisque ce sont les investisseurs qui supportent le risque de crédit. La classification dans la catégorie des prestataires de services de paiement ou de services financiers doit être évaluée séparément, compte tenu des différents risques financiers en jeu. En Allemagne, le règlement des transactions monétaires qui transitent par des plates-formes est effectué par un établissement de crédit réglementé, c'est-à-dire que la réglementation couvre tous les risques. En principe, il faut évaluer les innovations au cas par cas. La même logique s'applique aux monnaies virtuelles telles que le bitcoin : les monnaies virtuelles étant considérées comme des instruments financiers en Allemagne, leur utilisation doit être approuvée par les autorités financières.

Ce survol de la réglementation allemande montre que, si une fintech reste non encadrée, c'est parce que l'on ne peut pas, à juste titre, la considérer comme un établissement financier et non parce que les autorités ne la prennent pas en compte. Et inversement, toute fintech qui cherche à échapper à une réglementation justifiée s'exposera à des poursuites. La réglementation financière prend systématiquement en compte tous les risques pertinents d'un établissement financier. L'activité bancaire sans recours aux banques – *via* un intermédiaire financier proposant tous les services d'une banque sans être considéré comme une banque par les autorités de surveillance – n'est donc pas conciliable avec la réglementation financière existante.

1 *D'autres pays européens recourent à d'autres définitions.*

Pour analyser les autres objectifs politiques relatifs aux fintechs, il faut partir de la réglementation financière existante, en tant que cadre systématique qui s'applique également à toute entreprise reposant sur les TI. L'objectif du *« level playing field »* a une implication évidente. Divers critères permettent de déterminer si l'on est en présence d'une concurrence loyale ou non. À la lumière de ce qui précède, l'égalité de traitement d'entités dont les activités sont équivalentes doit être envisagée dans une réglementation tenant compte du risque. Ce qui peut, bien sûr, inciter les nouveaux acteurs peu familiers avec la réglementation à se concentrer sur les segments du secteur bancaire qui ne sont pas encadrés, sachant que les acteurs déjà en place ont une chance égale d'opérer sur ces segments. Cependant, il pourrait être pertinent pour les autorités de contrôler les opérations que les établissements encadrés effectuent sur les segments non réglementés. Par exemple, les risques non financiers associés aux innovations peuvent nuire à la viabilité d'une banque, ce qui légitime des contrôles ciblés. Aussi, j'ai la conviction que la prise en compte du risque doit être prioritaire dans la hiérarchie des objectifs de réglementation. D'ailleurs, c'est certainement ce qui incite les autorités de réglementation à prêter attention aux nouvelles menaces que les entreprises non régulées peuvent faire peser sur la stabilité financière.

Il existe également un enjeu politique. En effet, on espère souvent que, grâce à des améliorations qualitatives, les entreprises numériques innovantes constitueront une source de croissance économique supplémentaire. En effet les innovations visent généralement à faciliter les opérations bancaires, à accroître l'efficience, à cibler des segments bancaires hier non rentables et à intensifier la concurrence. Les pouvoirs publics réfléchissent donc à la mise en place d'un environnement réglementaire propice à l'innovation. La stratégie numérique européenne compte plusieurs initiatives qui vont dans cette direction en cherchant à encourager l'innovation numérique dans toute l'Union européenne. Certains pays ont lancé des programmes spécifiques pour favoriser la croissance des fintechs, dans l'optique d'accroître, au niveau national, une concurrence encore faible. Néanmoins, en Allemagne, ces préoccupations sont secondaires car la concurrence est déjà vive sur le marché bancaire, et la réglementation axée sur les perspectives de risque. Le mandat de stabilité financière suppose de la neutralité vis-à-vis des innovations financières, à condition que celles-ci n'induisent pas de nouveaux risques ou n'exacerbent pas les risques systémiques existants. De nouveaux mandats des autorités de réglementation et de surveillance qui ont pour effet de promouvoir les services innovants pourraient générer dans ce cas des conflits d'intérêts. Étant donné la nécessité de choisir entre le soutien à l'innovation et une réglementation et une supervision tenant suffisamment compte du risque, il est impératif de mettre en place des garde-fous institutionnels pour que la réglementation et la supervision restent la priorité absolue. Une séparation institutionnelle entre la fonction de supervision et le soutien à l'innovation est appropriée. De plus, étant donné qu'ils pourraient amplifier les effets secondaires naissants, les instruments de soutien doivent être soigneusement sélectionnés. Comme pour les innovations financières antérieures, nous pouvons escompter des gains d'efficience et des avantages potentiels, en termes d'accroissement du portefeuille clients, sans pour autant être en mesure de prévoir toutes les conséquences délétères, les effets secondaires et l'instabilité dont pourraient s'accompagner les changements socio-financiers dûs à la numérisation.

2| Quelles menaces pour le secteur encadré ?

L'objectif de stabilité financière appelle à maintenir le cadre réglementaire actuel, mais des questions se posent en ce qui concerne à la fois la supervision microprudentielle et la surveillance macroprudentielle. À l'heure de la transformation technologique et sociale, le principe sur lequel repose la supervision microprudentielle n'est pas celui d'une composition sectorielle rigide. Au contraire, il faut permettre aux forces du marché de proposer de meilleures solutions. Il convient de s'attacher non pas à préserver le *statu quo*, mais l'adaptabilité des établissements financiers dont l'activité est vitale pour le secteur financier et pour l'architecture financière (Dombret, 2015a). Pour ce faire, les autorités de surveillance doivent s'assurer de la capacité des établissements encadrés à transformer leurs activités et, *in fine*, leur profil de solvabilité et de risque de liquidité.

La capacité à s'adapter étant étroitement liée au potentiel de profit futur, la rentabilité devrait donc constituer un important indicateur de l'adaptation des banques à la transformation numérique. À l'évidence, les entreprises innovantes ont un impact considérable sur les stratégies des banques. Si les fintechs – terme qui désignera ici tous les nouveaux acteurs non régulés – accentuent les contraintes qui pèsent sur les modèles économiques des banques, il est toutefois difficile de savoir dans quelle direction va le marché. L'un des atouts économiques incontestables des fintechs est leur capacité à « écrémer » les services lucratifs en ciblant les segments les plus rentables de la chaîne de valeur du secteur bancaire. Les innovations qui s'appuient sur les TI permettent de proposer des solutions pratiques aux clients et d'abaisser les coûts en automatisant les processus. De surcroît, la spécialisation dans certains services aboutit souvent à une organisation moins complexe et à des hiérarchies horizontales, ce qui, à son tour, facilite l'innovation. Alors que ces stratégies favorisent la désagrégation des chaînes de valeur, d'autres favorisent les services proposés par un seul et unique prestataire. Il en découle des économies d'échelle, une notoriété, des synergies entre services et une meilleure connaissance de la réglementation. En résumé, les innovations qui reposent sur les TI promettent davantage qu'un jeu à somme nulle entre les nouveaux acteurs et les banques classiques : certaines innovations ciblent des segments du marché qui n'avaient pas encore été exploités, tels que les prêts reposant sur le *big data* destinés à des catégories démographiques qui, hier, étaient difficiles à coter, ou des services supplémentaires pratiques. De leur côté, les banques établies de longue date peuvent découvrir de nouvelles activités rentables et, grâce aux TI innovantes, réduire leurs coûts de fonctionnement et améliorer leur gestion du risque. Bien que la liste ci-dessus ne soit pas exhaustive, elle montre que le changement technologique va donner naissance à un paysage diversifié, dans lequel des établissements de crédit, des sociétés d'investissement, des services de paiement traditionnels et novateurs et des fintechs non régulées, pourront se faire concurrence et coopérer les uns avec les autres.

Les services innovants qui ciblent l'ensemble de la chaîne de valeur des prêts, des paiements et des commissions bancaires représentent un tout autre défi. Le point commun de la plupart de ces nouveaux concepts est un effet de réseau, qui peut donner naissance à des structures de marché monopolistiques. En s'appuyant sur l'infrastructure internet et les *smartphones*, une entreprise suffisamment grande peut tirer profit des faibles coûts unitaires et des fortes synergies découlant, par exemple, de la vente croisée et du *big data*. On considère généralement les géants actuels des TI comme des envahisseurs particulièrement performants. Cependant, pour les raisons citées plus haut, aucun établissement financier intégré n'échappera à la réglementation et aux contrôles. L'avantage concurrentiel des nouveaux acteurs réside dans leur avance technologique, et non dans leur capacité à exploiter un vide réglementaire. Les banques classiques doivent rester attentives aux répercussions potentielles sur leur rentabilité à long terme.

Non seulement le numérique influe sur la rentabilité du modèle économique des banques, mais il induit également des risques opérationnels spécifiques au sein des établissements. L'impératif de continuité de l'activité et de fiabilité des services engendre une pression sur le processus de transformation des TI. De surcroît, les services et les processus qui reposent sur les TI ne sont pas à l'abri d'une erreur à l'instar des êtres humains. La confidentialité, l'intégrité et la disponibilité des données s'avèreront de plus en plus cruciales, et de nouvelles formes de risque opérationnel, telles que la manipulation d'algorithmes, pourraient apparaître. La manipulation d'algorithmes est un exemple de risque contre-intuitif. Même si l'on considère que les applications informatiques améliorent la transparence des opérations bancaires et permettent de traiter tous les clients de la même façon, les algorithmes pourraient faciliter la manipulation de résultats ou produire des biais inattendus. Il est probable que ces problèmes ne se limiteront pas à certains établissements. Face à la montée des cyber-risques, une coopération nationale et internationale s'impose entre les banques, ainsi qu'entre les autorités de régulation et de supervision. Cette catégorie de risques englobe aussi les risques liés aux réseaux basés sur les TI. Les attaquants cherchent à profiter de la possibilité d'accéder à des cibles dans le monde entier, de leur propre capacité à apprendre rapidement, et même de la division du travail. Il incombe aux établissements financiers de contrer ces menaces grandissantes en prenant des initiatives à même de renforcer la connaissance mutuelle et de préserver leur réputation.

3| Menaces non couvertes par la régulation et la supervision actuellement en vigueur

Les autorités de régulation et de supervision disposent actuellement d'instruments et de pouvoirs pour gérer les risques qui découlent de l'émergence d'activités bancaires reposant sur les TI. Pour que ce cadre soit efficace, il faut que les nouveaux objectifs de la réglementation correspondent aux règles existantes, faute de quoi on risque de dissocier artificiellement des problématiques connexes, tout particulièrement si l'on considère qu'en principe, les banques pourraient elles-mêmes fournir les services proposés par les fintechs. Appliquer un traitement réglementaire spécifique aux fintechs pourrait conduire à une distorsion de l'égalité des règles et affaiblir les forces du marché.

Afin de préserver la stabilité financière, les superviseurs doivent suivre de près les évolutions de l'ensemble du système financier. On ne peut pas faire confiance aux marchés pour internaliser les risques systémiques qui résultent des externalités. Ces problématiques ont joué un rôle important lors de la dernière crise financière. Nous avons notamment compris qu'il n'était pas possible de se contenter de combler les lacunes de la réglementation dont certains ont profité. C'est pourquoi il faudra surveiller étroitement les risques systémiques potentiels liés aux innovations technologiques (Dombret, 2015b). Néanmoins, étant donné la diversité des fintechs, il semble difficile de dresser la liste complète de ces risques. En ce qui concerne le financement participatif *(crowd funding)* et les prêts participatifs *(crowd lending)* par exemple, si des mécanismes de contrôle efficaces ne sont pas mis en place, l'asymétrie des informations relatives à la solvabilité des acteurs pourra générer un aléa moral sur les plates-formes non réglementées, à l'instar des modèles *« originate-to-distribute »* pendant la crise. La protection des consommateurs pourrait devenir cruciale étant donné que nombre d'innovations sont déployées au niveau de l'interface client. Le Comité mixte des autorités européennes de surveillance (2015) a notamment analysé les risques afférents au conseil en investissement automatisé, que l'on appelle souvent les « robots-conseillers ». Cette innovation bancaire, qui a suscité une attention considérable, part du principe que, même dans un monde très informatisé, l'accès des consommateurs à l'information et leur capacité à traiter cette information sont généralement limités. Le Comité a pointé les risques liés aux failles dans le fonctionnement de ce type d'outil, ainsi que les risques découlant du recours massif au conseil automatisé. Par exemple, les problèmes relatifs à la protection des consommateurs indiquent que les outils de conseil automatisé peuvent indirectement nuire à la stabilité du secteur financier. Les banques ne sont pas les seules à pouvoir proposer les services de robots-conseillers, mais ces outils eux-mêmes peuvent – dans certaines circonstances, qui dépendent du modèle économique – échapper à la régulation. Pour protéger les consommateurs, il faut donc s'intéresser à ces problèmes naissants.

Compte tenu du large éventail de produits et de modèles économiques innovants en cours d'introduction dans le secteur financier, une stratégie de priorisation est requise. La régulation ne saurait reposer uniquement sur la théorie. Toute innovation peut induire des effets secondaires critiques, mais, du point de vue de la stabilité financière, il est nécessaire de déterminer si un nouveau produit ou une nouvelle activité est susceptible de gagner suffisamment en importance pour influer sur l'ensemble du système, plus particulièrement en matière de risque de financement, de liquidité et de crédit, ainsi qu'en terme de complexité et de transparence. Le suivi des effets des innovations peut se voir comme un compromis qui autorise l'expérimentation tout en permettant de parer immédiatement aux menaces. Néanmoins, ce suivi devrait aussi cibler, en amont, les innovations qui pourraient entraîner des effets disruptifs sur des segments entiers d'activité, même si, pour l'instant, elles semblent peu significatives.

Face à ces problèmes naissants, les autorités de contrôle prudentiel devront trouver les réponses adéquates, qui peuvent consister soit à adapter et à améliorer la réglementation financière applicable aux nouveaux modèles économiques, soit à créer une nouvelle sphère de réglementation. Pour s'assurer de la cohérence du cadre réglementaire, les interventions devront reposer sur une évaluation approfondie du risque et respecter le principe « même activité, même risque, mêmes règles ». Par exemple, le problème de la confidentialité des données relatives aux consommateurs ne concerne pas uniquement les établissements financiers. C'est pourquoi l'Europe

cherche actuellement à définir des normes harmonisées, applicables à l'ensemble de l'économie, afin d'empêcher des attaques ciblées qui porteraient atteinte à la confidentialité des données. Il faudrait éviter de réglementer différemment des activités présentant le même risque.

4| Éviter les pièges de la réglementation

Malgré la vitesse impressionnante avec laquelle les acteurs innovants et les nouvelles technologies pénètrent dans le secteur financier, la réglementation ne devrait pas chercher à opérer une séparation artificielle entre les fintechs, d'un côté, et la banque traditionnelle, de l'autre. Une telle dichotomie ne serait ni pertinente ni appropriée au regard de la réglementation actuelle et de la composition du secteur : bien qu'il puisse exister de bonnes raisons de promouvoir un environnement propice à l'innovation pour les fintechs, ces considérations doivent être prises en compte indépendamment des objectifs de supervision et de régulation. De plus, des mandats différents pourraient exposer les superviseurs à un risque de conflit d'intérêts.

Nombre d'idées innovantes en sont encore au stade du développement et n'ont en conséquence que peu d'impact, sachant que leurs effets secondaires et les risques qu'elles pourraient induire n'ont pas encore été clairement identifiés. Du point de vue de la stabilité financière, les fintechs ne requièrent pas un traitement particulier, mais une réponse bien structurée. C'est aussi pourquoi on recommande aux régulateurs d'adopter une position neutre vis-à-vis de la transformation du secteur. Les banques, ainsi que leurs superviseurs, doivent s'assurer de la capacité du secteur à s'adapter rapidement aux innovations, afin que l'offre bancaire soit parfaitement cohérente.

Par ailleurs, compte tenu des risques naissants, la future réglementation devra s'appuyer sur le cadre réglementaire existant, qui s'appuie sur l'analyse du risque, c'est-à-dire en tenant compte du risque et non de la technologie elle-même. C'est la raison pour laquelle, à mon avis, les innovations numériques pourraient induire de nouveaux risques qu'il faudra surveiller dès leur apparition. En effet, malgré la transparence et la neutralité apparentes de la banque informatisée, il se peut que les activités numériques, à l'intérieur et à l'extérieur des établissements régulés, continuent de pâtir de l'asymétrie d'information et d'incitations inappropriées, ainsi que d'autres risques susceptibles de devenir systémiques s'ils surviennent de plus en plus fréquemment. D'une manière générale, on considère que l'ensemble apparemment homogène que constituent les fintechs et leurs innovations appelle une réponse plurielle de la part des autorités financières. Qui plus est, si l'on veut que le risque soit correctement pris en compte en ce qui concerne les innovations financières les plus pertinentes et les plus pratiques, cette réponse devra être compatible avec le cadre réglementaire actuel afin de s'assurer du respect du *level playing field*.

Bibliographie

Accenture (2015)
« The Future of Fintech and Banking. Digitally disrupted or reimagined ? », disponible en ligne : *http://fintechinnovationlablondon.co.uk/media/730274/Accenture-The-Future-of-Fintech-and-Banking-digitallydisrupted-or-reima-.pdf*

Autorité bancaire européenne (ABE) (2015)
« Opinion on lending-based crowd funding », disponible en ligne : *https://www.eba.europa.eu/documents/10180/983359/EBA-Op-2015-03+(EBA+Opinion+on+lending+based+Crowdfunding).pdf*

Comité mixte des autorités européennes de surveillance (2015)
« *Joint Committee Discussion Paper on automation in financial advice* », disponible en ligne : *https://www.eba.europa.eu/documents/10180/1299866/JC+2015+080+Discussion+Paper+on+automation+in+financial+advice.pdf*

Dombret (2015a)
« Digital Darwinism and the financial industry – A supervisor's perception », discours au colloque EBS (18/9/2015), disponible en ligne : *http://www.bundesbank.de/Redaktion/EN/Reden/2015/2015_09_18_dombret.html*

Dombret (2015b)
« Banking on big data – Different policy issues? », déclaration lors de la troisième *Frankfurt conference on Financial Market Policy « Digitizing Finance »* (6/11/2015), disponible en ligne : *https://www.bundesbank.de/Redaktion/EN/Reden/2015/2015_11_09_dombret.html*

Statista (2016)
« Zahl der in Deutschland tätigen Fintech-Unternehmen im Jahr 2015 nach Geschäftsbereichen », disponible en ligne : *http://de.statista.com/statistik/daten/studie/436311/umfrage/fintech-unternehmen-in-deutschland-nach-geschaeftsbereichen/*

L’essor des fintechs et leur réglementation

Serge DAROLLES
Professeur
Université Paris-Dauphine

La crise financière de 2008 a engendré une perte de confiance et a conduit à un nouveau panorama du secteur financier. L’essor du phénomène fintech attire les nouvelles générations qui se détournent des acteurs traditionnels. L’adaptation numérique du secteur bancaire et financier au sens large repose sur une évolution vers une plus grande productivité via *de nouveaux outils conduisant à réduire les coûts de distribution. Ces évolutions soulèvent des questions quant à leurs impacts pour les banques, la réaction de ces dernières, les risques encourus avec l’émergence de nouvelles pratiques. Les régulateurs se confrontés à de nouveaux enjeux qui s’articulent autour des problématiques d’équités envers les différents acteurs et de la protection des utilisateurs.*

Le terme « fintech » n'est autre que la contraction des mots « finance » et « technologie ». Il désigne l'ensemble des *start-ups* technologiques qui concurrencent les acteurs traditionnels des secteurs bancaire et financier. La catégorie regroupe des services variés allant des plates-formes de financement participatif aux solutions de paiement mobiles et des outils de gestion de portefeuille en ligne aux transferts d'argent internationaux. Les fintechs attirent autant l'attention des utilisateurs de services bancaires que celle des fonds d'investissement anticipant les évolutions futures du secteur financier. Même les groupes de distribution ou les opérateurs de télécommunication veulent s'appuyer sur leurs réseaux existants pour proposer des services financiers. Toute cette effervescence soulève un certain nombre de questions sur le futur secteur financier qui émergera de la transformation numérique en cours. Quel sera le rôle des banques traditionnelles ? Les fintechs grandiront-elles avec ou sans les banques ? Quels seront les nouveaux risques induits pour les utilisateurs de services bancaires ?

Cet article aborde ces différentes questions avec un focus particulier sur le rôle qu'a joué dans le passé, et que jouera demain, la régulation financière. Nous analysons dans une première partie les raisons du développement des fintechs au sein du secteur financier. Les explications se trouvent à la fois du côté de l'offre, avec la transformation numérique, et du côté de la demande, avec l'apparition de nouvelles pratiques de consommation. La crise financière de 2008 a également joué un rôle clé dans ce phénomène, au travers notamment des nouvelles régulations des acteurs historiques et de la montée en puissance de la défiance des consommateurs envers les banques. Dans une seconde partie, nous analysons les réactions des grands acteurs traditionnels et les différentes stratégies qui s'offrent à eux. Nous voyons comment acteurs historiques et nouveaux entrants créent des liens qui pourraient préfigurer l'organisation industrielle du secteur financier de demain. Enfin, dans une dernière partie, nous abordons les challenges qui se présentent au régulateur et explorons différentes approches pouvant assurer à la fois un traitement équitable des acteurs historiques et des nouveaux entrants, et la protection des utilisateurs de services financiers.

1| L'ÉMERGENCE DES FINTECHS

Cette première section aborde trois thèmes liés aux évolutions récentes des secteurs bancaire et financier. Nous commençons par discuter les effets de la crise financière de 2008, au niveau de la régulation des acteurs historiques mais également sur la confiance des clients envers leurs banques. Puis nous analysons les modifications du comportement des clients des services bancaires. Enfin, nous abordons la transformation numérique, véritable déclencheur du phénomène fintech.

1|1 Crise financière, régulation et confiance

La crise financière de 2008 est à l'origine de nombreux bouleversements au sein de ces secteurs. Le premier d'entre eux est la prise de conscience du risque systémique lié aux activités des grandes institutions financières. Il s'en est suivi le développement de mesures sensées quantifier ce risque[1]. La régulation financière des banques s'est durcie. En particulier, la notion de contribution au risque systémique d'une entité financière a permis d'identifier les institutions financières d'importance systémique (SIFI). Des réserves règlementaires supérieures ont été imposées aux banques par le Comité de Bâle sur le contrôle bancaire (CBCB), cela afin de couvrir ces nouvelles contributions individuelles au risque global. Cette régulation a eu pour effet d'exercer une double pression sur le bilan des banques. Directement, en augmentant les réserves réglementaires, et donc en obligeant les banques à réduire leur activité ; indirectement, en ciblant les banques comme les grands responsables de la crise financière.

À la sortie de la crise financière, de nombreux clients, et notamment ceux des jeunes générations, ont perdu la confiance qu'ils avaient dans les banques. Comment pouvaient-ils continuer à croire en des agents économiques qui avaient provoqué la crise ? Des agents de plus sauvés de la faillite grâce à des injections massives d'argent public. Si les banques ne sont pas capables de gérer les risques qu'elles prennent, il est difficile de suivre leurs conseils ou de leur confier son épargne. Les nouvelles générations

1 *Voir par exemple Benoit (S.), Colliard (J.-E.), Hurlin (C.) et Pérignon (C.) (2016)* : « Where the risks lie: a survey on systemic risk », Review of Finance, *à paraître, pour une revue de la littérature récente sur le risque systémique.*

sont prêtes à se détourner des acteurs traditionnels et n'attendent plus que l'émergence de nouveaux acteurs, n'ayant pas de responsabilité dans la dernière crise et qui proposent une approche innovante des services financiers.

1|2 De la consommation à l'utilisation de services financiers

En plus d'avoir une image dégradée des banques, les jeunes générations ont des habitudes de consommation différentes de celles des générations précédentes. Elles ont grandi avec la notion d'offres dédiées, adaptées à leurs besoins, en opposition totale avec les pratiques de masse proposées par les banques et les acteurs traditionnels du secteur financier. On est passé de la notion de client, qui consomme ce qu'on lui propose, à celle de l'utilisateur de services financiers. Le client traditionnel est passif, il choisit dans un univers fini de produits sur étagère ou de services préétablis. Le nouvel utilisateur est actif, il s'attend à ce qu'on lui donne accès aux outils lui permettant de construire sa solution personnalisée. Prenons l'exemple de la gestion d'actifs. Alors qu'un réseau bancaire propose le même produit d'épargne au maximum de clients afin de réaliser des économies d'échelles, le client devenu utilisateur s'attend à recevoir une offre modulable, adaptée à ses caractéristiques individuelles et à ses objectifs de placement. Seule une interactivité forte, uniquement possible *via* les plates-formes en ligne, peut permettre l'adéquation entre les attentes des utilisateurs et les produits ou services proposés.

Les fintechs ont dès le début ciblé les jeunes générations, habituées à l'interactivité et au sur mesure. Mais cette stratégie n'est pas sans risque. Le niveau moyen des actifs de ces générations est faible comparé au reste de la population, et notamment aux générations les plus âgées qui possèdent des actifs financiers importants. La viabilité économique des nouveaux entrants dépend alors de leur capacité à attirer rapidement suffisamment d'actifs. Deux facteurs importent en effet : le nombre de clients et la taille moyenne des actifs de chaque client. Or, même en attirant de nombreux clients des jeunes générations, les fintechs auront du mal à être rentables tant que les actifs des jeunes générations resteront faibles. Auront-elles alors le temps de croître avec les actifs des jeunes générations pour devenir au final rentables ? Même dans l'affirmative, il n'est pas évident qu'elles puissent garder captive cette clientèle. En vieillissant, les jeunes générations vont faire face à des problématiques d'épargne de plus en plus complexes. Les solutions proposées par les *robo-advisors* (conseil en gestion automatisée) sont basiques et peu adaptées aux situations rencontrées par les clients des fintechs. Une ligne de partage claire se crée entre les *robo-advisors*, adaptés aux clients dont les actifs sont faibles, et qui ont principalement pour objectif d'éviter de payer des frais élevés, et les acteurs traditionnels, dont les clients ont des actifs financiers plus importants qui nécessitent une expertise beaucoup plus poussée. Il n'est pas sûr de voir un jour une fintech rentable si elle perd ses clients au fur et à mesure qu'ils deviennent rentables.

Si les acteurs traditionnels veulent attirer ces clients rentables, il faudra qu'ils évoluent pour offrir le même niveau d'interactivité. En ce sens, les *robo-advisors* d'aujourd'hui symbolisent les innovations qui amèneront les acteurs traditionnels à faire évoluer leur relation client et à proposer de nouvelles approches. Ces offres ne sont encore réservées qu'aux clients des banques privées, mais elles seront dans le futur également offertes à une part plus importante des clients des grands réseaux traditionnels. Ce n'est qu'à ce prix que les grands acteurs pourront survivre au passage consommateur/utilisateur.

1|3 La transformation numérique

La transformation numérique des secteurs bancaire et financier n'est pas un phénomène nouveau. Le *trading* haute fréquence et les stratégies d'arbitrage associées en sont un bon exemple. Il est devenu courant d'analyser sur des périodes de temps très courtes, inférieures à la seconde, l'évolution des prix sur un marché, de construire des stratégies d'arbitrage basées sur des règles statistiques, puis de prendre instantanément des positions afin de parier sur les fluctuations des prix à très court terme. Dans cet exemple, l'aspect important de la transformation numérique est la capacité à traiter une série de tâches répétitives et à enchaîner ces traitements à des vitesses inconnues jusque-là. Les coûts de mise en œuvre sont longtemps restés un frein important à la généralisation de ces approches systématiques. Ils concernent à la fois l'acquisition de l'information et son traitement et ont joué le rôle

de barrière à l'entrée écartant les nouveaux acteurs. De plus, cette première transformation numérique, notamment dans l'industrie de la gestion d'actifs, a uniquement concerné la production et n'a pas touché la distribution. L'acheteur d'une part de fonds d'investissement dans un réseau bancaire continue de recevoir par courrier à une fréquence trimestrielle un rapport standard donnant la performance de son investissement. Ce rapport ne tient compte ni de ses objectifs spécifiques d'investissement (financement de la retraite, placement en vue d'un investissement immobilier), ni des autres investissements qu'il détient dans son portefeuille.

La seconde étape de la transformation numérique, liée à l'éclosion des fintechs, est plus profonde. Elle commence avec la mise à disposition d'outils permettant d'améliorer simultanément l'ensemble de la chaîne de création de valeur. L'évolution récente des solutions informatiques apporte ainsi des solutions à la fois du côté de la production (bases de données, outils d'aide à la décision) et du côté de la distribution (canaux numériques, connaissance des clients, adaptabilité de l'offre aux caractéristiques des clients). Ces évolutions permettent à de nouveaux entrants de trouver leur place dans l'industrie en se développant sur des niches, celles de l'interactivité et du sur mesure recherchées par les nouvelles générations et en proposant des services dont les coûts sont bien plus faibles que ceux facturés par les acteurs historiques.

Dans cette industrie, la relation client a longtemps été considérée comme réservée aux grands réseaux bancaire et financier car le coût d'acquisition client était élevé. Les nouveaux entrants, mais aussi d'autres acteurs non financiers (opérateurs de télécommunication, chaînes de distribution) peuvent s'appuyer sur les évolutions technologiques pour proposer de nouveaux services à une base de clientèle existante ou beaucoup plus facile à créer, car désireuse de services plus que de produits prêts à consommer. Dans la gestion d'actifs, cette seconde transformation numérique touche également simultanément production et distribution. Le gérant utilise de plus en plus le concours d'outils d'analyse de données et de gestion des risques sophistiqués pour créer les produits. Mais c'est surtout au niveau de la distribution cette fois que les évolutions importantes ont lieu. Le nouveau client, l'utilisateur du service, reçoit une offre qui s'adapte à ses attentes. Pour cela, il faut que le distributeur en sache le plus possible sur son client. D'où la généralisation des métriques, informations quantitatives que le distributeur récupère en observant le plus finement possible les comportements de consommation globaux de son client. En inférant statistiquement par exemple son revenu et le montant mensuel de sa consommation, il peut évaluer le montant d'épargne disponible et proposer des stratégies d'investissement adaptées. Ces approches, basées sur l'analyse statistique, trouvent tout leur intérêt dès lors que la base clientèle atteint une taille conséquente. Il est alors possible de projeter le comportement d'un client donné sur les comportements passés des clients identifiés comme appartenant au même groupe. C'est ainsi qu'il est possible de prédire le comportement futur d'un client en fonction de ses caractéristiques et de lui proposer des offres dédiées.

2| Les réactions des acteurs traditionnels

Les acteurs traditionnels ne restent pas sans réaction face à la montée en puissance des fintechs. Leur stratégie digitale peut se résumer en une simple question : faire ou acheter ? Nous discutons dans ce paragraphe ces deux alternatives, puis nous traçons une troisième voie – à mi-chemin entre les deux précédentes, qui pourrait préfigurer une synthèse entre les compétences des acteurs traditionnels dans la gestion du « *core banking system* » (système d'information global de la banque) et l'agilité des nouveaux entrants.

2|1 La difficulté de faire

Nous avons abordé dans le paragraphe précédent la profonde transformation numérique qui touche l'industrie financière. Comme pour les autres industries touchées, l'évolution est conduite par les nouveaux entrants et non par les acteurs historiques. Dans l'industrie financière, les fintechs peuvent profiter de la dette technique portée par les acteurs traditionnels, et les banques notamment. La notion de dette technique est directement reliée à celle de dette financière. La conception d'un système d'information induit des coûts futurs, qui peuvent être assimilés à des intérêts à payer. L'ensemble des coûts induits représente la dette technique. Ainsi,

plus un système devient complexe, ou plus il résulte de mises à niveau successives, plus il porte une dette élevée. Un grand groupe bancaire issu de la fusion de plusieurs banques est un bon exemple. Le système d'information global a dû intégrer différentes composantes existantes. Il raconte l'histoire de la banque et les différentes étapes importantes de sa construction. Il ne sera jamais aussi performant qu'un système d'information global construit pour le périmètre d'affaire actuel de la banque. La gestion d'actifs fournit un autre bon exemple. L'innovation financière a créé des instruments financiers de plus en plus complexes. Elle a nécessité le développement de systèmes d'enregistrement et de contrôle plus sophistiqués. En parallèle, les nouvelles règlementations, de plus en plus contraignantes, ont eu des effets similaires. La plus grande partie des moyens informatiques déployés ces dernières décennies l'ont ainsi été pour faire face à ces deux phénomènes. Les systèmes d'information actuels ressemblent à des mille-feuilles résultant de la mise en production successive de versions évoluant au gré de l'innovation financière et des nouvelles régulations. Cette complexité a constitué pendant un certain temps une barrière à l'entrée, repoussant les nouveaux entrants. Mais tout cela est aujourd'hui remis en cause. Les fintechs ont accès à des solutions techniques innovantes permettant d'intégrer les conséquences de l'innovation financière et de la réglementation dès la conception, à moindre coût. Rien ne semble pouvoir les arrêter. Elles sont en position idéale pour profiter à plein du peu de degrés de liberté offerts aux acteurs historiques par la dette technique accumulée.

Les acteurs historiques réagissent en tentant de faire évoluer non seulement les compétences techniques de leur équipe de développement informatique mais également leur mode d'organisation. La transformation numérique impose ainsi une évolution des méthodes de gestion de projet, avec l'adoption par les directions des systèmes d'information des grands groupes des modes de développement agiles jusque-là employés par les *start-up* technologiques. La connaissance métier reste essentielle, notamment du fait de la complexité règlementaire, mais l'élément critique réside dans la capacité des équipes à développer des outils interactifs et proches des nouveaux usages clients. Les acteurs historiques ont en main tous les éléments pour réussir cette transformation : la connaissance métier, le réseau, l'historique de la pratique des clients, la sécurité des opérations effectuées et les ressources financières. On les imagine donc se lancer dans une déclinaison numérique de la banque classique offrant à leur clientèle une approche différente de l'expérience client, tout en se basant sur l'expérience métier qu'elles possèdent déjà. C'est ce que de nombreux acteurs traditionnels ont tenté de faire avec plus ou moins de succès. Les raisons de leurs difficultés sont nombreuses. Le souci de ne pas cannibaliser l'activité traditionnelle, les échecs des expériences passées ou la difficulté de mobiliser efficacement les équipes internes peuvent expliquer que les acteurs traditionnels sont peu enclins à investir massivement dans la transformation numérique. Les banques ne réussiront dans cette voie que si elles arrivent à motiver leurs équipes internes à adopter de nouvelles méthodes de travail, tout en capitalisant sur leur principale force qui reste la connaissance client. Cette synthèse ne sera pas simple à mettre en œuvre.

2|2 La tentation d'acheter

Que ce soit en termes d'investissement en capital ou de rachat de fintechs, les acteurs traditionnels des secteurs bancaire et financier sont très peu actifs. Les banques sont quasiment absentes du marché de l'investissement en capital, alors même qu'elles prennent régulièrement des participations dans des *start-ups* de manière indirecte *via* des fonds d'investissement en capital. Les quelques exemples d'investissements qui ont eu lieu répondent à des schémas précis. Il s'agit soit de moderniser un service existant de la banque ou d'acquérir une technologie nouvelle, soit de favoriser le développement de la fintech ciblée. En effet, la présence d'une banque au capital permet de rassurer le régulateur et d'obtenir plus facilement l'agrément nécessaire au lancement de l'activité.

Les exemples de rachat d'une fintech par un acteur traditionnel restent encore plus rares. Les banques semblent avoir peur de casser la dynamique de la fintech ou redoutent la difficile fusion avec les équipes internes de développement. Là encore, le principal moteur reste l'acquisition d'une technologie ou d'une équipe permettant de faire évoluer rapidement l'offre de services de l'acteur historique. La fintech adossée à la banque classique devient un moyen de se doter à court terme de nouveaux services et de faire évoluer plus facilement la relation client vers un mode interactif et dédié.

2|3 La synthèse possible

Enfin, une troisième voie de collaboration, spécifique au secteur qui nous intéresse, voit le jour. Pour vendre des services ou des produits financiers, les fintechs ont besoin d'avoir accès à des partenaires qui maîtrisent le « *core banking system* ». Les banques peuvent alors dans ce contexte faire de la prestation de services et vendre en marque blanche leur expertise. Certaines banques ont choisi cette méthode pour créer des liens avec les fintechs. Elles se positionnent sur la prestation de service et l'accompagnement des fintechs sur le cœur de métier bancaire. Ainsi, plusieurs acteurs de paiement s'appuient sur des plates-formes existantes et les plates-formes de distribution de produits d'épargne vendent des solutions construites à partir de produits commercialisés par les banques. En retour, la banque peut observer directement les évolutions de la relation client. En effet, opérer des services pour les fintechs permet de faire évoluer les prestations afin de répondre aux demandes de celles-ci et donc, indirectement, aux demandes des utilisateurs finaux de services bancaires.

Ce type de relation engendre une remise en cause de l'organisation actuelle de la distribution de produits financiers. On peut imaginer de nouveaux modèles de distribution impliquant des fintechs captives ou non. La banque deviendrait une plate-forme de conception de produits, vendus en marque blanche *via* les fintechs, capables de s'ajuster beaucoup plus facilement aux évolutions des attentes des utilisateurs. La filialisation trouve alors tout son sens car elle permet à la plate-forme de sécuriser ses canaux de distribution. Le seul risque du modèle est de voir la fintech, qui a la relation client, devenir plus grosse que la plate-forme concevant les produits financiers. Les établissements financiers ont-ils réellement la capacité de les accompagner dans leur développement ?

3| Le rôle du régulateur

Face aux changements profonds que subissent les secteurs bancaire et financier, le régulateur doit éviter deux écueils. Le premier est de trop protéger les acteurs historiques en érigeant des barrières à l'entrée entravant le développement des nouveaux entrants. Cela irait à l'encontre de l'innovation financière et donc de la compétitivité de la place financière qu'il supervise. Le second est de favoriser au contraire les nouveaux entrants qui n'auraient pas à subir les mêmes contraintes règlementaires que les acteurs historiques. Deux exemples illustrent ce débat. Ils sont donnés par l'identification des clients et concernent les solutions de paiement en ligne et les services d'agrégation de comptes bancaires. Un client peut choisir de nombreux modes de paiement différents. Pour ce qui est de la procédure d'identification, la tendance est clairement en faveur de l'adoption de solutions simplifiées, plus ergonomiques que l'approche classique identifiant/mot de passe. Ces solutions sont alors en rupture avec les solutions d'identification utilisées par les banques, ce qui soulève des questions de sécurité. La même problématique est rencontrée par les services d'agrégation de comptes bancaires. Ces applications ont besoin de récupérer auprès des banques les informations concernant l'activité de leurs clients. Pour cela, le client doit transmette les identifiants relatifs à ses différents comptes à l'agrégateur, qui les utilisera ensuite de manière intensive afin de construire une vue globale de la situation financière du client. Là encore, un problème de sécurité se pose. Le régulateur peut alors émettre des recommandations concernant la sécurité des paiements dématérialisés ou l'accès en ligne aux comptes bancaires, mais ce sont au final les utilisateurs qui décident ou non d'adopter une technologie.

La directive européenne sur l'accès aux données bancaires [2] couvre les nouveaux usages et services innovants positionnés entre la banque et ses clients. Avec cette directive, les nouveaux prestataires de services de paiement sont soumis aux mêmes règles que les autres établissements de paiement. Mais, en contrepartie, les banques sont obligées de fournir à ces prestataires un accès aux informations de leurs clients. Elles ne peuvent plus par exemple empêcher un agrégateur d'accéder aux données d'un de ses clients en déconseillant à ces derniers de donner à un tiers l'autorisation d'accès à leur compte. Le coût de financement des infrastructures nécessaires à cette interconnectivité est une première question. Mais la question cruciale reste celle de la sécurité, car le partage et l'utilisation des identifiants peuvent favoriser les « cyber-attaques ». Un prestataire de paiement attaqué peut involontairement propager

2 *Cf.* Revised Payment Services Directive (2015): « Guidelines on the security of internet payments », European Banking Authority's Guidelines.

l'attaque dont il fait l'objet à toutes les banques de ses clients. Les banques réclament le renforcement des exigences de sécurité envers ces nouveaux acteurs et remettent en cause les systèmes d'authentification proposés. Elles reçoivent en continu des demandes de données à remonter *via* les codes de leurs clients, mais sans savoir si c'est le client ou l'opérateur tiers qui est à l'origine de ces demandes. Une meilleure traçabilité des demandes de connexion constitue clairement une première étape. Mais les banques estiment qu'elle n'est pas suffisante et demandent également l'utilisation de systèmes d'authentification forte. L'opérateur tiers devrait dans ce cas redemander une authentification avant chaque demande auprès de la banque. Un agrégateur de compte qui chaque matin demanderait à son client de s'authentifier de nouveau pour chacun des comptes qu'il possède perdrait cependant tout son intérêt. Ces exemples montrent qu'il ne sera pas aisé pour le régulateur de concilier innovation et sécurité.

3|1 Égalité et concurrence…

Le régulateur a un rôle difficile car ses décisions influencent directement les conditions de la concurrence entre acteurs historiques et nouveaux entrants. Il doit simultanément assurer des conditions identiques à tous les acteurs, promouvoir une place financière innovante et sécurisée, mais également veiller à la compétitivité de la place financière. L'action du régulateur suisse concernant le blanchiment d'argent est une illustration intéressante. Des modifications de l'ordonnance de la FINMA [3] sur le blanchiment d'argent ont été directement imposées par les changements technologiques. Ainsi, de nouvelles dispositions dans cette ordonnance couvrent les activités de paiement en ligne et les procédures d'identification. S'il est désormais possible de s'authentifier en ligne, le régulateur suisse a défini des seuils spécifiques au-dessous desquels aucune identification formelle des clients n'est demandée. C'est un bon exemple de la manière de faire évoluer la réglementation de manière à ne pas bloquer l'utilisation des nouvelles technologies et les nouvelles manières de consommer des services financiers.

Plus généralement, il semble clair qu'au-delà de la réglementation proprement dite, le régulateur doit analyser les incitations reçues par les agents et comment ceux-ci modifient leur comportement en fonction de ces incitations. Il doit également garder une version globale et éviter d'appliquer des réglementations spécifiques à chaque acteur en fonction de la catégorie dans laquelle il se classe. Cela aurait tendance à compartimenter le secteur financier, éviter l'apparition de nouveaux acteurs et décourager l'innovation financière. Les acteurs existants sur un marché seront toujours favorisés si la réglementation maintient hors du marché les nouveaux entrants. Inversement, un régulateur pourrait avoir tendance à maîtriser la régulation des acteurs traditionnels qu'il connaît bien et se montrer plus laxiste vis-à-vis des nouveaux entrants, à l'activité nouvelle, et sans un historique de crises suffisant pour connaître les risques liés à leur activité. Au final, nous pouvons voir combien il est difficile pour le régulateur de trouver le bon équilibre, qui permet à la fois la survie des acteurs existants, le développement de l'innovation apportée par les nouveaux acteurs et au final une saine concurrence au sein de la place financière.

Cependant certains principes généraux peuvent être dégagés. Respecter une totale neutralité vis-à-vis des évolutions technologiques constitue clairement le premier principe. La réglementation doit favoriser une concurrence saine entre les différents acteurs, qu'ils proposent des approches traditionnelles ou, au contraire, qu'ils aient recours à des solutions technologiques nouvelles. Il faut donc veiller à éliminer tous les obstacles qui pourraient limiter le développement des nouveaux entrants. Un deuxième principe est de garder une régulation globale qui couvre l'ensemble des acteurs, plutôt que de traiter séparément les différents types d'acteurs en fonction de leurs caractéristiques, au risque de segmenter artificiellement le marché et, par là, de limiter la concurrence entre les acteurs. Le fait de traiter une transaction de manière traditionnelle ou en ligne ne doit jouer aucun rôle dans la manière dont cette transaction est vue par le régulateur. Seuls les risques liés à la transaction elle-même doivent être pris en compte, non la manière dont elle s'effectue. Enfin, le dernier principe doit rester la protection des utilisateurs du système financier, et du système lui-même. Le régulateur doit agir dans l'intérêt des utilisateurs, il doit assurer leur protection dans un environnement changeant qui

3 *Autorité fédérale de surveillance des marchés financiers (Suisse).*

peut engendrer l'apparition de nouveaux risques que l'utilisateur n'aurait pas su anticiper. Il est clair que respecter les différents principes énoncés plus haut n'est pas une tâche simple, et que privilégier un des principes pourrait aller à l'encontre des autres. Le rôle du régulateur est de trouver le bon équilibre. Par exemple, s'il veut rester neutre vis-à-vis des évolutions technologiques, le régulateur doit bien évaluer les apports de l'innovation financière et identifier dans la régulation actuelle les règles susceptibles de freiner l'innovation. On a discuté dans l'exemple introductif la question de l'authentification. Les technologies permettant de rendre plus simple cette étape sont aujourd'hui très nombreuses, les solutions d'identification variées et les risques associés très différents. Un rejet en bloc de la notion d'identification en ligne pourrait bloquer l'innovation et le développement de solutions nouvelles apportant des réponses aux questions soulevées par les solutions existantes. Permettre l'identification en ligne pour des transactions dont la somme est inférieure à un certain montant permet au contraire de mettre en œuvre les solutions d'identification – et donc à terme de les faire progresser – en limitant le risque de fraude au montant, faible, de la transaction. Ainsi, il est possible de satisfaire à deux des principes énoncés précédemment pourtant difficilement conciliables.

