FSR

FINANCIAL STABILITY REVIEW

APRIL 2016

FINANCIAL STABILITY IN THE DIGITAL ERA

20

BANQUE DE FRANCE
EUROSYSTÈME

110–020

Contents

Articles

Introduction

Constructing the possible trinity of innovation, stability and regulation for digital finance
François VILLEROY de GALHAU, *Banque de France* 7

New risks for financial stability

Digital banking and market disruption: a sense of *déjà vu*?
Jean DERMINE, *INSEAD, Singapore* 17

Digital risk: a strategic challenge and a growth opportunity for insurers
Nicolas SCHIMEL, *Aviva France* 25

Systemic risk in payments
Georges PAUGET, *Économie Finance et Stratégie* 37

Financial institutions and cyber crime – Between vulnerability and security
Quentin GAUMER, Stéphane MORTIER and Ali MOUTAIB, *École de guerre économique, Paris* 45

Where are the risks in high frequency trading?
Thierry FOUCAULT, *HEC Paris* 53

Regulation and policies to address these new risks

Making Europe's financial market infrastructure a bulwark of financial stability
Yves MERSCH, *European Central Bank* 71

Beyond technology – Adequate regulation and oversight in the age of fintechs
Andreas R. DOMBRET, *Deutsche Bundesbank* 77

The rise of fintechs and their regulation
Serge DAROLLES, *Université Paris-Dauphine* 85

The migration to online lending and the rise of private regulation of online financial transactions with business customers
G. Philip RUTLEDGE, *Bybel Rutledge LLP and BPP Law School* 93

The digital transformation of the financial sector: some concrete examples

Money and payments in the digital age: innovations and challenges
François VELDE, *Federal Reserve Bank of Chicago* 103

Future evolution of electronic trading in European bond markets
Elizabeth CALLAGHAN, *International Capital Market Association* 113

Emergence of big data: how will it impact the economic model of insurance?
Thierry DEREZ, *Covéa* 123

Big data challenges and opportunities in financial stability monitoring
Mark D. FLOOD, *US Department of the Treasury,* **H. V. JAGADISH,** *University of Michigan* **and Louiqa RASCHID,** *University of Maryland* 129

Implementation of real-time settlement for banks using decentralised ledger technology: policy and legal implications
Karen GIFFORD and Jessie CHENG, *Ripple* 143

High-frequency trading, geography concerns and the curvature of the Earth
Fany DECLERCK, *Toulouse School of Economics* 153

Contents

Glossary 161

Published articles 165

Introduction

Constructing the possible trinity of innovation, stability and regulation for digital finance

François VILLEROY de GALHAU
Governor
Banque de France

Innovation shapes the evolution of the financial system and plays a crucial role in economic development. Yet innovative technologies may also make more questionable contributions, like during the 2008 financial crisis. Given the potentially systemic impact of these innovations, central banks, supervisors and regulators monitor them carefully. They seek to understand the deep-seated changes and new practices that they bring, while identifying and assessing the benefits and risks to the financial system.

In recent years, digital technologies have made massive inroads in the industrial world, in areas ranging from telecommunications to the automotive business and robotics. These technologies are now spreading rapidly to the financial services sector.[1] More and more practical applications are emerging: mobile, contactless and instant payments; account information and payment initiation services; asset management; investment advice; data management and information storage, etc.

In this new digital era, financial innovation's centre of gravity looks to be shifting to new players, some of which lie outside the financial system. Technological innovations in the financial sphere are no longer solely driven by competitive pressures within the financial system itself, but by the arrival of outside firms with the expertise of new technologies. These new entrants are competing with usual players and challenging the methods used to deliver certain financial services.

The digital wave is also being supported by a new range of services, which is less geared towards the sale of innovative products and more centred on customers, offering instant access from anywhere to a vast array of diverse, affordable, integrated services. This paradigm shift, which has placed customers at the centre of concerns, reflects the influence of multiple factors, including:

- growing appetite for digital solutions, which has drastically altered consumption approaches, through the rise of online banking and the use by Internet service providers of data to obtain detailed intelligence about consumers' preferences and profiles;

- the public's clear mistrust of the banking world in the wake of the financial crisis;

- regulatory changes since 2008 aimed at promoting increased standardisation and transparency in financial transactions, which have also encouraged more electronic trading (by introducing recording or central clearing obligations, for example). Tougher regulations have additionally pushed up intermediation costs, opening the way to new entrants;

- the substantial developments in the field of storage and data management. The spread of "open data",[2] which has made it possible to exploit a wide variety of information collected about customers, played a potentially important role in the development of tools to store and process very large volumes of data (big data). In order to manage large-scale data flows, an adequate processing capacity is necessary. By offering an extensive information system that can be activated worldwide, the cloud allows for gains in responsiveness and speed and thus makes it possible to allocate costs to other business segments.

1 *See* Revue d'économie financière, "Innovation, technologie et finance: menaces et opportunités", *No. 120, December 2015.*
2 *The open data movement was initiated by the Public Sector Information (PSI) Directive of 2003 on the re-use of public sector information (Directive 2003/98/EC).*

As a result, an inventive, multi-faceted offering is emerging and reshaping the banking and financial landscape to create an ecosystem comprising a wide range of participants: traditional players such as financial institutions; operating alongside large international digital companies such as Google, Apple, IBM, Microsoft, Amazon and Facebook; telecommunications operators with a broad base of consumers and major capacity to innovate through mobile telephony; as well as the famous fintechs, which are innovative and often small-sized businesses specialising in financial technology.

This transformation of the financial sector, which is bringing non-financial firms into regulated financial activities, is impacting conventional banking models and changing the way the financial system works. The purpose of this article is to clarify different aspects [3] of this change by looking at: (1) how digital innovations are broadening the offer in banking services; (2) potential risks and new challenges to financial stability; (3) possible responses by central banks and financial system regulators and supervisors. We must therefore, dynamically, construct the possible trinity of innovation, stability and regulation.

1| Digital innovations broaden the offer of all banking services to varying degrees

The centre of gravity of the financial innovation process has shifted from the banking sector to new players previously outside the financial system but using digital technologies.

1|1 Payment services

Retail banking is characterised by highly standardised transactions and substantial fixed costs. These structural aspects offer fertile ground for competition from nimble digital firms that are less burdened by their cost structure. Accordingly, the rise of digital innovation in the retail payments sector paved the way for the emergence of a diverse range of low-cost payment solutions against the backdrop of rapid growth in online commerce. Back in 2007, the first European Payment Services Directive (Directive 2007/64/EC, PSD1) created a new category of payment services providers known as "payment institutions" to regulate the terms of this new competition.[4]

By the end of 2015, France had 24 authorised payment institutions, compared with three at end-2010. Although these new participants rely heavily on existing payment instruments issued or managed by banks (chiefly payment cards and credit transfers, plus direct debits to a lesser extent), they are successfully capturing market share at the expense of banking institutions. Overall payment flows processed by service providers authorised as payment institutions have risen to EUR 25 billion in 2014 but nevertheless continue to be dwarfed by the total flows managed by France's CORE retail payments system,[5] which exceeded EUR 5 trillion in 2014.

The digitisation of payment services is also taking more disruptive forms. For example, new providers not covered by the scope of PSD1 are emerging to connect consumers and merchants (third-party payment services providers) or to enable customers to view information on multiple accounts (account information service providers). Virtual currencies, particularly bitcoin, bring a shadow mechanism of money creation into play, even though their growth is still far exceeded by the commentaries and analyses devoted to them. By seeking to rival legal currencies, virtual currencies appear to introduce a major disruption by their ambition to challenge central banks' monopoly on issuance. Yet usage remains very small: daily amounts exchanged are coming in at less than EUR 100 million with fewer than 200,000 transactions, compared with EUR 70 billion in payments with 250 million transactions every day within the European Union.

1|2 Financing services

In the field of corporate financing too, digitisation is opening up opportunities for innovation, which, in a context of more stringent banking rules and lastingly low interest rates, is contributing to the

3 *The present article focuses on the changes in servicing clients and does not directly address the new features proposed by fintechs to banks, in particular for the credit analysis and debtors' scoring.*
4 *The second Electronic Money Directive (2009/110/EC) created a specific legal regime for electronic money institutions in 2009.*
5 *CORE (FR) is the French retail payment system. It is developed and managed by STET, a company owned by France's five largest banks, namely BNP Paribas, BPCE, Crédit Agricole, Banque Fédérative du Crédit Mutuel and Société Générale.*

diversification of supply outside the banking sector. Meanwhile, companies, particularly very small enterprises, small and medium enterprises, and intermediate-sized enterprises, have shown that they need alternative financing sources that are more closely tailored to their requirements. Against this backdrop, crowdfunding platforms have emerged, meeting the need for small amounts of debt or equity and rounding out existing financing approaches. In France, there were 86 crowdfunding platforms in March 2016, comprising 55 intermediaries providing loan-based crowdfunding, 27 crowdfunding advisers[6] and 4 dual-status platforms.[7] Amounts raised doubled in 2015 compared with the previous year, to EUR 297 million, and comprised EUR 197 million in loans, EUR 50 million in securities purchases and EUR 50 million in donations.[8] However, they are still limited with regard to the overall funding needs of firms.[9]

1|3 Investment services

Technological innovations are having a far more material impact on financial market transactions, and particularly on securities trading practices. High frequency trading (HFT) firms have established themselves as key players on equity markets,[10] accounting for 24% of trading volumes on European equity markets. HFT firms have two characteristics that enable them to carry out very large numbers of small trades with short-term investment horizons (often intraday): (i) ultra-fast access – just a few milliseconds – to trading platforms and market information; and (ii) trading algorithms that operate autonomously without human involvement when markets are open. Even though their economic and social benefits are dubious, the rapid development of HFT firms makes use of low entry barriers. These players tend to be non-banks with small or even negligible amounts of capital compared with traditional market makers, i.e. banks, whose regulatory capital requirements for trading books have increased.

2| The digitisation of financial services nevertheless poses new risks to financial stability

The development of digital instruments and services in the banking and financial sphere is to be welcomed, provided that these instruments and services meet the needs of consumers and investors, support productivity gains and make France's economy more competitive. Yet this development might not only reduce transaction security, or facilitate money laundering and terrorist financing, but also increase two traditional financial system risks (credit and liquidity risk).

2|1 Transaction security

The digitisation of financial services presents a challenge to central banks as they perform their task of ensuring safe financial transactions (payment, delivery and settlement).

In the area of payments, for example, the sources of risks have shifted with the arrival of new participants and payment methods. The growth of online commerce at the start of the 2000s was accompanied by the widespread use of remote payments involving credit cards but also to other innovative instruments: electronic wallets, solutions based on credit transfers from bank accounts and payments integrated within mobile apps that enable purchases to be made swiftly using smartphones.

More broadly, the significant growth of decentralised trading systems, driven for example by the blockchain technology encompassed in bitcoin,[11] could change the conditions in which central banks perform their duties. Such models could replace the traditional operating procedures of clearing houses, which are based on the aggregation and central clearing of flows, thus affecting collateral management frameworks and asset recording procedures. Yet, except for bitcoin, this technology is still very much in the

6 *Crowdfunding platforms that are based on securities purchases.*
7 *According to ORIAS, the entity that keeps the register of insurance intermediaries.*
8 *Source:* Financement participatif France *(association of crowdfunding professionals).*
9 *Crowdfunding has seen much more pronounced growth in the United States than in Europe overall because the market is more mature and because the economy's financing model is structurally more disintermediated.*
10 *See* Assessment of Risks to the French Financial System, *December 2015, on the Banque de France website.*
11 *Blockchain uses a distributed ledger and communication between the payers through a peer-to-peer mechanism. It allows for a safe exchange of information within a given community, without the intervention of a trusted third party.*

experimental stage. Before its development potential can be confirmed, various conditions will have to be satisfied in terms of security, cost, the ability to process large transaction volumes quickly and even the economic benefits of bypassing trusted third parties in certain activities.

2|2 Cyber crime

With its entry into cyberspace, finance finds itself exposed to cyber crime, that is, offences committed using computer or information networks and aimed at violating an institution's data or systems.

These risks have already been taken on-board by traditional financial firms, on which prudential regulations impose a requirement to have in place protection buffers to cope with shocks of any kind. Financial regulators also strive to ensure the proper design of financial institutions' IT security policies: skill-building and awareness-raising among staff, participation in regular crisis exercises, enhanced protection of internal systems through strict access controls, more extensive data encryption, and the introduction of intrusion-detection tools together with the periodic testing of effectiveness.

However, fintechs, with their Internet-based business models, are especially exposed to cyber risks. Given their small size and financial footprint, the occurrence of such a risk presents for them a clear threat to business continuity which is considerably larger than that to more traditional entities and which could affect the latter when they cooperate with fintechs. Fintechs must fully integrate these cyber risks and draw up IT security policies in line with best market practice. Regulating these risks will entail effective cooperation between the competent authorities not only in France, i.e. the Banque de France, the *Autorité de contrôle prudentiel et de résolution* (French prudential supervisory and resolution authority – ACPR) and the *Agence nationale de la sécurité des systèmes d'information* (National information system security agency – ANSSI), but also at the international level.

2|3 Money laundering and terrorist financing

The new players in this digital era must also be fully subject to the anti-money laundering and counter-terrorist financing (AML/CFT) regulations. Accordingly, these firms need to ensure that their AML/CFT systems are suited to their business and customer base but also to the way in which they commence business relationships with their clients – in general through non-face-to-face procedures – in order to protect against improper or fraudulent use of their innovative solutions.

2|4 Credit risk: for an assisted development of crowdfunding

Financial stability issues related to crowdfunding intermediaries appear limited for the time being given the amounts raised. The banking channel will continue to play an essential role as the primary financing source for small and medium enterprises, and intermediate-sized enterprises. However, it is possible that more vibrant growth will spur the development of large platforms that potentially attract much greater amounts. The regulator must therefore take care to ensure that the development of new financing channels does not undermine financial stability or the legitimate protection of individual investors.

For example, crowdfunding may entail risks related not only to assessing the quality of the project and the financed entity but also to the security and the sustainability of the platform through which the funds are transferred. In France, Order 2014-559 of 30 May 2014 on crowdfunding states that platforms must provide Internet users with all the information needed to assess their investment.[12] Above a certain size, or in the case of cross-border activities, a harmonised European standard is necessary that goes beyond the current patchwork legislation.

12 *This information includes notably the eligibility requirements and criteria for selecting projects and project initiators, the risks incurred by lenders and failure rates for projects (already) presented by the platform, and the liability of each party (lenders, project initiator, crowdfunding intermediaries) in the event of the project initiator's failure.*

The Order of 30 May 2014 also enabled crowdfunding intermediaries to enhance their analysis of financial risks by providing them with broad access to financial information. In particular, it authorised them to consult the Banque de France's companies database (FIBEN), which is a key tool for analysing and monitoring credit risk. This initiative is part of efforts to promote the reliability and the sustainable development of this new financing channel, while addressing financial stability issues.

2|5 Liquidity risk: for a tighter regulation of high-frequency trading

HFT's rapid rise is changing the organisation of equity markets and the business model of trading venues. By providing market liquidity without being subject to regulatory requirements in this respect, HFT traders could crowd out traditional market makers. The latter will be forced to close the technology gap if they wish to continue doing business. At present, though, HFT firms are not subject to any obligations towards exchanges or customers. As a result, the liquidity they supply could abruptly dry up in the event of market stress. Some HFT firms employ strategies that could be likened to new forms of market abuse or manipulation: for example, issuing disproportionate volumes of orders that are not intended for execution in a bid to slow the operation of trading venues and thus more easily take advantage of arbitrage opportunities, has the effect of altering market information.

This technology has increased the speed of information flows which amplifies market volatility and contagion across asset classes. High levels of correlation across many HFT strategies tend to magnify the transmission of shocks. Notably, trading algorithms could respond procyclically to a market event, causing prices and volumes to overreact, creating the risk of a self-fulfilling spiral triggered by cascading trades and potentially even unleashing a flash crash, especially during periods of risk aversion. If HFT firms are hit by heavy losses, their lack of adequate capital buffers could lead to failures, especially since these companies often take similar positions. These failures could then quickly affect their market counterparties.

Indeed, regulations governing the way in which HFT firms conduct their business will soon be introduced in the framework of the revision of the Markets in Financial Instruments Directive (MiFID II). MiFID II should come into force in January 2018 and provides notably for the authorisation of HFT firms and a standardised definition of the tick size, depending on the instruments and their liquidity. The Directive also includes pre- and post-trade transparency obligations that should improve knowledge of HFT activity on platforms and the accuracy of liquidity indicators, as well as robustness requirements for algorithms (stress tests and kill functions) that should enhance market resilience. But, more generally, HFT remains a field where regulators, including in the United States, appear to be persistently behind the curve compared with the firms and the technology. Closing this gap must be a priority of international discussions.

3| In order to reconcile innovation and stability, the Banque de France and the ACPR must adhere to two principles of action

Innovation and stability are rarely compatible, which is also the case in finance. The scope of this new financial ecosystem is not yet stabilised, the horizon for deploying new digital technologies is uncertain, and defining the regulatory framework to be applied to a wide variety of corporates is complex. The regulation of financial services created in the wake of the digital wave must be tailored to its specific risks. In the framework established by the regulator, the central bank and the supervisory authority must ensure that new risks stemming from the digital transformation of the financial system do not hinder them from fulfilling their financial stability mandate and that, all things being equal, innovations clearly strengthen the functioning of the financial system for the benefit of the economy. To this end, we must adhere to two principles of action: an absolute guarantee of payment and transaction security, and a commensurate adaptation of regulations to address the development of fintechs.

3|1 An absolute guarantee: the security of payments and transactions

In the framework of its mandate to oversee the security of payment instruments, the Banque de France strives to promote innovative, effective and safe payment solutions. In this respect, it ensures that the emergence of new players and new solutions does not reduce security.

An initial response can be found in the recent or pending amendments to current European legislation on payment services and markets in financial instruments. For instance, with the emergence of new service providers that were not covered by payment services regulations (see above), a review was undertaken that led to the adoption on 25 November 2015 of Directive (EU) 2015/2366 or the Second Payment Services Directive (PSD2). PSD2 does not impose capital requirements on service providers as they do not hold their customers' funds; but these providers must be covered by a professional civil liability insurance or comparable guarantee.

Well before this, the creation of the Observatory for Payment Card Security in 2001, under the aegis of the Banque de France, already fulfilled these objectives with regard to bank cards. The Observatory's promotion since 2008 of strong authentication solutions for online card payments was effective in contributing to a decrease in fraud rates for this channel (0.248% in 2014 compared with 0.269% in 2013). Its mandate should be extended to all cashless payment instruments, as the Ministry of Finance advised during the National Payment Conference (*Assises nationales des paiements*) that took place in June 2015.

We also endeavour to analyse and assess the resilience of financial institutions and market infrastructures. Since it is impossible to fully guarantee their IT security against a cyber attack, it is important to ensure that they can carry on or rapidly return to business as usual in the event of a malfunction of their IT system. At the international level, under the aegis of the Committee on Payments and Market Infrastructures (CPMI),[13] a report recommending measures to promote the resilience of systemic market infrastructures was issued for consultation in November 2015. Such initiatives must be pursued in all relevant bodies in order to cover other systemic entities (banks, insurance companies, investment funds, etc.).

As regards virtual currencies, the Banque de France issued a warning in December 2013 stressing that it could not guarantee their security, convertibility or value, and that their anonymous nature could promote the circumvention of rules relating to anti-money laundering and counter-terrorist financing. In order to better prevent these risks, the conversion of virtual currencies into legal tender via Internet platforms must be considered – given that legal tender is received, recorded and transferred – to be a payment service requiring the relevant authorisation. The ACPR published a position to that end in early 2014.

Moreover, discussions are underway at the Banque de France, and more broadly at the *Haut Conseil de stabilité financière* (the High Council for Financial Stability), as to how to monitor the development of initiatives concerning blockchain technology, both in terms of the possibilities it offers and the issues it raises notably in terms of security.

3|2 A commensurate adaptation of regulations to address the development of fintechs

Adapting regulations to accompany the dissemination of innovations

The fintech industry raises specific challenges for the regulatory authorities. Their rapid development leads regulators to anticipate and consider the most suitable strategies to ensure consumer protection and address financial stability issues. A balance must be found in terms of regulating these new players in order to avoid stifling the innovations that may be directly or indirectly beneficial to consumers (in the form of new services and a reduction in costs due to their competition with traditional players), and more generally to the economy and society (as they offer a new means to finance the economy).

Although the new players largely offer banking services (means of payment, fundraising, savings management, etc.), their often small size and the

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

original and fragile nature of their start-up-like business model raise doubts as to whether banking regulations mainly formulated for mature players should be applied to them. Specific regulations, allowing for a gradual adjustment of regulatory intensity, could be better suited to preventing the risks generated by fintech firms. For example, the regime for payment institutions was amended in France to include the possibility of light-touch authorisation[14] for small institutions with low payment transaction turnover.

Lastly, fintech companies, which mainly operate on the Internet, are not bound by borders. This raises questions as to the regulations that are still largely domestic or based on residency criteria (for example, consumer protection rules). The cross-border nature of technological innovation in the area of banking and financial services is a strong incentive for the regulatory authorities to coordinate their policies at the international level. A European statute could be defined for specific companies with a certain development threshold.

Supervising fintech firms with flexibility and vigilance

It is not always easy to legally qualify certain innovations, as illustrated by discussions on rules applicable to virtual currencies and to their trading platforms, with respect to the notions of payment instruments and payment services. The status applied to new activities can vary somewhat, reflecting a degree of regulatory flexibility to adapt to such activities and modulate the intensity of the supervision. In practice this can be relatively complex for project initiators, which are often IT specialists and more rarely finance professionals. In France for example, 62% of the 55 members of the French fintech association are regulated on the basis of ten or so different statuses.[15] According to their activity, entities are either supervised by the ACPR (71% of regulated entities), or by the *Autorité des marchés financiers* (French Financial Market Authority – AMF) (21% of regulated entities), or by both authorities (8% of regulated entities).

In addition to the simplification of regulations discussed above, a specific treatment must be applied to fintech firms in their authorisation request process in order to: clarify the applicable rules, decide under which regulatory framework projects fall, help compile their authorisation application dossier, etc. Lastly, in a certain number of cases, for example when the business model presented falls within different categories (e.g. investment services and lending or payment services), the dialogue between the national banking and market supervisory authorities must be stepped up in order to assist project initiators as much as possible.

The need to adapt supervision to the specific features of fintech companies will require setting up dedicated teams to assist them with obtaining an authorisation and to organise their supervision: this will be the case in France thanks to the creation of a joint unit between the ACPR and the AMF. This initiative will notably allow new players to identify their correspondent, ask questions and access answers to frequently asked questions. Furthermore, an advisory forum allowing for a continuous dialogue between supervisors and fintech companies will be set up to better understand innovations, in particular to identify necessary changes in regulations and foster the exchange of information between stakeholders.

Conclusion

Digitisation has undoubtedly brought benefits to financial services, in particular in terms of information and quality of execution. In this regard, the development of technological financial innovations is positive. Such innovations also foster the emergence of new processes and new players in the financial services industry. Nonetheless, they also entail risks that need to be addressed. Vulnerability analysis must be enhanced, regulations adapted, the security of transactions maintained, and prudential supervision must be both flexible and vigilant. In the long run, once the experimental phase is over, it will be necessary to ensure that the same rules apply to the same activities, irrespective of the players performing them. In order to ensure a level playing field, financial players must be regulated according to what they do and not what they are. Addressing the growing influence of borderless technology on the financial system will also require an international coordination effort. Such are the challenges that the public authorities will have to meet.