Il semble également difficile de traiter les fintechs, souvent très spécialisées, comme les acteurs traditionnels, beaucoup plus généralistes. Cette fois-ci, une solution pourrait être de créer de nouvelles catégories d'intermédiaires financiers, comportant des exigences moins élevées que celles prévues par la réglementation s'appliquant aux banques. Certaines règles peuvent être allégées sous certaines conditions, par exemple si aucune transformation de liquidité n'a lieu. Le nouvel entrant n'est pas réellement une banque s'il ne met pas en place cette transformation, les clients sont moins en risque et il n'est donc pas nécessaire de lui imposer la même réglementation qu'aux banques.

3|2 …Sans éluder les nouveaux risques

Si le progrès technique offre l'opportunité d'innover, il favorise également l'émergence de nouveaux risques, comme l'illustrent les deux exemples développés ci-dessus. Or, l'objectif principal du régulateur reste la protection des utilisateurs de services financiers et la stabilité du système financier. Nous analysons ici deux aspects qui doivent retenir son attention : la possibilité de « cyber-attaques » et les risques liés à l'externalisation de certaines activités traditionnelles des banques.

Les établissements des secteurs bancaire et financier sont des cibles privilégiées des « cyber-attaques », et le développement d'offres en ligne, se voulant simples et interactives, favorise ces attaques. Dans la pire des situations, on pourrait imaginer une série d'attaques qui mettraient à mal la liquidité des marchés et la solvabilité des intervenants. Pour le régulateur, la difficulté vient de l'évaluation de ces nouveaux risques. Il n'a pas d'historique permettant de définir des scénarios réalistes de risque. Il peut seulement, à partir d'une approche pragmatique, définir des scénarios-types d'attaque, et tester les dispositifs de défense des intervenants numériques à ces attaques. Le peu d'historique et le fait que l'innovation financière ouvre chaque jour la porte à de nouveaux scénarios d'attaque rendent cette tâche difficile. Seule une expertise sur le sujet permettra au régulateur de remplir efficacement sa tâche.

La seconde source de risque vient de l'externalisation de certaines des tâches de la chaîne de traitement des opérations financières. Avant la révolution technologique, il était habituel d'avoir un unique acteur soumis à la régulation. La banque effectuait en interne l'ensemble des tâches de la chaîne de création de valeur. Aujourd'hui, ce n'est souvent plus le cas, à la fois pour les acteurs traditionnels, mais aussi pour les nouveaux entrants. Du côté de la banque classique, la pression sur les coûts l'incite à confier à des prestataires externes une partie de ses tâches traditionnelles, notamment celles liées au traitement informatique des opérations. Elle a du mal à être aussi agile que les nouveaux entrants dans la maîtrise des nouvelles technologies. La tentation est alors grande d'externaliser les tâches à fort contenu technologique vers des acteurs plus agiles et susceptibles de mieux maîtriser les coûts. La chaîne de création de valeur s'en retrouve éparpillée entre la banque régulée et d'autres acteurs potentiellement non soumis à la régulation. Le système de surveillance comporte des trous. De plus, il est difficile d'anticiper comment évoluera la relation entre la banque et le prestataire de service si une crise met à mal la solvabilité de la banque. Le prestataire de service acceptera-t-il alors de continuer à effectuer les traitements informatiques si la banque est en difficulté ? On

voit bien qu'avec l'externalisation, économiquement viable dans les situations courantes, un nouveau risque de coordination apparaît lors des périodes de crise. De manière symétrique, on peut se demander si le défaut d'un prestataire de service ayant une position de monopole ne porterait pas un nouveau risque systémique.

Ces questions touchent aussi les nouveaux entrants. Dans le paragraphe précédent, nous avons vu que beaucoup de fintechs utilisaient les services des acteurs historiques pour le *« core banking system »*. Cela les aide dans certains cas à obtenir les agréments nécessaires au lancement de leur activité. Elles peuvent également se concentrer sur leur valeur ajoutée, la gestion de la relation client, sans avoir à supporter le coût de développement de l'outil de production des services. Ces nouveaux entrants sont ainsi des candidats naturels à l'externalisation. De plus, ils sont apparus dans le monde du collaboratif et du virtuel, et leur tentation sera toujours de chercher les solutions efficaces leur permettant de traiter à moindre coût les parties les moins rémunératrices de la chaîne de création de valeur. Les banques régulées fournissent aujourd'hui les services nécessaires. Mais qu'en sera-t-il demain ?

Pour le régulateur, les conséquences de ces phénomènes d'externalisation sont nombreuses, et la problématique liée à l'innovation technologique touche cette fois autant les acteurs historiques que les nouveaux entrants.

Conclusion

La réaction des grands acteurs traditionnels passe moins par des stratégies de rachat de fintechs que par des collaborations, et l'on voit se dessiner aujourd'hui des partenariats entre acteurs traditionnels et nouveaux entrants. Cela pourrait préfigurer l'organisation future des secteurs bancaire et financier.

Si la transformation numérique recèle un grand potentiel de croissance pour les places financières, il faudra s'assurer que les évolutions nécessaires de la régulation ne freinent pas l'innovation financière, et assurent la stabilité dont toute place financière a besoin pour offrir les services que les clients en attendent.

Le développement des prêts en ligne et la montée de la régulation privée des transactions financières en ligne avec les entreprises

G. Philip RUTLEDGE
Président
Bybel Rutledge LLP, Lemoyne, PA, États-Unis
Professeur invité, droit et régulation des valeurs mobilières
LL.M. Programme, BPP Law School, Londres

La régulation des services bancaires en ligne peut être envisagée à la fois au niveau public et au niveau privé. Le contexte public concerne la régulation au plan national qui a pour objectif premier de veiller à la sécurité et à la fiabilité des systèmes financiers nationaux, ainsi que de s'assurer d'un niveau adéquat de protection pour les consommateurs. Au niveau privé, la régulation s'applique à un établissement financier individuel, et répartit les responsabilités entre l'établissement et ses clients, via *un contrat qui définit les modalités de prestation des services bancaires.*

Tandis que les pouvoirs publics se sont attachés à renforcer les contrôles prudentiels dans le secteur financier réglementé dans le sillage de la récente crise financière, le développement des « fintechs », opérant soit en qualité d'intermédiaires pour l'offre de prêts en ligne, soit en qualité d'organismes de crédit en ligne n'acceptant pas de dépôts, a suscité moins d'attention.

La banque électronique est tenue de satisfaire à un certain nombre d'exigences relatives à la protection des consommateurs. En revanche, la plupart de ces exigences ne s'appliquent pas aux services qu'elle propose aux entreprises et qui constituent l'essentiel des transactions. Même si ces transactions peuvent relever du droit commercial national, nombre des modalités et conditions figurent dans des contrats bancaires. Ces contrats définissent la répartition des responsabilités entre le client et l'établissement financier, tout particulièrement en cas de transactions non autorisées, rendues possibles par des failles dans la sécurité des systèmes bancaires électroniques.

Cet article s'intéresse au développement de la régulation des services bancaires en ligne, au niveau individuel, instaurée par voie contractuelle, et aux divers facteurs qui expliquent cette évolution, notamment l'absence de régulation publique des « fintechs » et la grande diversité des procédures de sécurité mises en oeuvre par les entreprises clientes des établissements financiers.

Cet article traite de la « régulation privée » qui s'applique de plus en plus aux transactions financières réalisées en ligne par des établissements de dépôt, ou par des organismes de crédit qui n'acceptent pas les dépôts, pour le compte de clients professionnels, en particulier pour des petites et moyennes entreprises (PME). La régulation privée désigne ici les modalités contractuelles énoncées dans des conventions qui répartissent les risques entre l'entreprise cliente et l'établissement qui lui fournit des services financiers spécifiques. Nous nous attendons à ce que l'expansion des fintechs accélère la tendance d'un recours croissant à une régulation privée de plus en plus sophistiquée, par voie contractuelle.

Les entreprises de technologies financières (les fintechs) recourent à des algorithmes propriétaires et à des logiciels qui sont en capacité de traiter d'énormes volumes de données pour parvenir aux points de décision pour lesquels la fintech va associer des caractéristiques particulières. Dans le cas des prêts, cette analyse aboutit à un point de décision auquel s'appliquent des caractéristiques de prêts prédéterminées : montant maximum du prêt, échéance, taux d'intérêt, échéancier de remboursement du principal et des intérêts, flexibilité éventuelle des caractéristiques proposées, etc. Toutes les données relatives à l'emprunteur sont collectées *via* une application en ligne ainsi qu'auprès d'autres sources également en ligne, telles que les réseaux sociaux. Le temps nécessaire pour proposer une offre de prêt se mesure ainsi en minutes dans le cas d'une fintech et non en jours.

Une fintech met par exemple en avant que, pour prêter à une PME, il suffit que cette PME ait une ancienneté d'au moins 24 mois, qu'elle réalise un chiffre d'affaires annuel d'au moins 75 000 dollars, qu'elle n'ait pas récemment fait l'objet d'une procédure de faillite, que l'un de ses dirigeants détienne au moins 20 % du capital et qu'un dirigeant affiche un degré de solvabilité personnelle jugé correct. Pour obtenir un prêt ou une ligne de crédit d'un montant inférieur à 100 000 dollars, la PME n'aura pas besoin d'apporter de garantie, de présenter un plan prévisionnel d'activité, de faire inspecter ses locaux, d'être évaluée, ou de produire une police d'assurance-titres (*title insurance* [1]).

Les établissements de dépôt peinent à rivaliser avec le modèle de prêt des fintechs parce que, d'une part leurs procédures d'octroi de prêts ne reposent pas uniquement sur des données en ligne, et, d'autre part elles font l'objet d'un suivi réglementaire plus important. Cependant, nombre des entrepreneurs actuels ont grandi à l'heure d'internet, ce qui les incite à privilégier des établissements de crédit auxquels ils peuvent demander un prêt en ligne, où qu'ils soient (grâce, par exemple, aux technologies mobiles). En fonction de la réponse, qui est quasi instantanée, ils pourront soit accepter l'offre de prêt soit en comparer les modalités à celles proposées par d'autres financeurs. Si certains clients potentiels des fintechs sont sensibles au taux d'intérêt, d'autres peuvent estimer que la rapidité avec laquelle ils obtiendront un prêt et pourront disposer de l'argent pour accélérer leur développement justifie de payer un taux d'intérêt supérieur à celui qu'un établissement de dépôt est susceptible d'appliquer à l'issue d'une procédure plus longue.

Il se peut que certains établissements de dépôt, en particulier les plus grands, ne soient pas organisés pour répondre aux attentes des PME qui ont des besoins de financement plus réduits. C'est ce qui a récemment décidé une banque comme JP MorganChase à financer OnDeck, une plate-forme fintech basée aux États-Unis, pour accorder des prêts dont le montant n'excède pas 250 000 dollars. À propos du projet OnDeck, Jamie Dimon, président-directeur général de JP MorganChase, aurait affirmé : « c'est le genre de choses que nous ne voulons pas faire ou que nous ne pouvons pas faire ». Même si la taille de l'établissement de dépôt peut entrer en ligne de compte (par exemple, JP MorganChase *versus* une banque locale), la réglementation publique peut aussi influer sur les politiques et les procédures de prêt des établissements qui reçoivent des dépôts assurés.

Aux États-Unis, ce type d'établissement est soumis au contrôle d'au moins deux organismes publics distincts. En général, les *State-chartered banks* sont supervisées et contrôlées par le régulateur bancaire de l'État fédéré et par la *Federal Deposit Insurance Corporation* (FDIC). Les banques nationales relèvent, elles, de l'*Office of the Comptroller of the Currency* (une division du département du Trésor américain) et de la FDIC. Beaucoup d'établissements de dépôt dépendent de

1 Title-insurance : *forme d'assurance de responsabilité civile liée à l'immobilier principalement utilisée aux États-Unis.*

holdings bancaires qui sont supervisées et contrôlées par le conseil des gouverneurs du Système de la Réserve fédérale (*Federal Reserve System* – FRB), c'est-à-dire par la banque centrale américaine. Si l'établissement est considéré par le comité fédéral de surveillance de la stabilité financière (*Financial Stability Oversight Committee* – FSOC) comme un établissement financier d'importance systémique (*Significantly Important Financial Institution* – SIFI), il fait l'objet d'une réglementation renforcée. Des représentants des régulateurs publics peuvent être physiquement présents au sein des SIFI pour contrôler la conformité de leurs opérations.

Par définition, les organismes de crédit qui ne reçoivent pas de dépôts ne sont pas des banques et, comme ils ne recourent pas à des dépôts pour financer les prêts qu'ils accordent, ils ne sont pas soumis au même cadre règlementaire que celui qui s'applique aux établissements de crédit classiques. Cependant, en général, leurs prêts aux particuliers relèvent de la législation sur la protection des consommateurs au niveau fédéral et au niveau de l'État fédéré. Cette législation prévoit notamment, dans le cadre de l'information du consommateur, un délai de réflexion, période durant laquelle ce dernier peut renoncer au prêt sans frais, ainsi qu'un plafonnement des taux d'intérêt et des commissions bancaires, l'interdiction de l'obligation de souscrire à d'autres services (services d'évaluation ou assurance-titres, par exemple), et des sanctions en cas de politique de prêt discriminatoire ou prédatrice. Les établissements qui prêtent aux particuliers sans collecte de dépôt peuvent être tenus de s'enregistrer auprès d'un régulateur et peuvent être soumis à un contrôle de leur activité.

Concernant les prêts immobiliers aux ménages, les saisies et les nombreuses procédures collectives et amendes élevées infligées par les autorités à la suite de diverses allégations d'infraction aux règles régissant le marché des *subprime* ont engendré un coût qui pèse sur les comptes de bilan (et sur la valeur des titres) de beaucoup d'établissements de dépôt américains. C'est la raison pour laquelle nombre de ces établissements ont adopté des critères de prêt plus prudents.

Le directeur financier de Wells Fargo, institution financière américaine spécialisée pour les prêts aux grandes entreprises, aux banques et aux gouvernements (*money-centre bank*), l'a reconnu publiquement : interrogé à propos des prêts immobiliers que des organismes qui n'acceptent pas les dépôts accordent aux particuliers, il a déclaré que sa banque n'entendait pas prêter à des emprunteurs présentant un risque élevé, pas même à ceux qui satisfont aux exigences de la *Federal Housing Administration* : « c'est ce type de prêt qui ne pourra pas être remboursé, et ce sont ces défauts de remboursement qui poseront problème dans une dizaine d'années. Il n'est pas question pour nous de refaire la même erreur ». De plus, les nouvelles obligations énoncées dans la loi Dodd-Frank (*Dodd-Frank Wall Street Reform and Consumer Protection Act* de 2010) concernant les prêts immobiliers des ménages, ont incité les institutions financières de dépôt à se recentrer sur les prêts correspondant à la définition d'un « *qualified mortgage* » (prêt admissible), pour lequel on présume que l'emprunteur satisfait à des critères acceptables.

Étant donné que les établissements de dépôt ne souhaitent plus recourir à des pratiques de prêt qui se sont révélées extrêmement coûteuses pour eux, et compte tenu des nouvelles obligations imposées par la loi Dodd-Frank, il n'est pas étonnant de constater une migration des prêts immobiliers octroyés aux ménages, d'institutions financières de dépôts vers des organismes de prêts qui ne reçoivent pas de dépôts. En conséquence, d'après le *Los Angeles Times*, ces organismes ont émis 42 % des prêts hypothécaires en 2014, contre seulement 10 % en 2009, et ils représentent aujourd'hui quatre prêts immobiliers sur dix.

Bien que les prêts aux entreprises ne soient pas aussi encadrés que les prêts aux ménages, les institutions financières de dépôt qui en accordent sont régulièrement contrôlées par les superviseurs bancaires et doivent présenter un niveau de réserves obligatoires en capital suffisant pour absorber les pertes éventuelles constatées sur ces prêts. Ces réserves et les pratiques des établissements de dépôt font l'objet d'une catégorie spécifique dans le cadre du système de notation CAMELS (cotation sur une échelle de 1 à 5) utilisé par les autorités. En général, si la cotation obtenue lors d'un contrôle est supérieure ou égale à 3, le régulateur bancaire compétent demande à l'établissement de prendre des mesures correctives.

Il n'est pas étonnant de constater qu'aux États-Unis, les établissements de dépôt organisent généralement

leurs opérations de prêt en fonction des attentes du superviseur qui contrôle leurs activités. Même dans le cas où un établissement de dépôt obtient une cotation CAMELS de 1 ou de 2, le contrôleur bancaire peut identifier des questions qui requièrent l'attention du conseil d'administration et de la direction exécutive de l'établissement (*Matters Requiring Attention* – MRA). Ces MRA peuvent mettre en cause les procédures et la politique d'octroi de crédit sur laquelle l'établissement de dépôt se fonde pour analyser la solvabilité des emprunteurs et argumenter sa décision d'octroi de prêt aux entreprises.

Par exemple, la fintech citée plus haut a indiqué que, pour prêter moins de 100 000 dollars à une entreprise, elle n'avait pas besoin de disposer du plan prévisionnel d'activité de l'emprunteur potentiel, ni d'une évaluation de ses activités, ni de se rendre sur les lieux. En revanche, si un établissement de dépôt accordait un prêt selon des modalités similaires, le superviseur bancaire pourrait lui reprocher de ne pas avoir exiger le plan prévisionnel d'activité ou une évaluation des activités de l'emprunteur, ou de ne pas avoir rencontré ce dernier. Là encore, la différence tient au fait que, pour financer les prêts qu'il accorde, l'établissement puise, dans une large mesure, dans les dépôts assurés qu'il reçoit.

Le plus souvent, les organismes de crédit qui ne collectent pas de dépôts, et tout particulièrement les fintechs, recourent pour financer les prêts non pas aux déposants mais à des acteurs institutionnels (tels que des fonds communs de placement, des assureurs, des fonds de pension, des *family offices* ou des *money-centre banks* comme JP MorganChase), ainsi qu'à des particuliers ou des investisseurs institutionnels enregistrés, qui sont acheteurs d'instruments de dette, dans le cadre de transactions de placements privés ou d'offres de titres financiers enregistrées auprès de la *Securities and Exchange Commission* (c'est le cas, par exemple de la société de financement participatif Lending Club).

Le recours excessif des établissements de dépôt au financement de marché *via* l'émission de billets de trésorerie ou de titres de dette senior est considéré comme l'une des principales pratiques responsables de la récente crise financière, en particulier lorsque les marchés se sont brusquement désintéressés des instruments de dette à court et à long terme émis par les établissements de dépôt. Pour faire face à cette crise, les autorités de régulation ont alors pris plusieurs décisions : elles ont relevé significativement le niveau des réserves obligatoires, gelé pendant cinq ans le remboursement de certains instruments pouvant être considérés (intégralement ou partiellement) comme des fonds propres réglementaires, imposé le cantonnement (*ring-fencing*) des opérations de détail et encouragé l'utilisation d'instruments de dette automatiquement convertibles en capitaux propres en cas de forte érosion des fonds propres réglementaires ou de dépréciation très importante des titres.

Le renforcement des exigences en fonds propres réglementaires, l'aversion viscérale au risque envers les prêts aux ménages susceptibles d'entraîner à nouveau des amendes et des sanctions importantes (comme lors de la débâcle des *subprime*) et les règles additionnelles imposées aux établissements financiers américains par la loi Dodd-Frank ont pu avoir des effets cumulatifs entraînant une réduction des rendements offerts par les établissements de dépôt aux investisseurs.

Par conséquent, à l'heure où les investisseurs sont en quête de rendements dans un contexte global de taux d'intérêt bas, il n'est pas surprenant qu'ils réallouent leur capital en le transférant des établissements de dépôt vers des organismes qui ne collectent pas les dépôts et qui sont moins encadrés (en particulier les fintechs), ce qui a permis à ces derniers de lever d'importants volumes de fonds. Cependant, le financement des investisseurs institutionnels est souvent considéré comme du capital se déplaçant rapidement (*hot money*). Cette source de financement apparaît donc moins figée que les dépôts des ménages ou des entreprises et peuvent être plus facilement réalloués à d'autres fins, surtout lorsque l'on peut espérer en tirer de meilleurs rendements, pour un niveau de risque jugé équivalent.

En conséquence les inquiétudes des régulateurs en lien avec le brusque tarissement des sources de financement de marché en provenance des établissements de dépôt pourraient refaire surface, en particulier si les organismes de crédit qui ne perçoivent pas de dépôts voyaient disparaître leurs sources de financement institutionnel dans les mêmes proportions et aussi soudainement. Sachant que de plus en plus de ménages et d'entreprises empruntent auprès d'établissements qui ne collectent pas de dépôts, un éventuel « gel » du crédit de la part de ces financeurs pourrait affecter l'économie de manière significative. En effet les établissements de

dépôt pourraient ne pas être en mesure, ou ne pas souhaiter, prendre le relais.

Malgré la tendance notable d'une réallocation des prêts des établissements de dépôt vers des organismes qui ne collectent pas de dépôts, chaque financeur opère de plus en plus dans un environnement en ligne, sachant qu'un nombre important de fintechs opèrent exclusivement dans ce type d'environnement. Les institutions financières de dépôts ainsi que les organismes de financement sans collecte de dépôts qui réalisent des transactions financières pour le compte d'entreprises (pour lesquelles le niveau de réglementation publique est différent de celui qui s'applique aux prêts aux ménages) commencent à recourir à ce que nous appellerons ici la « régulation privée » pour l'offre de services financiers à cette clientèle. Cette régulation privée vise principalement à répartir les risques *via* un contrat conclu entre l'entreprise cliente et l'établissement qui lui fournit des services financiers en ligne spécifiques, que ce soit une insitution financière de dépôts ou bien un organisme de financement sans collecte de dépôts.

Bien que la régulation privée puisse concerner autant les établissements de dépôt que les organismes de crédit qui ne collectent pas les dépôts, le présent article se focalisera sur les établissements de dépôt, étant donné leur volume d'activité et le montant des transactions traitées de manière journalière, en particulier en lien avec les services de gestion de trésorerie destinés aux entreprises de toutes tailles (de la PME à la multinationale). Il étudiera les questions liées à la sécurité des systèmes et des données, aux demandes de transactions autorisées et authentifiées, à la détection et à la prévention des fraudes, ainsi qu'à la responsabilité juridique et à l'indemnisation.

1| Sécurité des systèmes et des données

Les modalités contractuelles relatives à la sécurité des systèmes sont axées, d'une part, sur la sécurité des systèmes informatiques qui permettent au client d'envoyer des instructions à l'établissement financier et, d'autre part, sur la sécurité des processus qui s'appliquent aux personnes autorisées à lancer des transactions en ligne avec l'institution financière. En ce qui concerne les systèmes informatiques, l'établissement financier impose à son client de satisfaire aux exigences minimales énoncées dans le contrat de services, lequel sera périodiquement révisé par l'établissement, et d'adopter des politiques et des procédures pour évaluer ses risques et pour analyser et inspecter ses systèmes chaque année. L'établissement peut également exiger que son client lui communique les résultats de cette évaluation, de cette analyse et de cette inspection.

Concernant les systèmes informatiques, l'établissement financier peut imposer de manière contractuelle au client de mettre en place et d'actualiser des procédures de sécurité spécifiques pour le matériel, les logiciels et la communication. Le client est également tenu d'équiper ses ordinateurs, ses systèmes informatiques et ses réseaux électroniques de dispositifs de sécurité d'un coût raisonnable, destinés à détecter tout acte de malveillance et à empêcher les tentatives de destruction délibérée de programmes, de contenus et d'instructions ou d'autres données électroniques stockées dans leurs systèmes informatiques et sur leurs réseaux électroniques, ou l'introduction de codes ou de programmes informatiques non autorisés.

L'obligation d'utiliser des procédures de sécurité telles que des codes, des noms d'utilisateur, des mots de passe, des numéros d'identification personnels (PIN) ou des jetons de sécurité (« moyens d'accès ») est elle aussi devenue une clause standard des contrats de services que les établissements financiers proposent à leurs clients. Dans ces contrats, les institutions financières imposent que la sécurité de tous les moyens d'accès relève exclusivement de la responsabilité du client, même lorsqu'elles sont mises en place par l'établissement. De plus, ce dernier impose à son client d'élaborer et d'instaurer des politiques et des procédures pour l'émission, la réémission, la modification et la sauvegarde des moyens d'accès, ce qui peut consister à interdire (i) leur partage, (ii) leur stockage dans des navigateurs, (iii) leur utilisation à des fins autres que pour les services fournis au titre du contrat de services et (iv) l'emploi de lettres, de chiffres et de symboles pouvant constituer une protection d'accès à des fins autres que l'accès aux services proposés par l'établissement au titre du contrat de services.

Étant donné le recours croissant par les clients des technologies mobiles pour transmettre leurs instructions, les établissements financiers exigent

qu'ils n'utilisent que des connections Internet sécurisées, qu'ils s'assurent que ces technologies répondent à certaines normes de sécurité (y compris en ce qui concerne le chiffrement) et qu'ils les testent périodiquement pour déceler et éliminer tout virus ou programme malveillant.

Face à la sophistication croissante des méthodes de piratage informatique, les établissements financiers incluent également dans les contrats de services diverses clauses spécifiant qu'ils ne garantissent pas à leur client que les sites Web, les serveurs, les réseaux et autres équipements de communication qui permettent à l'établissement financier, ou à un prestataire tiers, de proposer des services financiers en ligne ne contiennent aucun virus ou programme malveillant.

En outre, les établissements exigent que leurs clients adoptent et mettent en œuvre des politiques, des procédures et des systèmes pour un coût raisonnable, afin que les données soient reçues, stockées, transmises ou détruites de manière à empêcher leur perte, leur vol ou un accès non autorisé. Ces politiques, procédures et systèmes visent, notamment, à protéger les ordinateurs, les dispositifs mobiles, les documents papier et les supports de sauvegarde contre tout accès physique ou électronique non autorisé. Ils se conforment aux règles de destruction, en cas de nécessité, des documents papier ou électroniques, de sorte que les informations contenues dans ces documents ne puissent pas être lues ou reconstituées.

2| Personnes autorisées

Il existe un autre aspect qui compte tout autant que la sécurité des ordinateurs, des systèmes informatiques et des réseaux électroniques des clients : le nombre d'individus qui, chez le client, sont autorisés à envoyer des instructions à un établissement financier pour le compte du client (l'utilisateur autorisé) et le nombre d'individus autorisés par le client à authentifier les instructions envoyées par un utilisateur autorisé à l'établissement financier lorsque soit le client soit l'établissement demande des mesures d'authentification (l'authentificateur). Un client peut désigner différents individus comme étant des utilisateurs autorisés à effectuer différents types de transactions (par exemple des paiements de salaires ou des virements) ou différents niveaux de transaction (par exemple moins de 100 000 dollars ou plus de 100 000 dollars), ou lorsqu'une mesure d'authentification distincte est requise (par exemple pour les virements de l'étranger).

À ce titre, deux points préoccupent particulièrement les institutions financières. Premièrement, la documentation transmise par le client à l'établissement et qui identifie les utilisateurs autorisés et les authentificateurs en précisant leurs niveaux d'autorisation respectifs doit être à jour en permanence. Si un client n'informe pas son établissement financier de la fin (volontaire ou involontaire) de l'autorisation accordée à un utilisateur autorisé ou à un authentificateur, ou encore d'une modification du niveau d'autorisation d'un utilisateur autorisé ou d'un authentificateur, il ouvre une brèche importante dans la sécurité des transactions financières en ligne. En effet, l'établissement n'a pas d'autre moyen de savoir que son client ne considère plus les données d'identification de l'utilisateur autorisé ou de l'authentificateur comme valides pour l'émission d'instructions. Ces changements doivent impérativement être notifiés pour que l'établissement financier puisse effacer de ses systèmes informatiques l'identité d'un utilisateur autorisé ou d'un authentificateur et annuler, modifier ou réémettre des moyens d'accès.

La seconde grande préoccupation tient à l'efficacité de la politique et des procédures internes de sécurité du client qui sont applicables aux moyens d'accès employés par les utilisateurs autorisés et par les authentificateurs. Les établissements financiers craignent en particulier que des procédures de sécurité laxistes du côté du client (par exemple l'enregistrement des noms d'utilisateur, des mots de passe et des numéros d'identification personnels sur un navigateur) permettent trop facilement à un individu non autorisé d'utiliser un moyen d'accès, d'usurper l'identité de l'utilisateur autorisé et d'envoyer une instruction en ligne à l'établissement financier alors que cette instruction n'a pas été validée par le client mais a, pour l'établissement, l'apparence d'une instruction valide émanant du client. Autre risque, un utilisateur autorisé peut se procurer indûment un moyen d'accès auprès d'un collègue et ordonner une transaction financière en ligne pour un objet ou pour un montant pour lesquels il n'a pas reçu l'autorisation requise de la part du client (par exemple un utilisateur autorisé

à traiter des transactions relatives à la paye qui se procure un moyen d'accès auprès de la personne autorisée à régler les fournisseurs et qui ordonne un paiement depuis le client vers l'entreprise de son époux/épouse, sur la base d'une fausse facture).

3| Détection et prévention des fraudes

Les établissements financiers cherchent de plus en plus fermement à imposer à leurs clients, *via* des clauses des contrats de services, une obligation de détecter et de prévenir les fraudes. Non seulement des obligations contractuelles de suivi et de notification sont imposées aux clients, mais le client doit également accepter que, dans certaines circonstances, l'établissement suspende ou mette un terme à un service précis, voire à tous les services couverts par le contrat de services, sans en informer préalablement le client.

Par exemple, un client peut être contraint d'accepter que l'établissement financier prenne toutes les mesures nécessaires et appropriées pour empêcher qu'un quelconque service fourni par l'établissement soit utilisé à des fins de fraude vis-à-vis de l'établissement ou du client. Cette clause permet à l'établissement de suspendre un ou plusieurs services, immédiatement et sans préavis, et pendant la durée jugée nécessaire, ou encore de mettre fin auxdits services dès lors qu'il estime raisonnablement et en toute bonne foi que le client, un utilisateur autorisé, un authentificateur ou un tiers procède, ou tente de procéder, à l'aide de tout service fourni par l'établissement au client, à une transaction susceptible de représenter une fraude vis-à-vis de l'établissement ou du client, ou d'entraîner un préjudice pour l'un ou l'autre, ou d'être illicite là où elle est exécutée.

Lorsqu'un établissement financier suspend la prestation d'un service vis-à-vis d'un client, le client acceptera que l'établissement, à titre de condition préalable à la reprise du service suspendu, exige qu'il produise les informations, la documentation, les assurances ou tout autre élément que l'institution financière jugera appropriés. Dans le « monde réel », l'établissement peut suspendre un service à la suite de la détection d'une transaction non autorisée effectuée par une personne non autorisée avec les moyens d'accès d'un utilisateur autorisé à la faveur d'une faille dans la sécurité informatique interne du client. En pareil cas, l'établissement peut refuser de reprendre le service suspendu tant qu'il n'a pas l'assurance que son client a révisé sa politique et ses procédures internes de sécurité informatique. Pour obtenir cette assurance, il peut demander un audit indépendant de la politique et des procédures internes de sécurité informatique du client, puis vérifier que celui-ci a mis en œuvre toutes les recommandations formulées à l'issue de l'audit.

Les atteintes à la sécurité des données deviennent trop fréquentes ; elles ne concernent plus exclusivement les établissements financiers, mais touchent également d'autres participants aux transactions financières. Les trois éléments les plus importants sont la notification de ces atteintes, la réparation/prévention et la protection/coopération.

Notification. Dans leurs contrats de services, les établissements financiers peuvent imposer au client l'obligation de les informer sous un délai spécifié (par exemple, au plus tard, dans les 24 heures après la découverte) lorsque le client constate ou a des raisons de soupçonner une violation de ses moyens d'accès, ordinateurs, systèmes informatiques ou réseaux électroniques qui a entraîné, ou pourrait entraîner, la destruction, le vol, la manipulation, une fausse qualification, un accès non autorisé ou toute autre menace portant sur la sécurité de ces données, informations ou moyens d'accès. Après la découverte et la notification, le client peut être contraint de prendre toutes les mesures raisonnables, y compris le recours à des experts, afin de déterminer l'étendue de l'atteinte à la sécurité des données et de repérer les transactions concernées qui n'ont pas été autorisées par le client.

Réparation et prévention. Lorsqu'il découvre et notifie une atteinte à la sécurité des données, un client est dans l'obligation d'engager immédiatement des mesures de réparation et d'informer l'établissement financier de l'avancée des travaux. Afin d'éviter un préjudice encore plus grand, le client acceptera, après l'envoi à l'établissement d'une notification d'atteinte à la sécurité des données, que l'établissement puisse suspendre immédiatement, et sans préavis, un ou plusieurs services, voire mettre fin à l'intégralité des services rendus au client. Pour reprendre le service ainsi suspendu, l'établissement pourra exiger que le client lui apporte un degré élevé d'assurance que

la cause de l'atteinte à la sécurité des données a été correctement éliminée.

Protection et coopération. Dans les cas d'atteinte à la sécurité des données, il importe de protéger, par des méthodes d'informatique légale, le matériel ou les programmes qui peuvent avoir été impliqués dans cette atteinte. En particulier, dans la perspective de l'investigation qui sera menée par les autorités ainsi que par le personnel informatique de l'établissement financier, il convient d'isoler, de déconnecter et de protéger le dispositif ou le programme susceptible d'avoir subi une violation. Le client s'engagera également à coopérer pleinement avec les autorités et avec le personnel représentant l'établissement dans le cadre de l'investigation sur les causes de cette atteinte aux données. Il devra pour cela permettre l'accès aux membres du personnel concernés.

4| Responsabilité et indemnisation

Il existe une quatrième méthode permettant à un établissement financier de recourir à la régulation privée pour régir les transactions financières en ligne : l'allocation des risques. Pour ce faire, l'établissement précise les cas dans lesquels le client accepte que l'établissement n'ait aucune responsabilité, ou seulement une responsabilité limitée, ainsi que les circonstances dans lesquelles le client indemnisera l'établissement pour les préjudices qu'il a subis ou pour les frais qu'il a engagés en relation avec les transactions effectuées par l'établissement sur des instructions émanant du client.

Dans la mesure où il existe aux États-Unis une multitude de règles régissant l'allocation des risques relatifs aux consommateurs, nous nous concentrerons ici sur l'allocation des risques applicable aux clients professionnels. De plus, cette allocation des risques n'est généralement en rien contraire aux clauses de responsabilité qui figurent dans le code de commerce unifié (*Uniform Commercial Code*) adopté par la juridiction des États-Unis et qui s'applique aux clients professionnels.

Les quatre principaux cas pour lesquels les clients accepteront que l'établissement financier soit dégagé de toute responsabilité sont en général (i) la négligence commise par le client qui a permis à une personne non autorisée de se procurer les moyens d'accès nécessaires pour envoyer des instructions à l'établissement ; (ii) le manquement du client à se conformer aux règles de sécurité informatique, les réseaux électroniques et Internet ; (iii) la panne ou l'interruption du service par un fournisseur d'accès Internet et (iv) la suspension ou la résiliation d'un service par l'établissement sans préavis, dans les circonstances prévues dans le contrat de services (par exemple, pour prévenir la commission d'une fraude vis-à-vis d'un client ou de l'établissement).

Avec un client professionnel, le problème le plus fréquent est peut-être le cas dans lequel le client permet, par négligence, à une personne d'envoyer au nom du client des instructions à l'établissement financier alors que cette personne n'est ni un utilisateur autorisé ni un utilisateur disposant d'une autorisation pour le niveau de service requis, ou encore qu'il s'agit d'une personne qui, en réalité, n'est pas un utilisateur autorisé mais se fait passer pour tel, en utilisant ou non les moyens d'accès de l'utilisateur autorisé en question. Dans ces circonstances, le client accepte que l'établissement soit dégagé de toute responsabilité pour tout préjudice subi par le client ou pour tout préjudice subi par un tiers à la suite d'une action, de l'inaction, du retard à agir, de la négligence, de la conduite répréhensible ou de l'imprudence du client.

Dans les contrats de services conclus avec des entreprises, l'établissement financier imposera aux clients d'accepter de limiter la responsabilité de l'établissement aux cas dans lesquels ce dernier a pris part à des activités constituant une négligence grave ou une faute délibérée. De plus, le plafond des dommages et intérêts peut être calculé sur la base d'une formule spécifique, de manière à le faire correspondre à la totalité des honoraires payés par le client à l'établissement au titre du contrat de services pendant les douze derniers mois. De surcroît, le client devra renoncer à tout droit au remboursement des honoraires et des frais d'avocat, des honoraires d'experts témoins ou des honoraires d'arbitrage, ainsi qu'à tous dommages et intérêts spéciaux, accessoires, punitifs, exemplaires, compensatoires, multipliés ou consécutifs, indirects ou directs, de tout type, y compris, sans que cette liste soit exhaustive, pour les bénéfices ou les investissements non réalisés

et les opportunités manquées, pour les poursuites engagées à l'encontre du client par ses salariés, agents ou représentants, ou pour toute poursuite engagée par un tiers à l'encontre du client.

Afin de protéger les établissements financiers des poursuites intentées par des tiers qui pourraient avoir subi des préjudices ou supporté des frais du fait des actions ou des omissions d'un établissement pour les services couverts par le contrat de services, le client sera contraint de dégager de toute responsabilité l'établissement financier et ses dirigeants, ses administrateurs, salariés, actionnaires et représentants pour tous préjudices, frais, engagements et coûts résultant (i) de la négligence, de l'erreur ou du manquement du client à observer et à exécuter dûment toutes les modalités et conditions importantes du contrat de services, (ii) d'autres agissements répréhensibles du client (par exemple dans les cas où le client se sert d'un service fourni au titre du contrat de services pour se livrer à une activité illicite) ou (iii) de toute action ou omission de l'établissement financier sur la foi des informations communiquées à l'établissement par le client, sauf s'il est prouvé que les activités de l'établissement constituaient une négligence grave ou une faute délibérée en relation avec la prestation ou la non-prestation des services au bénéfice du client conformément aux modalités et conditions du contrat de services.

5| Obligation de médiation et d'arbitrage

En vertu des clauses d'élection du tribunal d'arbitrage figurant dans les contrats de services, les établissements financiers peuvent imposer au client que les litiges liés à la prestation de services financiers en ligne par l'établissement soient réglés par une procédure de médiation et d'arbitrage. Dans le cas de clients professionnels, le tribunal d'arbitrage retenu sera en général celui qui conviendra à l'établissement.

6| Quelques questions à l'intention des autorités

Cet article se penche sur la thèse selon laquelle les établissements de dépôt proposant aux entreprises des services en ligne de gestion de trésorerie ainsi que les organismes de crédit ne collectant pas de dépôts (qui représentent une part croissante du marché du crédit aux entreprises, et en particulier des prêts aux PME) se servent des dispositions contractuelles comme d'une forme de « régulation privée » pour gérer les transactions financières en ligne avec leurs clients professionnels. Si de plus en plus de transactions sont effectuées dans l'environnement en ligne, on peut s'attendre à ce que cette forme de « régulation privée » instaurée par voie contractuelle se développe et se sophistique davantage.

Il convient dès lors de se demander si une PME doit être traitée de la même manière qu'une grande entreprise et s'il faut lui prêter la même sophistication commerciale, et donc la même aptitude à comprendre ce qu'impliquent toutes les modalités et conditions semblables à celles décrites dans le présent article, et qui occupent une place de plus en plus grande dans les contrats de services financiers en ligne. S'agissant des dispositions de ces contrats prévoyant une obligation d'arbitrage, est-il judicieux d'imposer aux PME un tribunal d'arbitrage qui soit trop contraignant pour elles ?

Compte tenu de ce qui précède, faut-il préconiser l'élaboration, à l'intention des PME, de règles similaires à celles protégeant les consommateurs, sachant que l'on s'attend à ce que les PME soient de plus en plus consommatrices de services financiers en ligne proposés par les établissements de dépôt comme par des organismes de crédit ne collectant pas de dépôts, mais qu'elles ne présentent peut-être pas toujours la sophistication requise pour comprendre que les protections qu'elles tiennent pour acquises en tant que consommateurs individuels ne s'appliquent généralement pas dans le nouvel univers dans lequel elles opèrent désormais ?

La transformation numérique du secteur financier : illustrations

Monnaie et paiements à l'ère numérique : innovations et défis

François VELDE
Économiste senior et conseiller en recherche
Banque fédérale de réserve de Chicago

Les monnaies virtuelles à l'instar du bitcoin sont des protocoles qui permettent de maintenir un consensus parmi les participants quant à la propriété légitime d'actifs. La propriété est transférée en modifiant convenablement le consensus. Dans le domaine monétaire, l'actif n'est qu'une chaîne de transactions dont l'offre est restreinte, car la création de chaînes valides est limitée. Des protocoles similaires, reposant sur diverses méthodes d'établissement d'un consensus, peuvent faciliter le transfert simple ou complexe d'actifs financiers et réduire les coûts de transaction et d'enregistrement, mais cela au prix de changements coûteux. Les registres distribués remplacent la confiance entre les contreparties par l'adhésion au protocole. Les régulateurs devront adapter leurs cadres réglementaires pour s'assurer que les acteurs sur les marchés et dans les systèmes de paiement respectent les règles existantes et ne créent pas de nouveaux risques, mais aussi afin de protéger la confiance dans les nouveaux protocoles.

NB: Les opinions exprimées ici ne représentent pas nécessairement celle de la Banque fédérale de réserve de Chicago ou du Système fédéral de réserve.

L'apparition de monnaies numériques au cours des dernières années a soulevé un certain nombre de questions importantes. Une technologie peu connue, basée sur la cryptographie, est utilisée de façon inattendue et peut potentiellement modifier la manière d'effectuer des paiements. Le présent article examine certaines de ces questions.

Le sujet étant nouveau et complexe, j'utiliserai comme fil conducteur l'exemple le plus marquant d'une monnaie numérique, le système Bitcoin. J'expliquerai d'abord son fonctionnement, puis je soulignerai ses caractéristiques principales, avant de décrire les évolutions qu'il a provoquées et de conclure par ses implications pour la stabilité financière.

1| Le protocole Bitcoin

Il est important de garder à l'esprit que Bitcoin est un protocole, c'est-à-dire un ensemble de règles suivies par les utilisateurs pour envoyer et recevoir des informations sur internet. Toutefois, ces informations sont très structurées et l'objectif du protocole est très spécifique : il s'agit de diffuser des transactions authentifiées. Les bitcoins sont comparables à de la monnaie dans la mesure où ils constituent l'objet de ces transactions.

1|1 Description

Décrivons le protocole [1]. La meilleure façon de procéder est récursive : supposons que *A* est le propriétaire authentifié d'un bitcoin. Comment en transfère-t-il la propriété à *B* ? Ce processus se déroule en plusieurs étapes. Tout d'abord, il convient de noter qu'à chaque personne correspond une adresse, gérée par un « portefeuille », application résidant sur l'ordinateur de la personne et contrôlée par un mot de passe [2]. Pour transférer les fonds à *B*, *A* a uniquement besoin de l'adresse de *B*. Le portefeuille de *A* envoie un message de transaction qui prouve que *A* contrôle effectivement l'adresse de *A* et qui déclare que les fonds sont transférés de *A* à *B*. À ce stade, le message est assez comparable à un chèque ou à un ordre de paiement. Dans l'activité bancaire traditionnelle, l'ordre est envoyé à un payeur (par exemple, une banque) qui l'exécute. Dans le monde décentralisé des bitcoins, il n'y a pas de payeur. En effet, l'ordre est envoyé à l'ensemble des autres participants, indiquant « veuillez accepter le fait que *B* est désormais le propriétaire de ce bitcoin ». C'est la deuxième étape : le message de transaction est diffusé au réseau de participants, ou nœuds, dans le protocole. Les nœuds reçoivent des transactions d'autres nœuds et les transmettent après avoir vérifié le respect de certaines règles, notamment que chaque personne effectuant une dépense est le propriétaire valide des fonds. Pour ce faire, ils vérifient que *A* était le récepteur d'une transaction précédente enregistrée dans la liste de toutes les transactions valides, la « chaîne de blocs ».