14 *This light-touch regime is a possibility provided for in PSD2.*
15 *Payment institution, electronic money institution, payment service agents, electronic money distributors, investment firms, crowdfunding intermediaries, crowdfunding advisors, etc.*

New risks for financial stability

Digital banking and market disruption: a sense of *déjà vu*?

Jean DERMINE
Professor of Banking and Finance
INSEAD, Singapore

The article assesses the threat posed by digital banking as seen in the context of a long series of innovations in the banking sector that includes telephone banking, payment cards, the development of capital markets, internet, smartphones, and cloud computing. It focuses on the economics of banking services and banks' two main functions – as providers of liquidity and loans – and analyses whether these could be displaced by peer-to-peer and marketplace lending.

Digital banking is currently one of the main strategic issues faced by banks in terms of threats and opportunities. It raises also public policy issues: its impact on the profitability and solvency of banks, the protection of borrowers and investors, and the systemic importance of the new players, the fintechs starts-up specialised in financial services.

Even a casual reader of the press regularly comes across the impending death of banking. Fintechs – start-ups specialised in financial services – are disrupting banking markets. New payments systems have proliferated such as PayPal, Venmo, M-Pesa, Apple Pay, Android Pay, Alipay and Samsung Pay. Even social media platforms such as Facebook offer payment facilities. TransferWise and WorldRemit are competing with the incumbent Western Union for international transfers and remittances. On the credit side, Lending Club and Prosper, both in the United States, the British Zopa and Funding Circle, and the French Prêt d'Union are competing with established banks in the unsecured consumer loan market. The scale of the threat to the banking industry is summed up in the following:

"*They all want to eat our lunch. I mean every single one of them, and they are going to try*" (Jamie Dimon, Chairman and CEO of JP Morgan Chase, *Financial Times*, 26 February 2014). "*The aim is to inflict death by a thousand cuts. Fintech start-ups are nimble piranhas, each focusing on a small part of a bank's business model to attack.*" (*Financial Times*, 14 October 2015).

The cataclysmic predictions of the slow death of banking reminds me of similar gloomy forecasts made over the past 35 years. When telephone banking was introduced in the 1980s, there were fears that telephone companies would enter the banking industry and displace the incumbent players. But that did not happen – the banks themselves started to offer telephone based services.

At that time, I was consulted by a major British petroleum company, whose clients were using a credit card issued by the company to buy gasoline, about adding other financial services to the card for its millions of customers. It did not happen. Similarly, the Standard Chartered Bank in Hong Kong was nervous about potential competition from the "Octopus" card, a payment card used by millions travelers on the Hong Kong subway, particularly if other financial services were added to the card. Again, the threat of market disruption did not materialise.

When in the 1990s, capital markets – bonds and equity markets – were deregulated, it was predicted that direct finance would replace costly and inefficient indirect finance and financial intermediation. But the prediction turned out to be wrong: banking assets-to-GDP ratios grew in both developed and emerging economies.

At the turn of the millennium, as the internet bubble went up, bankers were terrified that Microsoft would enter their industry and enable customers to navigate online from one bank to another – such transparency of prices and product offers seemed set to undermine revenues. According to forecasters at the time, the end of "branch banking" was imminent, with severe bank restructuring and massive layoffs (as had happened in the coal and steel industries). Again, the threat failed to materialise. Indeed in several countries, banks opened more street branches, in response to customer preference for physical proximity.

More recently, the same has been said of the smartphone, essentially a computer with internet access in your pocket – purportedly poised to revolutionise the world of banking.

After 35 years of impending doom, it seems appropriate to ask whether digital banking will bring market disruption, or is it simply a fad and another case of *déjà vu*? Will banks adapt to control the technology or "will tomorrow be really different" with the supply chain of banking services dismantled by new players?

The objective of this paper is to analyse the sources of market disruption brought by digital technology and to identify public policy issues that need to be addressed. It is divided into four sections. In the first section, I review six fundamental services offered by banks. In the second, I attempt to identify the major changes in technology, and in the third, how they may disrupt the offering of banking services. In the final section, public policy issues related to marketplace lending are identified.

1| Economics of banking services: six main functions

In financial markets, economic units holding surplus funds, be they households or firms (or more rarely, governments), can finance directly economic units that are short of funds, such as other firms, households, or governments. Savers can buy bonds or shares issued by deficit units directly on the financial markets. This is referred to as *direct finance*. Where there is an intermediary between the units with surplus and those with a deficit, we refer to *indirect finance*. A bank

is one example of a financial intermediary, collecting deposits and granting loans. Others include insurance companies, pension funds, and investment funds, such as mutual funds or hedge funds.

Although the services provided by banks in financial markets are interrelated, we can distinguish six categories of increasing complexity (Dermine, 2015): underwriting and placement, portfolio management, payment (transmission) services, monitoring or information-related services, risk sharing, and advisory services.

Underwriting and placement: a first service provided by banks is to bring together savers and borrowers. Underwriting and placement of securities – bonds or shares – help borrowers (corporate firms or public institutions) to meet surplus units, and structure or customise the type of securities that meet the risk/return requirements of borrowers and lenders. In this function, the underwriter is involved not only in designing the security, but also in the valuation of assets and the pricing of securities to ensure that the terms of the issue are competitive. As investors may wish in the future to transform these claims into cash, consumption or other securities, they need to be exchanged. Brokers/dealers or market makers provide these services to ensure secondary trading and liquidity. In a pure underwriting and placement service, it is assumed that the return and risk of the securities can be properly defined, so that there is no major problem of asymmetric information (agency problem) between lenders and borrowers. In this case, monitoring is not an issue. With the underwriting and placement service, the end-investor holds directly the claims on deficit units.

Portfolio management: investors can acquire at a low cost a diversified portfolio of securities issued by deficit spending units. Mutual funds and UCITS (Undertakings for the Collective Investment In Transferable Securities) supply a diversified portfolio to the holders of its shares. The income derived from the financial assets is paid to shareholders less a fee paid to the fund manager. These funds exist for three reasons: to reduce the divisional costs incurred in issuing many securities, to provide a diversified portfolio to investors, and to delegate asset management to specialists who can assess economic prospects.

Payment mechanism: a third function of financial markets is the management of the payment system, i.e. to facilitate and keep track of transfers of wealth among individuals. This is the bookkeeping activity of banks realised by debiting and crediting accounts. Although the retail payment system is limited by regulation to a specific type of deposits (demand deposits), it could be achieved by debiting or crediting any type of liquid assets.

Monitoring and information-related services: private information held by borrowers leads to contracting problems, because it is costly to assess the solvency of a borrower or to monitor his/her actions after lending has taken place (Stiglitz and Weiss, 1981). Sometimes, it is useful to package these claims in a portfolio, and banks perform a useful function in reducing the costs of screening and monitoring borrowers. The delegation of screening and monitoring to banks has been shown to be an efficient mechanism (Diamond, 1984). This fourth category is linked to the first (underwriting and placement) but listed here as a separate service as it corresponds to those cases where significant information asymmetries make it difficult to issue financial claims traded on securities markets. While the second service (portfolio management) refers to the management of liquid assets, this fourth function refers to the management of an illiquid loan portfolio, often the largest part of a bank's balance sheet.

Risk-sharing service: an increasingly important function of banks is to make the market more complete, i.e. to provide some form of insurance against multiple sources of risk. First, banks not only supply diversified assets, but also organise efficiently the distribution of risky income earned on the asset pool. The debt holders receive a fixed payment while the shareholders receive the residual income. Other insurance services include interest rate insurance (floating rate lending with various ceilings on interest rates called *caps or floors*), inflation insurance with real contract, and liquidity insurance, i.e. option for a deposit holder or the holder of a line of credit to withdraw cash quickly at its face value (Diamond and Dybvig, 1983).

Advisory services: advisory services to corporations and individuals are a significant source of fee income. Advices on mergers & acquisitions or risk management to corporations, as well as on asset management, tax or succession planning to individuals are all services offered by banks.

In the next two sections, we identify technological innovations and evaluate how digital technology could disrupt the offering of bank services.

2| Disruptive technology in banking, a historical perspective

The following sections review the technological innovations (by a non-specialist) and their impact on the banking industry: electronic processing of data, telephone banking, internet, smartphones and cloud computing.

Electronic processing of data. According to Ali *et al.* (2014a), a major breakthrough that affected the payment system was the move from manual entry of debit/credit in a book ledger, to machine-readers of checks, and subsequently electronic payments. The payment business relies on the mastering of electronic data processing with debit and credit of accounts. In this area, banks have no source of competitive advantage vis-à-vis tech firms such as telephone or internet companies, as illustrated by the proliferation of new entrants/payments systems, including the mentioned M-Pesa, PayPal, Apple Pay, Samsung Pay, and Alipay developed by the Chinese retailer Alibaba.

Telephone (minitel) banking: a major benefit of telephone (minitel) banking was that access to bank information (such as to the account balance) and transactions could be initiated from any location outside the bank's branch and processed automatically with electronic data processing.

Internet: compared to telephone banking, the Internet allowed millions of users to access data more easily from distant locations and facilitated the entry of transactions. Coupled with the development of mathematical algorithms, it allowed the clearing and settlement of securities trade at low cost. This facilitated the entry of online brokerage and asset management firms such as Boursorama and Cortal in France, Banco BIC in Portugal or Binckbank in the Netherlands, Belgium and France. More recently, the Internet and mathematical algorithms combination has allowed the matching of investors and borrowers.

This is best illustrated by America's Lending Club, which has attracted a significant attention due in part to a successful IPO in December 2014 and the presence of well-known individuals on its board, such as Larry Summers, former US Treasury Secretary, and John Mack, former president of Morgan Stanley. Founded in 2006 in San Francisco by the French entrepreneur Renaud Laplanche, the current CEO, it is essentially a brokerage platform matching investors to individual borrowers. On the first day of trading (12 December 2014) the price of its shares issued at USD 15 jumped to USD 24.75, a 65 per cent gain.

Initially dubbed peer-to-peer (P2P) lending with individuals financing individuals, it has evolved into "marketplace funding" with large institutional investors such as pensions funds or hedge funds making these loans. According to Credit Suisse analysts (CS, 2015), the USD 4 billion loan volume issued by Lending Club in 2014 can be compared to a total addressable market (TAM) of USD 873 billion of unsecured consumer loans, reaching USD 1,171 billion if one includes unsecured loans to small and medium size enterprises (SMEs). The claim of Lending Club is that, unencumbered by an expensive set of physical branches and outdated IT, it can operate with a much lower cost base, offering better returns to investors and cheaper loans to individuals. On 11 January 2016 it was trading with a price-to-book of 3.5 but a share price of USD 9.24, significantly below the December 2014 issue price of USD 15. Available FICO credit scores on the credit worthiness of individuals in the United States allows to classify credit risk and investors can diversify by investing pieces of USD 25 into several loans. Lending Club relies on digital technology to solve the asymmetric information and divisibility issues mentioned earlier.

Smartphone with sensors: smartphones that combine computer power and internet access allow banking at any time, any place. In addition, sensors collect data on customer habits which allows big data analytics.

Cloud computing: progress in storage and transmission of data allows the aggregation of data and softwares in specialised places on the "cloud". This has an important impact on the bank value chain. Data and softwares no longer need to be stored in house but can be stored with a third party. Smaller firms can benefit from lower cost generated by economies of scale of the cloud company specialists.

3| Banking services and disruptive digital technology

To understand the impact of digital technology on banking markets, it is useful to group some of the banking services discussed in Section 1 into three categories: those related to data processing, to data analysis, and to the bank's unique balance sheet structure, as in Table 1.

The first column lists banking services that involve mostly electronic data processing. They include payment with debit and credit of accounts, the development of digital currencies such as bitcoins,[1] brokerage of securities including trading with algorithms, and the distribution of passively managed funds. It includes consumer loans for which credit risk can be quantified with external discriminatory factors. Easy access to external data and statistical packages to evaluate credit risk implies that the risk is commoditised. As this first set of services requires expertise in data processing and not in banking, they are attractive to new competitors. Entrants into the payment business – PayPal, Apple Pay, etc., and in international money transfers (TransferWise) illustrate the significance of the threat.

In many cases, banks have been able to respond. In France, they joined forces to introduce Paylib for online payment. In the online securities brokerage industry, Boursorama and Cortal have fought off competition, but have seen a significant reduction of the fee per transaction. Other industry responses have been cooperation with telephone companies (such as Apple), but again with a reduction of bank revenue due to sharing. Finally, when credit risk is quantifiable with external data and commoditised, it becomes a data processing game. This explains the success of Lending Club in penetrating the US unsecured consumer loan market. Section 4 offers a specific analysis of credit market disruption.

An open and significant issue for banks is whether the loss of the payment business implies the loss of the client relationship and cross-selling opportunities (World Economic Forum, 2015). It is not clear whether data-processing specialists want to enter banking services related to data analysis and balance sheet structure. This would require the acquisition of banks' expertise at great cost. This would only happen if clients valued a single point of entry for the purchase of financial services (payment and other banking services). So far, the growth of the online payment PayPal does not seem to have affected yet the banking businesses.

The second column includes services that require data analysis and specific banking expertise. Lending involves not only a supply of funds, but also the control of risk via assessment of collateral and, when the economy dives, loan restructuring and recovery. This requires specific banking expertise that cannot be easily copied by data processing specialists.

The third column includes banking services that rely on the unique balance sheet of banks and their ability to mismatch maturities. As stated above, banks provide liquidity insurance services in both deposit and credit markets by relying on a large pool of depositors and borrowers. This service cannot be easily imitated by pure data processors. Lending Club, it should be observed, does not engage in maturity mismatch but offers matched-maturity medium-term investment.

From this we can conclude that data-processing activities are under threat from specialist companies

Table 1
Banking services

Data processing	Data analysis	Bank's balance sheet
Payment, crypto-currencies (bitcoin)	Lending to SMEs (with evaluation of risk, collateral, monitoring of risk, restructuring, recovery)	Deposits: safe (as backed by deposit insurance and diversified loan portfolio) and liquid (withdrawable on demand)
Brokerage of securities (shares and bonds), passively managed investment funds	Advisory (corporate finance and risk management)	Credit lines (borrowers can access liquidity on demand)
Consumer loans (credit risk is quantifiable, commoditised)	Asset management (advisory on estate planning, actively managed funds, structured products)	

Source: Jean Dermine.

1 *The case of crypto-currencies is not discussed in this essay (Ali* et al. *2014b).*

such as telephone or internet companies. India, for example, has recently granted banking licenses to telephone operators to stir competition. And the announcement on 6 January 2016 by the French telephone operator Orange of its intention to buy the insurer Groupama's bank to launch a mobile bank in 2017 will be closely monitored. Banking services that are quantifiable with external data and commoditised are also subject to competition, such as Lending Club in the consumer credit market. A fundamental question arises as to whether banks will be affected by the loss of payment business and client relations. Agile banks can adjust by offering alone or in partnership the omni-channel distribution to meet the needs of the clients, but often with a reduction of bank revenue, which in turn implies pressures to reduce operating costs.

As bank lending is fundamental for the economy, a specific analysis of digital disruption in the lending market follows.

4| Digital disruption, bank lending, and public policy

We have seen how P2P and marketplace funding could disrupt two banking services: the resolution of asymmetric information and the division of investment into small amounts to allow diversification. While it is too early to know whether the potential will become reality, two observations must be made about the benign economic circumstances which favor the growth of that industry: an ultra-low interest rate environment and an economic recovery in the United States.

The very low interest rate environment has created an appetite for riskier assets and credit risk spreads, with institutional investors searching for yield. The US economic recovery has shifted attention away from the downside risk of a recession and loan losses. It is obvious that lending is not just about matching investors and borrowers, it is also the business of controlling risk and managing non-performing assets From that perspective, a remote internet-based company from San Francisco will be at a competitive disadvantage vis-à-vis banks with branches that are closer to its non-performing clients. The case of marketplace funding suggests that we classify lending into different types of credit risk and funding vehicles, as in Table 2.

Table 2
Digital disruption and lending

Data Processing	Data Analysis
High risk ("information sensitive": collateral valuation, risk monitoring, restructuring, recovery)	Insured deposits, unsecured deposits or bonds, subordinated debt and equity Banks keep "skin in the game".
⬇	Securitised loans with several tranches – Shadow banking Under current international regulations, banks keep "skin in the game".
Low risk ("information insensitive", such as a mortgage with a low loan-to-value ratio)	P2P, Marketplace funding Brokers do not keep skin in the game.

Source: Jean Dermine.

Digital technology allows direct finance with the matching of borrowers and investors. It is a low cost competitor to the banking industry. However, as discussed above, lending is more than the matching of investors and borrowers. It involves the control of risk after lending has taken place, the trading of claims if investors need to access liquidity, and the management of non-performing assets. Given the complexity of these lending services, it is useful to rank assets according to the degree of credit riskiness (from high risk to very low risk) as shown in the first column of Table 2.

Higher credit risk implies a need for risk monitoring and a higher probability of having to deal with non-performing assets. Moreover, the presence of credit risk with asymmetric information between the holder of an asset and a potential buyer may lead to a market breakdown due to the classical fear of buying a "lemon". Such "information sensitive" assets become illiquid in a recession, just when liquidity is most needed (Dang *et al.* 2013). For such assets, funding on the bank's balance sheet with a maturity mismatch allows the creation of liquidity and is something that cannot be replicated by a broker such as Lending Club that does not engage in maturity transformation.

At the other extreme are very safe assets, such as a mortgage with a very low loan-to-value ratio. These assets which are not affected by credit risk are "information insensitive" and therefore liquid. A broker is well placed to offer financing vehicules at a low cost. Classifying loans from risky to very safe, one can argue that higher risk transactions will remain on the balance sheet of banks, that lower risk can be securitised and that very safe assets can be handled with marketplace funding. This does not

necessarily imply market disruption as banks could replicate by offering similar products to investors.

Securitisation of loans and shadow banking were the source of the global financial crisis in 2007. Three issues were at stake: excessive borrowing, poor information available to investors in securitised vehicles and a severe maturity mismatch when loans were funded in structured investment vehicles (SIVs). Short-term commercial paper could not be rolled over in summer 2007 (Dermine, 2013).

P2P and marketplace funding are developing in a special situation of ultra-low interest rates and an economic recovery, at least in the United States. It remains to be seen how risk and losses will materialise during a recession or a period of rising interest rates. Marketplace brokers do not seem to perform maturity transformation, but it remains to be seen if institutional investors buying these loans do not perform maturity transformation. Protection of borrowers and investors and the identification and control of maturity mismatch in shadow banking must be addressed by regulators if we are to avoid history repeating itself (Kelly, 2014).

Conclusion

The disruption caused by digital technology is seen as sounding the death knell of banking, just as in the past with the birth of telephone (minitel) banking, the development of bonds and equity markets, the advent of internet and the smartphones, with a certain sense of *"déjà vu"*.

Two main sources of market disruption are analysed. The move of payment services to new players could break the banks' customer relation and cross-selling of products. However, it is far from clear how new players with expertise in data-processing could acquire at a reasonable price banking expertise in fields such as asset management or corporate advisory. Just as banks have adapted to new technology in the past with the development of omni-channel distribution, there is no reason why this would not be the case again.

With regards to the funding of credit risk, internet has facilitated P2P and marketplace funding. Furthermore, the environment for P2P has been extremely favorable, thanks to low interest rates and the expansion of economic activity. Such a benign environment for marketplace funding may not last. Moreover, nothing stops a bank from offering a similar loan brokerage facility.

As was the case with securitisation, public policy should ensure a minimum level of transparency for borrowers and investors. It must identify and control shadow banking with maturity mismatch, a major cause of a liquidity crisis. Banks have a unique role to play in providing liquidity and funding higher credit risk assets, which are often characterised by opacity. Digital technology, in my opinion, does not represent a fundamental disruption to these two banking services.

References

Ali (R.), Barrdear (J.), Clews (R.) and Southgate (J.) (2014a)
"Innovations in payment technologies and the emergence of digital currencies", *Bank of England Quarterly Bulletin* Q3, pp. 262-275.

Ali (R.), Barrdear (J.), Clews (R.) and Southgate (J.) (2014b)
"The economics of digital currencies", *Bank of England Quarterly Bulletin* Q3, pp. 276-286.

Credit Suisse (2015)
"Lending club, equity research", 21 January, pp. 1-22.

Dang (T. V.), Gorton (G.) and Holmström (B.) (2013)
"Ignorance, debt and financial crises", *mimeo*, pp. 1-34.

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

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

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

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

Kelly (G.) (2014)
"The digital revolution in banking", *Occasional Paper* 89, Group of Thirty, Washington DC, pp. 1-41.

Stiglitz (J.) and Weiss (A.) (1981)
"Credit rationing with imperfect information", *American Economic Review*, 71, pp. 393-410.

World Economic Forum (2015)
"The future of financial services", June, pp. 1-176.

Digital risk: a strategic challenge and a growth opportunity for insurers

Nicolas SCHIMEL
Director General
Aviva France

The insurance sector has always based its business model on the collection and exploitation of data – well in advance of many other industries – and now relies heavily on the computerised storage, use and control of data for its liabilities and, with the emergence of sophisticated financial techniques, for its assets. Actuaries, statisticians, financial managers and IT developers have always invested extensively in data processing and in mitigating the associated risks, so that for a long time the insurance industry was at the forefront in these fields. With the rapid unfolding of the digital age, however, data is now used intensively in all segments of the economy.

That said, the transition to a digital world poses specific and major risks for insurers: firstly from a strategic point of view, in that it could lead to profound changes in their traditional business models; secondly, from the point of view of operational security, as Solvency II has placed them under heightened pressure to ensure their long-term business continuity, making insurance one of the most sensitive sectors in terms of cyber risk, alongside banking and defence. Given the scale of the challenges, the insurance industry has equipped itself with both the means and the skills to tackle these operational risks.

The need to control their own exposure to cyber threats will prove an advantage for insurers, allowing them to play a key role in helping society deal with these risks. The digital transition has already raised the question of how to protect against this new danger, leading to the emergence of the very first cyber insurance policies. At the same time, it poses the challenge of how to provide cover for large or strategic organisations, a highly technical area that opens up opportunities for new, dedicated cyber protection ecosystems.

The risks associated with the digital age pose new challenges for insurers, consumers and compilers of historical data.

The mathematical exploitation of data is at the heart of modern insurance…

Modern insurance has always consisted of the evaluation of risk based on the collection and processing of reliable data. By applying mathematical algorithms to data, insurers estimate the likelihood of a risk materialising – and hence decide whether it is insurable – and then calculate the price of transferring that risk. Thus, the mathematical exploitation of data is at the heart of their business model, determining their strategic and competitive positioning, as well as their operating performance.

As advances in computer technology have boosted their calculation capacity and the sophistication of their models, insurers have developed increasingly complex risk assessment models to keep pace with changes in society.

…and is taking on new meaning with the data revolution

Today, the "big data" phenomenon is dramatically increasing the wealth and variety of data sources that can be used for risk modelling. This has profound implications for the industry, as exploiting this information could, in theory, revolutionise the way insurers do business.

Insurers face a major challenge to protect themselves against the growing threat of cyber attacks

Due to the often confidential and sensitive nature of the digital data they keep on file, insurers, and all economic organisations in general, are exposed to a growing threat of cyber attacks: theft or breach of client details, espionage, etc. The digital migration has increased companies' reach and created huge growth opportunities by transforming relationships with customers and enabling them to refine products and prices, automate administrative tasks and create new partnerships. However, it has also added new layers of complexity and vulnerability in terms of cyber resilience, for example by increasing their reliance on digital infrastructure that none of them can completely control (Deloitte, 2014).