À ce moment, le paiement de *A* à *B* n'est pas encore valide. Pour le devenir, il devra être authentifié en étant inclus dans la chaîne de blocs. Bitcoin est un système décentralisé : il n'existe donc pas de dépositaire de la liste. Chaque participant peut obtenir une copie de la liste et la modifier, mais il doit suivre les règles du protocole. C'est la troisième étape. Les nœuds du réseau qui désirent ajouter des éléments à la liste (nous verrons bientôt pour quelle raison) rassemblent des transactions récemment diffusées dans un bloc et commencent à « miner », c'est-à-dire à résoudre un problème numérique. Le problème comporte une formule (appelée algorithme de hachage) qui combine des textes d'une longueur arbitraire et produit une chaîne de caractères et de chiffres de longueur fixe (256 bits). Il est relativement facile de calculer la formule mais il est pratiquement impossible de l'inverser, c'est-à-dire de trouver les entrées qui produiront une sortie donnée. Le problème numérique consiste à trouver un nombre (à usage unique appelé le *nonce*) qui produira, en combinaison avec le dernier bloc de la chaîne de blocs et le bloc proposé, une chaîne commençant par *N* zéros. Le seul moyen d'y parvenir consiste à essayer de façon aléatoire différentes valeurs du *nonce*, jusqu'à ce que la chaîne qui en résulte respecte les exigences : ce processus nécessite de la puissance informatique. Plus *N* est

1 *Cf. Antonopoulos (A.) (2014) :* « Mastering bitcoin : unlocking digital cryptocurrencies », *O'Reilly Media, pour un compte rendu précis sur le plan technique mais d'une lecture aisée.*

2 *Au sens strict, A connaît une clé privée à partir de laquelle son adresse a été générée. Avec cette clé privée, A peut générer des « signatures », produits d'une fonction mathématique. La fonction est conçue de telle sorte que n'importe qui, sans connaître la clé privée, peut vérifier que la signature a été générée par la même clé privée que l'adresse. La signature sert donc de preuve publique que A connaît la clé privée : la propriété correspond à la connaissance d'une clé privée.*

élevé, plus il est difficile de le trouver, ou plus il faut de puissance informatique : c'est pour cette raison que *N* est appelé la difficulté.

Le premier mineur qui trouve un *nonce* diffuse son bloc sur le réseau, avec le *nonce*. Les autres nœuds calculent facilement la formule avec le *nonce* proposé et ajoutent le bloc à la chaîne de blocs. Le *nonce* sert à prouver que les mineurs ont fait des efforts pour résoudre le problème (« preuve de travail »). Mais pourquoi y ont-ils consacré ces efforts ? Parce qu'ils ont le droit d'inclure dans le bloc une transaction spéciale (appelée *coinbase*), sans que personne n'effectue de dépense, et qui leur accorde un montant spécifique : en d'autres termes, une récompense qui crée de nouveaux bitcoins et les attribue au mineur chanceux. Ce processus inciterait évidemment de nouveaux mineurs à rejoindre le réseau. Mais la difficulté est périodiquement ajustée par le protocole, sous forme d'une fonction de la durée nécessaire pour résoudre les 2 016 blocs précédents, afin de maintenir un taux moyen de six nouveaux blocs à l'heure [3]. Quant à la récompense, elle diminue de moitié tous les 210 000 blocs, tous les quatre ans environ (elle est actuellement de 25 bitcoins et devrait diminuer de moitié à l'été 2016).

Le minage étant décentralisé, la chaîne de blocs n'est pas une simple ligne droite. Il est possible que deux mineurs trouvent une solution de façon presque simultanée et ne soient pas informés de la réussite de l'autre. Par conséquent, il peut y avoir deux blocs valides servant de point de terminaison de la chaîne de blocs : une partie du réseau essaiera d'ajouter à un bloc tandis que le reste tentera d'ajouter à l'autre. Le protocole impose que la chaîne de blocs la plus longue soit toujours acceptée comme la chaîne légitime. Le problème des branches est généralement résolu assez rapidement, car il est peu probable qu'une autre coïncidence d'un bloc valide à chaque point de terminaison se reproduise. Une branche sera rapidement plus courte que l'autre et sera donc ignorée.

Cependant, ce mode de fonctionnement induit le principal risque du protocole, qui est bien connu. Une transaction peut être inclue comme valide dans un bloc qui est ensuite rejeté. Les risques d'être rejeté diminuent rapidement à mesure que les blocs sont ajoutés et ils sont nuls après six nouveaux blocs. Mais un mineur malintentionné pourrait essayer d'effectuer une « double dépense » en incluant volontairement une transaction dans un bloc valide et en créant ensuite une autre branche comprenant une seconde transaction à partir des mêmes fonds. Pour y parvenir, le mineur doit miner plus vite que le reste du réseau, ce qui serait possible, en moyenne, s'il dispose de plus de 50 % de la puissance de minage [4].

1|2 Caractéristiques du protocole

Nous pouvons maintenant comprendre comment la chaîne de blocs est validée. Dans le protocole Bitcoin, il s'agit d'une combinaison de la règle du consensus (la chaîne la plus longue est la chaîne légitime) et de la preuve de travail (un bloc valide inclut la preuve que du travail lui a été consacré). Le seul moyen d'altérer la chaîne de blocs consiste à proposer une chaîne valide plus longue, ce qui nécessite des efforts. Par ailleurs, plus on remonte dans le passé (plus on s'enfonce dans la chaîne), plus il est coûteux de créer une autre chaîne plus longue, puisqu'entre-temps le réseau ajoute constamment des blocs.

Le minage crée l'incitation à fournir le travail nécessaire à l'authentification ; celle-ci constitue sa propre récompense et il est moins coûteux d'être honnête que de tricher. Le minage régule également l'offre de bitcoins. Les bitcoins sont produits par le minage à un rythme qui diminue de façon géométrique au fil du temps, de telle sorte que la somme totale des bitcoins converge vers un nombre fixe.

Quel est l'objet de valeur dans le protocole Bitcoin ? C'est une séquence de transactions valides, démarrant d'une *coinbase* et finissant par son propriétaire actuel. D'une certaine façon, cela est comparable à un cadastre, mais les entrées dans la chaîne de blocs ne lient pas le propriétaire à un objet de valeur comme la terre, elles sont elles-mêmes l'objet de valeur.

3 *Le rythme d'un bloc toutes les dix minutes est seulement une moyenne ; la durée nécessaire pour miner un bloc est un processus de Poisson et peut ne pas prendre plus de quelques secondes. Les chances d'un individu de miner le bloc sont proportionnelles à sa part de la puissance informatique totale utilisée à miner.*

4 *Techniquement, il a besoin de moins de 50 % s'il s'abstient de diffuser ses blocs minés jusqu'à ce qu'il ait construit une chaîne plus longue que le reste du réseau.*

Elles sont similaires aux entrées sur le grand livre d'une banque centrale, sauf qu'il n'y a pas de banque centrale. Les bitcoins constituent une monnaie potentielle parce qu'ils sont artificiellement rares et, par leur conception même, faciles à transférer [5].

Mais, à la différence des monnaies précédentes, elle n'a pas d'autre utilisation (comme les métaux précieux), pas d'approbation du gouvernement (comme le cours légal) et ne représente pas l'engagement d'une entité (comme un billet de banque). Il convient d'ailleurs de souligner que le terme « minage » risque d'entraîner des analogies incorrectes. Le bitcoin n'est pas une monnaie basée sur une matière première comme l'or. Le minage fait référence aux ressources consacrées à assurer la sécurité du protocole, qui sont analogues aux ressources consacrées aux dispositifs anti-contrefaçon et aux camions blindés afin de garantir la sécurité des espèces. L'analogie appropriée pour une monnaie basée sur l'or serait la dépense pour affiner l'or et le transformer en pièces, certifiant ainsi son authenticité. Si l'or cesse d'être utilisé comme monnaie, le contenu des pièces peut être fondu et converti à d'autres usages. Un tel actif physique n'existe pas pour le bitcoin.

Le bitcoin peut être vu comme un droit : je possède les bitcoins si je connais le mot de passe d'un portefeuille dont l'adresse apparaît sur la chaîne de blocs comme étant autorisée à transférer ces fonds. Mais il s'agit d'un droit, non pas à l'égard d'une entité unique, mais envers l'ensemble des participants : en utilisant le même protocole que moi, ils sont prêts à accepter mon choix concernant le prochain propriétaire du droit. En d'autres termes, un bitcoin est la capacité à transférer un bitcoin. Ce droit n'a évidemment de valeur que s'il y a des participants pour le reconnaître ; mais à cet égard, le bitcoin n'est pas différent des monnaies fiduciaires qui, même soutenues par l'État, n'ont de valeur que si les autres leur en accordent.

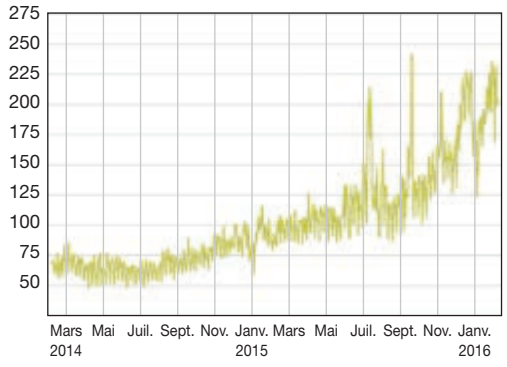
Le bitcoin n'élimine donc pas le besoin de confiance, mais il la place ailleurs : *A* et *B* ne doivent pas avoir confiance l'un en l'autre (ou en l'État) pour réaliser une transaction, mais ils doivent faire confiance au protocole.

1|3 Le bitcoin à l'heure actuelle

Indéniablement sophistiqué, le protocole Bitcoin a également démontré qu'il était viable, au sens strict où il est échangé et a une valeur. Lancé en 2009, il a été remarqué début 2013 et n'a cessé de faire parler de lui depuis lors. Il est difficile d'estimer le nombre d'utilisateurs, puisque chacun d'entre eux peut avoir un nombre indéterminé d'adresses, mais ils sont certainement des centaines de milliers voire quelques millions. Le nombre de transactions a régulièrement augmenté au fil du temps, passant de quelques-unes par heure à deux par seconde : c'est beaucoup pour une expérience informatique, mais inférieur de trois ordres de grandeur à la carte Visa (cf. graphique 1). Le taux de change dollar/BTC, qui a stagné en dessous de 10 dollars les premières années et a approché 1 000 dollars en novembre 2013, se situe au-dessus de 200 dollars depuis plus de deux ans et ressort actuellement (février 2016) à 380 dollars environ. À ce prix, les 15 millions de bitcoins existants représentent une valeur totale de 5 milliards dollars, ce qui est certes beaucoup pour une expérience, mais inférieur de quatre ordres de grandeur aux monnaies fiduciaires dans le monde. Par ailleurs, si une chose a de la valeur, elle vaut la peine d'être volée ; pourtant, le protocole Bitcoin a jusqu'à présent bien résisté au piratage. Il a également préservé sa suprématie par rapport à des centaines de concurrents et d'imitations [6].

Graphique 1
Nombre de transactions Bitcoin par jour

(en milliers)



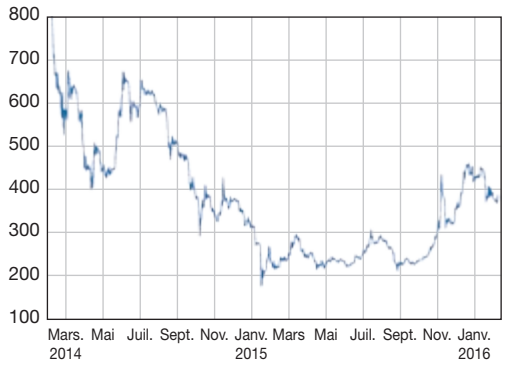
Source : blockchain.info.

5 *Ils sont également fongibles : deux bitcoins quelconques sont traités de façon identique et deux sommes quelconques peuvent être combinées. Cependant, ce n'est pas nécessairement le cas : les utilisateurs pourraient traiter différemment des pièces ayant des histoires différentes (c'est l'idée qui sous-tend les « pièces colorées »).*

6 *Cf. les capitalisations de marché de différentes monnaies fondées sur la cryptographie à l'adresse suivante :* http://coinmarketcap.com/all/views/all/

Graphique 2
Valeur d'un bitcoin

(en dollars)



Source : blockchain.info.

Le bitcoin n'est pas encore une monnaie au sens habituel d'un moyen d'échange généralement accepté. Cela s'explique en partie par l'instabilité de sa valeur. Le graphique 2 montre le prix du bitcoin en dollars au cours des deux années écoulées. Sa volatilité reste considérable : à 36 %, elle est plus forte que celle des matières premières ou des monnaies les plus instables. Jusqu'à présent, l'utilisation des bitcoins pour des achats de détail reste limitée, et une grande partie de l'activité est de nature spéculative. Les commerçants qui acceptent les bitcoins ne fixent pas les prix en bitcoins et convertissent en général immédiatement leurs recettes dans leur monnaie locale, laissant aux investisseurs la détention de cette monnaie. Cette situation se prolongera tant que le prix des bitcoins restera aussi volatil que par le passé : je veux bien accepter une monnaie en échange de biens parce que je compte l'échanger plus tard contre des biens, et je ne le ferai que si je peux me fier à sa valeur.

Le bitcoin a également eu sa part de mauvaise publicité liée à la faillite d'une plate-forme d'échange importante, *Mount Gox*, et à son utilisation par les participants au site illégal *Silk Road*, qui a fait l'objet d'un contrôle réglementaire. Mais il convient de distinguer la faillite d'un opérateur particulier de la performance du protocole lui-même, de même que la faillite d'un établissement financier n'invalide pas, en lui-même, une monnaie. Le protocole garantit un mécanisme de transactions, mais c'est aux utilisateurs de gérer leurs portefeuilles et de sauvegarder leurs mots de passe. Quant à l'utilisation du bitcoin pour des activités illégales, c'est un faux débat. Les espèces sont également propices aux activités illégales, et même plus propices à certains égards. Après tout, la chaîne de blocs garde un enregistrement de toutes les transactions. Il est vrai que les portefeuilles ne sont pas nécessairement liés à des identités physiques, mais s'ils le sont, ils peuvent fournir des preuves accablantes, comme l'ont montré les poursuites dans le cadre de l'affaire *Silk Road*.

1|4 Qu'envisager ensuite ? L'avenir de Bitcoin

L'avenir de Bitcoin reste une question ouverte. Il est peu probable qu'il puisse remplacer une des principales monnaies, ou même qu'il entre sérieusement en concurrence avec elles, mais il a démontré sa viabilité et son utilité [7]. Il est confronté à un certain nombre de défis, même si aucun ne semble insurmontable.

Si l'utilisation des bitcoins se généralise, la flexibilité deviendra une préoccupation. Le nombre de transactions par seconde a doublé au cours de l'année écoulée, mais la taille du bloc est limitée à 1 MB dans le protocole actuel, ce qui représente sept transactions par seconde. L'augmentation de la taille du bloc ne pose pas de difficulté technique majeure, mais soulève la question plus générale : comment les modifications sont-elles apportées au protocole Bitcoin ?

Le système Bitcoin est celui dont se servent les utilisateurs de bitcoins ; ils l'utilisent parce qu'ils y trouvent leur intérêt. Le protocole est une source ouverte (*open source*) : n'appartenant à personne, il est géré par un petit nombre de programmeurs qui cherchent à maintenir le consensus parmi les utilisateurs, mais il n'existe pas de mécanisme formel pour établir un consensus sur le consensus. Les propositions en vue d'augmenter la taille du bloc ont suscité de nombreux débats au sein de la

7 *Ali (R.), Clews (R.) et Southgate (J.) (2014) :* « The economics of digital currencies », Quarterly Bulletin, *Banque d'Angleterre, vol. 54, n° 3, p. 276-286.*
Banque centrale européenne (2015) : « Virtual currency schemes: a further analysis », *février.*
Banque des règlements internationaux, Comité sur les paiements et les infrastructures de marché (2015) : « Digital currencies », *novembre.*

communauté, soulevant le risque d'un *hard fork*, c'est-à-dire d'une scission dans la communauté des utilisateurs [8].

Plus généralement, tout élément du protocole pourrait être modifié (notamment, par exemple, la limite de la création de bitcoins), au risque de faire disparaître cette monnaie. Les bitcoins ont survécu à la concurrence extérieure, qui a essentiellement tenté d'améliorer le protocole de base, mais ils pourraient succomber à des schismes internes. Si Bitcoin continue de se développer, les tensions relatives à sa nature et à son objet augmenteront, de même que la nécessité de trouver un moyen de les résoudre.

À part ces aspects relatifs à la gouvernance, une autre question a trait à la concentration du minage. À mesure que la taille de la chaîne de blocs a augmenté, la vision initiale (légèrement utopiste) de Bitcoin comme un réseau de pairs a été remplacée, de façon peut-être inévitable, par un monde dans lequel les nœuds légers profitent du travail des nœuds lourds qui vérifient les transactions proposées et les diffusent : le minage devient une activité extrêmement spécialisée. En effet, les dernières années ont vu l'apparition de circuits intégrés propres à une application (ASIC), puces uniquement conçues pour gérer l'algorithme de hachage de Bitcoin. Le minage représente une activité importante, essentiellement localisée à l'heure actuelle en Chine, caractérisée par d'importants coûts fixes (conception des puces et fabrication des ordinateurs) et par des coûts marginaux entièrement dépendants du prix de l'électricité. Les caractéristiques du protocole (y compris la taille des blocs) favorisent-elles la concentration ? La question reste ouverte. Un mineur soucieux de ses intérêts ne voudrait sans doute pas devenir trop important, puisqu'une concentration excessive ouvre la possibilité de doubles dépenses, ébranle la confiance dans le protocole et ruine l'investissement du mineur. Mais un mineur mal intentionné pourrait avoir la motivation et (dans le cas d'acteurs gouvernementaux) les ressources pour obtenir une large part du marché.

Finalement, à mesure que les bitcoins ne sont plus seulement une expérience en matière de cryptographie mais deviennent des actifs transférables dotés d'une valeur réelle, ils entrent inévitablement en contact avec la législation, puisque le transfert de valeurs est un domaine fortement réglementé et cela de multiples manières. En tant que moyen de transfert de valeur, le bitcoin est confronté à une quantité de réglementations conçues pour éviter le financement d'activités illégales. En tant qu'actif transférable, le bitcoin relève de réglementations conçues pour promouvoir l'équité sur les marchés d'actifs. En tant qu'actif facile à détenir mais risqué (avec une valeur fluctuante), il devient un sujet de préoccupation à la fois pour les organismes de protection des consommateurs et pour les organismes chargés de réguler les entités essentielles pour l'économie et très sensibles aux actifs risqués, à savoir les institutions financières et notamment les banques. Je reviendrai à la question de la réglementation plus tard.

Si Bitcoin est confronté à des défis, il est également source de difficultés. Le fait que les bitcoins puissent facilement être transférés sur internet les transforme en moyens de paiement privilégiés, notamment pour les transferts transfrontières. Bien sûr, le protocole ne fournit qu'un volet d'une transaction : *A* transfère des bitcoins à *B*, mais ce que *A* reçoit de *B* est extérieur au protocole, et il peut s'agir de biens, de services ou d'une devise. L'utilisation de bitcoins dans un transfert transfrontière exige que *A* échange sa monnaie locale contre des bitcoins et que *B* échange des bitcoins contre sa monnaie locale. Le potentiel des monnaies numériques présente néanmoins une menace pour le système financier en place, y compris les banques (et, peut-être, les banques centrales). L'évolution dépendra en partie de la réponse des régulateurs, puisque les banques sont fondées à se plaindre du fait que l'avantage concurrentiel des monnaies numériques découle partiellement de leur non soumission aux coûts de mise en conformité. Cela dépend également des caractéristiques des monnaies numériques considérées comme intéressantes : le fait qu'elles contournent le système financier existant ou plutôt la commodité de l'utilisation par internet, une caractéristique que les banques (et les banques centrales) pourraient reproduire en émettant leurs propres monnaies numériques.

8 *Dans un* soft fork, *le nouveau protocole restreint les blocs qu'il accepte, mais si 51 % des mineurs passent au nouveau protocole, il dépassera naturellement toute chaîne qui suit l'ancien protocole, dont les suiveurs reconnaissent les blocs générés par le nouveau protocole. Dans un* hard fork, *le nouveau protocole accepte des blocs que l'ancien protocole n'accepte pas, donc une chaîne continuera à suivre l'ancien protocole à moins que 100 % des mineurs ne changent. L'augmentation de la taille du bloc entraînerait l'acceptation de blocs qui n'étaient pas acceptés auparavant.*

2| Au-delà des monnaies virtuelles

Bitcoin a été une expérience réussie, qui a permis de valider la possibilité d'une monnaie numérique décentralisée. Il l'a fait en combinant différents éléments existants de la technologie cryptographique dans un ensemble cohérent. Le succès de Bitcoin a attiré l'attention sur ces éléments, dont certains pourraient être choisis pour des utilisations liées aux monnaies numériques, tout en en étant distinctes.

2|1 Contrats intelligents

Rappelons que les bitcoins se basent sur des séquences de transactions authentifiées. On peut penser au bitcoin comme à une chaîne de transactions authentifiées se terminant par le propriétaire actuel, qui a la capacité de prolonger cette chaîne en y ajoutant une transaction supplémentaire. D'un point de vue technologique, les transactions qui forment les liens dans cette chaîne sont des éléments de code, des instructions exécutées par des applications qui mettent en œuvre le protocole. Certaines de ces instructions sont conditionnelles : par exemple, la transaction ne sera valide que si elle est signée par la clé privée du propriétaire actuel. Des déclarations conditionnelles plus complexes sont possibles, soit dans Bitcoin lui-même soit dans d'autres protocoles. La transaction pourrait exiger des signatures multiples ou pourrait être conditionnée à l'occurrence préalable de certains événements qui peuvent être vérifiés sur la chaîne de blocs : *A* paye *x* à *B* à la date *T* seulement si *C* a payé *y* à *D* avant la date *T-K*. De façon plus générale, les conditions pourraient être des événements extérieurs à la chaîne de blocs : la température à New York, la valeur de S&P 500, le résultat d'une élection.

Le terme de « contrats intelligents » pour désigner ces transactions n'est pas très judicieux, car il ne s'agit pas de contrats et ils ne sont pas intelligents. En fait, ils automatisent plutôt la réalisation des contrats, de telle sorte que ni le contrat ni sa réalisation ne puissent être contestés, car ils sont intégrés dans une chaîne de blocs publique et inaltérable.

Dans une certaine mesure, Bitcoin peut être utilisé pour des contrats intelligents, mais si ce n'est pas son objectif principal ; d'autres protocoles, comme Ethereum, sont conçus pour de tels contrats.

2|2 Registres distribués

Un autre élément du protocole Bitcoin a suscité beaucoup d'attention au cours de l'année écoulée : il s'agit de la chaîne de blocs, ou registre distribué [9]. La propriété essentielle de la chaîne de blocs est qu'elle garantit, au sein d'un ensemble de participants, un accord permanent et vérifiable sur les données (en particulier, qui possède quoi) de façon décentralisée. Différents acteurs du système financier, tels que les banques et les bourses, ont commencé à investir dans l'exploration du potentiel des chaînes de blocs pour servir leurs propres objectifs.

Il y a quelques différences importantes avec le protocole Bitcoin. L'une est intentionnelle : le but de Bitcoin est de créer un actif numérique transférable qui puisse être utilisé par n'importe qui et ne soit pas contrôlé par une entité unique. Pour les banques ou les bourses, l'objectif n'est pas de créer un nouvel actif ou de permettre une participation illimitée, mais d'enregistrer les transferts d'actifs existants au sein d'un ensemble de propriétaires identifiés. Par conséquent, le moyen d'obtenir le consensus entre les participants ne doit pas reposer sur une preuve de travail comme dans Bitcoin ; et effectivement, d'autres mécanismes sont utilisés dans certaines applications (par exemple, le protocole Ripple repose sur le maintien par les participants de listes individuelles de partenaires de confiance et sur des tours de vote successifs permettant de valider les ajouts à la chaîne de blocs). Plus généralement, l'ensemble des participants autorisés à lire le registre ou à lui écrire pourrait varier en fonction de l'application.

Ce que la chaîne de blocs peut offrir est un enregistrement inaltérable qui est mis à jour de façon automatique et sécurisée. Elle est intéressante pour les situations dans lesquelles l'enregistrement et la modification du statut de propriété sont réalisés par des infrastructures disparates et des processus fastidieux. Les registres distribués pourraient incontestablement

9 *UK Government Office for Science (2016)* : « Distributed ledger technology: beyond block chain ».

simplifier et accélérer les transferts, tout en permettant également des transactions plus complexes (telles que les contrats intelligents). Ils pourraient également être plus sûrs, puisque les enregistrements sont conservés dans de multiples endroits et sont difficiles à modifier. Ces avantages seraient plus importants dans des contextes où il est plus facile de faire confiance à un protocole qu'à une entité unique, bien que les registres distribués puissent également être un moyen efficace de coordonner les activités au sein d'une institution unique.

Mais l'utilisation de registres distribués pour des règlements bancaires ou des échanges de titres de créance n'est pas simple. Premièrement, ce qui les rend attrayants (leur simplicité par rapport aux systèmes existants) est également ce qui les rendra difficiles à mettre en œuvre : les systèmes existants devront être adaptés au registre, ou remplacés par lui. Deuxièmement, le problème subsiste de l'interface entre le registre et le « monde réel ». Alors que Bitcoin est indépendant (au moins pour un côté de chaque transaction, le transfert des bitcoins), dans des applications plus importantes, les entrées du registre se rapportent à des actifs préexistants (dépôts bancaires, titres de créance) dont la propriété est reconnue, mais pas définie ni réglementée, par le protocole. Si la propriété des actifs réside « en dehors de la chaîne de blocs », alors les événements sur le registre doivent être validés par le système juridique et réglementaire dans le cadre duquel les banques et les bourses fonctionnent. Bien sûr, ce problème d'interface serait largement simplifié si les structures juridiques concernées reconnaissaient le registre lui-même comme l'enregistrement authentique, ou si les actifs transférés étaient définis dans la chaîne de blocs, mais ces changements ne se produiront pas de sitôt.

Dans une large mesure, donc, les avantages de la technologie du registre distribué qui sont mis en avant ne découlent pas tant de la technologie elle-même que des changements que son application suppose au préalable.

2|3 L'internet de la valeur

Les partisans les plus enthousiastes des monnaies numériques établissent volontiers une analogie entre les débuts du Web mondial dans les années quatre-vingt-dix et la période actuelle. Pour certains, Bitcoin n'est rien moins que la pièce manquante de l'internet, un protocole servant au transfert de valeur, tout comme le protocole TCP/IP sert à transférer des données. La compréhension du potentiel de l'internet a été rendue difficile par l'absence de moyens d'y connecter facilement le monde réel et de convertir en données les informations que nous estimions importantes. Mais le matériel informatique et les logiciels se sont tellement améliorés qu'il m'est désormais possible, en quelque secondes, de partager une photo de mon déjeuner avec des milliers de personnes dans le monde entier. Peut-être arrivera-t-il la même chose avec l'internet de la valeur, une fois que l'interface entre les actifs et l'internet aura été améliorée.

Des questions fondamentales demeurent : ces innovations nous permettront-elles de faire ce que nous faisons déjà, mais mieux ? Ou nous donneront-elles la possibilité de faire ce que nous étions incapables de faire auparavant, comme des contrats intelligents par exemple ?

Si nous revenons à la parabole traditionnelle de la naissance de la monnaie résultant d'une double coïncidence de besoins, la monnaie rend possible des transactions qui n'auraient pu avoir lieu sans elle (tout comme le crédit). À mesure que nos vies et les objets que nous possédons et utilisons sont de plus en plus connectés à l'internet, les paiements deviennent de plus en plus faciles et des transactions qui n'auraient pu être envisagées auparavant deviennent possibles. En particulier, une des vertus des monnaies numériques est leur caractère divisible, qui est illimité ou presque (la plus petite subdivision du bitcoin est 1e-8, soit moins de 1-e03 cents), rendant ainsi possibles les « micropaiements » pour de tout petits services, qui pourraient eux-mêmes être fournis automatiquement. La notion de contrat intelligent est une autre possibilité fascinante. Finalement, la chaîne de blocs est plus qu'un registre, parce qu'elle ne consigne pas uniquement l'état actuel de la propriété, mais aussi tout son historique. Les implications d'un tel enrichissement de l'information n'ont pas encore été intégralement explorées.

3| Stabilité et perturbations

Qu'il s'incarne dans les monnaies virtuelles, les chaînes de blocs ou l'internet de la valeur, le

changement est inévitable. Le défi, pour les autorités de régulation et les responsables de politique économique est d'y répondre.

3|1 Une menace pour les monnaies existantes ?

Ce n'est peut-être pas un hasard que le système Bitcoin soit apparu en 2009, peu après la crise financière. Bien que l'article ayant initialement décrit ce protocole [10] cite le coût des intermédiaires financiers comme principale motivation, certains de ses premiers partisans étaient préoccupés non seulement par la stabilité du système bancaire existant mais aussi par la réponse apportée par les principales banques centrales à la crise et par l'augmentation de la taille de leurs bilans. L'indépendance du bitcoin vis-à-vis des pressions politiques et de l'erreur humaine, et ses règles d'offre monétaire inscrites dans le code semblaient promettre une stabilité inaltérable. De plus, l'émergence d'une monnaie déconnectée de tout État faisait écho à l'idée que Friedrich Hayek avait de la concurrence entre devises. Enfin, le code source ouvert et la structure de pair à pair (*peer-to-peer*) ont séduit ceux qui voyaient l'internet comme un modèle d'égalité entre les citoyens.

Six ans plus tard, Bitcoin est loin de supplanter le dollar et peu de ses partisans s'attendent à ce que cela arrive. Les monnaies numériques décentralisées telles que Bitcoin peuvent cependant constituer une solution alternative dans les économies dont les systèmes monétaires sont instables et peuvent se révéler attractives comme ont pu l'être les monnaies étrangères durant les épisodes d'hyperinflation observés dans le passé. Mais ils n'ont pas encore perturbé les systèmes de paiement existants dans les économies avancées et ne sont pas près de le faire.

Premièrement, le caractère démocratique des nœuds égaux a laissé place à une activité de minage assez concentrée et, comme cela a été évoqué précédemment, la gestion du protocole s'est révélée complexe. De plus, la performance des devises existantes, en termes de stabilité de la valeur, a été bien meilleure que ne l'avaient anticipé certains. L'assouplissement quantitatif n'a pas entraîné d'hyperinflation. Dans ce contexte, les monnaies numériques comme Bitcoin n'offrent aucune amélioration significative. Il n'existe aucune politique monétaire active en matière de bitcoin : l'offre de monnaie est mécanique et uniquement fondée sur le temps calendaire, sans retour d'information provenant de sa valeur de marché courante. Même Milton Friedman, qui avait prôné la règle des k % en matière de croissance de la monnaie, n'aurait pas été jusqu'à fixer définitivement le k à *0*. Une offre de bitcoins asymptotiquement fixée peut présenter des avantages par rapport à l'offre de monnaie incontrôlée d'une hyperinflation, mais affiche-t-elle de meilleures performances qu'une monnaie déjà stable ? Et si les monnaies virtuelles créent de la concurrence entre les devises, il ne s'agit toutefois pas du genre de concurrence envisagé par Hayek : l'économiste pensait à des entrepreneurs, et non des robots, entrant en concurrence pour offrir les meilleures devises.

3|2 Réponses réglementaires

La politique monétaire ne sera pas la première victime des monnaies numériques, mais les régulateurs ont pris acte des innovations qu'elles apportent.

Soit ils trouveront des moyens d'intégrer ces innovations dans le cadre existant, soit ils adapteront le cadre existant à ces innovations. La première réponse est plus facile et plus rapide et, naturellement, c'est celle qui a été adoptée jusqu'à présent. L'une des priorités était de s'assurer que ces innovations ne puissent offrir de nouveaux outils permettant de contourner la législation relative à la lutte contre le blanchiment des capitaux et le financement du terrorisme et une des premières décisions prise aux États-Unis a été, en mars 2013, l'applicabilité de la réglementation sur les intermédiaires financiers aux monnaies numériques. Le régulateur a décidé que les fonds qu'un intermédiaire financier reçoit d'une personne puis transmet à une autre pouvaient prendre la forme de monnaies numériques. La prévention de la fraude et la protection des consommateurs et des investisseurs constituent un autre aspect important du contrôle réglementaire.

10 *Nakamoto (S.) :* « Bitcoin: a peer-to-peer electronic cash system » (https://bitcoin.org/bitcoin.pdf). *Comme on le sait, Nakamoto est un pseudonyme et l'identité de l'auteur demeure inconnue.*

Aux États-Unis, certaines autorités de réglementation considèrent la monnaie virtuelle comme une matière première, pour d'autres, c'est une devise, tandis que d'autres encore la voient comme un investissement et ce, principalement, dans le but de l'intégrer dans leurs champs de compétences respectifs. Ce n'est pas forcément un signe d'incohérence, au contraire, cela indique plutôt que l'intégration des monnaies numériques dans le cadre réglementaire ne nécessite pas de déterminer leur nature. Les réglementations sont conçues pour prévenir certains actes et si ces actes peuvent être réalisés avec des monnaies numériques, alors ces réglementations s'appliquent.

Il est donc difficile de réguler le bitcoin en lui-même, parce qu'il s'agit d'un protocole et non d'actifs ou d'engagements appartenant à une personne, mais on peut réglementer les utilisateurs de bitcoins, en fonction de leurs intentions. Les banques sont régulées sur la base de la relation contractuelle et fiduciaire qu'elles entretiennent avec leurs clients, ce qui est transposable aux banques dédiées au bitcoin et aux plates-formes d'échange de bitcoins, d'autant plus que le bitcoin ressemble à une monnaie et permet d'améliorer ce qui existe déjà. Et même si réguler un protocole à code source ouvert n'est pas aisé, le protocole lui-même, ou le code reposant sur le protocole, peut, si cela est nécessaire à sa survie, s'adapter aux pressions réglementaires.

La réponse réglementaire sera plus difficile à apporter si l'innovation nous permet de réaliser des choses nouvelles, parce que dans ce cas, il pourrait être nécessaire d'adapter le cadre. Il est difficile de prévoir la façon dont cela se passera, mais on peut énoncer quelques remarques simples en guise de conclusion. Comme pour toute innovation informatique, les régulateurs devront avant tout scrupuleusement vérifier la sûreté des technologies en matière de registre en cas d'utilisation généralisée par les banques : dans la mesure où les registres distribués sont communément utilisés par des intervenants importants, ils ont des implications systémiques.

Les monnaies virtuelles et les registres distribués ne remplacent pas la confiance, ils la déplacent dans les protocoles. Il s'agit là d'un autre domaine que les gardiens de la stabilité financière devront suivre attentivement. Aux États-Unis, l'innovation est généralement considérée comme une bonne chose qu'il est préférable de laisser entre les mains du secteur privé, mais la finance est un domaine dans lequel les consommateurs (et les électeurs) comptent sur la supervision des pouvoirs publics pour garantir la confiance, *via* la garantie des dépôts ou la surveillance des marchés de titres. La crise financière mondiale a renforcé plutôt que diminué cette attente.

Enfin, deux questions importantes se poseront aux responsables de la politique monétaire. La première est liée au fait que les monnaies et registres virtuels, fondés sur la technologie de pair à pair, marquent une tendance vers un éloignement de la négociation centralisée. La seconde est de savoir dans quelle mesure leur utilisation réduira le besoin de liquidité en accroissant les règlements nets. Ces deux tendances, si elles se concrétisent, iraient à l'encontre des évolutions observées depuis le début de la crise financière mondiale.

L'évolution future de la négociation électronique sur les marchés obligataires européens

Elizabeth CALLAGHAN
Directeur, Pratiques de marché et politique de réglementation, marchés secondaires
Association internationale des marchés de capitaux

*La négociation sur les marchés obligataires subit aujourd'hui des changements sans précédent qui devraient se poursuivre au cours des prochaines années. Le modèle traditionnel de négociation des obligations, reposant principalement sur les teneurs de marché et le courtage traditionnel « à la voix », est en perte de vitesse. Cela résulte en partie de l'évolution naturelle des transactions sur obligations induite par le progrès technologique et la recherche d'efficacité en termes de coût, qui se traduit par l'augmentation des transactions électroniques. Le modèle de négociation traditionnel est aussi battu en brèche par des contraintes réglementaires réduisant la capacité des sociétés de courtage pour compte propre (*broker-dealer*) à prendre, tenir, financer ou couvrir des positions, et à fournir ainsi de la liquidité en tant que teneurs de marché. La mise en œuvre prochaine des nouvelles règles européennes de négociation respectant la norme MiFID 2 sera un autre élément clé accentuant l'ampleur de la transformation. On observe des signes annonciateurs de la nouvelle structure des marchés, mais personne ne peut prédire exactement à quoi ressemblera le marché secondaire pour les obligations à un horizon de cinq, sept ou dix ans. Nous ne pouvons que formuler des hypothèses. Il est en revanche certain que la négociation d'obligations doit s'adapter et innover pour durer. Cela touchera toutes les facettes de la négociation, y compris les acteurs humains, la technologie, ainsi qu'une réorientation de la stratégie du métier. Ce changement concernera la totalité du marché : les acteurs situés côté achat et côté vente, mais aussi les plates-formes de négociation et les autres fournisseurs de technologies de négociation. L'écosystème de l'activité de négociation d'obligations connaîtra de nouveaux entrants (potentiellement source de perturbations), des innovations par des acteurs déjà en place, des protocoles et des plates-formes de négociation adaptatifs. Ces changements, souvent analysés comme une évolution du marché des instruments à revenu fixe vers celui des actions, prendront néanmoins une autre forme que les précédents changements intervenus dans le domaine des actions, compte tenu des différences structurelles entre la négociation d'actions et celle des titres à revenu fixe. Globalement, la transformation sera difficile, la réglementation et la technologie jouant un rôle perturbateur pour les structures de marché existantes et posant de sérieux défis à de nombreux acteurs du secteur. Cependant, la transformation créera également des opportunités pour les intervenants de marché, dans un contexte d'innovation.*

Cet article porte sur l'évolution dans le futur de la négociation électronique sur les marchés obligataires européens. Il vise à compléter l'étude de la Banque des règlements internationaux (BRI) sur la situation actuelle de la négociation électronique sur les marchés de titres à revenu fixe, en faisant état de la contribution de la Banque de France. On trouvera dans ce qui suit la vision d'un professionnel des marchés quant aux évolutions futures du modèle de négociation de titres à revenu fixe. Un glossaire disponible à la fin de la revue couvre les termes les plus techniques utilisés dans le domaine de la négociation électronique.

L'évolution de la négociation électronique sur les marchés de titres à revenu fixe est souvent désignée par le terme d'*equitisation* des titres à revenu fixe. Il s'agit toutefois d'une simplification excessive. Les évolutions de la négociation électronique sur les marchés obligataires suivront une trajectoire très différente de celle du marché des actions. Cela s'explique par les grandes différences existant entre ces deux marchés :

- les actions et instruments assimilés – 6 810 titres admis à la négociation sur les marchés réglementés dans l'UE – font l'objet de 400 transactions par jour en moyenne ;

- les instruments à revenu fixe – plus de 150 000 titres de créance (référencés dans la base de données CUPID – *Computer Updated International Database* – de Xtrakter) –, font l'objet de 1,5 transaction par jour en moyenne [1].

Les marchés des titres à revenu fixe ont traditionnellement combiné les activités de teneur de marché et d'intermédiation (utilisant des courtiers intermédiaires – *inter-dealer brokers* – et des systèmes hybrides, électroniques et « à la voix », pour assurer la liquidité des titres), largement organisées autour des banques courtiers (*broker-dealers*) et d'un réseau construit sur les relations avec les clients. Le modèle était principalement :

- de courtier à client, *i.e.* de banque à gestionnaire d'actifs, gestionnaire de fonds de pension (côté achat) ;

- de courtier à courtier, *i.e.* de banque à banque ou de banque à courtier intermédiaire ;

- mais pas de client à client, *i.e.* de gestionnaire d'actifs à gestionnaire d'actifs.

Les pratiques de marché ont traditionnellement reposé sur les teneurs de marché, qui sont essentiellement des *broker-dealers* proposant à leurs clients des prix à l'achat et à la vente pour une sélection d'obligations, indépendamment de leur capacité à trouver une contrepartie vendeuse ou acheteuse au même moment, notamment parce que la coïncidence simultanée des besoins est hautement improbable sur les marchés obligataires. Lorsque les clients sont vendeurs d'une obligation, le teneur de marché présente un prix d'achat et inscrit le titre dans son inventaire, couvre sa position et cherche à le vendre, à un autre client ou à un *broker-dealer*, à une date ultérieure. Lorsque les clients sont acheteurs d'une obligation, le teneur de marché présente un prix de vente et vend le titre, il couvre cette opération, sur le marché des pensions si la vente est à découvert, et cherche à racheter l'obligation sur le marché à une date ultérieure.

En outre, une société de courtage pour compte propre (*broker-dealer*) doit comprendre trois composantes interdépendantes pour offrir des prestations de teneur de marché aux contreparties. La difficulté en est accrue par les règles prudentielles relatives à l'adéquation des fonds propres et à l'endettement qui rendent beaucoup plus onéreuses les transactions sur titres et dérivés. Les conditions suivantes doivent être remplies pour la réussite des activités de teneur de marché :

- la capacité à tenir un inventaire au bilan ;

- un marché des pensions liquide pour financer les positions longues ou couvrir les ventes à découvert ;

- la capacité à se couvrir sur les marchés de produits dérivés.

Les contraintes réglementaires réduisant la capacité des entreprises d'investissement à prendre, tenir, financer ou couvrir des positions, la source traditionnelle de liquidité des marchés obligataires est en cours de tarissement.

Enfin, il est important de noter que la structure du marché de titres à revenu fixe dans le cadre d'un

1 *Cf. Biais et Declercq – Academic Study, 2007, et article publié par l'ICMA, 2009.*

modèle de courtier à client a toujours reposé sur des prix affichés (tandis que les marchés d'actions reposent sur une confrontation des ordres). Les prix sont proposés uniquement en réponse à une demande d'une contrepartie portant sur un niveau de prix. Cette démarche étant unidirectionnelle, les détails concernant le processus de formation du prix (y compris le volume et la dimension réels) ne sont pas partagés avec le public. Par conséquent, les cotations et les prix transactionnels peuvent varier fortement selon le courtier pour une obligation donnée.

La structure des marchés obligataires a été décrite comme figée et résistante au changement. Toutefois, les marchés connaissent actuellement une transformation due à l'évolution naturelle (par exemple le progrès technologique et la recherche d'efficacité en termes de coûts) ainsi qu'aux effets de la réglementation. Le modèle traditionnel de négociation des obligations est en train de s'effondrer. On observe des signes annonciateurs d'une nouvelle structure, mais personne ne peut prédire exactement à quoi ressembleront les marchés secondaires pour les obligations à un horizon de cinq, sept ou dix ans. Nous ne pouvons que formuler des hypothèses.

Un avenir soumis à une sélection naturelle darwinienne

La négociation d'obligations doit s'adapter et innover pour durer. Cela touchera toutes les facettes de la négociation, y compris les acteurs humains, la technologie et impliquera une réorientation de la stratégie du métier. L'écosystème de l'activité de négociation d'obligations connaîtra de nouveaux entrants, potentiellement source de perturbations, des innovations par des acteurs déjà en place, des protocoles et des lieux de négociation adaptatifs.

De nombreux intervenants de marché s'accordent pour estimer que 80 % des revenus sont apportés par 20 % à 30 % des clients. Ce fait est aujourd'hui plus d'actualité que jamais. Les *broker-dealers* identifient des clients prioritaires et évaluent leurs clients en fonction des opportunités de ventes croisées plutôt que d'appliquer des stratégies de vente par produit (ou par région). Par exemple, les clients doivent être actifs au titre de plusieurs lignes d'activités, comme les produits dérivés, les marchés émergents, les actions, et si possible être également apporteurs de revenus dans d'autres régions du monde. Ainsi, l'ancien modèle de l'activité de teneur de marché est jugé par beaucoup en voie de disparition.

Cette évolution n'est pas sans conséquences. Les banques se restructurent et réorientent leurs stratégies. Elles deviennent courtiers faisant office d'agent intermédiaire pour le client (*agency broker*) ou acteurs de niche, ou se retirent complètement de certains domaines d'activité obligataires, ainsi qu'en témoignent aujourd'hui de nombreuses unes de médias.

D'aucuns se demandent si la notion traditionnelle de l'engagement en capital par monétisation de l'écart entre les prix acheteur et vendeur n'est pas en train de devenir un mode de négociation des obligations moins approprié, indiquant ainsi que le marché pourrait se tourner vers un modèle reposant davantage sur les commissions. Avec un modèle basé sur les commissions, les frais généraux liés aux modifications réglementaires (par exemple les coûts informatiques) seraient plus facilement répercutés sur les clients *via* les taux de commission (qui sont plus normalisés).

Côté achat mais aussi côté vente, les acteurs de marché se restructurent et réorientent leurs stratégies commerciales. Les coûts générés par le respect des exigences réglementaires augmentent considérablement. L'opinion du secteur est que, lorsque la réglementation MiFID 2 entrera en vigueur, de nombreuses petites entreprises du côté achat n'auront pas les ressources suffisantes pour se doter des équipements informatiques nécessaires impliqués par la législation. Elles courent aussi le risque de ne plus être éligibles au titre de la clientèle des *broker-dealers*. Que font alors les intervenants de marché ? Les plus avisés préparent l'avenir (notamment en modifiant la composition de leurs portefeuilles en fonction de la liquidité attendue, en réexaminant la couverture et le niveau de service du courtage et enfin en analysant les incidences de la réglementation sur la négociation).

1| Réorientation de la stratégie : les entreprises remanient leurs stratégies en raison du manque de rendement des titres à revenu fixe

Des courtiers ayant des stratégies de niche commencent déjà à apparaître. Il s'agit des plus petits courtiers (côté vente) qui consolident leurs activités, en s'appuyant sur des équipes réduites de négociation et de vente tout en utilisant des plates-formes électroniques de négociation pour atteindre davantage d'investisseurs. Ces intervenants deviennent les nouveaux spécialistes de certains secteurs ou compartiments des marchés obligataires, notamment du crédit. Ils combinent des activités de négociation et de *sourcing*, classiques et électroniques.

Les nouveaux entrants ou les acteurs en place présents dans les cinq à dix prochaines années seront innovants et utiliseront très probablement des solutions technologiques pour faire face aux défis du marché.

1|1 Les nouveaux entrants

Les nouveaux entrants ne seront pas freinés par l'héritage informatique fragmenté auquel sont confrontés les grands opérateurs en place. Ils peuvent donc être plus réactifs pour apporter des solutions aux difficultés du secteur. Ces outils, ces solutions et ces nouvelles entreprises reposeront sur une technologie avancée. Nous décrivons ci-après ces différents points et nous expliquons pourquoi certains de ces nouveaux entrants pourraient faire une entrée réussie dans le paysage de la négociation électronique.

Systèmes de gestion des ordres (*Order Management Systems* – OMS) et systèmes de gestion des exécutions (*Execution Management Systems* – EMS) – Ils permettent une transmission automatisée en continu (*Straight through processing* – STP) connectée aux systèmes internes au sein de l'établissement. Les avantages sont les suivants : une intégration sans heurt, efficace et transparente interconnectant la gestion du risque, la vérification du crédit et la gestion de la position – garantissant que les transactions se situent dans les limites de risque et respectant les obligations des clients. En résumé, les OMS et les EMS connectent le *front-office* au *back-office*, en améliorant l'efficacité, en réduisant les coûts et en atténuant les risques. Ils utilisent également la technologie de messagerie FIX (protocole de communication côté achat/côté vente), qui permet aux courtiers d'envoyer des ordres et d'utiliser divers protocoles tels que RFQ (demande de prix), RFS (demande de flux continu) et *pricing* indicatif avec d'autres intervenants de marché. FIX permet également la distribution de la liquidité entre les plates-formes et permet aussi les interactions avec les infrastructures de négociation d'autres intervenants de marché.

Analyse des coûts de transaction (*Transaction Cost Analysis* – TCA) – La TCA permet à une entreprise d'analyser le coût de la décision d'effectuer une transaction, sur une période spécifiée, par rapport à différentes références. Traditionnellement, la TCA est largement utilisée par les investisseurs en actions. La TCA pour les titres à revenu fixe était considérée comme un des domaines où il était le plus difficile de proposer une mesure des performances, en raison du manque de transparence et de données du marché. Il existe un décalage entre la TCA fournie par les vendeurs et les solutions élaborées en interne, s'agissant des rares informations actuellement disponibles sur les marchés de titres à revenu fixe. Dans les années à venir, la TCA pour les titres à revenu fixe progressera grâce aux données qui seront générées par la réglementation MiFID 2.

Outils d'analyse des données (de toutes sortes) – Les données non structurées comme la voix/l'e-mail/le *chat* posent problème pour prouver l'exécution des ordres au mieux. Une longue expérience de la négociation et des outils sophistiqués de traitement des données augmenteront le niveau de précision et permettront une approche presque scientifique de l'analyse des données. Cela favorisera une meilleure formation des prix à la fois pour les vendeurs et les acheteurs. En outre, les investisseurs finaux tireront profit de l'amélioration de la traçabilité des opérations et d'une plus grande responsabilité des vendeurs dans un cadre de *reporting* quant à l'exécution « au mieux ». Là encore, grâce aux données produites en grande quantité pour respecter la réglementation MiFID 2, l'ensemble des outils d'analyse permettant une mesure optimale des performances sera fortement amélioré.

***Trading* algorithmique des titres à revenu fixe** – Le *trading* algorithmique (programmes informatiques

complexes construits sur un ensemble défini d'instructions) est généralement lié aux négociations sur les actions. Cependant, les courtiers en actions qui l'utilisent y voient dorénavant une opportunité de rentabilisation de leurs investissements dans la négociation des titres à revenu fixe. À mesure que celle-ci exige davantage de technologie et qu'il devient plus facile d'obtenir des données (grâce à la réglementation MiFID 2) pour effectuer un contrôle *ex-post*, les courtiers en titres à revenu fixe utiliseront les algorithmes pour les négociations impliquant une faible intervention humaine (*low touch*) afin de remédier en partie aux conséquences des réglementations, telles que la compression des marges liée à la hausse des coûts. La progression du *trading* algorithmique sera essentiellement observée pour certains produits à revenu fixe liquides, comme les obligations d'État (c'est déjà le cas actuellement). Cependant, il est probable que les algorithmes deviendront plus attractifs pour d'autres instruments à revenu fixe à mesure que les données seront disponibles grâce à la réglementation MiFID 2.

Outils informatiques identifiant les « faux positifs » – Ces « faux positifs » (obligations classées comme liquides alors qu'elles sont illiquides – classement incorrect de la liquidité), qui sont un effet secondaire de la calibration de la liquidité de la réglementation MiFID 2, constituent une bizarrerie. Il s'agit probablement d'un des problèmes les plus importants soulevés par la réglementation MiFID 2. Les vendeurs sont concernés par ces faux positifs dans la mesure où ils affectent leur capacité de tenue de marché, et les acheteurs car ils risquent d'affecter la perception de la liquidité du portefeuille. Par conséquent, tout instrument susceptible de les identifier précisément sera extrêmement apprécié.

Services technologiques réglementaires – Tout service technologique ou toute entreprise de consultants susceptible d'aider les intervenants de marché (côté achat, côté vente et plates-formes) à respecter les règles et à maintenir la meilleure exécution prospérera dans les années à venir. Les prestataires efficaces identifieront pour le compte des entreprises les données nécessaires au respect des obligations réglementaires, tout en gérant les répercussions informatiques des réglementations.

Internalisation des ordres – Les sociétés qui gèrent plusieurs *desks* de négociation, sur différents fuseaux horaires ou dans différentes filiales, auront besoin d'un système informatique avancé qui permette d'internaliser automatiquement le flux des ordres. Ils exécutent donc les ordres en interne afin d'économiser les frais de courtage.

Réseaux d'information – *Sourcing* et agrégation de la liquidité. Ces réseaux fournissent une couche d'agrégation, proposant au courtier deux ensembles essentiels de fonctionnalités : une vue globale de la liquidité et un choix de protocoles de négociation et de mécanismes d'exécution. Le courtier utilise cette couche pour obtenir un aperçu précis et rapide de la liquidité disponible sur l'ensemble des marchés. Ces réseaux utilisent un degré élevé de technologie intégré dans les systèmes internes côté achat et côté vente. Cf. Algomi, B2Scan par exemple.

Réseaux appartenant à un consortium réunissant le côté achat et le côté vente – Efforts de collaboration entre le côté achat et le côté vente : les intervenants de marché se rejoignent avec pour but de créer de la liquidité sur les marchés obligataires. L'objectif est de permettre une transparence accrue sur le marché des intérêts de négociation entre acheteurs et vendeurs d'obligations autour des banques et des gestionnaires d'actifs. Cf. l'exemple de Neptune.

Ces réseaux collaboratifs utilisent une technologie standard ouverte permettant aux participants côté vente d'envoyer des indications de prix pré-négociation à leurs clients (gestionnaires d'actifs) qui les transmettent par le réseau aux gestionnaires d'actifs directement connectés. Les réseaux collaboratifs offrent une flexibilité quant à la connectivité. Les acheteurs peuvent recevoir des indications de prix pré-négociation de différentes banques dans un format standard utilisant une seule connexion (par exemple, le protocole FIX).

1|2 Les innovations des acteurs en place

***Hedge funds* contributeurs de prix** – Bien qu'ils ne soient pas des nouveaux venus, les *hedge funds* s'adapteront au nouvel environnement. Tandis que les intervenants traditionnels côté achat n'interviendront vraisemblablement pas comme contributeurs de prix dans les carnets d'ordres avec limite centralisés (*Central Limit Order Book* – CLOB) ou dans d'autres systèmes de négociation réservés

aux spécialistes, les *hedge funds* peuvent intervenir (à condition que cela soit compatible avec leurs stratégies de négociation) et fournir davantage de prix pour les actifs illiquides, renforçant ainsi la liquidité. Cela s'explique par le fait que les *hedge funds* n'ont ni la même structure juridique ni les mêmes missions que les gestionnaires d'actifs.

Teneurs de marché indépendants – Des teneurs de marché indépendants, spécialisés sur des instruments ou des secteurs, commenceront à apparaître. La baisse du coût de la technologie, combinée à son amélioration et à l'extension de son utilisation contribueront à faciliter l'apparition de ces sociétés, en réduisant la barrière à l'entrée. Cf. XTX Markets.

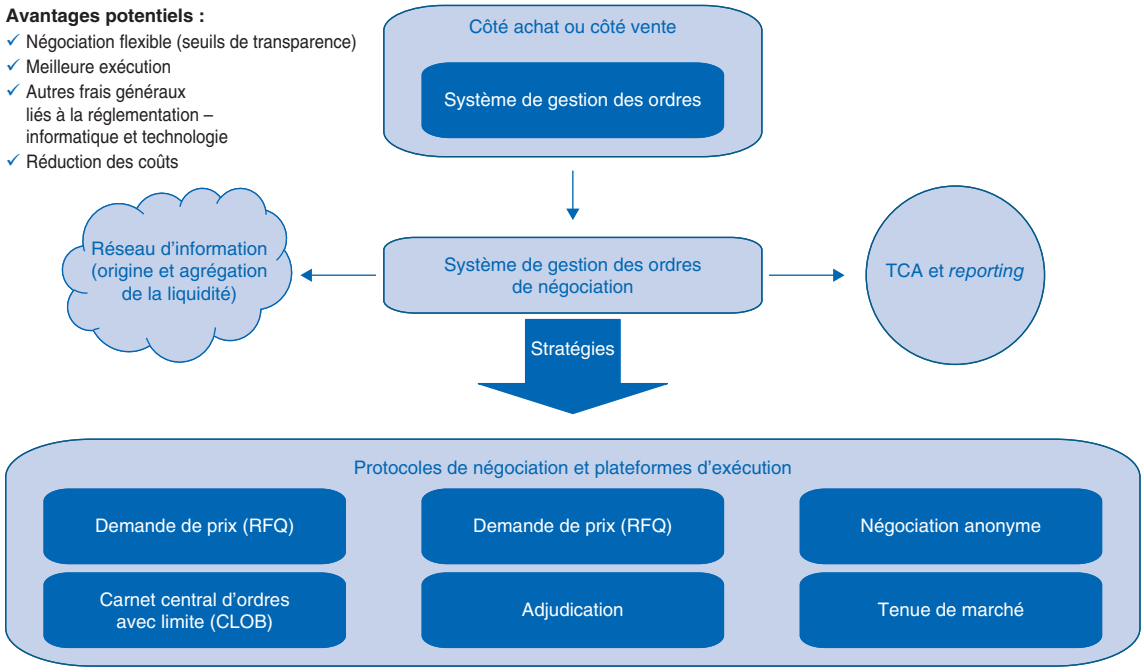
Négociation de niche – Les banques développeront également une expertise spécialisée et seront donc réputées pour la négociation et la tenue de marché pour certaines catégories d'actifs ou certaines régions. Ce sera notamment le cas pour les marchés émergents dont les titres à revenu fixe sont susceptibles, dans certaines circonstances, de produire un rendement plus élevé. La technologie permet également de connecter les clients à des experts régionaux du monde entier.

Négociation multi-actifs – Les banques et les intervenants côté achat portant plus d'attention à leurs résultats, il deviendra évident que certaines compétences et ressources informatiques peuvent être partagées. Il est trop coûteux d'avoir des infrastructures totalement séparées pour effectuer des transactions qui gagneraient à partager les connaissances sur les différentes catégories d'actifs. Il existe actuellement quelques *desks* multi-actifs du côté achat, mais nous assisterons à l'apparition d'autres structures dans les cinq à dix ans à venir, y compris du côté vente.

« Super-*desks* » ou « négociation externalisée » – Les grands intervenants régionaux côté vente et côté achat créeront de super-*desks* centralisés où ils auront des capacités de teneurs de marché à l'échelle mondiale. Nous observons déjà l'apparition de *desks* plus importants du côté achat, qui offrent des services de négociation à des sociétés plus petites pour leur permettre de bénéficier d'économies d'échelle. Cf. BNP Paribas Dealing Services par exemple.

Le niveau des dépenses pour tout ce qui a trait à la connectivité (accès aux plates-formes, aspects réglementaires, juridiques, informatiques et liés

Scénario de négociation externalisée



Source : ICMA.

aux risques) peut être si élevé que les gestionnaires d'actifs de niveaux 2 et 3 et les intervenants côté vente de moindres dimensions peuvent envisager d'autres solutions : la négociation externalisée peut devenir à ce titre une option tout à fait viable. Elle se pratique déjà actuellement, bien que ce ne soit que le début. Cependant, elle devrait se développer davantage dans les années à venir et devenir une plate-forme centralisée offrant des services pour la gestion réglementaire (même si les obligations réglementaires ne peuvent pas être externalisées) et des techniques de négociation évolutives. Elle pourrait déboucher sur une offre multi-actifs pour certaines opérations. De plus, le prestataire externe sera en mesure de prouver la meilleure exécution pour le compte de ses clients aux régulateurs et de publier le rapport de négociation. Il serait également en mesure de fournir à ses clients (en utilisant la TCA) un rapport sur la mesure des performances des courtiers.

Un meilleur accès aux teneurs de marché et une meilleure réponse de leur part devraient contribuer à des niveaux plus élevés de liquidité et devraient globalement améliorer la performance des portefeuilles, grâce à une négociation plus efficace. De plus, grâce aux économies d'échelle, ces « super-*desks* » obtiendront plus fréquemment les dérogations et les reports de la réglementation MiFID 2 attachés aux acteurs de taille importante (seuils réglementaires imposant une transparence obligatoire à la fois pour la pré-négociation et pour la post-négociation), conséquence de la concentration des négociations. Il est important de noter que cette « prestation » de négociation externalisée pourrait être utilisée pour le routage habituel des activités, pour des demandes spécifiques ou pourrait même être une société indépendante offrant un service consolidé centralisé.

Enfin, les salles de marché externalisées du futur peuvent être confrontées à différents protocoles et les appliquer sur la base de stratégies de négociation ciblées et de l'environnement de structure de marché, dans des situations de liquidité faible ou abondante : demandes de prix (RFQ), demandes de flux continu (RFS), négociations en bourse ou CLOB, tenue de marché de gré à gré, négociations anonymes et toutes les négociations potentiellement mondiales ou locales.

2| Évolution de la structure de marché – protocoles et plates-formes de négociation

Une chose est certaine : la négociation électronique (y compris les plates-formes et les protocoles de négociation) est au cœur de la planification réalisée par les dirigeants de haut niveau pour la refonte de la structure de marché. Les protocoles et les plates-formes de négociation traditionnels évolueront également et s'adapteront au nouvel environnement de la négociation électronique pour les obligations de caisse. La réglementation MiFID 2, associée à d'autres réglementations, sera le principal moteur d'un changement radical de la structure de marché. Certains spécialistes prédisent la disparition de protocoles que nous utilisons depuis des années, comme le courtage de gré à gré « à la voix ». Alors que la plupart pensent le contraire : pour ces derniers les plates-formes et les protocoles actuels existeront encore, mais leur importance évoluera considérablement au fil du temps ; ultérieurement, les plates-formes et les protocoles actuels seront rejoints par de nouvelles plates-formes et de nouveaux protocoles innovants.

Les plates-formes et les protocoles se divisent entre les catégories ci-après. Il convient de noter que les systèmes organisés de négociation (*Organised Trading Facilities* – OTF) et les internalisations des ordres systématiques (*Systematic Internalisers* – IS) rejoindront la catégorie « multilatérale » des plates-formes et des protocoles quand la réglementation MiFID 2 entrera en vigueur le 30 janvier 2018.

- Bilatéraux : demande de prix (RFQ), demande de flux continu (RFS), négociations de gré à gré y compris la tenue de marché [2].

- Multilatéraux : CLOB, bourses, systèmes multilatéraux de négociation (*Multilateral Trade Facilities* – MTF) et post-MiFID 2, IS et OTF, plates-formes croisées : anonymes ou semi-transparentes et enfin adjudications : négociations multilatérales achat/vente basées sur la durée.

Selon toute vraisemblance, l'évolution des protocoles et des plates-formes au cours des prochaines années s'effectuera par paliers. Il ne semble pas impossible que l'entrée en vigueur de la réglementation MiFID 2 entraîne d'abord un retour à une négociation en

2 *Les acronymes sont définis dans le glossaire en fin de revue.*

dehors des systèmes, le marché testant les implications d'un marché plus transparent (*lit*). Le marché s'habituant progressivement au nouvel environnement de négociation de la réglementation MiFID 2, l'utilisation des protocoles et des plates-formes électroniques devrait se développer. Il pourrait en résulter, par exemple, une augmentation des volumes négociés électroniquement, pour les transactions importantes ou illiquides, pour les acheteurs et les vendeurs.

Les plates-formes et protocoles électroniques seront de plus en plus utilisés, à des degrés divers. Les protocoles bilatéraux intégreront aussi davantage d'éléments électroniques. Le marché constate déjà une hausse des demandes de prix (RFQ) automatisées, où les intervenants côté achat demandent des prix aux courtiers dans un environnement plus contrôlé et plus vérifiable que celui du courtage traditionnel de gré à gré « à la voix ».

Les évolutions se feront au cas par cas. En effet, les protocoles et plates-formes multilatéraux ne conviennent pas tous pour tous les types de négociations. Nous analysons ci-après, avec quelques exemples, leur utilisation et leur évolution possible.

Négociation s'adressant à tous (*All-to-All*) – C'est la vraie définition de la négociation multilatérale (connexion des courtiers, des investisseurs et des autres intervenants de marché sur une plate-forme centralisée ouverte à tous). Les CLOB offrent un exemple de plate-forme de négociation ouverte à tous, avec des limites électroniques intégrées. Même s'ils sont les plus représentatifs de ce type de négociations, les protocoles et plates-formes de négociation anonymes, les protocoles hybrides de demandes de prix (RFQ) et même les adjudications peuvent aussi être considérés comme des *All-to-All*.

Les carnets d'ordres avec limite centralisés (CLOB) augmenteront, mais seulement pour les flux de faible taille, car les acheteurs ne sont pas mandatés pour contribuer aux prix et les publier sur les plates-formes.

Par ailleurs, personne (côté achat ou côté vente) ne voudra laisser un prix pour une taille importante ou pour un titre illiquide, prix susceptible d'être récupéré sur un CLOB. Dans ce cas, le prix sur le CLOB ne sera pas représentatif.

Il est intéressant de noter que, pour beaucoup, le volume de ces négociations limitées en taille augmentera, comme cela a été le cas pour les actions.

Les demandes de prix – RFQ – (bilatérales) – Seuls les protocoles capables de fournir un *pricing* crédible et cohérent auront une chance de réussir. Le prix doit être un prix actuel « acceptable » afin de pouvoir être négocié dans un cadre compétitif et concurrentiel. Même si les négociations multilatérales augmentent, les demandes de prix bilatérales ne disparaîtront pas. Une discussion entre acteurs menée dans un climat de confiance sur les détails d'une transaction sera toujours appréciée.

Pour les acheteurs, les demandes de prix présentent l'inconvénient suivant : lorsque les informations relatives à une négociation potentielle sont discutées, la transaction peut alors être conclue sur cette base. La « fuite d'informations » qui résulte de cette discussion peut avoir une incidence sur le marché (le prix s'établissant en défaveur des acheteurs). Cela explique la progression des plates-formes de croisement électronique (plates-formes de négociations anonymes).

Tenue de marché de gré à gré – Même si la tenue de marché devient une activité plus rare à l'avenir, elle sera toujours nécessaire, notamment lorsqu'un courtier côté achat souhaite une taille importante.

Pour les acheteurs, le risque est de ne pas obtenir auprès d'un teneur de marché un prix « exécutable » pour une obligation donnée, au moment où il en a besoin. Les vendeurs qui offrent leur bilan en traitant deviennent plus exigeants vis-à-vis des clients avec lesquels ils souhaitent traiter.

Plates-formes de négociation anonymes (multilatérales) – L'anonymat est un avantage pour les intervenants de marché qui souhaitent réaliser d'importantes opérations sans attirer l'attention car celle-ci peut influer sur les prix. Ces systèmes de négociation sont anonymes et/ou semi-transparents (*lit*) entre deux acteurs acheteurs (*buy-side*) ou un acteur acheteur (*buy-side*) et un acteur vendeur (*sell-side*). La formation des prix s'effectue de façon non-transparente (*dark*) puisque l'anonymat protège les participants.

Les plates-formes de négociation anonymes, notamment entre les acheteurs (*buy-side*), se développeront en suivant le modèle des actions. Cependant, comme pour les actions, seules une ou deux plates-formes verront le jour : en effet, la plupart des spécialistes estiment que 6 à 10 % seulement de l'ensemble des négociations seront réalisées sur ces

plates-formes (d'après un sondage effectué lors d'une conférence fin 2015).

Les acteurs ayant recours à ces plates-formes de négociation sont confrontés à un risque ; elles peuvent permettre d'apparier un acheteur et un vendeur de façon non transparente (*dark*) mais les protagonistes doivent avoir une idée du prix pour finaliser avec succès la négociation.

Internalisation systématique des ordres (*Systematic Internaliser* – SI) – La raison d'être du régime SI est de déplacer la négociation « *dark* », hors système, vers des systèmes « *lit* » en créant une égalité de traitement et une plus grande transparence des prix (en résumé, les SI empêchent l'activité de passer des systèmes « *lit* » au « *dark* », ils rendent transparents les marchés de gré à gré les plus actifs). L'exigence fondamentale d'un SI, par rapport à un non-SI, est qu'il est soumis à des obligations de transparence pré-négociation comparables à celles d'un marché réglementé, d'un MTF ou d'un OTF, ceci étant supposé soutenir la formation des prix pour les investisseurs.

La réglementation MiFID 1 a introduit le régime des SI, mais seulement pour les actions. La réglementation MiFID 2 élargit le régime des SI aux obligations. Le régime des SI dans la réglementation MiFID 2 s'articule sur une entreprise d'investissement qui, de façon organisée, fréquente et systématique, et pour des tailles significatives, exécute les ordres des clients en dehors d'un marché réglementé, d'une MTF ou d'un OTF en engageant ses propres capitaux.

Les SI doivent donner des prix fermes à la demande de leurs clients (à la taille standard du marché) pour les obligations liquides. Cependant, les SI ont la possibilité de limiter le nombre de transactions qu'un client peut réaliser et le nombre de clients à qui les prix sont fournis, tant que leur politique commerciale est établie de façon non discriminante. Les SI sont ainsi capables de gérer leur activité de négociation et les coûts et risques associés.

Du point de vue de la tenue de marché, les SI ne présentent pas d'avantage évident, car il n'existe pas de garantie de *pricing* compétitif. L'objectif du régime des SI n'est pas de fournir des prix ou de la liquidité, mais plutôt de la transparence sur le marché des transactions de gré à gré. Il pourrait arriver que certains investisseurs, dans le cadre de leur politique de meilleure exécution, demandent des prix aux SI pour des instruments spécifiques lors de négociations de gré à gré. Par ailleurs, le fait que pour une obligation il y ait un certain nombre de SI enregistrés pourrait être une composante de l'évaluation de la liquidité interne d'un investisseur.

Systèmes multilatéraux de négociation (*Multilateral Trading Facilities* – MTF) – Dans la réglementation MiFID 2, les exigences relatives aux MTF ont été alignées sur celles des marchés réglementés afin de créer une meilleure égalité de traitement. La plupart des plates-formes de négociation de type *agency* seront classées comme des MTF.

Systèmes organisés de négociation (*Organised Trading Facilities* – OTF) – À côté des MTF, ils constitueront un troisième type de système multilatéral (marchés réglementés, MTF et maintenant OTF) dans lequel de nombreux intérêts acheteurs et vendeurs peuvent interagir pour conclure des contrats. Les OTF ne s'appliquent pas aux actions. Ils entreront en vigueur avec la réglementation MiFID 2.

L'exécution des ordres au sein d'un OTF s'effectue sur une base discrétionnaire. Il existe deux niveaux distincts de discrétion pour l'opérateur d'un OTF : a) lorsqu'il décide de passer ou de retirer un ordre sur l'OTF, et b) lorsqu'il décide de ne pas apparier un ordre spécifique d'un client avec un autre ordre disponible dans le système à un moment donné, à condition que cela respecte les instructions spécifiques reçues d'un client et les obligations de meilleure exécution.

Un OTF n'aura pas le droit de négocier face à son compte propre ou face au compte propre de toute entité faisant partie du groupe d'entreprises de l'opérateur de l'OTF.

La plupart des spécialistes pensent que les courtiers intermédiaires (*inter-dealer brokers*) post-MiFID 2, lorsqu'ils exécutent un *name give-up*, seront les seules plates-formes de négociation classées comme OTF.

3| Évolution et restructuration des effectifs

Lorsqu'on observe l'évolution de l'activité de négociation et de la structure de marché, il est souvent plus simple de ne pas prendre en considération les personnes qui négocient. Comment ces personnes évolueront-elles

pour répondre aux besoins du futur ? De nombreuses restructurations des effectifs sont actuellement en cours dans les entreprises du côté vente. Elles s'expliquent essentiellement par les problèmes de performances des activités sur les titres à revenu fixe. Des activités rentables dans le passé ne le sont déjà plus ou ne le seront sans doute plus dans un avenir proche. Ces activités ont récemment enregistré des baisses de 20 à 30 % et parfois beaucoup plus. Par ailleurs, de nombreux intervenants du secteur ont déclaré que la disponibilité des bilans bancaires avait diminué d'un tiers environ. L'activité n'est pas assez importante pour maintenir des effectifs élevés de courtiers en obligations et de vendeurs. En 2015, nous avons fréquemment observé des réductions ou des « redimensionnements » d'effectifs. Cette tendance devrait se poursuivre car les entreprises s'adaptent à la modification de l'environnement de la négociation d'obligations.

Un des moyens de réduire les coûts et de rationaliser l'activité consiste à licencier le personnel le plus ancien et le plus expérimenté dans les domaines de la vente et de la négociation. Cependant, cela crée une culture de la « juniorisation », où non seulement les équipes diminuent, mais où les banques dépendent davantage de personnels plus jeunes et moins expérimentés. Les entreprises du côté achat se plaignent de jeunes opérateurs sur des *desks* de marché qui commettent des erreurs d'exécution et deviennent de plus en plus incapables de fixer des prix ou de gérer des positions. On constate également une réduction des vendeurs proactifs qui apportent des idées aux opérateurs du côté achat.

Cette tendance à la « juniorisation » et cette disparition des opérateurs et des vendeurs expérimentés entraînent des conséquences inattendues. Maintenant plus que jamais, les gestionnaires d'investissement suivent les « compétences » plus que le « nom de la société ». Pour le côté vente, le danger peut se matérialiser par le départ de clients

Ces importants mouvements sur l'échiquier provoquent de l'anxiété chez les personnels de la vente et de la négociation les plus anciens et expérimentés. Cependant, tout n'est pas nécessairement catastrophique. Tandis que les effectifs des vendeurs sont réduits, les effectifs des acheteurs augmentent. Les personnels expérimentés licenciés s'orientent maintenant vers le côté achat pour apporter leurs « compétences » directement vers les *desks* de gestion d'actifs. En outre, un grand nombre de ces « pièces de l'échiquier » se retrouvent désormais à la tête des différents nouveaux projets dans le domaine de la négociation électronique. Il est important pour le secteur de noter que ce mouvement sur l'échiquier du côté vente vers le côté achat peut aider les anciens acteurs du côté vente, mais cela ne signifie pas pour autant que ces acteurs apportent avec eux une contribution capitalistique.

La seule exception possible au phénomène de « juniorisation » et à la disparition de la négociation « à la voix » s'observe sur le compartiment des opérations de pensions. Sur ce marché, on estime encore que les courtiers plus anciens et expérimentés ajoutent de la valeur et apportent des qualités que le CLOB interbancaire ne peut pas apporter : les connaissances, la fluidité, la personnalité, l'expérience et la discrétion.

Enfin, de nombreux rôles réservés traditionnellement aux marchés des actions se retrouvent désormais sur les marchés des titres à revenu fixe. Il y a quelques années, personne dans la négociation des titres à revenu fixe n'avait jamais entendu parler de stratégie de structure de marché. Actuellement, nous pouvons constater l'apparition de rôles dans ce secteur avec des recrutements de « responsable mondial de la stratégie de la structure de marché du crédit », « responsable de la stratégie de liquidité et de la structure de marché », etc. En ces temps où il est difficile de réaliser des bénéfices, ces rôles s'avèrent vitaux pour la prise de décision concernant la rationalisation des activités et la compétitivité d'ensemble.

Conclusion

La négociation sur le marché obligataire connaît actuellement un bouleversement sans précédent, qui devrait se poursuivre dans les cinq à dix prochaines années. Il sera en grande partie douloureux, car la réglementation ne se mettra pas en place sans difficultés. La mise en place de la réglementation MiFID 2 et des autres réglementations aura certainement des conséquences sur les effectifs, la disponibilité des obligations et les futures stratégies d'investissement du côté achat.

Cependant, la réglementation et la technologie créent de nouvelles structures de marché. Tandis que cela posera des difficultés à certains acteurs du secteur, cela créera également des opportunités par le biais de l'innovation pour d'autres opérateurs. Ces participants deviendront à l'avenir les « survivants », au sens de Darwin, de la négociation électronique.

Émergence du *big data* : quelles évolutions du modèle économique de l'assurance ?

Thierry DEREZ
Président directeur général
Covéa

Amélioration de la connaissance de ses clients, nouveaux modèles tarifaires fondés sur une plus grande segmentation des risques, déferlement des objets connectés permettant le déploiement de nouveaux services personnalisés, etc. : les contours exacts du phénomène du « big data *» et de ses conséquences potentielles peuvent apparaître flous et les définitions différer d'une personne à une autre. Le sentiment est toutefois unanimement partagé que cette révolution technologique n'épargnera pas le secteur de l'assurance, et que les modèles économiques seront probablement largement différents d'ici quelques années, de ce qu'ils ont pu être par le passé.*

Cette perception est souvent associée à la perspective d'une démutualisation, résultant d'une individualisation poussée à l'extrême des offres et des tarifs d'assurance. Si le développement des nouvelles technologies et l'exacerbation des pressions concurrentielles pourraient effectivement aboutir à des segmentations beaucoup plus fines qu'actuellement, cette crainte doit toutefois être largement relativisée. Outre que des freins réglementaires existent et ne semblent pas en voie de diminution, une segmentation trop poussée irait à l'encontre de l'intérêt même des assureurs, en créant une volatilité des risques et des résultats excessive.

Des évolutions structurelles viendront également des nouveaux modes de relations entre les assureurs et leurs assurés (lors de la souscription et, plus encore, tout au long de la vie du contrat). À plus long terme, les mutations des risques sous-jacents eux-mêmes pourraient constituer des points de rupture structurels des modèles économiques de l'assurance. Le développement annoncé de la voiture sans conducteur en constitue un parfait exemple.

Dans ce cadre, l'accès aux données revêtira une importance décisive, susceptible d'avoir à terme un impact sur la stabilité financière. Il semble donc essentiel de définir des règles claires d'accès à ces données, fondées sur l'autodétermination et le libre choix de chacun.

Le *big data* : un phénomène protéiforme

Le phénomène du *big data* ou, dans une traduction francophone peu retenue, des mégadonnées, désigne l'émergence de données tellement volumineuses qu'elles ne peuvent être traitées avec les outils classiques de traitement de l'information. Cette évolution recouvre donc autant l'apparition des données elles-mêmes (en pratique des données numériques, toujours plus nombreuses et variées) que la capacité de les stocker et de les traiter au travers de méthodologies nouvelles et alternatives, ces deux aspects étant totalement indissociables l'un de l'autre.

On observe depuis plusieurs années des usages de plus en plus variés de ce phénomène, dans tous les segments de la connaissance (biologie, environnement, recherche aéronautique et spatiale, etc.) et dans tous les secteurs d'activité (automobile, grande distribution, secteur financier, etc.). Toutefois les perspectives de développement restent probablement encore largement insoupçonnées. Le champ d'analyse est surtout extrêmement variable, selon que l'on s'en tient à une définition stricte du phénomène, ou que l'on considère l'ensemble des usages pouvant indirectement naître de cette capacité nouvelle à traiter massivement les données. La frontière de cette deuxième acception est potentiellement mouvante puisque cela peut intégrer notamment des exemples de « plateformisation » (Uber) ou demain l'apparition de la voiture sans conducteur. Ces derniers développements ont en effet été permis, ou au moins favorisés, par les nouvelles capacités de traitement de l'information. Dans le cas d'Uber, la qualité de service repose par exemple étroitement sur la géolocalisation des clients et des véhicules, et sur la capacité à mesurer la demande dans l'instant afin d'adapter les tarifs et d'encourager l'offre. Dans le cas de la voiture autonome, les développements techniques dépendent également de l'analyse instantanée des informations captées, en provenance des autres usagers et des infrastructures de transport.

Le secteur de l'assurance n'échappe évidemment pas à la vague du *big data*, même si l'objectivité doit nous conduire à constater que le modèle économique n'a jusqu'ici pas été bouleversé. Les exemples d'application sont, là aussi, extrêmement diversifiés. Ils peuvent notamment concerner la relation client (meilleure connaissance des assurés et de leurs besoins, simplification des parcours de souscription, etc.), le développement de nouvelles offres ou modèles tarifaires (*pay how you drive*, bracelets connectés, etc.) ou, de manière moins visible pour le client, l'amélioration de l'efficacité opérationnelle (pilotage du portefeuille, détection des fraudes, etc.). Ces champs de développement sont protéiformes et concernent l'ensemble des directions ou services des organismes d'assurance ; il est donc difficile d'analyser le phénomène du *big data* et de ses conséquences potentielles sur le secteur de l'assurance dans son ensemble. Bien qu'une certaine interconnexion existe entre les différents aspects, nous essaierons ici d'analyser successivement l'impact sur les offres et la segmentation tarifaire (partie 1), sur la relation client (partie 2) et l'impact provenant de la mutation des risques sous-jacents eux-mêmes (partie 3).

1| Une segmentation tarifaire plus poussée, pas une individualisation des primes

Une des idées couramment entendues est que les assurés veulent aujourd'hui payer le « vrai prix de leur risque », c'est-à-dire la prime d'assurance qui correspond exactement à leurs caractéristiques et à leur comportement. Cette volonté, associée à la faculté croissante de comparer les prix – grâce aux devis en ligne ou aux comparateurs –, à la pression concurrentielle entre les acteurs et surtout à la capacité pour un assureur de connaître mieux chacun de ses clients pourrait, selon cette logique, aboutir demain à une totale individualisation des tarifs. Cette individualisation signifierait la disparition de ce qui est le fondement même de l'assurance : la mutualisation des risques, entre les assurés, entre les générations, entre les zones géographiques [1].

1 *Il ne faut toutefois pas confondre les notions de solidarité et de mutualisation. En effet, il est en principe possible de mutualiser des risques hétérogènes (la loi des grands nombres s'applique si les variables sont indépendantes, mais sans qu'elles soient nécessairement identiquement distribuées). L'assurance des risques industriels par exemple est une mutualisation de contrats et de tarifs sur mesure, donc individualisés.*

Cette considération doit être, sinon totalement écartée, du moins analysée avec une grande circonspection

Un client a, de manière générale, le souhait d'obtenir le meilleur service au meilleur prix. En assurance, cela correspond aux garanties les plus protectrices possibles compte tenu de son profil, assorties de services performants et d'une expérience utilisateur fluide, le tout au prix le plus contenu. Mais cette prime doit-elle pour autant correspondre, au moins aux yeux de l'assuré, au « vrai prix du risque » ? S'il en était ainsi, l'assurance constituerait une singularité, se distinguant de l'ensemble des autres activités économiques. Dans la plupart des approches économiques, le client définit en effet le prix qu'il estime légitime – son consentement à payer – en fonction de l'usage qu'il retire d'un bien ou d'un service, des équilibres de l'offre et de la demande qui sont à l'œuvre sur le marché, mais également de la régulation. Cette dernière peut prohiber certains modes de tarification, en vertu d'un consensus social ou au nom d'un objectif de politique publique. Le consentement à payer peut donc différer très substantiellement du prix de revient réel du bien ou service. Cela explique qu'un consommateur puisse accepter d'acheter des produits intégrant des marges élevées (luxe, *smartphones*, etc.) ou, qu'à l'inverse, il n'ait pas conscience de payer des prix parfois inférieurs aux prix de productions pour des produits ou services fortement subventionnés (transports, certains produits agricoles, etc.).

De manière tout aussi fondamentale, la notion même de « vrai prix du risque » ne correspond pas dans le domaine de l'assurance à une réalité mathématique intangible. Cela ne découle pas d'une mesure incontestable dont la perception serait identique entre l'assureur et l'assuré, ni même pour l'ensemble des assureurs. L'assurance repose, dans son fondement même, sur des calculs d'hétérogénéité, notion qui est souvent abusivement assimilée à celle d'aléa. Si l'assuré est bien exposé à un ensemble d'aléas, ce ne sont pas ces aléas que peut directement appréhender l'assureur, mais bien des hétérogénéités entre ses assurés dans la survenance des sinistres, qui sont la manifestation *ex post* de ces aléas [2]. Quelles que soient les sophistications actuarielles utilisées ou les jugements d'experts, les tarifications ont toutes pour point de départ des moyennes établies sur des populations considérées comme homogènes, et de tailles suffisamment importantes pour que l'application de la loi des grands nombres puisse avoir un sens statistique. Cette assimilation abusive entre l'aléa et l'hétérogénéité peut d'ailleurs parfois être source de malentendus, et faire perdre de vue que les mesures de risques purement quantitatives (par exemple Solvabilité II) résultent avant tout d'une appréciation indirecte des risques, et ne peuvent donc par essence atteindre qu'imparfaitement leur objectif (VaR à 99,5 % à horizon un an pour l'exemple précité). Mais cela doit surtout nous faire prendre conscience que le « vrai prix du risque » n'existe pas, et constitue par construction même une notion subjective qui différera d'un assureur à l'autre. En effet, le « vrai prix du risque » correspondrait au coût moyen de la catégorie d'assurés considérée mais, outre que deux assureurs peuvent avoir des statistiques légèrement distinctes sur une catégorie donnée, la catégorisation elle-même n'est pas univoque. Les progrès de la médecine permettant d'isoler un facteur de risque conduiront par exemple à découper une catégorie en deux. L'accès à telle ou telle information fournie par un *smartphone* ou un objet connecté permettra également de découper une catégorie en deux, mais différemment. Deux assureurs distincts assigneront ainsi un « juste prix » différent à un même assuré en fonction des données dont ils disposent. Un couple {assureur ; assuré} donné, plongé dans deux sociétés différemment évoluées technologiquement ou imposant des contraintes d'exploitation des données différentes, verra de la même manière un « vrai prix du risque » différent.

Cela ne doit pourtant pas nous amener à conclure que le *big data* n'engendrera aucune modification de la tarification. Cela revient, au contraire, à poser la question de la segmentation : jusqu'à quel niveau de détail peut-on descendre pour construire des catégories homogènes d'assurés, suffisamment fines pour que la tarification soit adaptée (et donc compétitive), tout en restant assez vastes pour disposer de statistiques qui aient un sens ? La réponse est de nature technique, et à ce titre le *big data* peut constituer une évolution importante, mais elle est également et très fondamentalement de nature sociale et réglementaire.

2 *Cf. Frezal (S.) (2015) : « Aléa et hétérogénéité : l'amalgame tyrannique ».*

Nous assistons actuellement, et ce mouvement se poursuivra vraisemblablement dans les années à venir, à une forte tendance de segmentation des assurés, assortie de différenciations tarifaires plus marquées entre les « bons » et les « mauvais » risques. Ce mouvement est aujourd'hui d'ordre plus commercial que technique : la forte pression concurrentielle, couplée à la faculté de résiliation à tout instant née de la loi Hamon, peut conduire certains acteurs à concentrer leurs efforts sur certaines populations d'assurés jugées plus rentables. Il n'est pas à exclure que cela se renforce au gré des développements techniques. Par exemple, si les comportements au volant peuvent être modélisés de façon suffisamment fiable, ces informations pourraient devenir un élément central de la tarification de l'assurance automobile, en renforçant donc la segmentation tarifaire par rapport à la situation actuelle.

Mais jusqu'où cette segmentation peut-elle aller ? Il est difficile de répondre de manière définitive à cette question mais de nombreux éléments vont à l'encontre de l'individualisation totale des tarifs souvent agitée comme un chiffon rouge. Comme cela a déjà été évoqué, il existe des freins techniques : une segmentation excessive aboutirait à un découpage tel que les statistiques ne seraient plus pertinentes. Cela se traduirait donc par une volatilité excessive de la sinistralité sur chaque classe homogène de risque, dont le coût excéderait sans doute les gains marginaux obtenus en termes de tarification. Une segmentation excessive irait donc totalement à l'encontre de l'intérêt même des assureurs [3], et donc *in fine* des assurés. L'aspect temporel ne doit par ailleurs pas être occulté : en assurance, les tarifications sont usuellement établies pour une durée assez longue (généralement un an, avec au mieux un ajustement mensuel), ce qui limite l'intérêt d'une prise en compte de données instantanées. Une tarification trop segmentée pourrait en outre exposer les assureurs à une modification du risque mal maîtrisée pendant la période de garantie, liée par exemple à un changement de comportement de certains assurés.

Il existe, par ailleurs, des freins réglementaires. D'ores et déjà, la réglementation pose des limites strictes qui visent à éviter des discriminations et à opérer une solidarité. Cette solidarité est souvent intergénérationnelle (par exemple le système des coefficients de réduction/majoration en assurance automobile, qui tend à minorer la prime des jeunes conducteurs par rapport au coût réel de leur risque ; ou à l'inverse le plafonnement des écarts de tarifs entre les plus jeunes et les plus âgés dans les contrats de complémentaire santé référencés, qui diminue la prime de ces derniers). Cet encadrement ne semble pas prêt à s'estomper bien au contraire, comme en témoigne l'interdiction posée fin 2012 d'exercer des différenciations tarifaires entre les hommes et les femmes. Dans cette même logique, l'augmentation de la segmentation, si elle diminue demain les solidarités entre les assurés ou les solidarités intergénérationnelles, et plus encore si elle aboutit à des situations d'exclusion d'assurance, soulèvera inévitablement la question de son acceptabilité sociale et donc son encadrement réglementaire.