On a strategic level, therefore, the digital transformation not only raises opportunities, it also generates risks for insurers: operational risks related to the security of systems and data, as reflected in Solvency II, but also new risks, and all the problems that go hand in hand with any emerging market.

1| New models of insurance: threats and opportunities

The first danger that comes to mind in any discussion of digital risk in insurance is data and information system security or cyber risk. However, insurers face another, equally serious threat to their stability – the risk that the shift to a digital world will radically alter the way they do business.

The rapid and progressive integration of digital technology offers opportunities to transform traditional models of insurance

Big data has triggered an explosion in the quantity and variety of customer data gathered by non-insurance companies (telecoms operators, carmakers and, in general, all suppliers of connected devices), and it is likely they will soon collect more information on customer behaviour than insurers. These details can help to improve the pricing, monitoring and prevention of risks. But what will non-insurance companies do with the data? Will they sell it to the highest bidder in the insurance industry (as Google currently does)? Will they decide to appropriate certain tasks in the insurance value chain (distribution, risk selection, value-added risk prevention services) leaving insurers with the less commercially selective or profitable roles? How will this affect insurers? Will they lose the initial contact with the customer, affecting the way the relationship evolves commercially? Or will insurers end up competing to offer the cheapest management platforms, leading to a reduction in margins or even to sector concentration in a bid to achieve economies of scale?

The rise of new digital services and data could also reduce demand for traditional types of insurance cover, prompting a fall in business volumes. For example, the "internet of things" creates a virtuous circle in that it makes it easier to detect and prevent risks: connected or driverless cars are liable to have a much lower risk of accident, the creation of fleets of driverless cars will shift the market from a conventional B2C to a B2B model, the collection of information on road safety will make risk assessment more effective, and so on.

Big data could also lead to prices and policies being tailored to individual customer profiles (segment of one), with individuals considered a "good risk" having access to cheaper deals. The danger here is that the notion of risk pooling might disappear altogether and customers deemed high risk would find it too expensive to get insurance.

Another threat to traditional insurance models is the emergence of peer-to-peer insurance, which consists in pooling the premiums and exposures of a small group of coopted policyholders, with none of the usual exposure management techniques or technical reserves. For the time being peer-to-peer insurance appears to be limited and only concerns small exposures. However, players in the field have not yet exploited all the opportunities opened up by the increasing digitisation of customer-supplier relationships.

Lastly, the growth of digital technology also poses a threat to the long-term sustainability of the traditional insurance distribution model, where over 90% of products are sold through intermediation. For example, the development of multi-channel relationships, the emergence of new market players with a different approach to distribution, the direct online sale of insurance, the rise of robot-advisers and the increase in online self-service insurance all threaten to undermine conventional insurance distribution. If the latter is to survive, it will need to transform digitally and offer value to clients.

The extent of this transformation will depend on how readily consumers share their personal details

The sharing of personal data must be based on the principle of informed consent, given in a climate of trust and transparency and in full appreciation of the benefits and of the safeguards put in place. Aside from the fears individuals might have over the security of their details and the possibility of their fraudulent use, digitisation also prompts more philosophical questions over the desirability of a society in which everyone can be tracked, catalogued and recorded, with all the totalitarian risks this implies. The issue is prompting public debate and discussion is only set to intensify. Eventually this should result in more or less restrictive limits being placed on the collection, processing and use of personal data, all of which will affect the way business models evolve, including in insurance.

The appearance of newcomers in the insurance value chain raises the question of how they should be regulated

The rise of digital technology is paving the way for the increased offshoring of data collection, storage and processing, and of insurance services, or the migration of these activities to the cloud. This raises complex questions over the regulation of market newcomers, relating to the protection of users' personal data and the competitive landscape.[1] Although these elements of digital risk affect all segments of the economy, they are particularly significant in the insurance sector where data is at the heart of the business.[2]

A real threat to the financial stability of existing players in the insurance industry

The overhaul of existing insurance models will clearly offer opportunities to new entrants (e.g. telecoms

1 *The range of potential situations is broad: local actor; actor in a European Union country; free provision of services by an EU-based actor; actor based in a country which has signed agreements with the European Union; and, in extreme cases, disruptive models such as peer-to-peer insurance which does not fall within the scope of existing insurance regulations.*

2 *Public authorities are making efforts to ensure greater homogeneity and a level playing field for all players. The European directive on data protection (Directive No 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data), the positions adopted by EU competition commissioner Margrethe Vestager (La Tribune, 2015a) and by digital economy commissioner Günther Oettinger (La Tribune, 2015b) are steps in the right direction, but more needs to be done.*

operators, manufacturers of cars and other connected devices, peer-to-peer operators, Google, Apple, Facebook and Amazon), although not necessarily across the entire insurance value chain. Newcomers will instead be able to operate as niche players in the market, taking advantage of the decline in traditional types of cover, and of the competitive edge offered by digital innovation.

Insurers are thus going through a period of disruption. One advantage is that they are facing this strategic test later than many other industries, allowing them to learn from the experience of others. Players in the sector are keenly aware of the urgency, and have taken steps to adapt their models, and leverage digital technology to re-engineer their business and become more customer-centric. However, to really benefit from the opportunities of the digital age, they will need to make a huge cultural shift, becoming increasingly willing to question their methods, listen to their customers, test new initiatives and set up appropriate digital ecosystems with external partners (notably fintechs). Tomorrow's leaders will be those companies that can successfully enact this change.

2| INSURERS ARE TAKING CYBER RISK EXPOSURE INTO ACCOUNT AS PART OF THEIR SOLVENCY II REQUIREMENTS

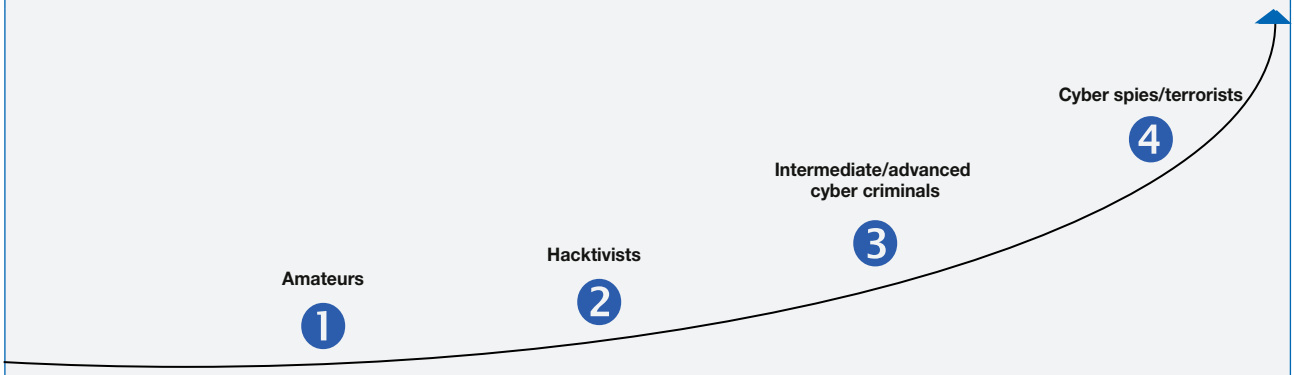
Cyber attacks are growing in sophistication and pose a risk to all segments of the economy

With the digital world unfolding at an accelerating pace and cyber criminals becoming ever more sophisticated, nimble and unpredictable, cyber attacks now pose a threat to all segments of the economy – from SMEs to multinationals, public sector organisations to NGOs. Despite widespread awareness of the risks, and an increase in investment in cyber defence (up 24% worldwide in 2015; see PwC Consulting, 2016b), a total of 43 million cyber incidents were recorded globally in 2014 (see PwC Consulting, 2015).

In addition, cyber criminals are changing their strategies and becoming increasingly savvy. The trend

Box 1

Cyber attacks are changing in nature and becoming increasingly sophisticated



	Amateurs (1)	Hacktivists (2)	Intermediate/advanced cyber criminals (3)	Cyber spies/terrorists (4)
Objectives & Targets	• Often with no set objective; small-scale scams targeted at individuals, experiments • Random targets (standardised techniques)	• Political motives (e.g. Anonymous); emotional issues • Targets linked to their demands	• Financial motives (e.g. theft of bank details) • Opportunistic targets	• Theft/ compromise of data as part of a targeted attack against a state or organisation • Advanced Persistent Threat (APT): long-term targeted attacks
Organisation	• Not organised	• Organised	• Highly organised • Highly professional, with knowledge of technology and of the business	• Highly organised • Highly professional, with knowledge of technology and of the business

Sources: CERT IST, SOPRA, Swisscom.

Box 2

What are the potential consequences of cyber risks?

- *Theft of intellectual property or commercially sensitive information*
- *Business disruption/interruption*
- *Data and software deletion/destruction*
- *Direct financial losses (e.g. extortion payments, theft of funds)*
- *Third party liabilities*
- *Reputational loss*
- *Physical damage*
- *Cost of investigation/response*

Other parties liable to be affected:
- *Customers*
- *Employees*
- *Suppliers, service providers*

Source: HM Government (2015).

now is to hack into an organisation's information system via its employees (e.g. using fake emails), and use both business-specific and technological techniques to collect and extract key data for resale or to extort payment.

The form a cyber attack takes differs according to the sector being targeted: e.g. industrial espionage in the technology sector, theft or breach of personal data and service disruption in the services sector, including in public services.

The global annual cost of cyber crime was estimated at over EUR 400 billion in 2014.[3] Moreover, with the economy growing increasingly interconnected, the fallout from cyber attacks can spread by domino effect well beyond the original target, making cyber resilience a key priority for all organisations.

Public authorities have seized firmly on the issue of cyber security

The fact that public authorities have actively taken steps to improve cyber resilience, both at European level (with an agreement on a set of EU rules on cyber security (European Parliament, 2015) and the future EU General Data Protection Regulation or GDPR)[4] and at national level, demonstrates just how important a threat cyber crime poses. In France, the government has already taken concrete action to mitigate cyber risk, with the creation of the *Agence Nationale de la Sécurité des Systèmes d'Information* (ANSSI or National Information Systems Security Agency) and the publication of the 2014-2019 defence spending plan.

As users of personal data, including sensitive information, insurance companies will be directly affected by the future EU GDPR. Scheduled to take effect in 2018, the text is expected to strengthen the powers of sanction of the French data protection authority (the CNIL), and make insurers – as well as other organisations – liable to heavy fines if they are found to have been at fault in the event of a data leak (e.g. non-compliant data processing methods, failure to notify the CNIL or the victims of a data leak). The launch of class action in France in 2014, and the fact that consumers are increasingly being made aware of the need to protect their data, should also place organisations under greater legal and financial pressure to handle sensitive data appropriately.

Up to now, the insurance sector has been relatively unaffected by cyber attacks

The first cyber attack in the insurance industry only took place in 2014, and was targeted at the British insurance broker Brightside (Insurance Speaker, 2014).

This relative freedom from cyber attacks is primarily due to the fact that the insurance sector has been slow to embrace digital technology. Nonetheless, attacks directed at insurers are set to increase both in frequency and seriousness over the medium to long term, which explains why the sector is rushing to catch up from a digital perspective. A 2014 study by the World Economic Forum showed that half the insurance companies surveyed saw the risk of a cyber attack as a challenge with major implications.

The fact that, in 2015, one of the leading US health insurers, Anthem, was the victim of a cyber attack big

3 *See Center for Strategic and International Studies (2014). The authors estimate the global annual cost of cyber crime at between EUR 375 billion (conservative estimate) and EUR 575 billion (maximum), but say the figure is more likely to be over EUR 400 billion.*

4 *The EU General Data Protection Regulation should apply to all organisations using personal information, and is expected to require them to inform customers and the CNIL if they have suffered a cyber attack liable to compromise personal data.*

enough to have potentially resulted in a massive theft of personal data (Reuters France, 2015) underscores the size of the stakes involved.

Solvency II increases the need for more professional management of cyber risks

Insurers have a longstanding and in-depth understanding of both financial and insurance risks. However, Solvency II also places an increasing onus on insurers with regard to the management of operational risk, by obliging them to include the latter in their risk based capital models. The directive explicitly defines operational risks as "*the risk of loss arising from inadequate or failed internal processes, personnel or systems, or from external events*." In its present form, Solvency II includes legal and modelling risks as forms of operational risk. However, the category will need to be extended to cover threats such as fraud, security risk and failure to protect data – all of which are similar to cyber risk.

Some broad categories of cyber risk are emerging, although the environment has not yet stabilised

Individual insurers are liable to want to create their own definitions and categories of cyber risk, which should, at the very least, include cyber attacks.

One approach is to use an existing operational risk taxonomy, such as that proposed by ORIC International (the Operational Risk Insurance Consortium). In this latter case, insurers can share anonymised information via ORIC on possible and proven risk (benchmarks).

As the table shows, cyber risk can cause operational failures in areas as diverse as accounting, human resources and customer service. Similarly, cyber attacks can have a huge impact on customer relationships, legal liability and commercial operations. The rapid transition to a digital world is exacerbating those risks, both for financial institutions and their customers: day-to-day interaction is now conducted online, increasing exposure to the threat of identity theft and service disruption. We are now faced with a paradox: digital technology can help us to better control risks and make them rarer, but can also make them more serious and harder to detect when they do materialise.

The difficulty of measuring cyber risk

Like all operational risks, cyber risks are directly linked to the complexity of an organisation. They have multiple causes and consequences, making them difficult to describe, quantify and analyse. Indeed, the financial effects of cyber incidents can be both direct (operating losses linked to business disruption, cost of technical processing/repairs, financial compensation for damages caused to third parties, legal fees, etc.) and indirect

Extract of the ORIC risk taxonomy, including exposure to cyber risk

Event-type category (Level 1)	Categories (Level 2)	Activity (Level 3, non-exhaustive)
Internal fraud	Unauthorised activity	Unreported or unauthorised transactions Falsifying personal details
Theft and fraud	Theft or destruction of assets Disclosure of confidential information Accounting irregularities	
External fraud	Systems security	Theft of information Viruses
Business disruption and system failures	Systems	Hardware Software Outages/disruptions
Execution, delivery and process management	Transaction capture, execution and maintenance	Data entry error Accounting error Incorrect unit pricing/allocation Inadequate process documentation
Monitoring & reporting	Failed mandatory reporting Inaccurate external reporting	
Customer/client account management	Payment to incorrect customer/client Incorrect payment to customer/client	

(damage to the company's reputation which can negatively affect future sales, opportunity costs linked to the time spent by staff on restoring IT systems rather than on growth activities, etc.). Moreover, constant evolutions in technology, as well as in the associated risks and safeguards, make it even harder to effectively assess the threat, and any attempt to evaluate the impact of a digital incident will quickly become obsolete.

Estimating cyber risk by evaluating its impact on capital

Solvency II requires insurers to calibrate their solvency capital requirement so that it corresponds "*to the Value-at-Risk of the basic own funds of an insurance or reinsurance undertaking subject to a confidence level of 99.5% over a one-year period.*" (Art. 101 (3) of Solvency II).

Insurance companies must therefore estimate the financial impact of any risk that has a 0.5% probability of occurring over a one-year period, and this approach is also applied to cyber risk.

There are three possible methods for calculating this impact:

• **The loss distribution approach** (LDA) – The statistical modelling of potential losses using internal data (or market data). One of the difficulties with this approach is generally the paucity of data on large observed losses, which makes it hard to calibrate the statistical model.

• **Scenario analysis** – This is the most common approach. Business experts and risk managers develop a joint narrative describing the risk and the way in which it can arise, right up to its impact on operations and the financial costs incurred. The probability of each step in the scenario actually occurring is then estimated, along with an amount for each type of cost. The advantage of this approach is the clarity of the risk description, and the refined analysis of possible causes and effects. On the downside, however, it is not sufficiently flexible to take account of interactions between risks.

• **Estimation using Bayesian networks** – This is an extension of the previous approach, in that it uses scenarios to describe how a risk materialises into an occurrence. However, event probabilities or estimates of one-off losses are replaced by a complete probability distribution, which includes possible interdependencies between variables. This approach offers a more refined analysis and a better understanding of the risks – particularly of how extreme losses could arise. The modelling software can also be used to carry out sensitivity analyses.

The management of cyber risk is becoming increasingly sophisticated

As with other risks, managing exposure to cyber risk in insurance requires robust and mature processes, particularly in light of the rapidly evolving landscape of cyber attacks and of their potential impacts. Hackers are becoming increasingly nimble and sophisticated in their methods, raising the need for adequate responses that are commensurate with the stakes involved.

Insurers have adopted a holistic, integrated and cross-disciplinary approach to managing cyber risk, comprising the following actions:

Upstream:

• identification and analysis of risks: mapping of cyber risks based on the identification of critical intangible assets, internal and external vulnerabilities, key software, stakeholders, etc.;

• development of defence capabilities: this involves taking a segmented approach to risk and includes managing IT equipment (e.g. installation of firewalls and antiviruses that are kept up to date and tightly managed), managing access and user rights for sensitive business applications and servers, protection of data (i.e. identification and classification of key data), management of electronic signatures, etc.;

• development of a pro-active and permanent framework for detecting risks: for example, setting up a collective cyber incident watch (in conjunction with research bodies or the CERT – the French government cyber attack monitoring, alert and response centre) helps to increase insurers' awareness of the real or potential attacks to which they are exposed;

• implementation of preventive action: definition of cyber security strategies and best practices, raising of awareness among staff, compliance audits, real-time attack simulations, etc.

Downstream, i.e. in the event of an attack, the development of non-disruptive and rapid response/recovery capabilities:

- definition of intervention procedures, including a dedicated leadership structure;

- development of cross-business response capabilities (IT and other support functions: communications and public relations, legal functions, marketing, etc.);

- continuous testing of response capabilities and reporting of findings in the event of a response plan being activated.

In addition to these purely technical aspects, it is important to bear in mind that cyber crooks are becoming increasingly savvy, and are capable of hacking into systems via individual users' computers. Alerting staff to the dangers of cyber attacks should therefore form a core part of any cyber defence policy.

The supervisory authority has recognised the challenge cyber risk poses for the insurance sector

As part of its role in stabilising the financial system and protecting consumers, the French supervisory authority, the ACPR, also provides a framework for the fight against cyber crime, related to the principles of Solvency II. Its actions cover four main axes, described by General Secretary Edouard Fernandez-Bollo in a 2015 article in *Revue d'économie financière* as follows:

- "*Encouraging supervised institutions to put in place an effective structure to respond to the threat of cyber attacks;*

- *helping to better identify threats by maintaining a shared record of incidents at European level;*

- *adapting the monitoring of operational risk to better take account of the specific nature of attack threats;*

- *encouraging cooperation between actors in the public and private sectors.*"

3| Cyber risk: an opportunity to create a new type of insurance cover

Regulation and the current environment of heightened anxiety are fuelling demand for protection against cyber risk

Media coverage of recent large-scale cyber attacks (e.g. JP Morgan, Sony, Target) has grabbed public attention and helped to raise collective awareness of the threat of digital technology: no digital system is impenetrable and the repercussions of an incident can be huge.

It is worth noting that, in the United States, which has one of the most mature cyber insurance markets, the sector only began to take off at the end of the 2000s. This was largely due to the introduction of an obligation for companies to notify all parties concerned of leaks of personal data, along with the high financial costs associated with incidents and the filing of class action lawsuits.

In Europe, the obligation to notify stakeholders of data leaks currently only applies to telecoms operators and internet access providers. However, the forthcoming application of the EU data protection regulation in 2018 should extend this requirement to all organisations, and this should no doubt help galvanise the cyber insurance market.

Consequently, even though cyber insurance is currently concentrated in Anglo-Saxon countries and limited primarily to large corporations in the healthcare, technology and retail sectors, in France we should soon see it extending to smaller businesses, which tend to be less cyber resilient, as well as to individuals.

In general, the challenges of cyber security and associated impacts, as well as expectations in terms of cyber insurance and the responses of insurers will differ markedly depending on the type of actor concerned: large corporations or major organisations, including public sector bodies; intermediate-sized enterprises, SMEs or individuals.

The cyber insurance market is differentiated according to the three main categories of customer

In general, the primary objective of large organisations is to avoid cyber attacks, as the costs they generate can be excessive and the reputational damage hard to repair. Moreover, given that the threat of "extreme risks", as detailed below, raises questions over the extent to which large structures are actually insurable against cyber risk, this client category focuses more on fending off attacks through partnerships with third parties, including insurers.

In contrast, intermediate-sized companies and SMEs, which are traditionally less resilient to cyber attacks, tend to want insurance cover as they are less able to absorb the financial costs of an incident, and in some cases could even go bankrupt. They are also likely to want policies offering some form of expertise or services that they do not have internally (e.g. cyber-experts, risk prevention).

Lastly, individuals, whose cyber risk exposure is not particularly difficult to insure, are more likely to look for policies that include services and expertise to help manage the effect of an attack (e.g. e-reputation management or legal advice).

Cyber insurance poses a challenge for traditional methods of risk assessment and pooling and, by extension, for pricing

Limited hindsight with regard to cyber insurance, and the lack of historical data on incident occurrences, make it difficult for insurers to apply traditional methods of risk assessment and pooling, affecting their ability to accurately price cyber policies.

As this is a "new" risk from the point of view of insurance, having access to an extensive database of past claims would help underwriters to refine their actuarial calculations. By observing the frequency and intensity of previous occurrences, they could determine more precisely the maximum risk exposure of potential clients, helping them to decide whether the risk is insurable, set the amount of the excess and any policy exclusions, and calculate the premium.

One of the barriers to building this type of database is the fact that technologies are constantly and rapidly evolving, as are the capabilities of cyber crooks. Any attempt by insurers to categorise cyber threats for evaluation purposes on the basis of past incidents runs the risk of quickly becoming obsolete. In other words, the assumption of continuity, i.e. "*what was true yesterday is still true today*", simply doesn't apply

Box 3

The French cyber insurance market

• The French cyber insurance market has an estimated value of between EUR 405 and 570 million, and currently comprises around a dozen players (AIG, ACE, AGCS, ALLIANZ, XL, CAN, BEAZLAY, Munich RE, Zurich, AXA, etc.). According to a 2015 study by PwC, fewer than 5% of French businesses and 6% of individuals have a cyber insurance policy.*

• Cyber risk policies for businesses usually offer a combination of protection (damages, third party liability, services/expertise), and mainly cover the following:

	Cover offered by the insurer	Services and expertise offered by the insurer
Businesses	• Damages (e.g. cost of restoring data, operating losses, customer notification costs, publication costs, extortion payments) • Third party liability (e.g. legal defence costs if CNIL opens an investigation; e-reputation not usually well covered)	• Cyber security/Management of cyber incidents • Prevention • Crisis communication • Legal assistance • Monitoring
Individuals	• Cover for financial losses in the event of identity theft • Refund of online purchases in the event of a dispute with a vendor • Cover for damages caused by cyberbullying	• E-reputation management (removal/drowning of online information) • Legal assistance (legal information, help in legal proceedings) • Psychological assistance

**Gras Savoye.*

in the case of cyber risk. Moreover, two cyber attacks of the same type can have dramatically different consequences, depending on how they affect the targeted information system (IS), how quickly they are detected and how much information is stored, making it hard to evaluate cyber risk by category.

Another problem with using past claims is the fact that, at any given time, the number of cyber insurance policyholders will be small. With more customers, insurers can pool and offset exposures, according to the law of large numbers. But as with any emerging market, take-up of cyber insurance is still low.