2| LES ÉVOLUTIONS DE LA RELATION CLIENT

Un autre aspect de l'évolution du modèle économique de l'assurance liée au *big data* porte sur le domaine de la relation client. Le *big data* a en effet la faculté de modifier deux aspects fondamentaux : la connaissance du client, et la nature et la fréquence des relations que l'on peut entretenir avec lui. Le phénomène n'est toutefois pas propre à l'assurance et concerne l'essentiel des secteurs d'activités.

En termes de connaissance du client, le phénomène du *big data* poursuit dans le secteur de l'assurance une dynamique qui n'est pas nouvelle, et qui repose sur l'idée simple que plus on connaît un assuré, mieux on est à même de lui proposer des produits adaptés, au moment où il en a besoin. Au-delà des simples obligations de recueil des besoins du client et de conseil, cette dynamique a déjà conduit à un renforcement des informations demandées lors de la souscription ou du sinistre, ou à la meilleure utilisation de ces informations (développement des CRM [4]). Le *big data* peut amplifier ce phénomène, en agrégeant à ces données propres des données tierces (réseaux sociaux, objets connectés, etc.).

3 *Cf. Charpentier (A.), Denuit (M.) et Elie (R.) : « Segmentation et mutualisation, les deux faces d'une même pièce ».*
4 Customer Relationship Management.

C'est probablement surtout dans le domaine du *marketing* que le *big data* ouvre le plus de perspectives d'évolutions. La nature et la fréquence exponentielle des informations numériques disponibles (recherches internet, cookies, etc.) rendent possible une identification beaucoup plus fine que par le passé des besoins du client et pourraient donc permettre de s'adresser à lui au moment le plus adapté. Cela permettra de lui proposer, lors de la souscription, une offre parfaitement ciblée et, tout au long de la vie du contrat, des services mieux personnalisés. Cette mutation n'est pas exempte de dangers pour les acteurs du marché, et ouvre notamment le risque d'intermédiation (ou d'« uberisation », selon le sens que l'on veut donner à ce mot). Un nouvel acteur, capable de capter mieux que les autres ces flux d'informations pourrait ainsi s'intermédier entre les assureurs et les assurés, dans un rôle de courtier et capter une partie conséquente de la marge opérationnelle. Mais ce phénomène offre parallèlement des opportunités réelles d'amélioration de la relation avec l'assuré.

Ces phénomènes ne sont, encore une fois, pas propres à l'assurance mais touchent probablement ce secteur avec une acuité particulière. Parce qu'il s'agit d'une activité de service, ce service étant une promesse qui ne s'exerce qu'en cas de réalisation d'un sinistre, et parce que l'assurance reste dans bien des cas perçue par l'assuré comme une obligation autant que comme une protection. Les assureurs ont largement compris la nécessité de modifier cette perception, et travaillent depuis plusieurs années à un élargissement de leur rôle et à de nouveaux modes de relations avec les assurés (prévention, développement de nouveaux services). Les évolutions numériques, et le *big data* en particulier, peuvent concourir à cet élargissement en conduisant à des interactions plus nombreuses et mieux ciblées. Le développement des objets connectés peut à ce titre être intéressant, en offrant tout à la fois la possibilité aux assurés de transmettre à leurs assureurs davantage d'informations, et à ceux-ci de sortir définitivement d'un simple rôle de payeurs de sinistres.

Tout cela n'est possible que si les assureurs parviennent à rassurer pleinement leurs assurés sur l'utilisation qui est faite de leurs données. Cela nécessite notamment de démontrer que les données librement communiquées serviront à une meilleure personnalisation des offres ou des services, et non à une sélection abusive des risques. Le cadre réglementaire est déjà aujourd'hui extrêmement contraignant en matière de protection des données personnelles et de respect de la vie privée des clients – avec des règles encore plus strictes en matière de santé. Une certaine méfiance subsiste toutefois indiscutablement, qui ne pourra être levée que par une meilleure communication de la part des assureurs, sur le cadre dans lequel s'exercent la transmission et l'utilisation de ces données.

3| La mutation des risques sous-jacents, un bouleversement potentiel de l'assurance

Un troisième aspect lié aux capacités nouvelles de capter et d'appréhender les données porte sur une modification de la nature même des risques. Cette évolution, si elle est moins immédiate que les deux précédentes, n'en est que plus structurante puisque certaines d'activités d'assurance pourraient purement et simplement disparaître, au profit de nouveaux risques et donc de nouvelles opportunités d'assurance.

Nous n'aborderons pas en détail ici la question du cyber-risque, qui mérite une réflexion propre. Si la cyber-assurance, dont le marché reste encore limité – total de primes de 2,5 milliards d'euros en 2015, collectées essentiellement aux États-Unis – est vraisemblablement destinée à augmenter significativement dans les années à venir, son développement est conditionné par la capacité à mesurer réellement les risques dans un univers en très rapide évolution. En outre, continue à se poser pour les entreprises le choix entre l'option d'une solution technique (sécurisation des données et des infrastructures, *back up*, etc.), ou celle d'une solution assurantielle.

L'émergence de la voiture autonome constitue en revanche un exemple particulièrement intéressant d'une mutation possible (sinon probable) des usages ou des risques, heurtant de plein fouet le secteur de l'assurance. Ce développement est là encore étroitement lié aux nouvelles capacités à traiter dans l'instant des flux toujours croissants de données : données captées des autres véhicules en circulation, des infrastructures elles-mêmes, demain données transmises par ces dernières, etc.

La maturité et plus encore la vitesse de déploiement de cette technologie sont incertaines et dépendent de nombreux paramètres : évolutions techniques bien sûr, cadre réglementaire, capacité à convaincre les utilisateurs à grande échelle, ce qui nécessite de démontrer une sinistralité maîtrisée, etc. Il est donc difficile de définir à quel horizon une portion significative du parc automobile sera constituée de voitures sans conducteur. Mais le phénomène lui-même semble inéluctable.

Il est difficilement contestable que ces développements ne pourront qu'avoir des conséquences extrêmement structurantes pour le secteur de l'automobile et, par ricochet, sur celui de l'assurance automobile. Plusieurs études existent sur le sujet, tentant de quantifier ces phénomènes. L'une d'entre elles [5] conclut que l'émergence de la voiture sans conducteur, couplée avec les nouveaux usages qui pourraient en résulter, pourrait aboutir à une diminution de plus de 50 % du parc automobile à horizon 2040. Nombre de ménages pourraient en effet décider de ne plus posséder de véhicules en propre (ou au moins d'en diminuer le nombre) et d'avoir recours à la place à des services de location, s'il devient possible d'avoir accès de façon presque instantanée à un véhicule autonome au lieu que l'on souhaite. Ce choix découlerait directement du coût comparé entre l'achat d'une voiture et l'usage, même régulier, d'un véhicule autonome loué. Par répercussion, cela pourrait entraîner une baisse générale de la sinistralité – et donc des primes d'assurance versées – et une bascule substantielle de l'activité de l'assurance automobile, d'une assurance individuelle vers une assurance de flotte. Tout cela sans même évoquer la question juridique épineuse de la responsabilité en cas de sinistre : constructeur automobile, exploitant, éventuel fournisseur de la solution informatique ?

Toutes ces anticipations ou estimations, les auteurs de ces études le reconnaissent bien volontiers, sont à considérer avec précaution. Outre les incertitudes sur la vitesse de déploiement mentionnées plus haut, la modification des usages dépendra de la perception même de l'automobile qu'auront les générations futures. Mais cet exemple illustre clairement comment une rupture technologique, née du traitement des données et des progrès de l'informatique, peut modifier la nature même d'un risque et constituer un bouleversement de l'activité d'assurance.

4| Conclusion : l'accès aux données, point décisif de la bataille concurrentielle et enjeu potentiel de stabilité financière

L'ensemble de ces aspects soulève la question fondamentale de l'accès aux données. Il est, en effet, incontestable qu'un acteur parvenant à capter mieux que les autres certaines sources de données clés disposera demain d'un avantage concurrentiel. Le phénomène sera évidemment décuplé s'il peut s'assurer d'un accès exclusif à des flux d'informations. Cela souligne l'aspect plus que jamais vital d'une bonne « expérience client ». Dans l'ensemble des secteurs où l'on a pu récemment constater un phénomène d'intermédiation, les acteurs responsables de celle-ci (Uber, Airbnb, mais aussi Google pour la téléphonie mobile) ont réussi à s'imposer grâce à une proposition de service simple, fluide et efficace qui a su convaincre les utilisateurs. C'est cette offre qui leur a permis d'avoir un accès privilégié aux données de leurs clients et de conforter leur situation, et non l'inverse. La bataille commerciale ne se gagne donc pas grâce aux données, mais bien grâce à une expérience client inattaquable, qui elle-même donne accès aux données. On peut à ce titre souligner un certain décalage entre les attentes des clients, qui anticipent une offre de service toujours plus fluide et instantanée, notamment au travers des canaux numériques, et le cadre réglementaire (par exemple en matière de vente à distance de services financiers) qui ne permet pas toujours d'y répondre pleinement.

Il peut toutefois exister des cas où l'excellence de l'expérience client ne suffit pas à s'assurer l'accès à certaines données spécifiques. L'illustration la plus probante est celle de l'automobile, en cas de développement de véhicules autonomes reposant sur une technologie unique ou même, à plus court terme, si quelques constructeurs ou équipementiers contrôlent l'ensemble des données récoltées par les « véhicules intelligents ». Mais ce phénomène peut potentiellement être étendu à d'autres branches d'assurance de particulier (par exemple en assurance habitation du fait des objets connectés), l'assurance

5 *Cf. Johnson (B. A.) (2015) : « Disruptive mobility », Barclays Research Department.*

d'entreprise semblant, du moins pour quelque temps, moins concernée. Cela a évidemment des conséquences commerciales potentielles importantes. On a évoqué plus haut le risque d'intermédiation. Celui-ci se combine, pour les assureurs, avec celui d'être mis en concurrence les uns avec les autres par des acteurs tiers qui détiendraient un accès exclusif à certaines technologies ou données clés.

Même si cela ne constitue pas réellement une menace à court terme, cela peut également entraîner des conséquences en matière de stabilité financière. Si des acteurs importants peuvent du jour au lendemain perdre une part significative de leur activité et de leur rentabilité, du fait de la perte d'accès à certaines données clés, cela peut engendrer une fragilité pour le système dans son ensemble. L'existence même de ce risque modifierait probablement, par répercussion, la stratégie d'investissement des assureurs afin de tenir compte de cette plus grande incertitude (réduction des actifs risqués, diminution de la duration des actifs, etc.). Compte tenu des masses en jeu, et du fait que ce phénomène serait alors constaté dans l'ensemble des marchés mondiaux, l'impact sur le financement de l'économie serait très significatif. Ces risques apparaissent aujourd'hui assez théoriques et diffus. Cet aspect ne doit toutefois pas être totalement ignoré dans les réflexions futures.

À plus court terme, il importe de définir un cadre clair d'accès aux données. Afin de garantir une concurrence saine et plus encore une protection satisfaisante des données personnelles et de la vie privée des individus, cet encadrement devrait proclamer le principe de l'autodétermination, c'est-à-dire le droit pour chacun de décider de l'usage fait de ses données personnelles. De la sorte, chaque individu pourrait décider de les transmettre librement à un tiers et, symétriquement, de lui demander ultérieurement de les supprimer. Dans un univers, où l'accès à l'information occupera plus que jamais une place centrale, il apparaît essentiel de créer les conditions de la confiance, ce qui nécessite avant tout une grande transparence.

Le *big data* : défis et opportunités pour la surveillance de la stabilité financière

Mark D. FLOOD
Directeur de la recherche
Bureau de la recherche financière
du département du Trésor américain

H.V. JAGADISH
Professeur d'ingénierie électrique et d'informatique, chaire Bernard A Galler
Université du Michigan

Louiqa RASCHID
Professeur de systèmes d'information
Université du Maryland

*Les données enregistrées ou transmises au sein du secteur financier et lisibles électroniquement représentent un volume dont la croissance exponentielle a des conséquences importantes en termes de suivi macroprudentiel. Le principal défi qui se pose est celui de l'évolutivité (*scalability*) des institutions et des processus, compte tenu de la variété, du volume et de la vitesse de cet afflux massif de données (*big data*). Un tel déluge de données offre également des opportunités sous la forme de flux d'information nouveaux, rapidement disponibles et de grande valeur, à un niveau de détail et de granularité plus poussé. Une différence d'échelle peut devenir une différence de nature, les processus préexistants étant dépassés alors que l'on voit émerger des réponses innovantes.*

Malgré l'importance et l'omniprésence des données sur les marchés financiers, les processus de gestion de cette ressource fondamentale doivent s'adapter. Cela vaut en particulier pour la stabilité financière ou l'analyse macroprudentielle, domaines dans lesquels les informations provenant des régulateurs du monde entier doivent être rassemblées, vérifiées et intégrées pour élaborer une image cohérente du système financier afin de soutenir les décisions de politique économique. Nous examinerons les principaux défis que posent l'accroissement du volume et de la diversité des données financières pour la surveillance du risque systémique. La discussion s'articule autour de cinq grandes missions de surveillance dans le cycle de vie habituel des données prudentielles.

*NB : Les points de vue et opinions exprimés ici sont ceux des auteurs et ne représentent pas nécessairement la politique ou la position officielle de l'*Office of Financial Research *ou de la direction du Trésor américain. Les auteurs remercient Greg Feldberg, Julie Vorman et David vun Kannon pour leurs précieux commentaires. Les commentaires sont les bienvenus, tout comme les suggestions d'amélioration, et doivent être adressés aux auteurs.*

1| Contexte

Les données massives (*big data*) représentent plus qu'un simple accroissement des besoins de stockage ou que la collecte de données à partir de plates-formes de média sociaux comptant des millions de participants. Le caractère « massif » de ces données constitue le symptôme de problèmes d'évolutivité à un ou plusieurs niveaux, ce que résument les « quatre V », à savoir volumétrie, vélocité, variété et véracité (IBM, 2016). Le terme de « données massives » est trompeur, car il suggère que le caractère « massif » est intrinsèque aux ensembles de données : plus exactement, ce caractère massif décrit la relation entre un ensemble de données et le contexte de son utilisation [1]. Un ensemble de données est trop massif pour un cas spécifique d'utilisation lorsqu'il devient impossible, d'un point de vue informatique, de le traiter à l'aide des outils traditionnels (MongoDB, 2016). L'évolutivité est une contrainte forte pour n'importe quel processus, en cas d'extrapolation trop poussée. Le *big data* peut créer un point d'inflexion où les différences d'échelle impliquent des différences transformationnelles en termes de coûts et de bénéfices associés à l'utilisation des données.

Les données massives ne sont pas le seul défi qui se pose aux autorités de supervision de la stabilité financière, dont le champ d'action recouvre potentiellement l'ensemble du système financier et qui sont confrontées à la question de l'évolutivité des données dans de nombreux domaines [2]. Des facteurs économiques fondamentaux, tels que l'incertitude macroéconomique, les conditions du crédit, la volatilité des marchés, la liquidité et le risque de contagion, demeurent au cœur des préoccupations. Dans le domaine du mesurage, le principal défi tient souvent au manque plutôt qu'à l'excès d'informations à intégrer, analyser et rendre exploitables. Récemment, certaines publications officielles, telles que le rapport sur la stabilité financière (*Financial Stability Report*) de l'*Office of Financial Research* (OFR, 2015), ont mis l'accent sur la tâche primordiale que représente le comblement des lacunes en matière d'informations : le niveau de couverture des données, leur qualité, et la possibilité d'accès à celles-ci sont-ils insuffisants pour que les autorités de surveillance accomplissent leurs missions dans le cadre de leurs mandats ? Les questions existentielles de disponibilité des données doivent prendre le pas sur les questions d'évolutivité relatives à leur gestion. Le récent *One Bank Research Agenda* de la Banque d'Angleterre (2015) considère que les données massives, notamment les flux d'informations continus (*news feeds*), les média sociaux et les données relatives aux transactions, constituent des sources d'informations inexploitées potentiellement importantes pour la recherche dans le domaine de l'activité de banque centrale.

Avec la prolifération des technologies de captage de l'information dans tous les secteurs de la société, appréhendée pour l'essentiel à travers nos interactions avec l'internet et les réseaux cellulaires, de nombreux secteurs d'activité se trouvent simultanément confrontés à des problèmes d'extensibilité liés au *big data*. Ces défis révolutionnent divers domaines, notamment les statistiques officielles (Kitchin, 2015), la recherche scientifique (Hey *et al.*, 2009), la vente au détail (Manyika *et al.*, 2011), la santé (Horvitz, 2010) et même l'art (Somerset House, 2015). Le secteur des services financiers n'est pas épargné. Casey (2014) identifie six catégories générales de données s'assemblant pour former un stock de données massives pertinentes pour les banques centrales : macroéconomiques, données d'enquêtes, provenant d'institutions financières, provenant de tiers, microéconomiques et non structurées (rapports, média sociaux, etc.). Nous mettons l'accent sur les données officielles collectées par les superviseurs macroprudentiels, mais un grand nombre des questions examinées concernent également d'autres catégories de données.

Il en résulte que de nouveaux ensembles de données émergent de diverses sources, notamment des

1 *Diebold (2012) fait la remarque suivante : « ….*dans vingt ans, le lecteur rira sans doute de mon affirmation implicite actuelle selon laquelle un ensemble de données de 200 gigabits est important *», puis il souligne que le Grand collisionneur de hadrons, le plus grand accélérateur de particules du monde, génère aujourd'hui un pétaoctet (10^{15} octets) de données par seconde.*

2 *Nous nous intéressons davantage aux questions de gestion des données qu'aux spécificités des autorités de surveillance réglementaire. Nous utilisons les termes suivants de façon interchangeable afin d'éviter d'alourdir le texte : « autorités de surveillance (ou de supervision) de la stabilité financière », « superviseur macroprudentiel » et « superviseur du risque systémique », qui font référence aux autorités, tant nationales qu'internationales, responsables de la sensibilisation et de la réponse aux crises et aux perturbations du secteur financier.*

collectes officielles, avec, par exemple, les détails relatifs à l'exposition au risque dans le cadre des tests de résistance, des tiers fournisseurs avec la veille de marché et les plates-formes de média sociaux, et des moteurs de recherche sur l'internet public. Ces nouvelles sources partagent une caractéristique commune : une forte augmentation des exigences en matière de données. Les activités de négociation, par exemple, progressent de manière exponentielle et à un rythme de plus en plus élevé (Flood, Mendelowitz et Nichols, 2013, graphique 1 ; Kirilenko et Lo, 2013, p. 51). La croissance continue de la puissance des capacités de traitement informatique et l'automatisation de la finance ont conduit les superviseurs à se réorienter vers une régulation « fondée sur les données » ; cf. par exemple, Stein (2015), CFPB (2013) et FRB (2015) [3]. Un exemple marquant de supervision fondée sur les données est constitué par la collecte et l'analyse des clauses contractuelles détaillées des prêts bancaires et des portefeuilles de négociation dans le cadre des programmes de tests de résistance menés aux États-Unis et en Europe depuis la crise financière de 2007-2009. L'ampleur du problème dépasse inexorablement la capacité de certains processus préexistants dans lesquels les missions d'inspection et d'analyse sont réalisées par des êtres humains. « Vous ne pouvez pas résoudre des problèmes exponentiels avec des solutions linéaires » ; il faut combattre l'informatique par l'informatique [4].

L'exploitation de ces nouvelles ressources nécessitera des approches innovantes de la gestion de données et de l'analyse statistique, ce dont les autorités de surveillance de la stabilité financière ont pris bonne note. Ces défis peuvent se poser dans les situations les plus inopportunes, par exemple au milieu d'une crise financière. Les usages potentiels des données massives s'appliquent à l'intelligence contextuelle du processus, ainsi qu'aux pics de charge des ressources analytiques au cours d'épisodes de tensions sur les marchés. Une réponse efficace nécessite une évaluation des facteurs sous-jacents à l'œuvre.

Dans de nombreux secteurs, l'expérience montre que le point de transition, à partir duquel l'évolutivité commence à être contraignante, est susceptible d'apparaître dans l'une des quatre grandes dimensions du *big data*, généralement appelées les « quatre V ». Au plan macroprudentiel, il s'agit par exemple des points suivants :

• **Volumétrie** : pour résumer, il s'agit simplement de la taille (en octets) d'un ensemble de données, qui peut exercer une pression sur le stockage et les ressources informatiques. Les ensembles de données économiques modernes excèdent souvent la capacité de traitement des bases de données relationnelles à l'aide du langage de requête structurée SQL (*Structured Query Language*), créant ainsi un marché pour les outils dits « *NoSQL* » (Not Only SQL), d'après Varian (2014). Dans certains cas, on peut atténuer cette charge en agrégeant ou en compressant les données. Le passage à un audit analytique centré sur les données pour l'analyse réglementaire des enregistrements comptables financiers (AICPA, 2015) constitue un exemple de mission de surveillance financière qui enregistrera un accroissement significatif du volume de données par rapport aux pratiques préexistantes.

• **Vélocité** : le rythme auquel les données arrivent, pouvant surcharger la bande passante du réseau et ralentir l'analyse en temps réel (O'Hara, 2015). La supervision macroprudentielle recouvre par exemple la surveillance en temps réel des flux de données à haute fréquence durant un krach éclair (Berman, 2015). Par leur conception même, les sociétés de *trading* haute fréquence (THF) transmettent des rapports et des messages liés aux transactions à la limite technique de la latence du réseau, pesant ainsi sur le débit des processus situés en aval.

• **Variété** : la diversité des schémas, ou structures formelles, de données en provenance de différentes structures, qui peut exercer des tensions sur les processus d'intégration des données (Halevy, *et al.* 2006). Cela s'applique à l'intégration des systèmes préexistants après une fusion bancaire et également à l'intégration à l'échelle du système. C'est le cas par exemple de l'alignement et de la synchronisation des

3 *Pattison (2014) offre une interprétation de cette tendance du point de vue du secteur. Récemment, des conférences sur les données massives dans le cadre de la surveillance financière ont été accueillies par la Banque d'Angleterre (Bholat, 2015), la Sveriges Riksbank (Hokkanen* et al.*, 2015) ainsi que par la Banque centrale européenne et l'Institut international des prévisionnistes (*International Institute of Forecasters – *IFF ; 2014).*

4 *Attribué au professeur Banny Banerjee (Chase, 2015).*

Schéma
Le cycle de vie des données prudentielles

Source : Office of Financial Research.

procédés d'identification d'entités juridiques pour une large gamme d'ensembles de données gérés de façon indépendante (Rosenthal et Seligman, 2011). Sans coordination, l'alignement des enregistrements d'identifiants entre *n back offices* nécessite (n^2-n) mises en cohérence entre eux ; par exemple, 10 *back offices* impliquent 90 mises en cohérence (Flood, 2009).

• **Véracité** : un taux d'erreur élevé sur les données peut affecter les processus de validation, d'intégration et de curation de données (Dong et Srivastava, 2013). Le maintien de la qualité des données détaillées et granulaires relatives aux portefeuilles des banques dans le cadre des tests de résistance en constitue un exemple (Hunter, 2014). L'intégrité des données étant souvent évaluée en réconciliant les données point par point, la pression liée à la véracité des données peut s'accroître de façon exponentielle avec les volumes de données.

Dans la suite de cet article, nous relieront ces problèmes de flexibilité liés au *big data* aux défis particuliers auxquels sont confrontées les autorités de surveillance de la stabilité financière en termes de données. Le rapport sur la stabilité financière de l'OFR (OFR, 2015) organise ces questions autour de trois axes : la portée, la qualité et l'accès. Globalement, ces trois dimensions permettent de répondre aux questions suivantes : quelles données collecter ? Comment gérer et utiliser au mieux les données ? Qui devrait avoir la possibilité de voir les données ?

Dans les sections suivantes, nous abordons ces mêmes questions, mais l'analyse est organisée en fonction des cinq phases importantes du cycle de vie habituel des données massives (Jagadish *et al.*, 2014), en les plaçant dans le contexte de la surveillance financière. Le schéma 1 présente ces phases : collecte, nettoyage, intégration, analyse et partage.

2| Collecte des données

La première étape de la supervision fondée sur les données est la collecte d'informations concernant les participants au système financier. La collecte de données est un exercice d'instrumentation du système et le niveau de résolution appropriée du mesurage constitue une préoccupation fondamentale en termes de conception. Le processus de mesure revient nécessairement à réaliser une projection d'un système financier profondément nuancé sur un espace de mesure discret, des détails importants risquant par conséquent d'être perdus dans le processus. Une façon de remédier à la déperdition (c'est-à-dire le degré de perte d'information lié à la projection) est d'améliorer la résolution au sein du processus de mesurage, permettant ainsi aux utilisateurs d'atteindre un niveau de détail supplémentaire. S'agissant des données de stabilité financière, la résolution recouvre quatre dimensions fondamentales : la couverture, la fréquence, la granularité et le niveau de détail.

Couverture : traditionnellement centrée sur les données comptables microprudentielles des sociétés financières, par exemple les rapports 10-K de la *Securities and Exchange Commission* (SEC, 2014), et les données sur les prix et la volatilité des marchés financiers, telles que celles utilisées dans le cadre des exigences de fonds propres de Bâle, fixées aux États-Unis par le Système fédéral de réserve et l'*Office of the Comptroller of the Currency* (FRB-OCC, 2013). Toutefois, la crise a démontré que des vulnérabilités peuvent apparaître au niveau des angles morts qui ne sont pas couverts par la collecte de données formalisée. Ainsi, en septembre 2008, « les régulateurs étaient loin d'en savoir assez sur les activités de produits dérivés de gré à gré de Lehman Brothers et d'autres banques d'investissement, qui étaient pourtant des opérateurs de premier plan dans ce domaine » (FCIC, 2011). Une des réponses a été de mettre l'accent sur l'identification et la correction

de ces lacunes dans les données. Récemment, par exemple, l'OFR a travaillé avec d'autres régulateurs à la collecte de nouvelles données sur les opérations de pensions bilatérales et les accords de prêts de titres (Baklanova, *et al.*, 2015). Au plan international, l'initiative *Data Gaps* du G20 constitue l'effort le plus marquant visant à étendre l'information prudentielle. Les ministres des Finances du G20 et les gouverneurs des banques centrales ont lancé l'initiative *Data Gaps* après la crise de 2009, avalisant la mise en œuvre de 20 recommandations par le Conseil de stabilité financière (CSF) et le Fonds monétaire international (FMI) ; cf. CSF-FMI (2015) et Cerutti, *et al.* (2014).

Fréquence : se rapporte à la résolution temporelle des mesures. La plupart des collectes de données sont fondées sur des instantanés discrets répétés de certains aspects du système financier visant à constituer un ensemble de données mesurées à des intervalles de temps réguliers, tel que la collecte mensuelle des avoirs détenus par les fonds d'investissement monétaires réalisés par la SEC (2016). On suppose habituellement que les données sont échantillonnées à intervalle régulier et fini à partir d'un processus sous-jacent continu évoluant dans le temps. L'économétrie traditionnelle fournit une large gamme d'outils permettant d'analyser des ensembles de données de panel, une observation stroboscopique périodique du système visant à collecter des observations à intervalles réguliers peut ainsi se révéler extrêmement utile à l'analyse. Malheureusement, l'hypothèse de lissage temporel ne tient pas toujours, notamment pour les risques systémiques, pour lesquels les vulnérabilités microprudentielles peuvent être masquées par de l'habillage des comptes et la soudaineté des événements macroprudentiels, alimentés par la panique des investisseurs et d'autres effets de rétroaction. Le résultat peut être une espèce de « cécité d'échantillonnage », dans lequel le phénomène étudié peut avoir lieu entre deux échantillons instantanés. Une fréquence d'échantillonnage plus élevée ne remédie pas forcément à cette cécité. À mesure que la fréquence des observations s'accroît, le bruit de microstructure domine de plus en plus les informations sur les séries de prix, ainsi que sur la volatilité réalisée correspondante et les estimations de corrélation (Aït-Sahalia et Jacod, 2014).

Granularité : définit le niveau et les techniques d'agrégation des données, qui est habituellement réalisée en calculant la somme ou la moyenne par rangées dans un tableau de base de données. Ce procédé présente des avantages et des inconvénients. L'agrégation est une conversion qui entraîne une perte d'information, ce qui incite à acquérir l'information au niveau de résolution le plus élevé possible pour ensuite fournir des relevés agrégés et/ou filtrés en fonction des besoins. Il est plus facile de se débarrasser d'informations que d'en recréer. D'autre part, calculer la somme et la moyenne permet de réduire les volumes de données bruts, de lisser les erreurs de mesure aléatoires et de préserver la confidentialité. La piste d'audit consolidée (*Consolidated Audit Trail* – CAT) planifiée par la SEC collectera et identifiera chaque ordre, annulation, modification et transaction exécutée pour toutes les actions et options cotées sur l'ensemble des marchés américains (SEC, 2012). La CAT atteint un niveau sans précédent de granularité dans le domaine de l'information financière. Au terme de cinq ans d'activité, la CAT devrait générer plus de 100 milliards d'enregistrements par jour, occupant quotidiennement plus de 20 téraoctets de stockage pour finalement dépasser les 20 pétaoctets (Rauchman et Nazurak, 2013). Toutefois, au-delà de la charge opérationnelle que représentent le développement et la maintenance des logiciels ainsi que d'autres routines (Rossi, 2014), l'agrégation introduit d'autres défis. Elle peut masquer d'importantes nuances en termes d'exposition au risque. Il est par exemple bien connu que les mesures agrégées de la performance ne saisissent pas tous les détails du risque de portefeuille (Foster et Young, 2010).

Détail : se rapporte aux attributs spécifiques saisis pour chaque entité (par exemple une entreprise ou une transaction) inclus dans la couverture ; habituellement présenté en colonnes dans un tableau de base de données. Par exemple, le véhicule visant à faciliter les déclarations obligatoires pour les transactions sur obligations du secteur privé (*Transaction Reporting and Compliance Engine* – TRACE), développé par la *Financial Industry Regulatory Authority* (FINRA) existe en deux versions, confidentielle et publique, selon que l'ensemble de données inclut ou non les identifiants de la contrepartie pour chacune des transactions. La version confidentielle permet une analyse beaucoup plus détaillée des interactions entre opérateurs, générant potentiellement des informations importantes sur la concentration des positions et de la formation de la liquidité. Les préoccupations liées à l'agrégation, telles que les coûts de stockage et la confidentialité, affectent également le détail, mais elles ne sont pas les seules questions liées à l'évolutivité se posant dans ce domaine.

Le contenu informatif d'un ensemble de données peut facilement se détériorer, car les processus situés en aval filtrent, normalisent et agrègent les données. La documentation relative à la provenance des informations, ainsi que d'autres métadonnées clés peuvent-être perdues au fil du temps ou bien le lien avec le contexte d'origine qui rendait ces données significatives peut être rompu (Buneman et Tan, 2007). Le contenu informatif d'un ensemble de données peut également s'accroître avec le temps, *via* l'intégration d'autres sources de données (Zhao *et al.*, 2004). Il est donc important de se préparer à de nouvelles phases d'organisation et d'intégration des données au moment de leur saisie.

Les exigences en matière d'information prudentielle se modifient au cours du temps, à mesure que les conditions de marchés évoluent. Par conséquent, il est souvent difficile de formuler avec précision et à l'avance les exigences relatives aux données. Dans certains cas, les autorités de surveillance de la stabilité financière souhaiteront rassembler des informations à des fins de recherche plutôt que pour satisfaire les besoins immédiats de surveillance, ou bien pour tester la validité de modèles ou encore pour la réconciliation d'autres sources d'information. Surtout, les exigences en matière de données peuvent changer brusquement et de façon imprévisible durant une crise financière. Cela constitue un argument fort en faveur de normes robustes applicables aux données permettant aux organes de supervision d'intégrer rapidement de nouvelles sources de données durant les épisodes de tensions.

3| Nettoyage des données

Les problèmes d'évolutivité affectent également la phase suivante, le nettoyage des données, généralement réalisé par le biais d'une série de vérifications et de transformations qui rendent un jeu de données conforme à une liste formelle de contraintes d'intégrité. De nombreuses collectes officielles sont très structurées et les données sont issues de processus qui garantissent un niveau d'exactitude de référence, comme la comptabilité en partie double ou la compensation et le règlement. Ces contrôles de l'intégrité ne s'appliquent pas nécessairement à des flux de transactions brutes, comme la CAT ou TRACE. En captant le flux de messages de transactions brutes, la CAT risque de présenter du bruit dans le flux de messages (annulations de cours, annulations de transactions, etc.). Compte tenu de l'interaction quotidienne effective de millions de personnes (investisseurs, opérateurs de marché, courtiers, etc.) avec un système financier hétérogène et dispersé, ce bruit va être de plus en plus prégnant à mesure que la capture de données se rapproche de la source. Par exemple, des données non structurées comme les flux des réseaux sociaux apparaissent dans la recherche sur le risque systémique, utilisant l'analyse des sentiments pour améliorer les prévisions de tensions financières.

La qualité des données est une question pratique importante, car des signaux incorrects peuvent compromettre la qualité de l'analyse et entraîner des décisions infondées (Osborne, 2012). Plus les volumes de données augmentent, plus la charge représentée par le nettoyage des données s'alourdit (Dahu et Johnson, 2003). Certains outils permettent d'effectuer de façon automatisée le nettoyage des données (Ram et Do, 2000), le contrôle qualité (Pipino, *et al.*, 2000), et l'intégration (Bernstein et Haas, 2008) des données. Ils doivent être adaptés pour pouvoir être utilisés avec des données financières, mais cela ne signifie pas que la tâche soit aisée ; Burdick, *et al.* (2015) décrivent certains défis liés à leur mise en œuvre. Le Comité de Bâle sur le contrôle bancaire (CBCB) a noté que la moitié des banques d'importance systémique interrogées (15 sur 30) ont du mal à mettre en œuvre les principes aux fins de l'agrégation des données sur les risques définis par le CBCB en 2013 et déclarent qu'elles ne respectent pas complètement le principe 3 (exactitude et intégrité des données). Des données ponctuelles laissent penser qu'il sera difficile pour un certain nombre d'établissements de respecter pleinement ces principes d'ici 2016 (CBCB, 2015). L'*Enterprise Data Management Council* coordonne les efforts dans le secteur financier pour améliorer la qualité des données tout au long du processus de diffusion de l'information (EDMC, 2015).

Il existe de bonnes raisons, tant techniques que comportementales, pour que la qualité des données des informations financières ne relève pas simplement de diligences supplémentaires. Sur le plan comportemental, les banques peuvent être incitées à compromettre l'exactitude de leur *reporting* par un habillage des comptes (Munyan, 2014) ou la publication frauduleuse d'informations erronées (Benston *et al.*, 2004). D'un point de vue opérationnel, le ratio signal/bruit peut diminuer

avec l'augmentation de la granularité. Le THF offre un exemple des limites de la granularité (temporelle). La priorité traditionnelle « prix-temps » pour le routage des ordres, sur laquelle se fonde la meilleure exécution, se heurte à l'objectif de la SEC d'encourager la concurrence entre les plates-formes de négociation dans le cadre de la réglementation NMS (SEC, 2015). Cependant, la priorité de temps est impossible à faire appliquer de manière précise dans la mesure où les décisions relatives aux négociations dans le THF interviennent plus vite que la résolution temporelle des horloges système (Lombardi, 2006).

La dernière mise à jour en date de la règle 7430 de la FINRA requiert que les plates-formes de négociation se synchronisent dans la seconde sur l'horloge atomique du *National Institute of Standards and Technology* (NIST) (FINRA, 2016). Une tolérance d'une seconde crée une latitude énorme lorsque le temps de réponse pour l'exécution d'une transaction est de l'ordre d'une milliseconde (Hasbrouck et Saar, 2013). De plus, les erreurs opérationnelles dans les systèmes de THF, comme le flux d'ordres de vente à l'origine du *flash crash* de mai 2010, peuvent générer des actions éclairs exerçant en très peu de temps un impact cumulé considérable. De nombreuses bourses et leurs membres THF disposent d'un éventail de techniques pour sécuriser leurs systèmes avec des interruptions rapides des transactions (Clark et Ranjan, 2011), mais ces techniques ne sont pas encore appliquées partout.

4| Intégration et représentation des données

La surveillance de la stabilité financière nécessite souvent la prise en compte simultanée de multiples secteurs financiers. Une vision globale est essentielle, car les vulnérabilités qui ne sont pas apparentes dans les établissements considérés isolément peuvent émerger au niveau du système dans son ensemble. Toutefois, elle peut créer des difficultés d'évolutivité pour la dimension « variété ». Par exemple, l'analyse du risque de crédit des entreprises peut nécessiter d'analyser conjointement des données relatives aux obligations de sociétés, aux *swaps* de défaut, aux prêts bancaires et aux capitaux propres des entreprises. Les économistes sont habitués à fusionner des jeux de données au cas par cas, mais il n'est pas facile d'adapter ce processus à une autre échelle. L'enregistrement des crédits hypothécaires montre à quel point l'intégration peut être défaillante à l'échelle du système, malgré de très nombreuses initiatives pour qu'il fonctionne correctement. Les systèmes de données des marchés hypothécaires aux États-Unis n'ont pas été en mesure de traiter l'augmentation des volumes de titrisation avant la crise de 2007-2009, rendant incertain le statut juridique de nombreux prêts et contribuant au désastre des saisies immobilières à grande échelle (Hunt, *et al.*, 2014).

À plus long terme, l'apparition d'un système d'identifiants d'entité juridique (*legal entity identifier* – LEI) normalisé à l'échelle internationale sera d'une grande aide pour les travaux d'alignement de données financières en grand nombre (GLEIF, 2014). Mais le LEI seul est insuffisant pour une intégration de qualité élevée. L'alignement des données ne constitue qu'une première étape vers une intégration complète, mais elle est de grande ampleur. Des efforts sont en cours pour enrichir l'identification simple des LEI de première génération afin d'appréhender des relations de propriété complexes (OFR, 2015) et faire correspondre le LEI et d'autres systèmes d'identification. Des techniques plus avancées permettraient d'identifier les appellations courantes des institutions financières dans les actualités et sur les réseaux sociaux pour les réconcilier avec les identifiants formels. Par exemple, Xu *et al.* (2016) ont identifié les entités nommées dans des prospectus de titres adossés à des prêts hypothécaires résidentiels (RMBS) à partir d'une liste de noms d'institutions vendant des titres adossés à des actifs.

Dans le domaine de la surveillance macroprudentielle, l'OFR et le NIST ont financé le *Financial Entity Identification and Information Integration Challenge* (défi de l'identification d'entité financière et de l'intégration de l'information) pour développer de nouvelles technologies en vue d'une automatisation de l'alignement des identifiants et de l'identification des entités dans des jeux de données financières et des sources textuelles (NIST, 2016). L'objectif est de créer une base de connaissances de référence, ainsi que quelques prototypes d'instruments, reliant entre eux des répertoires hétérogènes d'identifiants d'entités provenant de diverses sources pour faciliter l'intégration des informations, tant dans les données structurées comme l'archivage réglementaire, que dans les données non structurées comme les articles d'actualité et les réseaux sociaux. Le tableau ci-après offre un aperçu du problème, en listant une série

Tableau
Relier les identifiants d'entités

Identifiant	Description
JPM	Symbole pour la cotation sur le *New York Stock Exchange*
0000019617	*Central Index Key* (CIK) attribuée par la *Securities and Exchange Commission*
1039502	RSSD ID attribué par le *Federal Reserve Board*
815DZWZKVSZI1NUHU748	Identifiant d'entité juridique (LEI) attribué par la *Global LEI Foundation*
J.P. Morgan	Nom de la société utilisé dans les stories du *Wall Street Journal*

Source : Office of Financial Research.

d'identifiants communément utilisés pour une seule entreprise, JPMorgan Chase and Co., *holding* financière regroupant elle-même des milliers de filiales.

L'identification de l'entité est l'aspect le plus basique d'un problème plus général de représentation des données et de gestion des métadonnées. Les métadonnées apparaissent le plus souvent sous forme de dictionnaires de données ou de schémas formels, qui structurent et décrivent la gestion des jeux de données. Les défis d'évolutivité qui apparaissent dans le cas de l'alignement des identifiants s'appliquent également à l'alignement des schémas. L'identification de la catégorie d'instrument est une zone de recoupement entre l'intégration de schémas et la surveillance systémique. Tout gestionnaire de portefeuille est libre de classer ses positions selon le schéma qu'il définit, mais les autorités de surveillance de la stabilité financière ont besoin d'identifier immédiatement les expositions communes à plusieurs portefeuilles, et donc les schémas. L'OFR, par exemple développe une base de données de référence pour les instruments financiers (*Financial Instrument Reference Database*) afin de remplir une mission qui lui a été confiée par le Dodd-Frank Act (OFR, 2015). Comme les participants et les régulateurs ont des typologies préexistantes pour satisfaire leurs besoins locaux, une base de données de référence des instruments sera confrontée aux difficultés de la correspondance des schémas et de l'intégration sémantique.

Toutes ces activités de conservation et d'intégration devraient permettre d'améliorer la qualité des données. La réconciliation d'un jeu de données avec d'autres jeux de données alignés, en respectant la logique de sa cohérence interne et des règles d'intégrité externes est une technique importante. À l'inverse, des problèmes de qualité des données dans l'un quelconque des systèmes source peuvent affecter l'ensemble intégré. Dans un échantillon donné, le coût lié à la maintenance de métadonnées au niveau des attributs dépend linéairement du nombre d'attributs. Toutefois, sans cadre de gestion des métadonnées, les coûts de passage à l'échelle peuvent augmenter à un rythme qui croît avec l'alignement des métadonnées provenant de sources multiples. Flood (2009) souligne que l'intégration des métadonnées est par essence instable s'agissant de la gestion du risque financier, l'innovation entraînant une évolution continuelle des produits financiers, des modèles de risque et des priorités stratégiques.

Il existe des techniques permettant un alignement des schémas automatisé et assisté par ordinateur et la mise en œuvre des exigences de cohérence, entre les schémas et par rapport aux règles d'intégrité des données établies (Bernstein et Haas, 2008 ; Rahm et Bernstein, 2001). Des ontologies formelles destinées à organiser les définitions et les termes peuvent être un outil utile pour gérer la cohérence sémantique des métadonnées entre les différents schémas (Noy, 2004 ; Flood *et al.*, 2010). Traditionnellement, cet effort de sémantique a été mené par des juristes et des experts de domaine. Les ontologies formelles peuvent alléger la charge, servir de référence externe pour la réconciliation et exposer les détails de leur modèle conceptuel aux nouveaux arrivants et à des utilisateurs occasionnels qui sans cela seraient dépassés. Les normes en matière de données peuvent également être utiles pour l'intégration (OFR, 2015), mais des normes efficaces requièrent l'élaboration d'abstractions correctes, et cela représente souvent un travail éprouvant. On en trouve un exemple dans la collaboration de l'OFR avec la *Commodity Futures Trading Commission* et les régulateurs internationaux en vue d'améliorer les normes d'information financière et d'élaborer des taxonomies partagées pour des référentiels de données sur les *swaps*.

5| Modélisation et analyse des données

L'analyse est une composante centrale de la supervision macroprudentielle et les autorités de surveillance de la stabilité financière investissent

beaucoup dans le développement de boîtes à outils permettant d'évaluer les conditions financières. En outre, le système financier étant un organisme en évolution, les autorités de surveillance macroprudentielle doivent elles aussi innover pour garder une série de modèles adaptés aux institutions et aux pratiques de marché existantes. Le résultat est que le système financier et la boîte à outils macroprudentielle doivent évoluer en parallèle dans le temps, chacun répondant aux innovations de l'autre. Le rapport sur la stabilité financière de l'OFR (2015) fait ressortir cette dynamique, par exemple, avec deux chapitres couvrant la surveillance permanente des menaces pesant sur la stabilité financière et l'évaluation des politiques en vigueur, suivis de deux chapitres consacrés à l'amélioration de la collecte des données et aux recherches en vue de perfectionner la boîte à outils.