A final difficulty is the interdependency between cyber risks, due to the growing IS interconnection and the tendency for cyber attacks to spread rapidly by contagion, far beyond their initial target and even across national borders. This makes it hard for insurers to apply the principle of risk diversification, as there is a strong correlation between the individual exposures in their portfolio. Even geographical diversification through reinsurance is difficult.

How can we increase the cyber risk cover offered to large businesses or organisations?

Cyber attacks aimed at a large, strategic corporation or organisation can be likened to terrorist attacks or natural disasters – the main difference being that cyber incidents are becoming increasingly frequent and, for the time being at least, have a much less dramatic impact on individuals. To the extent that a large-scale cyber attack on a corporation or organisation has the potential to generate systemic repercussions, its financial consequences could prove way too large for any insurer or reinsurer to cover.[5]

At business level, however, it is precisely these "extreme risks" that risk managers are concerned about and want to protect against.

How can insurers guarantee that the policies they sell are economically viable, and that they can actually provide the specified cover if an "extreme risk" occurs? Finding answers to this question will require in-depth discussions, notably on the possibility of:

- risk underwriters (insurers and reinsurers) pooling together to insure a large and/or sensitive corporation;

- creating a digital protection ecosystem, combining not just insurers and reinsurers, but also cyber security service providers specialised in the professional management of cyber incidents, technology watch and risk mapping, as well as the government which can act as the insurer or reinsurer of last resort and encourage best practices (awareness-raising among the general public, and tightening of regulatory requirements within a framework of international cooperation).

In addition to the issues of insurability and risk assessment, cyber insurance also prompts new questions that go beyond the realm of insurance

Individuals are increasingly conducting their personal lives online, using social networks, emails, smartphones and internet shopping, storing personal data in the cloud, and declaring personal details on public agency websites. All this behaviour is currently regarded as normal and harmless. However, it raises important questions when individuals come to take out cyber insurance, relating to risk assessment, the ownership of digital assets and who should take responsibility for handling the risk.

The market now expects insurers to provide risk prevention and other services

Given the scale of the potential fallout, preventing cyber attacks is absolutely crucial, and insurers are well-placed to assist with this goal, for example, by supplying individual and business customers with best practices in cyber security and anonymised information on incidents experienced by other customers in their database.

5 *A study by Lloyds estimates the economic impact of a cyber attack on the North American power grid, causing a blackout in 15 US states, at between USD 243 billion and 1.0 trillion, and the total claims paid by the insurance industry at between USD 21.4 and 71.1 billion. The data breach suffered by Sony's PlayStation network in 2011 generated costs of around USD 170 million. The Office of Professional Management (OPM) data leak detected in 2015 could cost some USD 330 million.*

However, the technicality and complexity of the risks also means that, as well as helping with prevention, insurers need to set up strategic partnerships with experts in cyber security. This would enable them to better identify the individual needs of new customers, the measures already in place and the risks to which they are exposed, and carry out regular IS audits throughout the duration of the insurance policy. By way of example, certain insurers have set up partnerships with companies such as Thalès and Cassidian (EADS) aimed at increasing companies' awareness of cyber risk and of the need to take preventive action and boost their response capabilities.

In addition, some insurers offer business customers training in crisis management along with advisory services in the event of an attack. Individual customers can also take out e-reputation policies that offer expert help in identifying and dealing with sources of reputational damage, as well as legal assistance if required.

Conclusion

In the space of just a few years, the risks of the digital transition have taken on huge proportions and urgently need to be addressed by all key players in the economy.

In his 2014 book, *The Near Zero Marginal Cost Society*, Jeremy Rifkin – author of *The Third Industrial Revolution* in 2011, and one of the first to predict the economic impacts of a digital age – concluded that there were striking similarities between the digital upheaval and climate change, in that both are undesirable consequences of human progress, both have global causes and consequences, and both have the potential to spark an uncontrollable chain reaction.

In reality, while climate change could indeed spiral out of control, digital risk will only trigger a global catastrophe in extreme cases such as a terrorist war (a nuclear attack by terrorists, for example) and if society, through extreme negligence, fails to put in place adequate defences. The action already undertaken by national governments, a large part of which is not yet visible, is a clear sign that this risk can be brought under control.

With regard to insurance, the recognition of the threats and implementation of risk detection and management capabilities can be regarded as the basic response for today's digital economy, rather than being at the forefront of the field. Indeed, in coming years, regulations such as the EU GDPR and other sector-specific rules will no doubt oblige financial actors to reinforce their security measures. There may not even be a need for a plethora of sector-specific rules, as cyber risk poses a universal threat, and will require close cooperation between industries together with a more integrated approach.

In conclusion, it is possible to identify three main focuses for action to help the insurance industry deal with the risks and opportunities of the digital age:

- Ensure that cyber risk is adequately taken into account in ORSA reports. This will mean defining pragmatic regulatory requirements that are suited to the nature of insurance activities and to the associated risks, and that combine input from both the regulator and industry players in order to provide insight into and methodological guidelines on cyber risk, notably for vulnerable players.

- Identify and, if possible, frame the legal risks linked to the use of personal data, so that they are more visible and therefore more insurable. This needs to be achieved without waiting for the relevant jurisprudence, as the latter takes a long time to emerge and, in the meantime, the legal uncertainty makes it difficult to adequately anticipate risk.

- Foster the development of the cyber insurance market, which currently offers insufficient products. Insurers have the perfect combination of skills – advisory/prevention/compensation – to manage these risks effectively in the French economy and ensure greater economic stability. This means insurers will also need to ensure they have adequate techniques in place to manage their strategic and operational risk (including cyber risk) as only by doing so can they earn a position of trust and become guarantors of stability.

References

ANSSI (2011)
"Information systems defence and security – France's strategy".

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 cybercrime".

Deloitte (2013)
"Cyber-crime fighting".

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

European Parliament, press release (2015)
"MEPs close deal with Council on first ever EU rules on cybersecurity".

L'expansion/L'Express (2014)
"*Cyberattaques : un nouveau marché prometteur pour les assurances*".

Fernandez-Bollo (É.) (2015)
"*Institutions financières et cybercriminalité*", *Revue d'économie financière*.

Fédération française des sociétés d'assurance
"*Les conditions d'assurabilité des cyber-risques*".

HM Government/Marsh (2015)
"UK cyber-security – The role of insurance in managing and mitigating the risk".

IBM (2015)
"IBM 2015 cyber security intelligence index".

Institut d'assurance (2015)
"*Les cyberrisques : conséquences pour l'industrie de l'assurance au Canada*".

Insurance Speaker (2014)
"*Brightside : un acteur du secteur de l'assurance victime d'une cyberattaque*".

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

Marsh (2015)
"European 2015 cyber-risk survey report".

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

PwC Consulting (2016)
"Turnaround and transformation in cybersecurity".

Pwc Consulting (2016)
"*Le marché de la cyber-assurance : la révolution commence maintenant*".

Reuters France (2015)
"*La 2e compagnie US d'assurance santé cible d'une cyberattaque*".

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".

Systemic risk in payments

Georges PAUGET
Chairman
Économie Finance et Stratégie

Payment platforms in the retail and market segments have continued to operate without major mishaps during the recent financial crises, coping with occasional spikes in transaction volumes. Although gratifying, these performances must not cause the risks associated with payment platforms to be underestimated. However, an analysis of the systemic risk in payments cannot be confined to the risk associated with these platforms, even if they play a key role within the overall system. The question has to be tackled more holistically by applying the risk analysis methods used in banking and finance to the payments sector. The following article applies these methods to retail payments, an area that is undergoing far-reaching structural change and whose role is to ensure the security and traceability of commercial transactions.

Systemic risk could be triggered by[1] the failure of a major participant or an external shock that abruptly disrupts the system in a similar manner in both the areas of banking and finance. Participant failure is obviously a danger in the payments sector. But an external shock could also be a trigger, if, say, an event causes a crisis of confidence in a given payment instrument or if a sudden change to tax rules or regulatory requirements results in flight out of certain payment categories. Aware of the situation, regulators have stressed the systemic importance of these platforms and set in train the process of identifying and managing the risks that they pose.[2]

To capture the systemic risk posed by payments, we first identify the changes affecting payment systems (Part 1), before discussing (Part 2) vulnerabilities within these systems that create the potential for a systemic crisis.[3]

1| Changes in the payment sector

Payments are undergoing three big sets of changes. The first is directly linked to the accelerated deployment of innovative technologies, since payments are one of the areas of banking where technological advances are having the greatest impact. Second, changes are arising as new types of usage develop in connection with the digital revolution. Third, regulatory changes are affecting firms' business models and forcing them to make adjustments.

1|1 Accelerated deployment of innovative technologies

This phenomenon can be considered from different angles, including the rise of mobile phones and their expanding range of functionalities and capabilities, and the proliferation of commercial applications available online. The application of these innovations to payment systems has major ramifications. The arrival on the market of global companies specialising in new technologies and either partnering or competing with the major card schemes testifies to the fact that payments have moved out of the banking sphere to become fully integrated with the commercial sector at both the business and operational levels. As a consequence, global, not simply national or European, strategies are being developed and rolled out, although firms may be taking a gradual country-by-country approach to this process. This situation is expected to lead to heightened competition. In parallel, the emergence and swelling ranks of fintechs point to the strength of payment markets and their appeal to tech firms. The initial success of these start-ups will lend added weight to this trend. If past experience in other sectors is any guide, these innovative young businesses will be acquired by larger firms seeking to add a new dimension to these innovations, in which they themselves become key players. These developments will likely drive concentration among large international players, led by mobile providers and internet and telecommunications firms, with niche players surviving by virtue of their flexibility or quality of service.

Another change that is modifying the structure of payment systems is that infrastructures are playing a key role in moulding the overall system. Competition between infrastructures is leading to changes to participants' business and technological models. Two types of infrastructure are in competition, and the struggle is set to become fiercer. The way these infrastructures develop will gradually shape the payment systems landscape. Card schemes, which occupy a central position in developed economies, will continue to expand.[4] Contactless payments, the ability to use cards for any transaction amount, electronic wallets and use of virtual cards for sensitive transactions are all factors that will enable card schemes to maintain their position, although their relative importance is expected to wane over time as mobile phones are increasingly used as payment terminals. Precisely because of this development, it is thought that automated clearing houses (ACHs) will take on a more prominent role.[5] Here again, concentration can be expected. Processing volumes directly determine cost prices, so this is an area where economies of scale really come into play.

1 *Financial Stability Board (FSB)* et al. *(2009).*
2 *FSB (2015).*
3 *Pauget (2012).*
4 *Pauget (2016).*
5 *Edgar, Dunn & Company (2015).*

A third type of infrastructure using blockchain technology could also emerge, although that prospect looks remote right now. This kind of infrastructure is decentralised, in contrast to card schemes or ACHs, which work by centralising transactions. Blockchains can be used to certify execution of transactions. But while some see considerable promise in this technology, it has genuine drawbacks. First, its execution capabilities are subject to time and volume restrictions. Second, transactions are not traceable, so there is a lack of transparency. As with any innovation in its emergent phase, however, blockchains are set to evolve and the existing limitations may be removed over time.

Accelerated deployment of innovative technologies is not the only thing reshaping payment systems, though. With new technologies, usages are changing and demand for services is taking new forms.

1|2 The digital revolution is driving changes in usages

These changes are affecting consumers but also merchants and payment systems operators. As payments increasingly go electronic, behaviours are changing and new expectations are emerging. This is giving more power to brands. If physical devices are used less, consumers need a trusted point of reference, which is what brands offer. In payments, banks have a definite edge over other operators, which may have recognised brands, but not often ones that are associated with payments.[6] Consumers may be reluctant to give their money to firms that do not have an established name in banking. To maintain their advantage, banks will have to engage in major sales and marketing operations and achieve high levels of reliability in execution. They will further increase their advantage by continuing to cooperate with card schemes. Overly direct competition between these two types of players will inevitably lead to value destruction. The strategies followed should seek to differentiate payment systems according to country or region.