L'analyse des données est souvent l'aspect le plus déterminant du paradigme du *big data* et plusieurs des approches communément citées, comme la segmentation (*clustering*) de données et la détection de communautés, se prêtent bien à l'identification de profils à partir des données. Les chercheurs empiriques sont naturellement attirés par les échantillons de données vastes et encore inexplorés qui émergent des actualités archivées, des flux de négociation et des réseaux sociaux (par exemple, Bholat *et al.*, 2015; Mamaysky et Glasserman, 2015; Nyman *et al.*, 2014). L'exploration de ces nouvelles sources de données en est à son tout début et de nouveaux résultats empiriques fascinants retiennent l'attention des chercheurs. Cependant, comme le processus générateur de données sur les marchés financiers est généralement endogène, les régularités empiriques issues des seules données (c'est-à-dire indépendantes du modèle) auront à faire face à des obstacles supplémentaires pour justifier leur validité. En général, si l'inférence causale est un objectif principal, ce qui est souvent le cas pour les analyses de l'action des autorités, une simple analyse prédictive et la sélection d'un modèle axé sur les données peuvent être d'un usage limité (Einav et Levin, 2014).

Les défis du passage à l'échelle créent pour l'analyse des données massives, comme pour les autres phases de leur traitement, des problèmes et des opportunités. Une difficulté pour l'économétrie traditionnelle face au *big data* réside dans la sélection du modèle. Comme il existe peu de contraintes sur les spécifications, la sélection de variables sur un jeu de données non structurées peut générer un nombre arbitraire de régresseurs potentiels. Même des données structurées peuvent donner lieu à une explosion combinatoire des spécifications. Sala-i-Martin (1997), travaillant avec 62 variables explicatives possibles dans une équation de croissance classique, est devenu célèbre pour avoir utilisé deux millions de spécifications distinctes. Cette prolifération de spécifications crée un potentiel pour l'exploration de données. Mais ce qui est généralement mis en avant comme une fonctionnalité puissante de l'analyse de données massives est inacceptable pour l'économètre classique. Comme de nombreuses sources de données massives, par exemple les actualités archivées, sont une nouveauté pour l'économétrie financière, il n'existe pas encore beaucoup de contraintes théoriques pour restreindre l'univers des spécifications acceptables. S'agissant des questions sur la politique à mener, l'analyste est potentiellement fortement incité à trouver la « bonne » réponse, de sorte que les taux de fausse découverte constituent un véritable sujet de préoccupation (Fan *et al.*, 2014 ; Domingos, 2012).

Dans certains cas, une correction de Bonferroni suffit pour corriger le taux de faux positifs apparaissant naturellement dans un grand échantillon (Curme *et al.*, 2014); Alanyali, *et al.*, 2013). Dans d'autres cas, résoudre le problème n'est pas aussi simple. Donoho et Stodden (2006) considèrent la « *fat regression* » ou le problème dit « $P >> N$ », où le nombre de variables explicatives dépasse très nettement le nombre d'observations. En pareils cas, les points de données N sont peu densément répartis dans un espace de mesure de plus grande dimension et les principaux éléments de la théorie asymptotique à la base de l'économétrie traditionnelle volent tout simplement en éclats. Varian (2014) décrit d'autres approches. Dhar (2013) souligne l'importance du pouvoir prédictif hors échantillon comme critère de sélection du modèle. Le point essentiel est que les données massives nécessitent de nouvelles approches, et pas seulement du matériel plus puissant.

6| Partage des données et transparence

La dernière série de tâches de gestion des données porte sur les données disponibles une fois collectées, nettoyées, documentées et analysées. Les données sont une ressource destinée à aider la prise de

décision, l'élaboration de règles et la définition d'une politique, et à fournir un cadre pour d'autres analyses. Dans de nombreux cas, le superviseur rend publiques ou partage de manière sélective les données collectées ou les analyses qui en sont faites dans le cadre de son obligation de rendre compte, pour assurer la transparence vis-à-vis des investisseurs ou pour soutenir la prise de décision dans un secteur. Dans ce rôle, les superviseurs assurent le traitement de la séquence entrées-processus-sorties. Elles entrent les données brutes (collectées de façon règlementaire, flux de données de marché, etc.), les transforment *via* différents processus analytiques en artéfacts (résultats de régression, agrégats pour le secteur, rapports sur la stabilité financière, outils de visualisation, etc.), et les diffusent à des groupes d'utilisateurs ciblés (public ou tableaux de bord du risque sectoriel, outils de visualisation statique ou interactive contribuant à la recherche ou à la prise de décision, archivage de l'état du système en vue d'une analyse historique et/ou comptable, etc.).

La diversité des groupes d'utilisateurs, qui va des hautes autorités de contrôle au grand public, signifie que le partage des données revêt des formes multiples. Dans certains cas, comme pour le *Billion Prices Project* utilisé pour la mesure de l'inflation (Rigobon, 2015), les chercheurs utilisent des données volumineuses, librement accessibles pour élaborer de nouvelles approches utilisables pour des travaux classiques sur les statistiques officielles. Dans le cas des données relatives à la stabilité financière, la confidentialité est parfois un sujet de préoccupation supplémentaire (Flood *et al.*, 2013). Là encore, la possibilité de s'étendre (*scalability*) affecte le processus. Par exemple, la publication de statistiques agrégées à partir d'informations sensibles est restreinte. Aux États-Unis, les autorités de supervision financière et les organismes statistiques sont confrontés à une série de lois et règlements protégeant la vie privée et la confidentialité qui encadrent ces statistiques (Flood *et al.*, 2013, Section 3 et Annexes A et B). En Europe, le principal texte juridique est la réglementation relative à la protection des données (Howell, 2014). Les méthodes classiques de contrôle de la communication incluent la suppression de champs clés, le « floutage » des données (c'est-à-dire l'ajout de bruit) et le regroupement de données (c'est-à-dire le remplacement d'attributs détaillés par des catégories plus brutes), mais la ré-identification visant à rapprocher une information personnelle anonymisée de son véritable propriétaire, par exemple grâce à des attaques par appariement mettant à profit d'autres sources de données, peut souvent mettre en échec ces techniques préexistantes (Emam *et al.*, 2011). Pour des raisons analogues, le Bureau du recensement (*Census Bureau*) des États-Unis ne demande plus les numéros de sécurité sociale pour ses enquêtes sur les revenus (*Survey of Income and Program Participation*), car les participants ont progressivement appris à ne pas fournir cette donnée (McNabb *et al.*, 2009). Au final, la faisabilité de la divulgation de statistiques issues de données confidentielles est un problème délicat, qui nécessite de peser les bénéfices pour la politique à mener, les contraintes juridiques et les capacités techniques des autorités de surveillance, des utilisateurs finaux et des opposants potentiels qui pourraient compromettre le partage d'informations.

La visualisation, au sens ancien selon lequel une image vaut mille mots, est souvent déterminante pour la compréhension humaine. L'homme est doté d'une capacité considérable et très évoluée de perception et d'apprentissage visuels, ce qui, pour la reconnaissance des formes, lui donne dans de nombreux cas un avantage comparatif par rapport à d'autres outils. On peut également dynamiser ces compétences innées par l'analyse visuelle, qui enrichit les images statiques en plaçant une personne dans la boucle pour contrôler la restitution de manière interactive. Selon le processus correspondant au « mantra » de Shneiderman (1996), (vue d'ensemble, zoom et filtrage, puis détails à la demande), les outils qui apportent une amélioration sélective de la résolution sur des jeux de données volumineux permettent de cumuler les avantages des deux concepts la profondeur et la portée, simultanément. Flood *et al.* (2016) font ressortir quatre grandes missions macroprudentielles, pour lesquelles la visualisation peut jouer un rôle essentiel : donner du sens, établir des règles, définir une politique et assurer la transparence. La visualisation interactive est particulièrement précieuse pour donner du sens, lorsque l'exploration non supervisée représente une partie essentielle de la tâche.

7| Conclusions

Les autorités de surveillance de la stabilité financière sont clairement confrontées aux défis du *big data*, en raison de la taille exceptionnelle du système

sous surveillance. La question centrale est celle de l'extensibilité. Les données massives deviennent un problème lorsque l'échelle des jeux de données nécessaires dépasse largement les outils disponibles pour leur traitement suivant plusieurs grandes dimensions : volumétrie, vélocité, variété et véracité. En d'autres termes, le caractère massif n'est pas en lui-même un attribut du jeu de données, mais il rend plutôt compte du volume, de la vélocité, etc. de l'échantillon *au regard* de la capacité des processus disponibles. Les données décrivant l'intégralité du système financier peuvent être massives sur l'une des quatre dimensions, dépassant les capacités des processus analytiques préexistants, qui sont souvent d'une nature fondamentalement microprudentielle.

Le LEI, désormais mis en œuvre à l'échelle internationale, est un bon exemple du rassemblement de la communauté financière autour de l'élaboration d'« une solution non linéaire à un problème non linéaire ». Les autorités de surveillance devraient s'intéresser plus largement à une sémantique partagée ainsi clairement définie, entretenue avec rigueur (par exemple, grâce à des ontologies formelles). Le dispositif d'identification du LEI est l'exemple le plus simple et le plus basique de partage de terminologie financière. Lorsqu'elles sont combinées aux solutions les plus récentes en vue de l'extraction d'entités nommées et le rapprochement avec l'indication d'entités dans des contrats financiers (Xu *et al.*, 2016), les normes ouvertes comme le LEI peuvent permettre à l'analyse microprudentielle de s'appuyer sur des données massives (NIST, 2016). Les superviseurs macroprudentiels doivent rester vigilants pour reconnaître dès leur apparition les défis du passage à l'échelle des données.

Le secteur financier et les exigences en termes de données pour assurer sa surveillance vont évoluer en parallèle. La structure adoptée par le secteur s'adapte à la surveillance et *vice versa*. Par exemple, les exigences en fonds propres de Bâle pesant sur les bilans des banques pour la concentration des expositions sur crédits hypothécaires ont favorisé un arbitrage réglementaire, la finance hypothécaire se déplaçant vers les marchés de la titrisation (Ambrose *et al.*, 2005), où elle échappait à un programme de surveillance intensive que les contrôleurs bancaires avaient développé au fil des ans. Pour boucler la boucle, les exigences en matière de données pour la surveillance de la finance immobilière ont considérablement augmenté depuis la crise, au moins aux États-Unis.

Le secteur génère plus de données et les autorités de surveillance en collectent davantage, une tendance qui n'a fait que s'accélérer depuis la crise, et qui crée de nouveaux défis en termes de passage à l'échelle, comme les limites de qualité qui empêchent l'interprétation des nouvelles données collectées, à la granularité très élevée. Les efforts pour améliorer la qualité des données tout au long de la chaîne de diffusion de l'information (par exemple, EDMC, 2015) sont un élément incontournable de la solution. Dans le même temps, l'intégration de cette information détaillée sur les créances hypothécaires, souvent au niveau du prêt, avec d'autres sources de données, pose des problèmes de confidentialité nouveaux et importants, comme les attaques par appariement (*linkage attacks*), qui peuvent déjouer les techniques classiques de masquage des données. De nouvelles méthodes visant à évaluer et garantir la confidentialité des données dans ce contexte apparaissent, mais elles doivent encore être adoptées largement comme faisant partie de la panoplie de la surveillance prudentielle. Les créances hypothécaires ne sont qu'un exemple d'un enseignement plus général : les autorités de surveillance macroprudentielle doivent se tenir au courant des nombreuses techniques qui apparaissent pour relever les défis du paysage informatique du *big data*.

Bibliographie

Aït-Sahalia (Y.) et Jacod (J.) (2014)
« *High-frequency financial econometrics* », *Princeton University Press*.

AICPA (2015)
« *Audit analytics and continuous audit: looking toward the future* », AICPA.

Alanyali (M.), Moat (H. S.) et Preis (T.) (2013)
« *Quantifying the relationship between financial news and the Stock Market* », *Scientific Reports*, 3(3578).

Ambrose (B. W.), LaCour-Little (M.) et Sanders (A. B.) (2005)
« *Does regulatory capital arbitrage, reputation, or asymmetric information drive securitization?* », *Journal of Financial Services Research*, 28(1), octobre, 113-133.

Baklanova (V.), Caglio (C.), Cipriani (M.) et Copeland (A.) (2016)
« *The US bilateral repo market: lessons from a new survey* », *OFR Research Brief* (16-01), janvier, *https://financialresearch.gov/briefs/files/OFRbr-2016-01_US-Bilateral-Repo-Market-Lessons-from-Survey.pdf*

Banque d'Angleterre (2015)
« *One bank research agenda* », *Discussion Paper*, février, *http://www.bankofengland.co.uk/research/Documents/onebank/discussion.pdf*

Benston (G.), Bromwich (M.), Litan (R. E.) et Wagenhofer (A.) (2004)
« *Following the money: the enron failure and the state of corporate disclosure* », *Brookings Institution Press*.

Berman (G. E.) (2013)
« *Transformational technologies, market structure, and the SEC* », remarques lors de la conférence SIFMA TECH, New York, *http://www.sec.gov/News/Speech/Detail/Speech/1365171575716*

Bernstein (P. A.) et Haas (L. M.) (2008)
« *Information integration in the enterprise* », *Communications of the ACM*, 51(9), septembre, 72-79.

Bholat (D.) (2015)
« *Big data and central banks* », *Bulletin mensuel* de la Banque d'Angleterre, T1, 86-93.

Bholat (D.), Hansen (S.), Santos (P.) et Schonhardt-Bailey (C.) (2015)
« *Text mining for central banks* », *Centre for Central Banking Studies Handbook* (33), *http://eprints.lse.ac.uk/62548/1/Schonhardt-Bailey_text%20mining%20handbook.pdf*

Buneman (P.) et Tan (W.-C.) (2007)
« *Provenance in databases* », in : *Proceedings of the 2007 ACM SIGMOD International Conference on Management of Data*, 1171-1173.

Burdick (D.), Hernandez (M.), Ho (H.), Koutrika (G.), Krishnamurthy (R.), Popa (L. C.), Stanoi (I.), Vaithyanathan (S.) et Das (S. R.) (2015)
« *Extracting, linking and integrating data from public sources: a financial case study* », document de travail, septembre, *http://ssrn.com/abstract=2666384*

Casey (M.) (2014)
« *Emerging opportunities and challenges with central bank data* », support de présentation, octobre, *https://www.ecb.europa.eu/events/pdf/conferences/141015/presentations/Emerging_opportunities_and_chalenges_with_Central_Bank_data-presentation.pdf?6074ecbc2e58152dd41a9543b1442849*

Cerutti (E.), Claessens (S.) et McGuire (P.) (2014)
« *Systemic risks in global banking: what available data can tell us and what more data are needed?* », chapitre16 dans : *Risk Topography: Systemic Risk and Macro Modeling*, Brunnermeier (M. K.) & Krishnamurthy (A.) (Eds.), *University of Chicago Press*, 235-260.

Chase (R.) (2015)
« *Peers inc: how people and platforms are inventing the collaborative economy and reinventing capitalism* », *Public Affairs*.

Clark (C.) et Ranjan (R.) (2011)
« *How do exchanges control the risks of high speed trading?* », *Policy Discussion Paper* (2011-2012), Federal Reserve Bank of Chicago, *https://www.chicagofed.org/publications/policy-discussion-papers/2011/pdp-2*

Comité de Bâle sur le contrôle bancaire (2015)
« *Progress in adopting the principles for effective risk data aggregation and risk reporting* », janvier, *http://www.bis.org/bcbs/publ/d308.htm*

Comité de Bâle sur le contrôle bancaire (2013)
« *Principles for effective risk data aggregation and risk reporting* », janvier, *http://www.bis.org/publ/bcbs239.htm*

Conseil des gouverneurs du Système fédéral de réserve (2015)
« *Enhancements to the Federal Reserve System's Surveillance Program* », note, décembre, *http://www.federalreserve.gov/bankinforeg/srletters/sr1516.htm*

Conseil des gouverneurs du Système fédéral de réserve et *Office of the Comptroller of the Currency* (FRB-OCC) (2013)
« *Regulatory capital rules: regulatory capital, implementation of basel iii, capital adequacy, transition provisions, prompt corrective action, standardized approach for riskweighted assets, market discipline and disclosure requirements, advanced approaches risk-based capital rule, and market risk capital rule* », *Federal Register*, 78(198), octobre, 62018-62291.

Conseil de stabilité financière et Fonds monétaire international (2015)
« *The financial crisis and information gaps: sixth progress report on the implementation of the g-20 data gaps initiative* », rapport technique, septembre, *http://www.fsb.org/wp-content/uploads/The-Financial-Crisis-and-Information-Gaps.pdf*

Consumer Financial Protection Bureau (2013)
« *Strategic Plan: FY 2013 - FY 2017* », *http://files.consumerfinance.gov/f/strategic-plan.pdf*

Curme (C.), Preis (T.), Stanley (H. E.) et Moat (H. S.) (2014)
« *Quantifying the semantics of search behavior before stock market moves* », *Proceedings of the National Academy of Sciences*, 111(32), 11600–11605.

Dasu (T.) et Johnson (T.) (2003)
« *Exploratory data mining and data cleaning* », *Wiley-Interscience*.

DeCovny (S.) (2014)
« *A fair exchange* », *CFA Institute Magazine*, septembre/octobre, 32-35.

Dhar (V.) (2013)
« *Data science and prediction* », *Communications of the ACM*, 56(12), décembre.

Diebold (F. X.) (2012)
« *On the origin(s) and development of the term "big data"* », *PIER Working Paper* (12-037), septembre, *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2152421*

Domingos, (P.) (2012)
« *A few useful things to know about machine learning* », *Communications of the ACM*, 55(10), octobre, 78-87.

Dong (X. L.) et Srivastava (D.) (2013)
« *Big data integration* », in : *29th International conference on data engineering* (ICDE), 1245-1248.

Donoho (D. L.) et Stodden (V. C.) (2006)
« *Breakdown point of model selection when the number of variables exceeds the number of observations* », dans : *IJCNN '06. International Joint Conference on Neural Networks*, 2006, *http://academiccommons.columbia.edu/item/ac:140168*

Einav (L.) et Levin (J.) (2014)
« *Economics in the age of big data* », *Science*, 346(6210), novembre.

Emam (K. E.), Jonker (E.), Arbuckle (L.) et Malin (B.) (2011)
« *A systematic review of re-identification attacks on health data* », *PLoS ONE*, 6(12), e28071.

Enterprise Data Management Council (2015)
« *Data management capability assessment model: version 1.1* », rapport technique, *http://www.edmcouncil.org/dcam*

Fan (J.), Han (F.) et Liu (H.) (2014)
« *Challenges of big data analysis* », *National Science Review*, 1(2), juin, 293-314.

Financial Crisis Inquiry Commission (2011)
The financial crisis inquiry report: final report of the national commission on the causes of the financial and economic crisis in the United States, U.S. Government Printing Office, janvier.

Financial Industry Regulatory Authority (2016)
« *OATS reporting technical specifications* », rapport technique, janvier, *http://www.finra.org/industry/oats/oats-technical-specifications*

Flood (M. D.) (2009)
« *Embracing change: financial informatics and risk analytics* », *Quantitative Finance*, 9(3), avril, 243-256.

Flood (M. D.), Katz (J.), Ong (S.) et Smith (A.) (2013)
« *Cryptography and the economics of supervisory information: balancing transparency and confidentiality* », document de travail de l'OFR (0011), septembre, *http://financialresearch.gov/working-papers/files/OFRwp0011_FloodKatzOngSmith_CryptographyAndTheEconomicsOfSupervisoryInformation.pdf*

Flood (M. D.), Kyle (A.) et Raschid (L.) (2010)
« *Knowledge representation and information management for financial risk management* », rapport technique, juillet, *http://irix.umiacs.umd.edu/docs/FIWreport-FINAL.pdf*

Flood (M. D.), Lemieux (V. L.), Varga (M.) et Wong (B. W.) (2016)
« *The application of visual analytics to financial stability monitoring, Journal of Financial Stability* », à paraître, *http://www.sciencedirect.com/science/article/pii/S1572308916000073*

Flood (M. D.), Mendelowitz (A.) et Nichols (W.) (2013)
« *Monitoring financial stability in a complex world* », chapitre 2, *Financial Analysis and Risk Management: Data Governance*, Analytics and Life Cycle Management, Springer, 15-46.

Foster (D. P.) et Young (H. P.) (2010)
« *Gaming performance fees by portfolio managers* », *Quarterly Journal of Economics*, 125(4), novembre, 1435-1458.

Global Legal Entity Identifier Foundation (2014)
« *Annual Report 2014* », *https://www.gleif.org/en/about/governance/annual-report#*

Halevy (A.), Rajaraman (A.) et Ordille (J.) (2006)
« *Data integration: the teenage years* », *Proceedings of the 32nd International Conference on Very Large Data Bases* (VLDB '06), 9-16.

Hasbrouck (J.) et Saar (G.) (2013)
« *Low-latency trading* », *Journal of Financial Markets*, 16(4), novembre, 646–679.

Hey (T.), Tansley (S.) et Tolle (K.) (2009)
« *The fourth paradigm: data-intensive scientific discovery* », Microsoft Research.

Hokkanen (J.), Jacobson (T.), Skingsley (C.) et Tibblin (M.) (2015)
« *The Riksbank's future information supply in light of big data* », *Economic Commentaries* (17), Sveriges Riksbank.

Horvitz (E.) (2010)
« *From data to predictions and decisions: enabling evidence-based healthcare* », rapport technique, septembre, *http://archive2.cra.org/ccc/files/docs/init/Healthcare.pdf*

Howell (C. T.) (2014)
« *Privacy and big data* », chapitre : 4 « *Big Data: A business and legal guide* », Kalyvas (J. R.) & Overly (M. R.) (Eds.), Auerbach Publications, 33-54.

Hunt (J. P.), Stanton (R.) et Wallace (N.) (2014)
« *US residential-mortgage transfer systems: a data-management crisis* », chapitre 18, *Handbook of Financial Data and Risk Information II: Software and Data, Brose* (M.), Flood (M.), Krishna (D.) & Nichols (B.) (Eds.), Cambridge University Press, 2, 85-132.

Hunter (M.) (2014)
« *Statement by Maryann F. Hunter, Deputy Director, Division of Banking Supervision and Regulation, Board of Governors of the Federal Reserve System before the Committee on Banking, Housing, and Urban Affairs, U.S. Senate, Washington, D.C.* », *http://www.federalreserve.gov/newsevents/testimony/hunter20140916a.pdf*

IBM (2016)
« *The four v's of big data* », page internet, *http://www.ibmbigdatahub.com/infographic/four-vs-big-data*

International Institute of Forecasters (2014)
« *11th International Institute of Forecasters' Workshop: using big data for forecasting and statistics* », rapport technique, *https://forecasters.org/wp-content/uploads/11th-IIF-Workshop_BigData.pdf*

Jagadish (H. V.), Gehrke (J.), Labrinidis (A.), Papakonstantinou (Y.), Patel (J. M.), Ramakrishnan (R.) et Shahabi (C.) (2014)
« *Big data and its technical challenges* », *Communications of the ACM*, 57(7), juillet, 86-94.

Kirilenko (A. A.) et Lo (A. W.) (2013)
« *Moore's law versus murphy's law: algorithmic trading and its discontents* », *Journal of Economic Perspectives*, 27(2), printemps, 51-72.

Kitchin (R.) (2015)
« *The opportunities, challenges and risks of big data for official statistics* », *Statistical Journal of the International Association of Official Statistics*, 31(3), 471-481.

Lombardi (M. A.) (2006)
« *Legal and technical measurement requirements for time and frequency* », *Measure*, 1(3), septembre.

Mamaysky (H.) et Glasserman (P.) (2015)
« *Does unusual news forecast market stress?* », *Columbia Business School Research Paper* (15-70), juillet, *http://ssrn.com/abstract=2632699*

Manyika (J.), Chui (M.), Brown (B.), Bughin (J.), Dobbs (R.), Roxburgh (C.) et Byers (A. H.) (2011)
« *Big data: the next frontier for innovation, competition, and productivity* », *McKinsey Technical report*, *http://www.mckinsey.com/insights/mgi/research/technology_and_innovation/big_data_the_next_frontier_for_innovation*

McNabb (J.), Timmons (D.), Song (J.) et Puckett (C.) (2009)
« *Uses of administrative data at the Social Security Administration* », *Social Security Bulletin*, 69(1), 75-84.

MongoDB (2016)
« *Big data explained* », janvier, *https://www.mongodb.com/big-data-explained*

Munyan (B.) (2014)
« *Regulatory arbitrage in repo markets* », document de travail, décembre, *http://www.bmunyan.com/*

National Institute of Standards and Technology (2016)
« *Financial entity identification and information integration (feiii) challenge: about the challenge* », *https://ir.nist.gov/dsfin/about.html*

Noy (N. F.) (2004)
« *Semantic integration: a survey of ontology-based approaches* », *ACM SIGMOD Record*, 33(4), décembre, 65-70.

Nyman (R.), Ormerod (P.), Smith (R.) et Tuckett (D.) (2014)
« *Big data and economic forecasting: a top-down approach using directed algorithmic text analysis* », présentation, *http://www.ecb.europa.eu/events/pdf/conferences/140407/TuckettOrmerod_BigDataAndEconomicForecastingATop-DownApproachUsingDirectedAlgorithmicTextAnalysis.pdf*

Office of Financial Research (2015)
« *Financial stability Report* », décembre, *https://financialresearch.gov/financial-stability-reports/*

Osborne (J. W.) (2012)
« *Best practices in data cleaning: a complete guide to everything you need to do before and after collecting your data* », *SAGE Publications*.

O'Hara (M.) (2015)
« *High frequency market microstructure* », *Journal of Financial Economics*, 116(2), mai, 257-270.

Pattison (J. C.) (2014)
« *Data-driven regulation and financial reform: one perspective from industry on the financial crisis* », chapitre 5 in : *Handbook of Financial Data and Risk Information I: Principles and Context*, Brose (M.), Flood (M.), Krishna (D.) & Nichols (B.) (Eds.), *Cambridge University Press*, 1, 148-178.

Pipino (L. L.), Lee (Y. W.) et Wang (R. Y.) (2002)
« *Data quality assessment* », *Communications of the ACM*, 45(4), 211-218.

Rahm (E.) et Bernstein (P. A.) (2001)
« *A survey of approaches to automatic schema matching* », *VLDB Journal*, 10(4), décembre, 334-350.

Rahm (E.) et Do (H. H.) (2000)
« *Data cleaning: problems and current approaches* », *IEEE Data Engineering Bulletin*, 23(4), 3-13.

Rauchman (M.) et Nazaruk (A.) (2013)
« *Big data in capital markets* », discours, conférence ACM SIGMOD/PODS, New York, juin, *http://www.sigmod.org/2013/keynote_1.shtml*

Rigobon (R.) (2015)
« *Macroeconomics and on-line prices* », discours du président, *Economia: Journal of the Latin American and Caribbean Economics Association*, 15(2), printemps, 199-213. *http://www.cid.harvard.edu/Economia/contents.htm*

Rosenthal (A.) et Seligman (L.) (2011)
« *Data integration for systemic risk in the financial system* », chapitre 4 in : *Handbook for Systemic Risk*, Fouque (J.-P.) & Langsam (J. A.) (Eds.), *Cambridge University Press*, 93-122.

Rossi (C.) (2014)
« *Portfolio risk monitoring* », chapitre 3, *Handbook of Financial Data and Risk Information I: Principles and Context*, Brose (M.), Flood (M.), Krishna (D.) & Nichols (B.) (Eds.), *Cambridge University Press*, 1, 75-104.

Sala-i-Martin (X. X.) (1997)
« *I just ran two million regressions* », *American Economic Review*, 87(2), 178-183.

Securities and Exchange Commission (2012)
« *Consolidated audit trail* », *Federal Register*, 77(148), août, 45722-45814.

Securities and Exchange Commission (2014)
« *Form 10-K: annual report pursuant to section 13 or 15(D) of the Securities Exchange Act of 1934* », formulaire de déclaration, *https://www.sec.gov/about/forms/form10-k.pdf*

Securities and Exchange Commission (2015)
« *Rule 611 of regulation NMS* », note, Division of Trading and Markets, avril, *https://www.sec.gov/spotlight/emsac/memo-rule-611-regulation-nms.pdf*

Securities and Exchange Commission (2016)
« *Form N-MFP: monthly schedule of portfolio holdings of money market funds* », formulaire de déclaration, *https://www.sec.gov/about/forms/formn-mfp.pdf*

Shneiderman (B.) (1996)
« *The eyes have it: A task by data type taxonomy for information visualisations* », *Proceedings of the IEEE Symposium on Visual Languages*, 336-343.

Somerset House (2015)
« *Big bang data* », exposition, décembre, *http://bigbangdata.somersethouse.org.uk/explore/*

Stein (K. M.) (2015)
« *International cooperation in a new data-driven world* », Remarks to the Brooklyn Law School International Business Law Breakfast Roundtable, Securities and Exchange Commission, mars, *http://www.sec.gov/news/speech/2015-spch032615kms.html*

Varian (H. R.) (2014)
« *Big data: new tricks for econometrics* », *Journal of Economic Perspectives*, 28(2), 3-27.

Xu (Z.), Burdick (D.) et Raschid (L.) (2016)
« *Exploiting lists of names for named entity identification of financial institutions from unstructured documents* », document de travail, à paraître.

Zhao (Y.), Wilde (M.), Foster (I.), Voeckler (J.), Jordan (T.), Quigg (E.) et Dobson (J.) (2004)
« *Grid middleware services for virtual data discovery, composition, and integration* », *Proceedings of the 2nd Workshop on Middleware for Grid Computing* (MGC '04), 57-62.

Mise en œuvre du règlement en temps réel pour les banques utilisant la technologie du registre décentralisé : implications politiques et juridiques

Karen GIFFORD
Conseiller spécial en matière de réglementation mondiale
Ripple

Jessie CHENG
Directeur général adjoint des Affaires juridiques, Ripple
Vice-présidente, Payments Subcommittee of the American Bar Association Business Law Section's Uniform Commercial Code Committee

Une vague d'innovations est en cours dans le domaine de la technologie financière, avec des incidences tant sur les produits et services proposés aux particuliers et aux entreprises que sur les infrastructures de marchés financiers, notamment les systèmes de paiement et de règlement. L'ensemble de ces innovations est susceptible d'abaisser considérablement le coût des transactions financières, en provoquant un bouleversement qualitatif similaire à celui induit par l'avènement d'Internet dans les années quatre-vingt-dix, contribuant ainsi à l'inclusion financière au plan international tout en renforçant la stabilité systémique à l'échelle mondiale. Cet article nomme Internet of Value *(IoV) à la fois la série actuelle d'innovations à l'origine du bouleversement qu'il décrit et les futures innovations qui s'appuieront sur ces nouvelles technologies.*

De la même manière qu'Internet avait ouvert une nouvelle ère d'innovation rapide, de croissance économique et de gains de productivité, les promesses potentielles de l'IoV englobent un accroissement de la prospérité, de l'accès aux services financiers, de la stabilité et de l'innovation future ; toutefois, pour que ces promesses se concrétisent, un soutien aux niveaux sectoriel, réglementaire et politique sera indispensable.

*Cet article porte sur une innovation financière récente en particulier, celle du registre décentralisé ou de la technologie des chaînes de blocs (*blockchain technology*), et examine les ramifications juridiques et politiques de l'un des cas d'utilisation les plus largement discutés, celui du règlement en temps réel des paiements interbancaires. L'analyse se concentre sur deux éléments, la confiance et la coordination, tous deux fondamentaux s'agissant des lois et règlements actuels gouvernant les paiements. La technologie des registres décentralisés remplace certains facteurs opérationnels, voire juridiques, du système actuel de paiement ; pour autant, la confiance et la coordination restent des considérations pertinentes. La création et la mise en œuvre de cadres juridiques et de politiques appropriés sont fondamentales pour optimiser les avantages potentiels de cette technologie.*

Le fait qu'une révolution induite par la technologie soit en cours dans le secteur financier mondial est un lieu commun, si souvent réitéré que son sens s'est émoussé. Quelle est cette « révolution » et où nous mène-t-elle ? Une série d'innovations, dont l'informatique en nuage (*cloud computing*), les protocoles ouverts et les interfaces de programmation d'application (*application programming interfaces*, API), ainsi que les améliorations des capacités de stockage, d'analyse et de gestion des données, entre autres, ont considérablement réduit la durée et le coût des transactions financières individuelles, et pourraient annoncer de nouvelles avancées en termes d'efficacité. Cette évolution quantitative affectant le coût des transactions a entraîné un changement qualitatif : une explosion des créations de sociétés, d'incubateurs, de projets et de laboratoires d'innovation produisant de nouveaux produits et services à un rythme sans précédent, à destination d'une gamme d'entreprises et de particuliers plus large que celle jamais ciblée auparavant par le secteur.

La position développée dans cet article est que le secteur financier mondial est en train de connaître une mutation similaire à celle qui a résulté de l'avènement d'internet dans les années quatre-vingt-dix. L'expression *Internet of Value* (IoV) recouvre ici à la fois la série actuelle d'innovations à l'origine de la mutation décrite et les futures innovations qui s'appuieront sur ces nouvelles technologies. Dans la perspective de l'IoV, les mouvements de valeur – les transactions financières, dans l'ensemble – se produiront de manière aussi totalement intégrée que les mouvements d'informations sur Internet aujourd'hui.

Une bonne compréhension des implications d'un bouleversement systémique comme l'avènement de l'IoV doit s'appuyer à la fois sur une perspective d'ensemble et une vue de détail. Sans entrer dans le détail, l'IoV reste un concept général, mais, sans vision plus globale, les innovations techniques individuelles manquent de contexte. C'est pourquoi les ramifications pratiques, juridiques et politiques de l'IoV sont examinées ici de manière générale, et également par le prisme de l'impact d'une innovation particulière sur un type précis de transaction financière, en l'occurrence l'application du protocole Ripple aux transferts de fonds interbancaires dans le contexte transfrontalier.

I L'*INTERNET OF VALUE*

De la même manière que la baisse importante du coût de partage de l'information permise par internet a inauguré une ère d'innovation rapide, de croissance économique et de gains de productivité, les baisses correspondantes du coût des transactions financières permises par le développement de l'IoV devraient entraîner des changements de grande ampleur dans le système financier mondial. Les promesses potentielles de ces changements comprennent :

Prospérité – La baisse du coût et l'accélération de la vitesse des transactions atténuent les frictions et ouvrent la possibilité d'un nombre beaucoup plus grand de transactions, donc d'une activité économique nettement plus importante. S'il peut sembler évident qu'une baisse des coûts peut aboutir à une augmentation des transactions, pour parvenir concrètement à cerner le potentiel de l'IoV à alimenter la croissance économique, il peut être intéressant d'examiner l'impact de l'avènement d'internet sur les communications. Aux États-Unis, l'utilisation du courrier prioritaire a culminé en 2001, avec 103,7 milliards de courriers envoyés sur l'année [1]. En revanche, en 2014, le volume mondial quotidien de courriers électroniques envoyés atteignait en moyenne plus de 190 milliards [2]. Une évolution similaire dans le domaine financier signifierait une augmentation exponentielle du nombre de transactions financières au niveau mondial. Bien que nous soyons encore aux tout premiers stades de développement de l'IoV, les évolutions récentes suggèrent que ce type d'augmentation est à prévoir : ainsi, après la mise en œuvre partielle du système de paiement *Faster Payment System* au Royaume-Uni, le nombre de transactions autres qu'en espèces a nettement augmenté [3].

Inclusion financière – L'évolution de la structure de coût et la création de nouveaux circuits pour la fourniture de services financiers peuvent transformer des particuliers et des entités financièrement exclus en clients potentiellement intéressants. À ce jour, beaucoup d'initiatives d'inclusion financière se sont structurées essentiellement comme des efforts caritatifs. Bien qu'un grand nombre d'initiatives aient accompli des avancées impressionnantes dans

1 United States Postal Service, *volume de courrier prioritaire depuis 1926,* https://about.usps.com/who-we-are/postal-history/first-class-mail-since-1926.htm
2 The Radicati Group, Email Statistics Report, Executive Summary, *p.4.*
3 *Cf. Greene* et al. *(2014).*

l'élargissement de la portée des services financiers, en l'absence de modèle économique rentable, elles ne sont pas soutenables et peinent, voire, ne parviennent pas à maintenir leur existence, faute de financements externes. Après avoir beaucoup investi dans la recherche sur la question, la section *Financial Services for the Poor* de la Fondation Gates a conclu que la façon la plus efficace d'augmenter de manière significative l'accès des habitants des régions les plus pauvres de la planète à des services financiers officiels passe par le numérique [4]. En automatisant et en réduisant le coût des processus liés à la fourniture mondiale de services financiers, l'IoV offre la promesse d'une inclusion financière fortement élargie et durable.

Stabilité – Une plus grande participation au système financier mondial par une plus grande diversité d'entités favorise la solidité systémique en réduisant la surdépendance à un petit nombre de grandes entités. Les responsables politiques reconnaissent de plus en plus le rôle que l'inclusion financière peut jouer dans le maintien de la stabilité financière mondiale [5]. L'automatisation de systèmes précédemment manuels peut également réduire le risque opérationnel au niveau systémique.

Innovation – La baisse des coûts contribue à créer les conditions pour la création de nouveaux produits et services et, de la même manière que ni les participants de marché ni les décideurs politiques des années quatre-vingt-dix n'auraient pu prévoir l'apparition des smartphones, des applications de cartographie géolocalisée (GPS) ou des médias sociaux, il nous est impossible de savoir exactement comment l'IoV évoluera au cours des prochaines décennies. Ce que nous pouvons néanmoins affirmer avec un certain degré de confiance, c'est que l'évolution exponentielle de la capacité du système financier mondial à supporter des transactions favorisera probablement le développement de nouveaux secteurs. Déjà, les innovations en cours de développement qui exploitent l'IoV incluent des applications pour l'intégration de systèmes physiques et technologiques (souvent désignés par l'expression « Internet des objets ») qui pourraient permettre la mise en place de fonctionnalités telles que l'amélioration de la gestion des garanties et une automatisation plus poussée des financements commerciaux ; des contrats « intelligents » capables de rationaliser des processus tels que les dispositions de séquestre et l'origination des prêts hypothécaires, et des services tels que la sélection des comptes de paiement (par exemple le paiement avec des points de fidélité).

Cet article débute par une analyse des perspectives intentionnelles de l'IoV. Le potentiel de l'IoV en termes d'accroissement du commerce, d'opportunités, de croissance économique et de la prospérité qui l'accompagne, va à l'encontre du discours fréquent, et selon nous biaisé, ponctué de « perturbation », « désintermédiation » et « gagnants et perdants » qui irrigue souvent la discussion publique sur les évolutions technologiques dans les services financiers. S'il serait naïf de suggérer que tous les acteurs bénéficieront inévitablement du changement technologique, les évolutions abordées ici sont susceptibles d'aboutir à une augmentation rapide de la taille du « gâteau », avec potentiellement de fortes retombées positives pour ceux qui sauront bien s'engager sur la voie du changement, qu'ils soient des acteurs établis ou de nouveaux participants.

2| La technologie des chaînes de blocs comme mécanisme de paiement

Afin d'examiner l'IoV en des termes plus concrets et pratiques, portons notre attention sur une manifestation spécifique des avantages de l'IoV au niveau mondial : l'application du protocole Ripple aux transferts de fonds interbancaires transfrontaliers. Malgré une innovation technologique rapide au cours des dernières décennies, les paiements transfrontaliers restent complexes et imparfaits. La fragmentation des systèmes de paiement limite l'interopérabilité, oblige à dépendre d'un nombre de plus en plus restreint d'intermédiaires et accroît les coûts et les délais de règlement. En modernisant les soubassements des infrastructures de paiement, la technologie des chaînes de blocs (*blockchain*) peut réduire ces inefficiences structurelles et mettre des

4 *Cf.* Gates Foundation.
5 *Cf., e.g., Lagarde (2014), GPFI (2012) et Morgan et Pontines (2014).*

services de paiement transfrontaliers instantanés, moins coûteux et plus sécurisés à la portée d'un nombre plus élevé de particuliers et d'entreprises.

2|1 Le protocole Ripple comme exemple de technologie des chaînes de blocs

En termes simples, la technologie des chaînes de blocs est un registre décentralisé ou une base de données partagée et publique qui vérifie et enregistre de façon permanente les transactions. Les transactions effectuées dans cette base de données sont compensées au moyen d'un protocole, c'est-à-dire un ensemble de règles automatisées, sans passer par une contrepartie centrale pour exécuter et confirmer les transactions. Les protocoles sont très largement utilisés pour assurer le fonctionnement d'internet, la plupart des gens interagissent quotidiennement avec eux. Ainsi, les courriers électroniques sont envoyés au moyen d'un protocole, SMTP, qui les dirige pendant leur parcours de la boîte d'envoi de l'expéditeur à la boîte de réception du destinataire.

Fondamentalement, la technologie des chaînes de blocs représente un dispositif permettant d'établir la confiance entre les contreparties sans exiger une autorité centrale unique ayant la confiance de tous. Le protocole développé par Ripple en est un exemple.

Le protocole Ripple utilise un registre public partagé qui compense bilatéralement et règle les paiements entre banques et systèmes de paiement instantanément. Ce registre garde une trace des comptes et des soldes des participants, et les nouvelles transactions sont autorisées et réglées au moyen d'un processus appelé consensus, créé par Ripple et par lequel un ensemble de contreparties autorisées valident des transactions au travers d'un réseau distribué de serveurs. Ce processus implique qu'une « supermajorité » de serveurs acceptent mutuellement qu'une transaction au sein du réseau soit valide avant la mise à jour du registre [6]. Les serveurs font cela en utilisant une cryptographie pour vérifier en toute sécurité les transactions. C'est ce processus de consensus qui permet un règlement rapide et sûr au travers des registres décentralisés [7].

2|2 Utilisation de la technologie des chaînes de blocs pour gérer les paiements transfrontaliers

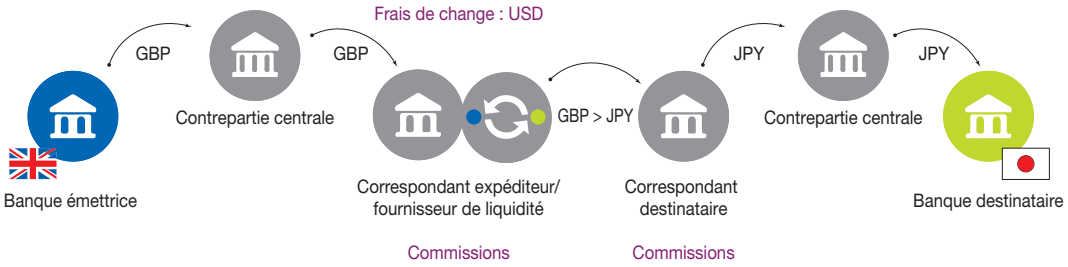
Les systèmes de paiement traditionnels se basent sur des tiers centraux de confiance pour traiter les paiements en toute sécurité. La confiance est tout particulièrement importante pour les paiements transfrontaliers, qui impliquent que de multiples parties dans différentes juridictions effectuent une série d'actions coordonnées. Les technologies des chaînes de blocs permettent à un système de paiement d'établir la confiance et d'opérer de manière entièrement distribuée, sans intermédiaires traditionnels comme les banques correspondantes. Le protocole Ripple peut être adapté à des systèmes de paiement sans forcément faire intervenir l'utilisation d'une monnaie numérique et en ayant recours à des monnaies fiduciaires (telles que le dollar américain, l'euro ou le yen) pour régler des transactions transfrontalières.

Supposons que la société Alpha, établie au Royaume-Uni, souhaite effectuer un paiement de 5 000 yens à la société Bêta, établie au Japon, pour régler un achat de produits, et qu'elle effectue ce paiement par virement bancaire. Dans un transfert de fonds classique, Alpha (l'initiateur) instruit sa banque (la banque Alpha) de payer, ou de faire payer par une autre banque, la société Bêta (le bénéficiaire). Ainsi, les sociétés Alpha et Bêta seraient seulement deux des nombreuses parties à ce paiement. Comme il est probable que les deux entités n'utilisent pas la même banque, la transaction ferait intervenir la banque Alpha et la banque de la société Bêta (banque Bêta) et, si aucune des deux ne possède un compte auprès de l'autre, d'autres intermédiaires (donc encore plus de parties). Une opération de change doit également avoir lieu, potentiellement avec cambiste tiers, afin que les fonds en livres sterling de la société Alpha puissent être utilisés

6 *Pour un examen plus détaillé des mécanismes autour du consensus, voir Schwartz* et al. *(2014)*

7 *Les registres décentralisés ne sont pas synonymes du registre distribué, spécifiquement utilisé par Bitcoin, également connu sous le nom de chaîne de blocs Bitcoin, ou par d'autres protocoles de monnaie numérique. Pour commencer, la dépendance au processus appelé «* proof of work *» (c'est-à-dire le « minage») utilisé par le protocole Bitcoin n'est pas nécessaire pour valider les transactions. La validation ne doit pas nécessairement dépendre de ce processus de « minage », grand consommateur de puissance de calcul, pour vérifier les transactions, tout comme la solidité du réseau n'est pas liée à la capacité de puissance de traitement qui lui est consacrée.*

Schéma 1



Note : Le diagramme ci-dessus décrit une transaction de paiement transfrontalier utilisant un système classique de banques correspondantes, les flèches illustrant le trajet des fonds, de la banque émettrice à la banque destinataire. Comme l'indiquent les points de rupture des flèches, le processus est séquentiel et fragmenté. Les étapes multiples faisant intervenir des processus manuels, en raison du manque d'interopérabilité entre les systèmes de paiement, accroissent la durée, le coût et le risque de la transaction.

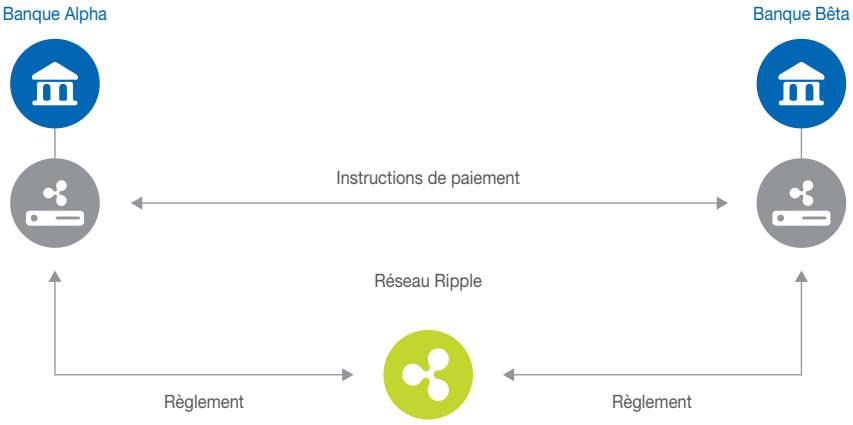
pour effectuer un paiement en yens à la société Bêta. Les parties doivent effectuer une série d'actions coordonnées pour que le paiement à la société Bêta puisse s'effectuer : chaque banque de la chaîne de paiements doit en effet créditer la banque en aval et recevoir un crédit de la banque en amont. Ces entrées au débit et au crédit doivent se compenser de manière à ce que, à l'issue de la transaction, il ne reste que le solde accru du compte de la société Bêta auprès de sa banque et le solde réduit de la société Alpha auprès de sa banque.

Cette coordination exige de la confiance, une condition obtenue par les systèmes de paiement au moyen de banques tierces de confiance, en l'occurrence les banques correspondantes. Dans l'exemple ci-dessus, les banques Alpha et Bêta dépendraient d'un tiers auprès duquel elles auraient toutes deux des comptes pour effectuer un règlement entre elles. Cette dépendance à une banque correspondante commune, que nous appellerons la banque Sigma, nécessite de faire confiance à la banque Sigma pour, entre autres, authentifier correctement la transaction et effectuer les vérifications nécessaires (concernant par exemple l'existence de fonds suffisants), créditer le compte de la banque Bêta du montant correct, et le faire de manière sécurisée. De manière plus générale, les banques Alpha et Bêta font confiance à la banque Sigma pour tenir un registre représentant correctement leurs soldes et pour que ce registre soit fiable, précis et honnête. Cet arrangement bien établi s'appuie sur un registre central, avec un règlement s'effectuant dans les comptes de la banque Sigma.

Il est évident que cette confiance et cette coordination s'inscrivent dans le cadre légal et réglementaire applicable aux paiements internationaux. Le contexte juridique encadrant les paiements internationaux reflète le caractère fragmenté des réseaux de paiement eux-mêmes. Bien que des efforts aient été déployés pour favoriser une uniformisation des règles régissant les paiements, dans les réseaux actuels de paiements transfrontaliers, différents corpus législatifs peuvent s'appliquer à une même transaction, à une même activité ou à une même contrepartie, avec pour conséquence possible l'application d'un régime juridique différent de celui prévu contractuellement. En réponse aux pressions commerciales appelant à une prévisibilité et une uniformité plus importantes des règles juridiques régissant les opérations internationales de valeur élevée, la Commission des Nations Unies pour le droit commercial international (CNUDCI) a mis au point en 1992 un modèle de législation sur les transferts internationaux de crédit que les différents pays peuvent choisir d'adopter. Le Parlement européen et le Conseil de l'Union européenne ont adopté en 1997 une directive s'appuyant sur les principes du modèle de législation de la CNUDCI (modifiée en 2007) [8], dans le but de promouvoir l'efficacité dans le cadre des paiements transfrontaliers au sein des Communautés européennes. Au niveau infranational, les cinquante États des États-Unis d'Amérique ont élaboré

8 *Directive 97/5/CE du Parlement européen et du Conseil du 27 janvier 1997 concernant les virements transfrontaliers ; Directive 2007/64/CE du Parlement européen et du Conseil du 13 novembre 2007 concernant les services de paiement dans le marché intérieur.*

Schéma 2



Note : Le diagramme ci-dessus décrit une transaction de paiement transfrontalier utilisant le protocole Ripple. Contrairement aux systèmes actuels, qui fonctionnent avec un règlement différé et un traitement séquentiel, sous le protocole Ripple, soit les paiements sont réglés intégralement et simultanément en temps réel, soit ils ne s'effectuent pas du tout – un processus appelé « atomic payments *». Cette manière de fonctionner élimine ou réduit un grand nombre des risques qui pèsent actuellement sur la dépendance à des intermédiaires s'agissant des paiements transfrontaliers, y compris le risque de crédit et le risque opérationnel.*

en 1989 l'article 4A du *Uniform Commercial Code*, un ensemble complet de textes de lois concernant les droits et les obligations associés aux transferts de fonds.

La technologie des chaînes de blocs peut révolutionner le cadre traditionnel des transferts de fonds, en remplaçant la nécessité d'une banque tierce de confiance (la banque Sigma) positionnée entre la banque Alpha et la banque Bêta. Compte tenu notamment de l'état fragmenté et intermédié des réseaux de paiements transfrontaliers (comme illustré dans le schéma 1), une infrastructure mondiale commune apporterait une nouvelle efficacité aux règlements financiers, avec des avantages directs pour le commerce international et l'inclusion financière.

Sur la base de l'exemple ci-dessus du paiement de 5 000 yens de la société Alpha, établie au Royaume-Uni, à la société Bêta, établie au Japon, la banque Alpha et la banque Bêta remplaceraient la tierce partie de confiance (banque Sigma) par une technologie de registre décentralisé. La banque Alpha et la banque Bêta utiliseraient le protocole Ripple pour effectuer simultanément une opération de change et une transaction de paiement par l'intermédiaire de n'importe quelle entité ayant un compte à la fois auprès de la banque Alpha et auprès de la banque Bêta (un fournisseur de liquidité) [9]. Ce fournisseur de liquidité peut être un client institutionnel de la banque Alpha et de la banque Bêta, par exemple un *hedge fund* ou un courtier négociant (*broker dealer*), acceptant d'intervenir en cette qualité et dûment autorisé à le faire par la banque Alpha et la banque Bêta. La banque Alpha vendrait des livres sterling et achèterait des yens au fournisseur de liquidité à un taux de change convenu. La technologie du registre décentralisé serait alors utilisée comme système de paiement contre paiement permettant à la banque Alpha à la fois de régler la transaction de change avec le fournisseur de liquidité et de régler son obligation de paiement à la banque Bêta en temps réel, avec transparence et atomicité [10].

Tout comme dans le cas d'une transaction effectuée à travers le réseau traditionnel de banques correspondantes, comme décrit dans l'exemple

9 *Remarquons que, contrairement à certains protocoles de chaînes de blocs «* trustless *», Ripple incorpore la confiance de plusieurs manières. Dans cet exemple, la confiance intervient en ce sens que (1) un fournisseur de liquidité doit détenir un compte à la fois auprès de la banque expéditrice et de la banque destinataire pour pouvoir remplir son rôle dans la transaction, et (2) le protocole Ripple contient lui-même une fonctionnalité d'autorisation qui permet aux participants de préciser les entités avec lesquelles ils acceptent d'effectuer des transactions.*

10 *Le terme « atomicité » est utilisé dans le domaine technologique pour désigner des actions intrinsèquement liées. Contrairement aux systèmes de paiement actuels, qui fonctionnent avec un règlement différé et un traitement séquentiel, sous le protocole Ripple, soit les paiements sont réglés intégralement et simultanément en temps réel, soit ils ne s'effectuent pas du tout.*

ci-dessus, ce transfert de fonds nécessiterait que la banque Alpha débite le compte de la société Alpha dans ses registres et que la banque Bêta crédite le compte de la société Bêta dans les siens. Les banques Alpha et Bêta, quant à elles, utiliseront le registre distribué pour coordonner certains enregistrements comptables au lieu d'effectuer le règlement entre elles par l'intermédiaire de la banque Sigma. Plus spécifiquement, la banque Alpha devrait augmenter le solde qu'elle doit au fournisseur de liquidité du montant en livres sterling qu'elle lui vend et, en même temps, la banque Bêta devrait réduire le solde qu'elle doit au fournisseur de liquidité du montant de l'obligation de paiement (c'est-à-dire le montant de yens que la banque Alpha a acheté au fournisseur de liquidité). Le protocole Ripple effectue simultanément toutes ces transactions. Les banques Alpha et Bêta utilisent donc les chaînes de blocs pour communiquer, coordonner, valider et enregistrer leur crédit et débit dans les comptes du fournisseur de liquidité.

3| Risques et avantages potentiels de la technologie des chaînes de blocs dans le contexte transfrontalier

Fondamentalement, cette solution de paiements décentralisés basés sur la cryptographie supprime l'intermédiaire. Ce faisant, son effet global est de réduire les risques inhérents à tout système bancaire intermédié. Pour les banques Alpha et Bêta, la technologie des chaînes de blocs élimine le risque que la banque Sigma puisse devenir insolvable alors qu'un montant élevé est dû à ses contreparties de paiements (risque de crédit) ou qu'elle ne dispose pas à un moment donné des fonds nécessaires pour régler un paiement exigible (risque de liquidité) [11].

En supprimant l'obligation traditionnelle d'une relation avec une banque correspondante pour exécuter la transaction, la technologie des chaînes de blocs réduit également le risque systémique. La dépendance du système financier mondial à un groupe concentré de contreparties centrales privées augmente les expositions au crédit et à la liquidité résultant du système intermédié actuel. Le système financier mondial est particulièrement vulnérable compte tenu de la tendance récente à la diminution des risques (*de-risking*) dans le monde bancaire international – c'est-à-dire la tendance parmi certaines banques à refuser les clients situés dans des régions à risque, ou faisant partie de secteurs économiques risqués, et à mettre fin à des relations de correspondant avec certaines autres banques avec lesquelles elles collaborent dans le cadre de transferts monétaires mondiaux [12]. Les coûts croissants et les incertitudes concernant les obligations de diligences comptent parmi les principales raisons avancées par les banques pour justifier cette tendance [13]. En conséquence, le nombre de banques ayant une envergure mondiale suffisante pour fournir des services de banque correspondante est en diminution, avec des conséquences néfastes sur l'inclusion financière mondiale et l'accès aux services financiers internationaux.

Outre qu'elle réduit les risques de crédit et de liquidité, la technologie des chaînes de blocs atténue le risque opérationnel systémique. En effet, comme la technologie des chaînes de blocs ne dépend pas d'une entité centralisée, elle est plus résistante à ce risque. Les systèmes de paiement centralisés sont sensibles aux faiblesses des systèmes d'information ou des processus internes, aux erreurs humaines, aux défaillances de gestion, ou aux perturbations causées par des événements extérieurs, avec pour conséquences une réduction, une détérioration ou une panne de leurs processus de règlement [14]. Ces défaillances opérationnelles peuvent causer des retards, des pertes, des problèmes de liquidité, et dans certains cas aboutir à des risques systémiques et à des crises de la liquidité ou à des problèmes opérationnels qui affectent l'ensemble du système financier. En revanche, de par leur nature de registre décentralisé diffusé à travers un réseau, Ripple et les protocoles semblables incluent intrinsèquement un certain nombre de sauvegardes redondantes

11 *Cf. Comité de la Banque des règlements internationaux sur les systèmes de paiement et de règlement et Comité technique de l'Organisation internationale des commissions de valeurs,* Principles for Financial Market Infrastructures (PFMI)*, p. 19, 36-45, et 57-63, avril 2012.*
12 *Comité de la Banque des règlements internationaux sur les paiements et les infrastructures de marché (2015).*
13 *Id.*
14 *Cf. BRI, CSPR et CTOICVM (2012), PFMI p. 20 et 94-100.*

dans leur technologie de base – qui peuvent se compter par milliers, soit beaucoup plus qu'on en trouve habituellement dans un système centralisé de paiement. S'agissant du risque systémique, la technologie des chaînes de blocs a le potentiel de réduire les risques pour les participants, de favoriser la transparence et d'améliorer la stabilité financière. Un cadre de paiements transfrontalier décentralisé remplace le modèle traditionnel en étoile (*hub-and-spoke*) dans lequel la faillite non contrôlée ou l'incapacité d'une contrepartie centrale à fonctionner comme prévu peut conduire à des perturbations systémiques simultanées pour les établissements et les marchés dépendant de cette contrepartie. Dans le cas en particulier où les services de paiement transfrontaliers sont concentrés entre un petit nombre de contreparties centrales fournissant leurs services à des établissements et marchés interconnectés, ces interdépendances complexes accroissent le risque de propagation rapide, imprévisible et à grande échelle des perturbations aux marchés [15]. À l'inverse, la technologie des chaînes de blocs relie tous les établissements participants les uns aux autres au sein d'un réseau, ce qui permet à chacun d'obtenir rapidement et efficacement un substitut pour les paiements critiques en cas de défaillance d'un établissement. En outre, la technologie est conçue pour permettre l'accessibilité et encourager l'inclusion à l'échelle mondiale. Sa structure de règlement neutre intègre et traite toutes les devises et tous les participants sur un pied d'égalité, indépendamment de leur taille. La technologie peut également être intégrée pour fonctionner en interconnexion avec les systèmes de paiement existants, ce qui réduit les frictions entre les participants et accroît l'efficacité. En donnant aux établissements l'assurance que leurs obligations de paiement seront honorées sans délai, même durant les périodes de perturbations sur les marchés ou de chocs financiers, la technologie des chaînes de blocs peut être une source importante de solidité sur les marchés financiers.

Bien entendu, comme pour toute nouvelle technologie, il subsiste une certaine incertitude concernant la technologie des chaînes de blocs. L'intégration de toute nouvelle technologie financière s'accompagne inévitablement de risques opérationnels et techniques ; toutefois, dans le cas des registres décentralisés, le principal risque qui subsiste tient à l'application des lois et des réglementations relatives aux transactions effectuées au moyen de cette technologie. Pour qu'un cadre décentralisé de transfert de fonds puisse fonctionner, il est indispensable que les droits et les obligations des parties soient connus avec certitude et clarté, y compris le moment où certains droits sont créés et où certaines obligations s'éteignent [16]. Comme nous l'avons remarqué, les paiements transfrontaliers s'effectuent actuellement dans un environnement comportant un certain degré d'incertitude juridique. En l'absence d'un cadre législatif ou réglementaire harmonisé à l'échelle mondiale, les règles des contrats privés et des système de paiements privés vont combler cette lacune à l'heure où la technologie des chaînes de blocs reste récente et où son adoption ne fait que commencer. Toutefois, l'internationalisation et la rapidité accrue des échanges commerciaux et financiers autorisées par l'IoV entraîneront des pressions commerciales dans le monde en faveur d'une plus grande certitude et d'une harmonisation internationale plus large du droit qui régit ces transactions internationales. Ce processus d'harmonisation nécessitera une participation et une collaboration internationales et, dans le cas de traités et de convention, un engagement national de les mettre en œuvre.

4| Considérations politiques

Pour pouvoir tenir ses promesses au mieux, l'IoV a besoin d'un cadre politique, juridique et réglementaire mondial adapté. Actuellement, alors que les gouvernements examinent les manifestations des stades embryonnaires de l'IoV, certains se concentrent sur les risques posés par l'introduction de nouvelles technologies dans le secteur financier mondial, ou envisagent les mesures qui permettront de limiter ou de contrôler ces risques. Toutefois, compte tenu de son potentiel à favoriser la prospérité, l'inclusion et la stabilité financière, peut-être que le plus grand risque associé à l'IoV serait que des mesures étatiques divergentes ou une inertie internationale

15 *Cf. BRI, CSPR et CTOICVM (2012), PFMI p. 9-10 et 18.*
16 *Cf. BRI, CSPR et CTOICVM (2012), PFMI p. 18 et 21-25.*

l'empêchent d'atteindre pleinement son potentiel.

Nous invitons les dirigeants de la planète à tirer profit des précédents historiques dans l'examen des questions politiques soulevées par l'IoV. À l'origine, internet est né de la collaboration des pouvoirs publics, des universités et du secteur privé ; dans l'examen de l'IoV, les décideurs politiques pourraient utilement s'inspirer de ce modèle. Contrairement aux dirigeants des années quatre-vingt-dix, qui découvraient la première émergence d'un marché réellement mondial, les décideurs politiques actuels peuvent s'appuyer sur les enseignements du passé. À cet égard, les évolutions suivantes, notamment, pourraient fournir des modèles utiles aujourd'hui :

- Normes ouvertes (*Open standards*)

Les normes ouvertes ont joué un rôle pivot dans le développement d'internet. Les normes ouvertes telles que HTTP et TCP/IP sont les piliers d'internet tel que nous le connaissons [17]. Aujourd'hui, dans le domaine de la finance mondiale, les normes ouvertes telles que Ripple permettent de penser que des avancées similaires pourraient être possibles dans le monde financier.

Les normes ouvertes présentent de nombreux avantages potentiels pour le monde financier. Elles garantissent l'interopérabilité ; elles sont indispensables pour relier les registres des banques et les réseaux de paiements qui ne sont pas actuellement en mesure de communiquer. Les normes ouvertes sont également plus robustes que les solutions propriétaires, et permettent une sécurité accrue ainsi que des méthodes de prévention des fraudes. Elles favorisent la concurrence sur le marché et créent un environnement équitable permettant aux innovateurs de développer des produits avec la plus grande portée possible.

Les normes ouvertes favorisent l'élaboration d'une réglementation basée sur les intervenants ; et, dans une large mesure, internet a été administré avec succès, le cas échéant, par des groupes privés, intervenant sans but lucratif. Bien que les groupes basés sur les intervenants ne soient pas toujours la solution idéale, ils ont la flexibilité et la versatilité nécessaires pour réagir plus rapidement que les organismes gouvernementaux aux évolutions de la technologie et des marchés. Le soutien politique à un élargissement de l'utilisation des normes ouvertes aux transactions financières serait un moyen important par lequel les dirigeants mondiaux pourraient soutenir la création d'un IoV robuste.

- Principes de base pour un environnement juridique et réglementaire adapté

Nous sommes à la veille d'une mutation majeure du secteur financier mondial, et une harmonisation progressive des normes et des règles internationales est nécessaire pour réaliser tout le potentiel de cette vague d'innovation. La participation et la collaboration mondiales sont nécessaires pour permettre au droit commercial international d'évoluer au rythme de l'innovation de la technologie financière. Loin de jouer un rôle « perturbateur », de nombreuses entreprises de technologie financière, à l'image de Ripple, se sont engagées à travailler main dans la main avec les parties prenantes internationales pour clarifier et renforcer le consensus autour des principes fondamentaux susceptibles de guider les efforts futurs d'élaboration des politiques. À cet égard, l'ensemble des discussions portant sur les principes et les politiques qui se sont déroulées aux premiers temps d'internet peut utilement servir de point de départ.

Les dirigeants mondiaux ont appris à reconnaître le potentiel de croissance économique qu'internet pouvait apporter, et les années quatre-vingt-dix ont été une période d'efforts coordonnés par les décideurs politiques de la planète pour assurer qu'internet puisse soutenir un marché mondial dans l'intérêt de tous les participants. Ces efforts ont été officialisés par la déclaration de Bonn sur les réseaux d'information mondiaux [18], ainsi que par ce qu'on a appelé le cadre général pour le commerce électronique (*Framework for Global Electronic Commerce*) aux États-Unis [19].

Cette initiative visait à créer un environnement juridique pour le commerce mondial qui soit

17 *Cf. Ito (2009).*
18 *Cf. Union européenne (1997).*
19 *Cf. La Maison Blanche, États-Unis (1997).*

simple, prévisible, favorable à la concurrence et cohérent. Elle a abouti à des efforts concrets et constructifs, tels que la reconnaissance juridique des signatures électroniques [20] et la création de l'ICANN (*Internet Corporation for Assigned Names and Numbers*) [21], ce qui a favorisé la croissance du marché électronique mondial qui existe aujourd'hui sur internet. Les principes de base présentés dans l'initiative mondiale de 1996 restent d'excellentes références pour créer un environnement mondial juridique et réglementaire pour l'IoV.

5| Conclusion

Le potentiel de l'IoV pour porter l'économie internationale à un nouveau niveau plus élevé d'inclusion financière, de prospérité et de stabilité systémique présente de formidables possibilités. Les améliorations au système financier mondial ne pourront toutefois être apportées qu'avec le soutien d'un cadre mondial harmonisé adéquat. L'heure est venue pour les décideurs politiques de réfléchir à la meilleure manière de préparer le terrain.

20 *Cf. Uncitral (1996).*
21 *Cf. Département du commerce, États-Unis (1998).*

Bibliographie

Banque des règlements internationaux, Comité sur les infrastructures de paiement et de marchés (2015)
« *Correspondent banking, Consultative Report* », p. 8-10, octobre, *http://www.bis.org/cpmi/publ/d136.pdf*

Banque des règlements internationaux, Comité sur les systèmes de paiement et de règlement et Comité technique de l'Organisation internationale des commissions de valeurs mobilières (2012)
« *Principles for financial market infrastructures* (PFMI) », avril, *http://www.bis.org/cpmi/publ/d101a.pdf*

Département du commerce, États-Unis (1998)
« *Management of Internet names and addresses* », Policy Statement, juin, *https://www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses*

Gates Fondation
Strategy Overview, Financial Services for the Poor, *http://www.gatesfoundation.org/What-We-Do/Global-Development/Financial-Services-for-the-Poor*

Global Partnership for Financial Inclusion (GPFI) (2012)
« *Financial inclusion – A pathway to financial stability? Understanding the linkages* », First Annual Conference on standard-setting bodies and financial inclusion, *Issues Paper*, Issue 3, 29 octobre, *http://www.gpfi.org/sites/default/files/documents/GPFI%20SSBs%20Conference%20%20Issues%20Paper%203%20Financial%20Inclusion%20%E2%80%93%20A%20Pathway%20to%20Financial%20Stability_1.pdf*

Greene (C.), Rysman (M.) et Schuh (S.) (2014)
« *Costs and benefits of building faster payment systems: the UK experience and implications for the United States* », Federal Reserve Bank of Boston, *Current Policy Perspectives*, n° 14-5, p. 27-35, 10 octobre.

Ito (J.) (2009)
« *Innovation in open networks* », 30 octobre, *http://joi.ito.com/weblog/2009/10/30/innovation-in-o.html*

Lagarde (C.) (2014)
« *Empowerment through financial inclusion* », address to the International forum for financial inclusion, Mexico, 26 juin, *https://www.imf.org/external/np/speeches/2014/062614a.htm*

La Maison Blanche, États-Unis (1997)
« *A framework for global electronic commerce* », juillet, *http://clinton4.nara.gov/WH/New/Commerce/*

Morgan (P.) et Pontines (V.) (2014)
« *Financial stability and financial inclusion* », Asian Development Banking Institute, Working Paper n° 488, juillet, *http://www.adb.org/sites/default/files/publication/156343/adbi-wp488.pdf*

Schwartz (D.), Youngs (N.) et Britto (A.) (2014)
« *The Ripple protocol consensus algorithm* », Consensus Whitepaper, *https://ripple.com/consensus-whitepaper/*

Uncitral (1996)
« *Model law on electronic commerce* », *https://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf*

Union européenne (1997)
« *Global information networks: realising the potential* », Ministerial Declaration, juillet, *http://web.mclink.it/MC8216/netmark/attach/bonn_en.htm#Heading01*

Trading à haute fréquence, géographie et courbure de la Terre

Fany DECLERCK
Professeur de finance
Toulouse School of Economics

Pour les traders *à haute fréquence, la fragmentation, l'information, la vitesse et la proximité aux marchés sont primordiaux. Aujourd'hui, sur les marchés financiers, chaque nanoseconde compte ; dès lors une surenchère est probable, les* traders*, les plates-formes ou les investisseurs se faisant concurrence pour être le plus rapide. La littérature théorique démontre également que les* traders *à haute fréquence peuvent aggraver la sélection adverse au détriment des autres* traders *et perturber, sur le long terme, le contenu informationnel des prix des actifs. Dans ce contexte, régulateurs et chercheurs empiriques sont désormais confrontés à des défis majeurs. De nombreux éléments tendent à indiquer que le* trading *à haute fréquence (THF) a contribué à améliorer la liquidité et le processus de découverte des prix. Néanmoins les évidences empiriques montrent également que les* traders *à haute fréquence exploitent, à l'encontre des* traders *plus lents, les informations de marché qu'ils reçoivent et analysent ultra rapidement. Enfin, la stratégie des investisseurs institutionnels consistant à travailler les ordres (*slice and dice*) ne semble pas suffisante pour éviter le risque de détection par les* traders *à haute fréquence. En effet, si, lors de la première heure suivant le passage d'un ordre, les* traders *à haute fréquence agissent comme teneurs de marché, ils accroissent ensuite les coûts de transaction pour le* trader *institutionnel.*

«Après la Seconde Guerre mondiale, un titre appartenait à son propriétaire pendant quatre ans. En 2000, ce délai était de huit mois. Puis de deux mois en 2008. En 2013, un titre boursier change de propriétaire toutes les 25 secondes en moyenne, mais il peut aussi bien changer de main en quelques millisecondes. »
Alexandre Laumonier (2014)

La microstructure de marché se concentre quasi exclusivement sur la façon de se procurer de l'information et de la mettre à profit. Avant l'ère technologique, l'un des atouts majeurs du *trader* de la Bourse de Chicago *(Chicago Board of Trade)* était ses chaussures. Des chaussures à talons compensés, pour être précis, qui augmentaient la taille d'une hauteur pouvant aller jusqu'à 8 centimètres[1]. Il s'agissait là d'une tactique simple mais efficace pour voir et être vu des autres *traders,* au-dessus des bras qui s'agitaient en tous sens et des mains qui se tendaient sur le parquet où s'effectuaient les transactions. La Bourse de Chicago a accepté ses premiers *traders* de sexe féminin en 1969 : le but n'était pas de promouvoir l'égalité hommes femmes, mais, fait intéressant, les autres *traders* semblaient mieux entendre leur voix plus aiguë. Cette forme d'« amateurisme » a été suivie d'une période d'incroyables innovations mathématiques et technologiques. Processus qui a totalement remodelé le secteur financier.

Neuf hommes, basés à Chicago, Londres, New York et Santa Fe, ont été les pionniers de cette avancée. Un des premiers pas a été Instinet, une société fondée par Herbert Behrens et Jerome Pustilnik. Lancée en 1969, cette nouvelle plate-forme de négociation, entièrement automatisée, transparente et anonyme a commencé à faire concurrence à la Bourse de New York (*New York Stock Exchange*). Son principal atout était de permettre une négociation directe entre banques, fonds communs de placement et sociétés d'assurance, sans attentes et sans l'intervention de spécialistes.

En 1977, Thomas Peterffy (Interactive Brokers), un programmateur informatique autodidacte, s'est acheté un siège de teneur de marché à l'*American Stock Exchange* et a commencé à développer un logiciel de *trading* algorithmique (ou *algo trading*) visant à remplacer les procédures manuelles par des procédures automatisées plus efficientes. En 1987 il a créé le premier cyborg, ou *trader* à haute fréquence, en utilisant un simple ordinateur IBM, pour réaliser des transactions sur le Nasdaq[2].

Dans le même esprit, Josh Levine et Sheldon Maschler, qui ont été rejoints par la suite par Jeff Citron, ont tiré profit d'une faille du système d'exécution des ordres de petit montant sur le Nasdaq (*Nasdaq Small Order Execution System* – SOES) pour réaliser des transactions à l'aide d'un logiciel algorithmique et dégager des bénéfices importants. Ces algorithmes automatisés intégraient, en continu et conjointement, la gestion du risque de position et les opportunités de *trading* présentes sur SOES. Comme dans les jeux vidéo, les *traders* avaient juste à cliquer sur les boutons achat ou vente. Ces algorithmes ont fini par donner naissance à Island, l'une des premières plates-formes électroniques de négociation aux États-Unis.

Enfin, en 1985, James Doyne Farmer, Norman Harry Packard et Jim McGill (The Prediction Company) ont combiné le *trading* algorithmique, la théorie du chaos et les systèmes complexes pour éliminer la composante bruit des informations fondamentales pour prévoir les prix des titres financiers.

Ces neufs pionniers ont réussi à associer l'informatique, les mathématiques, la physique et la finance. En 2014, dans ses recherches en anthropologie parues sous le titre *6/5*, Alexandre Laumonier apporte un éclairage très précieux, indispensable sur l'histoire des marchés financiers.

Pourtant, un dernier ingrédient manquait encore : les innovations dans le secteur des télécommunications. Avant le télégraphe, au début des années 1840, il fallait deux semaines pour qu'une information relie Wall Street à Chicago. Avec l'invention du télégraphe, la même information pouvait être envoyée en seulement deux minutes. En septembre 1949, *Long Lines Magazine* annonce la mise en place d'un système de micro-ondes entre New York et Chicago : l'information se transmet dès lors en quelques 3,3 microsecondes par kilomètre[3].

1 *Les autorités boursières faisant preuve de vigilance afin de s'assurer que personne ne serait favorisé par des procédés déloyaux, la Bourse de Chicago a fait appliquer des règles sur la hauteur des talons. Une image reproduisant les chaussures à talons compensés de la Bourse de Chicago peut être vue au musée de l'histoire de Chicago* https://www.flickr.com/photos/chicagohistory/3429555190
2 *Thomas Peterffy en fournit une illustration dans le documentaire The Wall Street Code :* https://sniperinmahwah.wordpress.com/2013/11/05/the-wall-street-code/
3 http://meanderful.blogspot.fr/2014/08/historic-us-microwave-links-and-ny-to.html

De nos jours, afin de gagner encore quelques nanosecondes, des entreprises comme Anova, spécialisée dans les réseaux à faible latence pour les transactions boursières, installent des réseaux laser à très grande vitesse, non seulement entre la Bourse de NewYork (à Mahwah, New Jersey) et le Nasdaq (à Carteret, New Jersey), mais également entre les bourses de Londres et de Francfort. Si la vitesse doit être encore accrue, les intermédiaires financiers peuvent alors payer afin de placer leurs serveurs au sein des centres de données des bourses sur lesquelles ils interviennent, une pratique appelée *co-location*.

Si ce regard historique apporte un éclairage sur la progression vers le *trading* à haute fréquence, Biais et Foucault (2014) définissent les *traders* à haute fréquence de la façon suivante : « *Les THF visent à minimiser les " temps de latence " : essentiellement le temps nécessaire pour qu'ils reçoivent les messages (par exemple, une mise à jour des prix de cotation ou le statut de leurs ordres) des plates-formes de négociation, traitent cette information, et y réagissent en renvoyant de nouveaux ordres (ordres au prix du marché, ordres à cours limité, ou annulations) s'appuyant sur cette information.* » La vitesse et la proximité par rapport aux marchés sont donc des données importantes.

Les principales caractéristiques du THF[4] sont les suivantes : a) important flux intrajournalier de messages (ordres, prix ou annulations) ; b) émission massive d'ordres annulés très peu de temps après ; c) décomposition d'un ordre en plusieurs ordres de petite taille ; d) dénouement des positions à la fin de chaque séance (pour éviter de porter au jour le jour des positions importantes non couvertes).

1| Quelques points théoriques relatifs au *trading* à haute fréquence

En raison de la fragmentation des marchés et des caractéristiques du THF, les investisseurs se doivent de pouvoir rassembler et traiter de très grandes quantités de données de marché et d'informations directement exploitables par les ordinateurs (Declerck et Lescourret, 2015). Une conséquence de cette fragmentation des marchés est donc la nécessité d'investir dans des technologies de THF pour pouvoir traiter toutes ces informations issues de plusieurs marchés et pouvoir envoyer leurs ordres sur la plate-forme proposant les meilleurs prix. Les entreprises doivent également s'abonner auprès de fournisseurs de données et d'informations pour alimenter leurs stratégies de THF.

1|1 Surinvestissement

Sur les marchés financiers contemporains le temps de latence est devenu critique ; chaque nanoseconde compte et toute information, si minime soit-elle, est importante. Biais *et al.* (2015) ont élaboré un modèle dans lequel les institutions à haute fréquence peuvent rechercher des prix attractifs simultanément sur toutes les plates-formes de négociation, mais peuvent également effectuer des transactions fondées sur une information privilégiée (par exemple le rendement des actifs). Ces autres *traders* n'ont pas cet avantage et doivent donc supporter un coût de sélection adverse plus élevé. Dans leur modèle, les auteurs analysent les décisions d'investissement optimales dans les technologies du THF, leurs conséquences en termes de bien-être, et les interventions possibles des autorités pour atteindre un niveau d'investissement socialement optimal dans les technologies à grande vitesse. Premièrement, ils démontrent que ce niveau d'investissement socialement optimal est, en général, différent de zéro. Deuxièmement, les technologies du THF améliorent le bien-être social et aident les intermédiaires financiers à appréhender la fragmentation des marchés. Toutefois, l'accès ultra-rapide à des prix de marché génère bien une externalité négative. Comme les intermédiaires ne prennent pas en compte cette externalité négative, ils surinvestissent, ce qui conduit à une surenchère dans laquelle toutes les institutions finissent par investir dans les technologies ultra-rapides.

Richborough (Kent, Royaume-Uni) est un exemple récent de ce genre d'investissement colossal : pour être sûre que même la courbure de la terre ne perturbera pas sa capacité à transmettre des données à l'Europe continentale, la société Vigilant Global a tenté d'ériger un pylône de 324 mètres, soit 12 mètres de plus que la tour Eiffel. Cette mégastructure devait envoyer des ondes par laser de l'autre côté de la Manche pour le compte des sociétés de *trading* à haute fréquence. Le projet a suscité l'opposition des membres du conseil municipal du village, qui ont

4 *MiFID II, Article 4(1)(40).*

voté à l'unanimité contre le pylône de Vigilant[5]. Les choses ne devraient pas en rester là pour autant à Richborough, puisqu'une autre société, New Line Networks, projette désormais de construire son propre pylône dans la ville[6].

Avec ce type d'infrastructure, les bourses doivent également investir dans des technologies ultra-rapides si elles veulent attirer le flux d'ordres. Cela est confirmé par Pagnota et Philippon (2015) qui démontrent que les marchés financiers se font concurrence lorsqu'il s'agit d'attirer les investisseurs dans le choix de la place boursière et du volume de leurs transactions. Dans leur modèle, les plates-formes avec les délais de latence les plus faibles facturent des frais de transaction plus élevés et attirent les *traders* à haute fréquence. La concurrence entre plates-formes accroît les volumes et l'efficience des prix, mais l'entrée et la fragmentation peuvent être trop coûteuses, et il peut en résulter un investissement excessif dans la vitesse. Un exemple de cette concurrence entre plates-formes de négociation liée au temps de latence est la construction par Euronext, principale bourse d'Europe continentale, d'un centre de données ultra-moderne à Basildon (une banlieue de Londres) afin de se rapprocher des banques d'investissement et des *hedge funds*.

Enfin, pour améliorer leur capacité de suivi des ordres placés sur les marchés financiers, la course à cette latence réduite peut également avoir lieu entre fournisseurs et consommateurs de liquidité, entraînant des investissements socialement non optimaux. Bongaerts *et al.* (2015) s'intéressent à cet effet de fourniture de liquidité des *traders* à haute fréquence. Ils mettent tout d'abord en évidence que la complémentarité entre fournisseurs et consommateurs de liquidité accroît le nombre des transactions et peut donc induire un sous-investissement dans la vitesse si les bénéfices extraits des transactions sont suffisants. Cela étant, si les bénéfices issus des transactions diminuent avec la fréquence des transactions, une surenchère est plus probable.

1|2 Asymétrie d'information

Les *traders* à haute fréquence s'appuient sur deux caractéristiques principales : une infrastructure totalement informatisée et un accès ultra-rapide aux plates-formes de négociation et à l'information de marché. Grâce à la rapidité de leurs technologies, ils peuvent repérer les signaux et ensuite prévoir les mouvements de prix plus vite que les autres *traders*. Biais *et al.* (2015) démontrent que les *traders* à haute fréquence sont capables d'effectuer des transactions sur la base de ces informations. L'article théorique de Foucault *et al.* (2016) considère un modèle dynamique de négociation sur la base d'informations publiques et d'un accès plus rapide à du contenu informationnel[7]. Un spéculateur et un intermédiaire compétitif ont accès à un signal sur le rendement à long terme d'un actif risqué (information publique). Aussi longtemps qu'un spéculateur à haute fréquence peut exploiter des informations privées reçues plus rapidement et, précises, sur la valeur à long terme et à court terme, il fondera ses transactions d'abord sur l'évolution des prix à court terme et ensuite sur l'information fondamentale de long terme, même si ces deux informations sont contradictoires. Ce modèle aide à la compréhension des transactions d'achat-vente des *traders* à haute fréquence sur de très courtes périodes (de quelques millisecondes à quelques nanosecondes). Cela étant, le spéculateur à haute fréquence utilise également des informations pérennes pour ses opérations et, néanmoins, afin d'éviter une forte diminution du profit global, les *traders* haute fréquence exploitent les informations fondamentales en négociant de façon plus agressive à court terme qu'à long terme.

Tandis que Foucault *et al.* (2016) s'intéressent aux stratégies directionnelles des *traders* à haute fréquence, Aït-Sahalia et Saglam (2014) étudient, dans un cadre dynamique, l'activité de tenue de marché des *traders* haute fréquence. Les résultats font apparaître des bénéfices plus importants, un niveau de liquidité et un taux d'annulation plus élevés dans des conditions de marché normales si le teneur de marché haute fréquence est en situation de monopole. Le modèle prédit également que l'offre de liquidité décroît lorsque la volatilité des prix augmente. L'introduction de la concurrence entre teneurs de marché haute fréquence améliore la liquidité pour les investisseurs finaux.

1|3 Information et processus de découverte des prix

Depuis Foucault *et al.* (2016), nous savons qu'un spéculateur à haute fréquence réalise ses transactions de manière plus agressive à partir d'informations vite

5 *Pour plus de précisions sur cette histoire, consulter le blog Sniper in Mahwah :* https://sniperinmahwah.wordpress.com/
6 http://www.kefmast.co.uk/
7 *L'information peut être issue de sites internet d'entreprises, d'institutions financières, d'organismes réglementaires, de journaux, de Twitter, de Facebook, de blogs, etc.*

périmées et plus passive à partir d'informations de long terme. Ce comportement a deux conséquences. Premièrement, conformément aux conclusions de Biais *et al.* (2015) les *traders* à haute fréquence peuvent produire une sélection adverse au détriment des autres *traders*. Deuxièmement, les transactions des THF contribuent au processus de découverte des prix : elles révèlent plus d'informations sur l'évolution des prix à court terme et moins d'informations sur l'évolution des prix à long terme ; globalement le processus de découverte des prix n'est pas affecté négativement par le THF.

La dernière question théorique abordée dans cette étude a trait à la qualité et au coût de l'information. Aujourd'hui, sur les marchés, l'information est facilement, directement et électroniquement accessible à l'ensemble des investisseurs, mais elle reste onéreuse même si son coût a diminué au fil du temps. Les modèles statiques prédisent que, en raison de l'accroissement du nombre des informations disponibles, le processus de découverte des prix devrait s'améliorer (Grossman et Stiglitz, 1980 et Verrechia,1982). Exploiter les informations afin d'obtenir un signal de qualité reste néanmoins consommateur de temps. En l'espèce, Dugast et Foucault (2016) montrent que la diminution du coût de l'accès aux données peut perturber le contenu informationnel des prix des actifs à long terme.

Deux catégories d'informations se distinguent dans leur modèle dynamique : les données brutes et les données retraitées. La première est un signal bruité et la seconde est une information fondamentale, dont le bruit a été retiré. Un investisseur peut acquérir des informations brutes ou retraitées, mais ces dernières arriveront plus tard et sont plus coûteuses. Plus le coût des données brutes diminue, plus les investisseurs sont enclins à les exploiter *via* des transactions, ce qui améliore le processus de découverte des prix à court terme. Si le contenu informationnel des données brutes est faible cela entraîne dès lors une mauvaise évaluation du prix des actifs financiers et crée ainsi des opportunités de profits sur la base des informations fondamentales. En revanche, si le signal brut est suffisamment fiable, il peut entraîner un effet d'éviction : le bénéfice attendu des données retraitées est si faible que la demande pour ces données se tarit. Dans ce cas le prix final ne révèlera pas totalement la valeur de l'actif. Les *traders* à haute fréquence sont, à l'évidence, une catégorie d'investisseurs susceptibles de réaliser des transactions fondées sur des données brutes.

2| Évidences empiriques

Lorsqu'on analyse les effets du THF sur la qualité du marché, il est essentiel de garder à l'esprit l'insuffisance des données (Biais et Foucault, 2014). Certes, les chercheurs empiriques peuvent examiner l'impact du THF aux États-Unis et en Europe, mais les données disponibles sont très limitées[8]. Cette situation soulève des questions quant à la robustesse des conclusions empiriques. La quasi-totalité des études empiriques utilisent une définition fondée sur les données pour identifier les *traders* à haute fréquence. Un intermédiaire est classé comme société de THF s'il négocie uniquement pour compte propre (*proprietary trading*), si le nombre de ses transactions est important, ses positions (son inventaire) sont en moyenne closes quotidiennement et son taux d'annulation des ordres est élevé. Ces échantillons, selon les critères de sélection, excluent les arbitragistes ou les *desks* de THF des banques d'investissement, ou au contraire se concentrent sur les sociétés de THF jouant le rôle de teneur de marché.

2|1 Vitesse et qualité de marché

Nous savons que le THF peut conduire à une surenchère, dont la liquidité serait alors la victime collatérale (Biais *et al.*, 2015, et Bongaerts *et al.*, 2015). Cependant, la plupart des éléments dont on dispose laissent à penser que le THF a contribué à améliorer la liquidité et le processus de découverte des prix. En se basant sur les négociations du NYSE sur une période de cinq ans, Hendershott *et al.* (2011) constatent une relation positive entre le THF et la liquidité de marché. Ils utilisent alors l'introduction du système Autoquotation en 2003 comme événement exogène afin d'étudier la causalité entre vitesse et liquidité. À la suite de cette introduction, ils observent une baisse des *spreads* effectifs et du coût de la sélection adverse (uniquement) pour les actions à forte capitalisation. Les prix deviennent plus informatifs et l'offre de liquidité s'améliore. Brogaard *et al.* (2014) indiquent que les *traders* à haute fréquence permettent un meilleur contenu informationnel des prix : ils soumettent des ordres à cours limité

8 *La plus connue est la base de données du Nasdaq, qui reprend les négociations de 26 sociétés identifiées par le Nasdaq comme* traders *THF, parmi 120 actions cotées au Nasdaq et au NYSE sélectionnées de manière aléatoire.*

pour intégrer les informations fondamentales dans les prix et des ordres au marché immédiatement exécutables (*marketable orders*) contre le flux d'ordres pour absorber les pressions temporaires sur les prix. Ainsi, grâce à leur capacité à prévoir les variations de prix à très court terme, ils contribuent à la stabilité du marché. De plus, les *traders* à haute fréquence ne sortent pas du marché lors des périodes de tension.

En utilisant une base de données canadienne non publique sur la période de juin 2010 à mars 2011, Boehmer *et al.* (2015), avec une définition endogène des *traders* haute fréquence, concluent que les sociétés de THF ne déstabilisent pas les bourses. Comme Hasbrouck et Saar (2013), ils ne constatent pas d'augmentation de la volatilité du prix des actions. En utilisant la même base de données canadienne sur la période du 15 octobre 2012 au 28 juin 2013 pour 15 actions à forte capitalisation, Brogaard *et al.* (2015) se focalisent sur les ordres à cours limité des *traders* à haute fréquence. Les auteurs démontrent que ces ordres sont plus riches en contenu informationnel et sont presque deux fois plus fréquents que les ordres à cours limité des non-THF. En résumé, il semble que les sociétés de *trading* à haute fréquence facilitent l'offre de liquidité et la découverte des prix.

2|2 Vitesse et externalités négatives

L'accélération des négociations peut réduire les frictions et les coûts de transaction, mais elle peut également engendrer des externalités négatives. Les frictions sont les suivantes : sélection adverse, risques liés à la détention d'un portefeuille (ou inventaire) et problèmes d'agence et d'incitations. En 2012, le marché boursier Nasdaq OMX de Stockholm a proposé une amélioration de son offre existante de colocation : chaque intermédiaire pouvait choisir (ou non) de payer des frais supplémentaires pour accélérer sa rapidité de négociation. Brogaard *et al.* (2016) utilisent une base de données non-publique permettant l'observation directe de données lorsque la firme de *trading* a souscrit à ce nouveau service de colocation. L'utilisation d'un modèle Probit leur permet de montrer que cette amélioration a été choisie essentiellement par les teneurs de marché à haute fréquence. En utilisant une approche de différence des différences, ils démontrent que cette mise à jour du système électronique de cotation entraîne une amélioration de la liquidité *via* une réduction du risque lié à la détention d'un portefeuille, et que ces progrès profitent à la fois aux *traders* à haute fréquence et aux *traders* plus lents. Enfin, les données indiquent que les ordres passés par les *traders* à haute fréquence reflètent l'accès privilégié aux informations de marché. Cet avantage informationnel est cohérent avec un coût de sélection adverse plus élevé pour les *traders* non haute fréquence (Brogaard *et al.*, 2014 et Brogaard *et al.*, 2015).

Conformément à ce dernier résultat, Menkveld et Zoican (2015) montrent que le nouveau système de négociation introduit en 2010 sur le Nasdaq OMX, tout en réduisant le temps de latence des échanges, accroît également les *spreads via* une sélection adverse plus élevée. Ainsi, l'augmentation de la vitesse de négociations peut réduire la liquidité de marché. Weller (2016) trouve également un lien négatif entre les *traders* à haute fréquence et le contenu informationnel des prix.

En utilisant des données provenant d'Euronext et de l'Autorité des Marchés Financiers, Biais *et al.* (2016) observent la qualité de la connectivité des *traders* au marché et s'ils négocient pour compte propre. Ils montrent que les *traders* pour compte propre, qu'ils soient rapides ou lents, offrent de la liquidité en se positionnant en sens inverse du flux d'ordres avec des ordres au marché immédiatement exécutables. Ces *traders* pour compte propre permettent ainsi d'absorber les chocs de liquidité sur le marché, même pendant les périodes de forte volatilité, et réalisent un profit positif en agissant de la sorte. Par ailleurs, les *traders* à haute fréquence apportent également de la liquidité en soumettant en carnet des ordres à cours limité. Cependant, seuls les *traders* pour compte propre peuvent agir ainsi sans subir de pertes. Ce résultat laisse penser que la technologie n'est pas suffisante pour gérer le coût de sélection adverse ; une structure d'incitation à une gestion optimale des inventaires est également nécessaire.

2|3 Investisseurs institutionnels

Une préoccupation surgit régulièrement lors de l'examen de l'impact des *traders* à haute fréquence sur la liquidité globale du marché : la baisse sensible des quantités disponibles en carnet et, en corollaire, la réduction importante de la taille des transactions. Par conséquent, les investisseurs institutionnels doivent en permanence travailler leurs ordres de grande taille en petits lots en adoptant une stratégie de *slice and dice*. La littérature empirique nous a

également appris que les *traders* à haute fréquence ont une meilleure capacité pour extraire les signaux du carnet d'ordres et sont capables de prévoir les variations de prix à très court terme (Brogaard *et al.*, 2014, Brogaard *et al.*, 2015 et Biais *et al.*, 2016). Il semble donc que les investisseurs institutionnels doivent faire face à un risque accru de détection de leurs ordres par les *traders* à haute fréquence. Dans ce contexte, les investisseurs institutionnels ont fait part de leurs inquiétudes quant aux coûts de transaction qu'ils doivent désormais payer. Anand *et al.* (2013) constatent effectivement une hausse de 33 % de ces coûts pour les investisseurs institutionnels sur les marchés boursiers américains entre 2005 et 2010.

L'analyse empirique de Van Kervel et Menkveld (2016) confirme cette hypothèse. Leur base de données non publique leur permet de reconstituer chaque jour les ordres primaires (*parent orders*) à partir des ordres secondaires (*child orders*). Ils disposent également d'informations directes sur les transactions réalisées par les *traders* à haute fréquence. Lors de la première heure suivant le passage d'un ordre institutionnel, ces *traders* à haute fréquence agissent comme teneurs de marché, mais ils prennent ensuite des positions sur plusieurs heures qui augmentent les coûts de transaction pour le *trader* institutionnel. Les *traders* à haute fréquence ne sont pas capables de détecter immédiatement les ordres institutionnels, mais dès qu'ils le font, ils traitent contre ces ordres.

Korajczyk et Murphy (2015) comparent le comportement des *traders* à haute fréquence à celui des teneurs de marché officiels. Ils démontrent que les *traders* à haute fréquence apportent, en moyenne, beaucoup plus de liquidité sur les ordres primaires des institutionnels que les teneurs de marché implicites, endogènes. Pour les ordres des institutionnels les plus importants, les *traders* à haute fréquence offrent toutefois moins de liquidité, tandis que les teneurs de marché officiels accroissent leur apport de liquidité.

Conclusion et implications pratiques

La négociation électronique, la fragmentation des marchés, les améliorations technologiques et les changements réglementaires ont créé de nouveaux entrants sur les marchés boursiers : les *traders* à haute fréquence. Il est également important de noter que les résultats de Pagnota et Philippon (2015) concordent avec les réglementations qui incitent à une augmentation de la concurrence et de la fragmentation (par exemple, la MiFID, Reg. ATS et Reg. NMS).

Lorsqu'on observe l'impact du THF sur la qualité du marché, on constate une meilleure découverte des prix et une plus grande liquidité du marché. Les résultats sont plus contrastés en ce qui concerne les externalités négatives telles que la sélection adverse et la course à l'investissement. La nature opaque des sociétés du THF et de leurs algorithmes a conduit les régulateurs à proposer des ajustements de la microstructure du marché afin de ralentir les plates-formes de négociation (durée de vie minimum des ordres, enchères périodiques, taxe). Biais *et al.* ont étudié trois régulations possibles : l'interdiction du THF, la coexistence de marchés à haute et à basse fréquence et une taxe pigouvienne sur la technologie du THF. Seule cette dernière permet un niveau socialement optimal d'investissement dans la technologie à haute vitesse. Dans le cadre de leur modèle, Aït-Sahalia et Saglam (2014) analysent également trois réglementations s'appliquant au THF : une taxe sur les transactions, des temps d'attente minimum avant de pouvoir annuler un ordre et une taxe sur les annulations des ordres. La première mesure n'améliore pas l'offre de liquidité, tandis que les deux autres l'améliorent en périodes de faible volatilité, mais la dégradent lorsque la volatilité est élevée.

Les régulateurs cherchent également à reconstituer la séquence des événements sur l'ensemble des marchés financiers *via* une horloge unique afin de détecter les comportements de *trading* prédateurs ou illégaux. Cependant, comme la vitesse des installations de *trading* haute fréquence a presque atteint les limites physiques de la vitesse de la lumière, il n'est simplement pas possible de séquencer précisément des transactions si rapides. Sur les échelles de temps les plus infimes, les événements rapides qui se produisent sur des places géographiquement dispersées ne se succèdent pas de façon claire et sans ambiguïté. Au lieu d'essayer de mettre en œuvre des ralentisseurs, les régulateurs devraient peut-être envisager au contraire d'accélérer l'accès aux plates-formes de négociation afin de protéger les ordres de grande taille des investisseurs institutionnels pour éviter la détection de ces ordres par les *traders* à haute fréquence.

Enfin, tandis que les chercheurs et les régulateurs s'interrogent sur l'impact de la colocation et sur la mise en œuvre d'une horloge unique, plusieurs sociétés de courtage cherchent à bénéficier d'un nouvel avantage dans les négociations grâce à l'espionnage (*snooping*) de haute technologie. C'est ainsi que Genscape, Remote Sensing Metrics LLC ou DigitalGlobe sont à l'avant-garde d'un secteur en pleine croissance qui utilise une technologie sophistiquée de surveillance et de traitement des données afin de fournir aux *traders* des informations non publiques. Leurs outils sont constitués d'un réseau privé breveté de moniteurs placés sur le terrain, d'un suivi du fret maritime, de radars infrarouges, de moniteurs à fréquence électromagnétique, de photographies aériennes à haute résolution et d'images de satellites. Ils fournissent ces données *via* des flux directs branchés sur les systèmes de négociation des intermédiaires financiers. Les clients de Genscape comptent des banques comme Goldman Sachs Group Inc., JPMorgan Chase & Co et Deutsche Bank AG, des *hedge funds* comme Citadel LLC et d'importantes sociétés de courtage comme Trafigura Beheer BV.

Bibliographie

Aït-Sahalia (Y.) et Saglam (M.) (2014)
« High frequency traders: taking advantage of speed », *mimeo*.

Anand (A.), Irvine (P.), Puckett (A.) et Venkataraman (K.) (2012)
« Performance of institutional trading desks: an analysis of persistence in trading costs », *Review of Financial Studies*, vol. 25, p 557-598.

Biais (B.), Declerck (F.) et Moinas (S.) (2016)
« Who supplies liquidity, how and When? », *mimeo*.

Biais (B.) et Foucault (T.) (2014)
« High-frequency trading and market quality », *Bankers, Markets and Investors*, vol. 128, p. 5-19.

Biais (B.), Foucault (T.) et Moinas (S.) (2015)
« Equilibrium fast trading », *Journal of Financial Economics*, vol. 116, p. 292-313.

Boehmer (E.), Li (D.) et Saar (G.) (2015)
« Correlated high-frequency trading », *mimeo*.

Bongaerts (D.) , Kong (L.) et Van Achter (M.) (2016)
« Trading speed competition: can the arms race go too far? », *mimeo*.

Brogaard (J.), Hagströmer (B.), Nordén (L.) et Riordan (R.) (2016)
« Trading fast and slow: colocalisation and liquidity », *Review of Financial Studies*, à paraître.

Brogaard (J.), Hendershott (T.) et Riordan (R.) (2015)
« Price discovery without trading: evidence from limit orders », *mimeo*.

Brogaard (J.), Hendershott (T.) et Riordan (R.) (2014)
« High frequency trading and price discovery », *Review of Financial Studies*, vol. 27, p. 2267-2306.

Declerck (F.) et Lescourret (L.) (2015)
« Dark pools et *trading* haute-fréquence : une évolution utile ? » , *Revue d'Économie Financière*, vol. 120, p. 113-125.

Dugast (J.) et Foucault (T.) (2016)
« Data abundance and asset price informativeness », *mimeo*.

Foucault (T.), Hombert (J.) et Rosu (I.) (2016)
« News trading and speed », *Journal of Finance*, vol. 71, p. 335-382.

Grossman (S.) et Stiglitz (J.) (1980)
« On the impossibility of informationally efficient markets », *American Economic Review*, vol. 70, p. 393-408.

Hasbrouck (J.) et Saar (G.) (2013)
« Low-latency trading », *Journal of Financial Markets*, vol. 16, p. 646-679.

Hendershott (T.), Jones (M.) et Menkveld (A.) (2011)
« Does algorithmic trading improve liquidity? », *Journal of Finance*, vol. 66, p. 1-33.

Korajczyk (R. A.) et Murphy (D.) (2015)
« High-frequency market making to large institutional trades », *mimeo*.

Laumonier (A.) (2014)
6/5, Zones Sensibles Éditions.

Menkveld (A. J.) et Zoican (M. A.) (2015)
« Need for speed? Exchange latency and liquidity », *mimeo*.

Pagnotta (E.) et Philippon (T.) (2015)
« Competing on speed », *mimeo*.

Van Kervel (V.) et Menkveld (A.) (2016)
« High-frequency trading around large institutional orders », *mimeo*.

Verrechia (R.E.) (1982)
« Information acquisition in a noisy rational expectations economy », *Econometrica*, vol 50, p. 1415-1430.

Weller (B.) (2016)
« Efficient prices at any cost: does algorithmic trading deter information acquisition? », *mimeo*.

GLOSSAIRE

Advanced persistent threat (APT)
Adversaire possédant un degré élevé d'expertise ainsi que d'importantes ressources pour créer des opportunités qui lui permettront d'atteindre ses objectifs par de multiples vecteurs d'attaque (cyber-attaque, attaque physique et fraude). Ces objectifs consistent en général à établir et à développer un ancrage au sein de l'infrastructure des technologies de l'information des organisations visées, en vue d'extraire des informations, de nuire aux aspects critiques d'une mission, d'un programme ou d'une organisation, ou de se positionner de manière à réaliser ces objectifs dans le futur.

Algorithmes ou *trading* algorithmique
Le *trading* algorithmique est le processus qui consiste à utiliser des ordinateurs programmés pour suivre un ensemble défini d'instructions (le plus souvent sur la base de la date et de l'heure, du prix, de la quantité ou d'un modèle mathématique). Les algorithmes servent souvent à passer des ordres de vente et d'achat lorsque les conditions définies sont réunies. Le *trading* algorithmique revêt un caractère systématique dans la mesure où il ne tient pas compte de l'influence des émotions humaines sur les activités de négociation.

Analyse des coûts de transaction
L'analyse des coûts de transaction est essentielle : elle consiste en une évaluation de l'écart entre deux prix possibles, la différence entre ces deux prix étant souvent appelée *slippage*. Plus particulièrement, l'analyse des coûts de transaction se rapporte au décalage lié à l'exécution (*implementation shortfall*), qui détermine la somme des coûts d'exécution et des coûts d'opportunité, encourus en cas d'évolution défavorable du marché entre le moment de la décision d'effectuer la transaction et l'exécution de l'ordre. Le programme d'analyse des coûts de transaction est conçu pour mesurer les performances, en indiquant aux gérants d'investissements s'ils payent des coûts de transaction trop élevés sur les marchés mondiaux à revenu fixe (relativement nouveau pour les revenus fixes). On rencontrait habituellement les analyses des coûts de transaction pour les actions, où elles permettaient de fournir aux clients un suivi trimestriel de leur processus de négociation en cours.

Big data
Les technologies du *big data* désignent une nouvelle génération de technologies et d'architectures conçues pour extraire une valeur économique de volumes très importants de données très variées.

Bitcoin
Le bitcoin est une monnaie numérique, décentralisée et partiellement anonyme, qui n'est garantie ni par l'État ni par aucune autre entité juridique, et qui n'est convertible ni en or ni en aucune autre matière première. Elle s'appuie sur le réseau *peer-to-peer* et sur la cryptographie pour préserver son intégrité, et a été évoquée pour la première fois en 2008 dans un document rédigé par Satoshi Nakamoto (pseudonyme).

Carnet central d'ordres avec limite
Système centralisé contenant les ordres sur titres avec limite provenant des spécialistes et des teneurs de marché. Ce système consolide les ordres avec limite de façon centralisée et comble l'absence de système national. Un *hard* CLOB exécute les ordres immédiatement ; un *soft* CLOB fournit des données qui facilitent la négociation mais sans exécution automatique des ordres.

Chaîne de blocs (*blockchain*)
Registre (livre comptable) de l'ensemble des opérations, regroupées en blocs et réalisées avec un dispositif (décentralisé) de monnaie virtuelle.

« *Dark* » *trading*
Le *dark trading* ou les *darks pools* (*pools* de liquidité opaques) sont des plates-formes de négociation électroniques privées opérant hors des marchés organisés publics. Elles ne publient pas immédiatement de cours acheteurs et vendeurs ni de prix des transactions. Elles permettent aux investisseurs institutionnels d'acheter et de vendre de gros blocs de titres de façon anonyme. Cela protège la confidentialité d'un placement et réduit l'impact sur le marché ainsi que les fuites d'informations.

De gré à gré
L'appellation « de gré à gré » peut être utilisée pour désigner les titres de créance qui sont négociés *via* un réseau de *broker-dealers* par opposition à une plate-forme multilatérale de négociation ou à un marché centralisé.

Demande de flux continu (RFS)
La demande de flux continu correspond à des prix mis à jour en continu, qui peuvent être fermes ou sur lesquels le courtier a le droit de « dernier regard » avant d'accepter de réaliser la transaction. Le modèle de demande de flux continu peut fonctionner en utilisant soit la voix (téléphone), soit une connexion électronique entre les parties à la transaction.

Demande de prix (RFQ)
Le modèle RFQ (demande de prix d'un client au courtier) a été la méthode de négociation standard sur le marché obligataire : le client demande un prix au courtier et peut ensuite choisir d'effectuer la transaction ou pas. Effectuées à l'origine à la voix, les demandes de prix se font aujourd'hui principalement *via* des plates-formes multi-courtiers.

Dépositaire central de titres
Un dépositaire central de titres est une entité qui : (i) permet le traitement et le règlement-livraison des transactions sur titres par inscription en compte ; (ii) fournit des services de conservation (la gestion des événements sur titres et des remboursements, par exemple) ; et (iii) contribue activement à maintenir l'intégrité des titres émis. Les titres peuvent être matérialisés (mais conservés chez le dépositaire) ou dématérialisés (c'est-à-dire qu'ils n'existent que sous forme d'enregistrements électroniques).

Direct Market Access (DMA)
Service offert par certains courtiers permettant à des investisseurs privés professionnels d'effectuer des ordres d'achat et de vente directement auprès des places boursières.

Faux positifs
Ce terme est utilisé dans la directive MiFID 2 pour désigner la classification à tort d'une obligation comme liquide alors qu'elle ne l'est pas (détermination de la liquidité des obligations). Selon la directive, les conséquences involontaires peuvent être les suivantes : l'impossibilité de liquider une position d'achat ou de vente, ou un prix excessivement désavantageux qui altère la performance de l'opération. Il y aura un changement de comportement aussi bien côté achat que côté vente en raison des faux positifs de liquidité perçus.

Fintechs
Les fintechs, contraction de « technologie financière », désignent les acteurs spécialisés dans la mise en œuvre d'innovations numériques et technologiques pour la sphère financière, qu'il s'agisse de la prestation de services extérieurs à des clients particuliers (nouvelles solutions de paiement, financement participatif, etc.) ou de processus internes (*big data, blockchain*).

Fuites de données
Les fuites de données se définissent comme la distribution accidentelle ou involontaire de données privées ou sensibles au profit d'une entité non autorisée. Les données sensibles des entreprises et des organisations recouvrent la propriété intellectuelle, les informations financières, les informations sur les patients, les données relatives aux cartes de crédit personnelles ainsi que d'autres informations dépendant de l'activité et du secteur.

GAFA
Abréviation de Google, Apple, Facebook, Amazon.

Informatique en nuage (*cloud-computing*)
Modèle permettant un accès réseau sur demande à un bassin partagé de ressources informatiques configurables (par exemple réseaux, serveurs, stockage, applications et services) qui peut rapidement être activé ou désactivé moyennant un effort minimal en matière de gestion ou d'interaction avec le fournisseur de service.

Internalisateur systématique
Internalisateur systématique est un terme de la première MiFID, utilisé pour les actions. Il a un périmètre plus large dans la MiFID 2 : il désigne une entreprise d'investissement qui, de façon organisée, fréquente, systématique et significative, agit lors de l'exécution des ordres des clients en se portant contrepartie pour compte propre en dehors d'un marché réglementé, d'une plate-forme multilatérale de négociation ou d'un système organisé de négociation. Les mesures de niveau 2 de la MiFID 2 définiront clairement les seuils pour devenir internalisateur systématique, en fonction des volumes de transactions par rapport aux qualificatifs « fréquente et systématique » et « significative ». De plus, la réglementation fournit des définitions quantifiables pour le caractère « fréquent et systématique » et « significatif ».

« Lit » trading
Le *lit trading* est effectivement l'opposé du *dark trading*. Contrairement au *dark trading*, où les prix auxquels les intervenants souhaitent négocier ne sont pas affichés, les plates-formes ou pratiques de *lit trading* affichent les ordres acheteurs et vendeurs sur les différentes obligations, d'où la transparence de ce type de négociation.

Marché réglementé (RM)
Un marché réglementé est un terme utilisé dans la MiFID pour désigner un opérateur d'un marché réglementé (opérateur de marché) qui assure la

rencontre dans le système de multiples intérêts acheteurs et vendeurs exprimés par des tiers pour les instruments financiers, conformément à des règles non discrétionnaires, d'une manière qui aboutit à la conclusion d'un contrat.

MiFID 2
L'objectif de la directive MiFID 2 est d'accroître la transparence, l'efficience et la sécurité des marchés en soumettant la majorité des produits autres que des actions ou instrument assimilés à un régime réglementaire robuste et en recentrant sur des plates-formes réglementées une part importante des négociations de gré à gré. Avec la MiFID 2, le champ de transparence qui recouvre habituellement les marchés d'actions sera en grande partie étendu aux négociations sur obligations. L'Europe va plus loin que la presque totalité des autres pays dans le monde, y compris les États-Unis, s'agissant des règles de transparence relatives aux opérations sur obligations. Le régime réglementaire de la directive prévoit des obligations de transparence pré-négociation et post-négociation. Cela aura un impact significatif sur la structure des marchés obligataires. Les obligations de transparence pré- et post-négociation seront calibrées pour différents types de structures de négociation sur les marchés obligataires. En outre, la transparence pré-négociation pour les instruments obligataires sera également calibrée pour les systèmes de négociation vocaux.

Monnaie virtuelle
Une monnaie virtuelle est un type de monnaie numérique, non réglementée, qui est émise et généralement contrôlée par ses développeurs, et utilisée et acceptée par les membres d'une communauté virtuelle déterminée.

Name give-up
Le courtage en *name give-up* identifie et présente des contreparties ayant fait part de leur volonté de négocier l'une avec l'autre et qui ont un crédit ou une compensation réciproque, et/ou lorsque deux ordres ou plus émanant de clients s'apparient. Ces contreparties passent un contrat directement l'une avec l'autre et/ou avec la chambre de compensation concernée à qui incombe l'obligation de règlement, et supportent elles-mêmes le risque de crédit de contrepartie. Le *broker-dealer* a pour objectif d'automatiser le processus d'échanges de messages lorsque cela est possible.

Négociation « s'adressant à tous »
Les plates-formes de négociation s'adressant à tous réunissent plusieurs parties côté achat et côté vente afin de déterminer les prix en affichant les ordres fermes qu'elles passent les unes auprès des autres, et pas seulement de courtier à client (*dealer-to-customer*) ou de courtier à courtier (*dealer-to-dealer*).

Paiements mobiles de personne à personne
Technologie en ligne permettant aux clients de transférer des fonds de leur compte bancaire ou de leur carte de crédit vers un autre compte de particulier *via* internet ou un téléphone portable.

***Peer to peer* (P2P)**
Un réseau *peer-to-peer* est un réseau informatique dépourvu de serveur central comme point de liaison, dans lequel chaque ordinateur joue le rôle à la fois de client et de serveur, ce qui lui permet d'échanger des données et des services avec chacun des autres ordinateurs au sein du réseau.

Plate-forme de négociation anonyme
Plate-forme sur laquelle les ordres d'achat et de vente sont visibles sur le marché mais ne révèlent ni l'identité de l'acheteur ni celle du vendeur. La négociation anonyme permet aux intervenants de marché d'effectuer des opérations en n'étant pas soumis à la surveillance et à la spéculation du marché. L'anonymat est un avantage pour les intervenants de marché qui souhaitent réaliser d'importantes opérations sans attirer l'attention, celle-ci pouvant influer sur les prix.

Protocole FIX
Terme informatique de *trading* électronique désignant la norme de messagerie internationale qui permet de réduire les coûts de connectivité des liaisons entre sociétés acheteuses et sociétés vendeuses ainsi qu'une réduction des coûts liée à l'intégration efficiente des processus internes et des opérations externes.

Registre distribué (*distributed ledger*)
Registre ouvert et décentralisé de l'ensemble des opérations réalisées par un système de paiement, par exemple. Technologie ouverte, transparente et *peer-to-peer*, elle perturbe les pratiques traditionnelles d'opérations, fondées sur des données centralisées et privées. Le registre distribué est une composante de la chaîne de blocs (*blockchain*), technologie sur laquelle s'appuient la plupart des monnaies virtuelles, notamment le bitcoin.

Réseaux d'information
Ils fournissent aux intervenants de marché une couche de technologie permettant d'avoir un aperçu global et rapide de la liquidité disponible sur l'ensemble des marchés. Les systèmes internes côté achat et côté vente doivent être dotés d'un degré élevé de technologie.

Système de gestion des exécutions (EMS)
Les systèmes de gestion des exécutions sont des applications informatiques utilisées par les investisseurs institutionnels pour afficher les données de marché et fournir un accès continu aux destinations de négociation aux fins d'exécution des ordres. Ils contiennent souvent des algorithmes fournis par les courtiers et des algorithmes indépendants, des données sur les marchés mondiaux et une technologie capable d'aider à prévoir certaines conditions de marché. Une des caractéristiques importantes d'un EMS est sa capacité à gérer des ordres sur plusieurs destinations de négociation, telles que les MTF, les *broker-dealers*, les *crossing networks* et les réseaux d'information électronique.

Système de gestion des ordres (SGO)
Un système de gestion des ordres est un système électronique s'appuyant sur un logiciel qui facilite et gère l'exécution des ordres sur titres, généralement par le biais d'un protocole FIX. Les systèmes de gestion des ordres sont utilisés à la fois côté achat et côté vente, même si les fonctionnalités offertes diffèrent légèrement entre les deux. Du côté achat, les systèmes de gestion des ordres viennent en appui de la gestion de portefeuilles en transformant les modifications envisagées pour l'allocation des actifs en ordres négociables pour le volet achat. Les SGO permettent aux sociétés d'entrer des ordres dans le système pour les router vers des destinations préétablies. Ils permettent aux sociétés de modifier, d'annuler ou d'actualiser les ordres. Lorsqu'un ordre est exécuté à la vente, le volet vente du SGO doit alors mettre son statut à jour et envoyer un rapport d'exécution à la société à l'origine de l'ordre. Un SGO doit également permettre aux sociétés d'accéder aux informations relatives aux ordres entrés dans le système, y compris les détails concernant tous les ordres en cours et les ordres exécutés antérieurement.

Système de négociation multilatérale (MTF)
Système multilatéral, exploité par une entreprise d'investissement ou un opérateur de marché, qui assure la rencontre entre de multiples intérêts acheteurs et vendeurs exprimés par des tiers sur des instruments financiers – au sein du système et conformément à des règles non discrétionnaires – de manière à aboutir à la conclusion d'un contrat. Le terme « règles non discrétionnaires » signifie que l'entreprise d'investissement qui exploite un système de ce type n'a pas de pouvoir discrétionnaire s'agissant de l'interaction des intérêts.

Système organisé de négociation (OTF)
Un système organisé de négociation, terme utilisé dans la directive MiFID 2, est un système multilatéral qui n'est pas un marché réglementé (RM) ou une plate-forme multilatérale de négociation (MTF) et dans lequel de multiples intérêts acheteurs et vendeurs exprimés par des tiers pour des obligations peuvent interagir dans le système d'une manière qui aboutisse à la conclusion d'un contrat conformément aux dispositions du Titre II de la MiFID 2. À la différence des marchés réglementés et des plates-formes multilatérales de négociation, les opérateurs des systèmes organisés de négociation peuvent choisir la façon d'exécuter les ordres, sous réserve des obligations de transparence pré-négociation et de meilleure exécution.

Trading algorithmique
Utilisation d'algorithmes informatiques permettant, de façon automatique, de prendre certaines décisions, de soumettre des ordres et de les gérer par la suite.

Trading haute fréquence
Sous-ensemble du *trading* électronique dans lequel un grand nombre d'ordres de petite taille sont envoyés au marché à grande vitesse, avec des délais d'exécution aller-retour généralement de l'ordre de la milliseconde.

ÉTUDES PUBLIÉES

Vous trouverez ci-dessous la liste de l'ensemble des articles publiés dans la *Revue de stabilité financière* depuis la première parution. Ces études sont disponibles sur le site internet de la Banque de France (*www.banque-france.fr*).

Novembre 2002

Eurosystème, zone euro et stabilité financière

Les dérivés de crédit, nouvelle source d'instabilité financière ?

Quel crédit accorder aux *spreads* de crédit ?

Le développement des clauses contingentes :
état des lieux et implications pour la stabilité financière

Infrastructures post-marché et stabilité financière

Le système CLS : une réponse au risque de règlement dans les opérations de change

Codes et standards internationaux :
enjeux et priorités pour la stabilité financière

Juin 2003

La volatilité boursière : des constats empiriques aux difficultés d'interprétation

Vers un « continuum de marché » ? Modèles structurels et interactions
entre marchés de crédit et d'actions

L'évolution des facteurs influant sur le comportement des gestionnaires
institutionnels : incidence potentielle sur les marchés de capitaux

Une revue analytique des instruments de transfert du risque de crédit

Normalisation comptable internationale et stabilisation financière

Vers un Code de bonne conduite volontaire pour restructurer la dette souveraine

Novembre 2003

Stabilité financière et nouvel accord de Bâle

Les fluctuations des prix d'actifs font-elles peser un risque
sur la croissance dans les grands pays industrialisés ?

Interactions entre cycles réels, cycles boursiers et taux d'intérêt : faits stylisés

Les défis de la gestion alternative

La protection des systèmes nets de paiement et de titres à règlement différé :
les exemples du SIT et de Relit

Vulnérabilités et surveillance du système financier international

Juin 2004

L'incidence des notations sur les dynamiques de marchés :
une revue de la littérature

Résultats de l'enquête de place française
sur les instruments de transfert de risque de crédit

Techniques de marché des dérivés de crédit : les *swaps* de défaut

Interdépendance des marchés d'actions : analyse de la relation
entre les indices boursiers américain et européens

Goodwill, structures de bilan et normes comptables

Novembre 2004

Bilan des « *stress tests* » menés sur le système bancaire français

Assurance et stabilité financière

La surveillance des moyens de paiement scripturaux : objectifs et modalités de mise en oeuvre

La robustesse des infrastructures post-marché et des systèmes de paiement

Gestion du risque de crédit et stabilité financière

Juin 2005

Le marché des CDO : modalités de fonctionnement et implications en termes de stabilité financière

Soutenabilité de la dette publique et crises des pays émergents : présentation des concepts et des instruments de diagnostic

Le risque de taux d'intérêt dans le système bancaire français

La gestion du risque de taux par les sociétés d'assurance-vie et les fonds de pension

Analyse par simulations de l'impact d'une défaillance technique d'un participant à un système de paiement

Novembre 2005

Surveillance prudentielle et évolution des normes comptables : un enjeu de stabilité financière

Capital réglementaire et capital économique

Portée et limites des VaR publiées par les grandes institutions financières

L'impact des chocs boursiers sur le crédit en France depuis le milieu des années quatre-vingt-dix

(Re) structuration des dettes souveraines. Où en est-on ?

Mai 2006

Mieux appréhender les risques du portefeuille de négociation

La liquidité de marché et sa prise en compte dans la gestion des risques

Productivité et prix des actifs boursiers

Les capitaux propres des entreprises et la stabilité financière : l'apport d'une approche par « les capitaux propres nets en risque ou *net worth at risk* »

Les progrès de l'intégration monétaire et financière en Asie

Les implications de la globalisation pour la stabilité financière

Décembre 2006

Les matières premières : une classe d'actifs à part entière ?

Les pays émergents forment-ils toujours une classe d'actifs homogène ?

Flux de capitaux et dynamisme du crédit dans les pays émergents

Les indicateurs d'aversion pour le risque peuvent-ils anticiper les crises financières ?

Liquidité bancaire et stabilité financière

Microstructure des marchés monétaires et financiers

Le dispositif de Bâle II : rôle et mise en œuvre du pilier 2

Avril 2007

Hedge funds

Hedge funds, transfert du risque de crédit et stabilité financière

Évolution et régulation des *hedge funds*

Quelle forme de régulation pour les *hedge funds* ?

Hedge funds et stabilité financière

Hedge funds et risque systémique

Stratégies de réplication des *hedge funds* : conséquences pour les investisseurs et les régulateurs

Hedge funds et *prime broker dealers* : éléments de proposition en matière de « bonnes pratiques »

Exigences de transparence et *hedge funds*

Risques et rendement des activités bancaires liées aux *hedge funds*

La supervision indirecte des *hedge funds*

Quelles sont les principales questions liées aux *hedge funds* ?

La surveillance des *hedge funds* : un point de vue de stabilité financière

Le monde des *hedge funds* : préjugés et réalité. La contribution de l'AMF au débat sur les stratégies de gestion alternative

Conditions financières, gestion alternative et risques politiques : tenter de comprendre notre époque

Les *hedge funds* sur les marchés émergents

Les fonds de *hedge funds* : origine, rôle et perspectives

Hedge funds : un point de vue de banque centrale

Février 2008

Liquidité

Liquidité et contagion financière

Les chaises musicales : un commentaire sur la crise du crédit

Liquidité de marché et stabilité financière

Dix questions à propos de la crise des prêts *subprime*

Qu'est-il advenu de la dispersion des risques ?

La gestion du risque de liquidité

La réglementation de la liquidité et le prêteur en dernier ressort

Déficits de liquidité : fondements théoriques

La liquidité sur les marchés mondiaux

L'impact de la directive MIF sur la liquidité des marchés financiers

Liquidité de marché et liquidité bancaire : interdépendances, vulnérabilités et communication financière

Actifs liquides, contraintes de liquidité et déséquilibres mondiaux

L'innovation financière et la frontière de la liquidité

Liquidité des marchés financiers et le prêteur en dernier ressort

Évolutions récentes de la liquidité intrajournalière dans les systèmes de paiement et de règlement

Octobre 2008

Valorisation et stabilité financière

Les défis de la valorisation dans un environnement changeant

La valorisation aux prix de marché convient-elle aux institutions financières ?

Définir un cadre adapté au fonctionnement des marchés de capitaux modernes – Les leçons de la crise récente

Révision des pratiques de valorisation sur l'ensemble du cycle économique : davantage de symétrie est nécessaire

Valorisation et fondamentaux

La prise en compte des événements extrêmes pour la valorisation d'options européennes

Juste valeur et stabilité financière : enjeux de marché et dynamiques stratégiques

Comment réagir face aux bulles des prix d'actifs ?

Réglementation, valorisation et liquidité systémique

Comptabilisation en juste valeur et stabilité financière

Procyclicité des systèmes financiers : est-il nécessaire de modifier les règles comptables et la réglementation actuelles ?

Valorisation dans l'assurance et crise financière

Instiller de la transparence dans l'information financière : vers l'amélioration du cadre comptable après la crise du crédit

Améliorer la comptabilisation en juste valeur

Septembre 2009

Le futur de la régulation financière

Quelle régulation financière pour l'après-crise ?

Le système bancaire parallèle : implications pour la régulation financière

Gérer la transition vers un système financier plus sûr

Réforme de l'architecture financière globale : un nouveau contrat social entre la société et la finance

L'approche macroprudentielle appliquée à la régulation et à la surveillance financières

Minimiser l'impact des crises financières à venir : six points incontournables pour réformer la régulation

Réflexions sur l'efficacité de la régulation financière

Le traitement des banques en difficulté

Credit default swaps et stabilité financière : quels risques ? Quels enjeux pour les régulateurs ?

L'avenir de la régulation financière

L'avenir de la régulation financière : échange de vues

Émergence d'une ébauche de régulation financière : défis et dynamique

Régulation-supervision : quelles perspectives pour l'après-crise ?

Au-delà de la crise : la réponse stratégique du Comité de Bâle

Juillet 2010

Dérivés – Innovation financière et stabilité

Repenser les marchés des dérivés de gré à gré pour garantir la stabilité financière

Les CDS : quels avantages et coûts collectifs ?

Fiat lux – Un jour nouveau sur les marchés de produits dérivés

Dette publique et interactions avec les marchés dérivés : le cas européen

Les produits dérivés : le point de vue d'un assureur

Credit default swaps et stabilité financière

Les *credit default swaps* – Innovation financière ou dysfonctionnement financier ?

Faut-il interdire la spéculation sur les marchés des obligations souveraines ?

Les marchés de produits dérivés de gré à gré en Inde : questions et perspectives

Produits dérivés de gré à gré et compensation centrale : toutes les transactions peuvent-elles faire l'objet d'une compensation ?

La finance du XXI^{e} siècle ne peut faire l'économie d'une bonne régulation des marchés dérivés de gré à gré

Risque systémique : une approche alternative

Produits dérivés OTC : défis pour la stabilité financière et réponses des autorités

Sous-collatéralisation et « réhypothécation » sur les marchés des produits dérivés de gré à gré

Silos et silences : les difficultés à déceler les problèmes liés aux instruments de crédit structurés et les leçons pour l'avenir

Réduire le risque systémique sur les marchés de dérivés de gré à gré (OTC)

Credit default swaps : Quels sont les risques et défis en matière de stabilité financière ?

Structure des marchés de dérivés OTC et profils de crédit des banques de financement et d'investissement

Contreparties centrales et stabilité financière : quelles leçons tirer de la théorie des réseaux et du risque endogène ?

Marché des CDS et marché obligataire : qui dirige l'autre ?

Risque de concentration et nombre optimal de contreparties centrales pour un actif unique

Février 2011

Déséquilibres mondiaux et stabilité financière

Déséquilibres mondiaux : le point de vue de l'Agence monétaire saoudienne

Les flux internationaux de capitaux et le repli vers les actifs sûrs aux États-Unis, 2003-2007

La stabilité financière confrontée aux afflux massifs de capitaux : le point de vue d'un marché émergent

Les déséquilibres mondiaux, le système monétaire international et la stabilité financière

Déséquilibres mondiaux : le point de vue de la Banque du Mexique

Complémentarité et coordination des politiques macroéconomiques et financières pour remédier aux déséquilibres internes et externes

Déséquilibres mondiaux : un problème commun à résoudre pour les économies avancées et les économies de marché émergentes

Équilibre mondial et stabilité financière : des objectifs indissociables pour un système économique mondial résistant

Déséquilibres mondiaux : le point de vue de la Banque d'Angleterre

Déséquilibres mondiaux et pays en développement

Les déséquilibres mondiaux : un point de vue sud-africain

La nature volatile des flux de capitaux : l'expérience indonésienne et les nouveaux rôles du FMI

Déséquilibres mondiaux et stabilité financière

Les déséquilibres mondiaux et les déséquilibres des comptes de transactions courantes

Les déséquilibres mondiaux vus au travers du prisme de l'épargne et de l'investissement

Déséquilibres mondiaux : le point de vue de la Banque de réserve d'Inde

Les défis intellectuels qui se posent à l'analyse de la stabilité financière à l'ère de la surveillance macroprudentielle

Renouer avec la stabilité et la croissance après la crise

La règle de Tinbergen revisitée : le maintien de la stabilité financière à l'aide d'outils macroprudentiels

Du taux d'épargne

Avril 2012

Dette publique, politique monétaire et stabilité financière

L'activité de banque centrale dans un contexte de dette publique élevée

Perspectives budgétaires et risques pour la viabilité budgétaire

Lorsque la dette souveraine des économies occidentales devient risquée

Le retour de la répression financière

L'histoire de deux excès : le lien entre risques de crédit du secteur financier et des emprunteurs souverains

Les banques, l'aléa moral et la dette publique

Solvabilité des emprunteurs souverains et stabilité financière : une perspective internationale

Stabilité, croissance et réforme de la réglementation

Le risque souverain est-il correctement traité par la réglementation financière ?

Contagion et crise de la dette européenne

Politique monétaire et dette publique

La clé d'un assainissement budgétaire réussi : coopération ou confrontation avec la politique monétaire ?

Domination monétaire dans la zone euro et défis budgétaires : une perspective théorique

Indépendance de la banque centrale et défaut souverain

La crise de la dette souveraine et la politique monétaire

Soutenabilité de la dette publique : condition préalable à la stabilité du système financier et des prix

L'importance de la confiance dans les efforts de stabilisation macroéconomique

Quelle politique pour la dette souveraine ?

Une relation risquée : l'interdépendance entre dette bancaire et dette souveraine et la stabilité financière dans la zone euro

Restaurer la croissance et l'optimisme pour une nouvelle ère budgétaire

Les lacunes de la structure institutionnelle de la zone euro

La crise de l'euro : quelques éléments de réflexion sur la réforme institutionnelle

Avril 2013

Les produits dérivés de gré à gré : nouvelles règles, nouveaux acteurs, nouveaux risques

Avril 2014

Politiques macroprudentielles : mise en œuvre et interactions

De la théorie à la mise en œuvre de la politique macroprudentielle

Cinq questions et six réponses sur la politique macroprudentielle

La gouvernance de la politique macroprudentielle

Du « *tapering* » à une politique préventive

Les problèmes d'action collective dans la politique macroprudentielle et la nécessité d'une coordination internationale

Une perspective macroprudentielle pour la réglementation des grandes institutions financières

L'incidence de la politique macroprudentielle sur l'intégration financière

La politique macroprudentielle européenne de sa gestation aux premiers balbutiements

La politique macroprudentielle en France : exigences et mise en œuvre

La mise en œuvre des politiques macroprudentielles : l'approche suisse

Les effets de la politique macroprudentielle sur les risques du marché de l'immobilier résidentiel : le cas de Hong Kong

La politique macroprudentielle en Corée – Principales mesures et approches

Cadre pour la conduite de la politique macroprudentielle en Inde : expériences et perspectives

Les enseignements de l'histoire de la politique macroprudentielle aux États-Unis

Politiques prudentielles et instruments quantitatifs : une perspective historique européenne

La politique macroprudentielle au-delà de la réglementation bancaire

Deux principes pour la réglementation macroprudentielle

Justification et évaluation de l'efficacité des instruments de fonds propres macroprudentiels

Marché immobilier : l'impact des mesures macroprudentielles en France

Trois critiques de la régulation prudentielle des banques

La politique macroprudentielle et les cycles d'offre de crédit

Interactions entre politiques monétaire et macroprudentielle

Avril 2015

Financement de l'économie : de nouveaux canaux pour la croissance

L'après-crise et le financement de l'économie : enjeux et défis pour la stabilité financière

Achever l'intégration du marché des capitaux

Quelles sont les conséquences du nouveau visage de l'intermédiation financière internationale pour les économies de marché émergentes ?

Quels financements pour soutenir la croissance des petites et moyennes entreprises et des entreprises de taille intermédiaire et préparer la compétitivité de demain ?

La relance de la titrisation

Soutenir une croissance durable : le rôle des systèmes bancaires sûrs et stables

En quoi un ratio de levier complémentaire peut-il améliorer la stabilité financière, les activités de prêt traditionnelles et la croissance économique ?

Comment faciliter l'accès des entreprises européennes au crédit bancaire ?

L'impact du nouveau paradigme réglementaire sur le rôle des banques dans le financement de l'économie

Impact de la réglementation financière sur le financement à long terme de l'économie par les banques

Les banques internationales et l'adoption d'un nouveau dispositif réglementaire : effets sur le financement des marchés émergents et des économies en développement

Le coût d'opportunité du collatéral mis en dépôt : réforme des marchés de produits dérivés et activité de prêt des banques

Éditeur
Banque de France
39, rue Croix des Petits-Champs – 75001 Paris

Directeur de la publication
Nathalie AUFAUVRE

Directeur de la rédaction
Ivan ODONNAT

Réalisation
Direction de la Communication

Demandes d'abonnement
Banque de France – 07-1397
Service de la pédagogie économique
9, rue du Colonel Driant – 75049 Paris Cedex 01

Imprimeur
Navis, Paris

Dépôt légal
Avril 2016

Internet
http://www.banque-france.fr/publications/revue-de-la-stabilite-financiere.html