Merchants and banks alike can no longer separate the sales act from the payment transaction. Knowledge of customers and their purchases provided by transaction data is becoming ever more decisive as the ability to obtain and harness this information directly affects commercial performances. With the boundary between banking and commercial transactions becoming more blurred, data processing investments are taking on strategic importance. These investments are costly and call on skillsets that are becoming increasingly hard to find. What is more, they have to be undertaken over shorter timeframes than are usual in banks' investment cycles. In this area, banks are competing with major international internet companies with substantial know-how and deep resources. Any hold-up in the necessary investments and hence in the ability to deliver new services will result in lost revenues. The foreseeable consequence of these various developments is continued concentration within the industry, even if (and this is not a contradiction) new fintechs are arriving on the scene with innovative advances that could alter the economics of the sector.

The third major change taking place in the payments sector involves evolving rules and their impact on the shape and intensity of competition.

1|3 New payment rules and their impact on corporate business models.

New rules, whether domestic or European, seek to increase competition in order to reduce trading costs and promote growth in transactions while ensuring good levels of security. Different economic blocks or countries may adopt different approaches to achieving the optimal efficiency/security trade-off, which could lead to non-standardised rules or practices that result in market fragmentation. Precisely for this reason, Europe's authorities have taken action on two levels.

First, they have broken up the monopoly enjoyed by banks in payments. By creating the category of payment institutions, the first Payment Services Directive (PSD 1) opened the market up to new players that are subject to less demanding capital requirements than banks because of the narrower scope of their business. These arrivals use new and less costly technologies and have brought a fresh outlook to the market. Moreover, unlike banks, they

6 *Ministère des Finances et des Comptes publics (2015).*

are unburdened by a technical or HR legacy, which may be challenging to manage. Start-ups such as telco or web operators used the new category to get a foothold on the market. This opening-up holds the seeds of another potentially important change for the sector, namely the separation of payment and deposit management activities, which is clearly the direction charted in the European Commission's 2012 White Paper. It could be that at some point in the future some firms handle payment processing while others specialise in services linked to harnessing the data contained in transactions. Banks will also be able to engage in these activities, but unlike other firms, they will continue to manage deposits, which they alone can guarantee.

The recently adopted Second Directive (PSD 2) further bolstered this trend by allowing new arrivals known as payment intermediaries to enter the market and offer new services, namely initiating transactions on accounts held by banks or payment institutions and/or providing consolidated information on accounts held by a customer with multiple institutions.

The entry of new players drawing on different experiences and know-how will increase and reshape competition. There is no doubt that this will enable new services to emerge as firms strive to differentiate themselves. Another effect of competition is that the prices of basic transactions have already been driven down and this process will continue as such transactions turn into utilities.

Europe's authorities have also acted directly and indirectly to adjust service prices. In the case of the interchange rate, they took indirect measures. Considering that interchange qualifies as an agreement because it leads *de facto* to setting a floor price for the service, the competition authorities challenged the rate and obtained a substantial reduction. This obviously led to lost revenues for banks, but it also altered the balance between banks according to whether their customer rosters chiefly comprise consumers or merchants. Some governments, France's included, took direct steps to regulate prices for basic banking services.

Taken together, technological advances, changes in the behaviour of consumers and merchants, regulatory developments and heightened competition are profoundly affecting the economics of the payment sector and changing the system's risk map. This map needs to be described to identify those risks that are potentially of a systemic nature.

2| Mapping risks in payment systems

There are two main causes of a systemic crisis:

- the failure of a systemically important participant, such as a bank, payment institution or an authorisation or clearing platform. Such status might be based on the entity's size and more specifically its presence within the system but could also reflect the participant's position in the network or the ability to substitute it, immediately or not, with another entity in the event of its failure;

- disruption of the overall system following an external shock, which is what happened recently in Greece. Fears of a government debt default weakened banks and the payment system was severely disrupted.

These twin sources of a system failure may be used to map the risks in a payment system.

2|1 Risks linked to operators

It is important here to draw a distinction between fraud risk and "major" risks.

Fraud risk is analysed, monitored and subject to corrective measures in every system, reflecting the fact that fraud has a two-fold impact. It generates losses for firms, but also, and more importantly, it can undermine participants' confidence in the system if it is too great in volume terms and/or too widespread.

Fraud is increasing steadily, slightly outpacing activity. In France, overall fraud involving payment cards was around EUR 150 million in the early 2000s and this had risen to approximately EUR 400 million by end-2015. Fraud committed abroad accounts for about half the total. The nature of activity has changed considerably too. Distance selling has tripled its share compared with a decade ago and has a fraud rate that is 20 times higher than that of a face-to-face

Europay MasterCard Visa (EMV) payment.[7] This fraud can be contained by developing the EMV protocol and technology and by stepping up cooperation between participants, including merchants, issuers and schemes. Illustrating this point, a feasibility study for the Monnet European card project found that several hundred million euros could be saved if the fraud identified by the Visa and MasterCard networks were handled within a European scheme.

Beyond the overall approach, anti-fraud measures need to be distinguished according to the type of fraud, i.e. whether it is committed by holders or merchants. The major networks keep close tabs on holder fraud. In distance selling, which is a highly exposed sector, this entails close cooperation between banks or payment institutions and e-merchants to analyse data and identify the source of fraud as quickly as possible. Merchant fraud represents the number-one risk of serious fraud for acquirers.[8] This type of risk is more complex to analyse, requiring thorough knowledge of merchants, their business models – particularly revenues – the payment chain, the content of merchant sites and products and services sold. This means that merchants' business profiles have to be continually updated.

While fraud is always costly and potentially disruptive, it is unlikely, given the systems in place, to be responsible alone for a systemic crisis. It is more properly classified as a system vulnerability. These are weaknesses that will not trigger a systemic crisis by themselves but that may nevertheless play a part in its spread.

The same cannot be said for the so-called "major" risks, which can disrupt a payment system or even shut it down, at least temporarily. These are low-probability, high-impact tail risks. To prevent and manage them, affected participants try to make them less likely to occur by setting strict operating rules, monitoring their enforcement through regular audits and following up on recommended corrective measures. If the risk materialises, arrangements to trigger alert procedures and set up crisis units are in place and regularly tested either at institution level or more broadly if supervisors so choose. Prevention and rescue plans are drawn up for each major risk.

A few cases of major risk deserve a more detailed examination.

First, failure of an authorisation or clearing platform, most of which are currently interbank platforms. Shareholder or user institutions must provide capital or guarantees to protect the platform and enable it to cope with incidents, even major ones. These platforms are obviously of systemic importance and supervisors need to check the quality of their management and capital adequacy. From this standpoint, the procedure followed is not going to be materially different from that applied to systemically important banks, although the risk is essentially an operational one.

Another source of major risk involves the simultaneous or near-simultaneous failure of several institutions. Measurements of systemic risk in the banking sector have shown that the failure of just 3% of institutions could cause a crisis.[9] Such an outcome is even more probable if a large number of institutions are affected. Preventing this type of risk is largely based on authorisation procedures for operators. The experience of senior managers and operating personnel, adequacy of resources relative to the volume and complexity of transactions handled, and the amount and quality of capital earmarked to cover risk are all factors to be taken into account. Setting high standards makes a decisive contribution to the security and stability of the system. Difficulties arise because authorisations are not subject to the same requirements across Europe. The resulting distortions are a source of fragility within the system. The existence of weak links in a highly interdependent system such as payments is a major potential risk factor. It could be exacerbated if, with implementation of PSD 2, payment intermediaries are subject to lower requirements than other participants, especially in the highly sensitive area of data protection. They should be made subject to similar requirements to those placed on payment institutions to prevent further distortions and stop new weaknesses from appearing. Moreover, implementation of these provisions must be more effectively coordinated at European level than it has been so far. Harmonisation should also apply to monitoring these various institutions.

7 *Source: GIE Cartes bancaires.*
8 *Source: Dalenys.*
9 *ECB (2015).*

Data capture or tampering is another major risk. Fraudulent use of these data could seriously undermine the confidence of consumers, merchants and the institutions that process transactions, creating the potential for a systemic crisis. Data security is an especially pressing concern as data volumes increase and information is processed by more and more participants.

A second possible cause of a systemic crisis concerns the vulnerabilities within any system that can set the stage for a crisis. These vulnerabilities are not themselves triggers, but their addition makes the system more instable. A situation can thus degenerate into a crisis because of an event that would not have had such a severe impact in another setting. This is why the analysis and management of systemic risk must include taking account of and mitigating these vulnerabilities.

2|2 Payment system vulnerabilities

Vulnerabilities can be divided into two main categories: those linked to new technologies and those associated with the rapid change in business models. They stem from the transformation of payment systems.

The vulnerabilities associated with new technologies are manifold and evolving.

In the first place, these technologies are spreading faster and faster.[10] A consequence of this is that all system participants, operators and supervisors alike, have very little time to adjust. Moreover, not everyone is adjusting or at least not everyone is adjusting at the same pace. This is leading to distortions within the system and hence to the emergence of weak links. Upgrading security protocols with the requisite resources represents one of the most sensitive areas.

A second risk associated with technological advances is the rise of real-time transaction processing. This trend is encouraging the growth of ACHs at the expense of card schemes. In such an environment, every transaction does not have to be authorised in advance, and the notion of payment guarantees associated with cards becomes meaningless as transactions are settled instantly. This could undermine card schemes and promote an increase in direct debits using mobile phones, for example.

A third risk involves the growing amount of data associated with transactions and their processing and aggregation by multiple participants. This risk could take on a new dimension. The data contained in or associated with transactions will be the source for new services to better inform consumers but also to reach out to them more effectively. There will therefore be more data and they will be more complex to process. Most importantly, though, this information will be held or transmitted by a larger number of players with inherently different levels of control, particularly in terms of security, increasing the risk of data compromise.

A fourth risk concerns the rise of virtual currencies. Admittedly these currencies, including the biggest one – bitcoin – still occupy a marginal position. Moreover, their development is constrained by their capacity to process transactions and the speed with which they do this. But these transactions fall largely outside the scope of regulation and supervision. It is only when such currencies are converted into legal currency that they come to the attention of supervisors.[11] This issue also deserves consideration because transactions within the virtual currency system are traceable but anonymous. This lack of transparency explains why bitcoin has been used to circumvent capital export rules in China and Russia.

In addition to the vulnerabilities linked to technological developments, there are others associated with changes to the payments business model, including the arrival of new entrants, changes to market structure and competition, and new rules.

For a long time, payments were a closed system in which banks were the only players. Seen as an extension of deposit management, the business was not typically considered to be a profit centre. In many European banking systems and especially in France, cross-subsidy mechanisms were introduced. Losses from managing cash and cheques were partly offset

10 *Edgar, Dunn & Company (2014).*
11 *ACPR (2014).*

by earnings from direct debits, credit transfers and card issuance and management, with deficits booked against income from non-interest bearing deposits.[12]

The arrival of new entrants challenged this integrated model and its cross-subsidies, leading to price reductions that were either encouraged or imposed by the authorities. Furthermore, for firms operating in the commerce and notably e-commerce sectors, payment is a sales accessory. Payment revenues are unrelated to sales revenues, so these entities can accept low remuneration for payment services. These price reductions have forced many operators to reorganise payment services production to stay competitive. Some firms are specialising in a particular segment of the value chain to improve their efficiency, sub-contracting for other firms that are acting as assemblers. A concentration/specialisation wave akin to that seen in other industries is taking place, resulting in a more complex system and greater interdependency between players. This could potentially exacerbate the system's weaknesses and specifically affect its ability to withstand shocks.

Regulations could further increase the vulnerabilities connected with these shifts in the business model.

Payments are like a heavy industry; they require highly specific skills and major and recurring investments with long depreciation periods. Firms are better placed to enhance their performances when the regulatory environment is stable. This is especially true in the case of rules concerning service prices.

Another factor of potential instability would consist in encouraging a separation between payment and deposit management, which would affect banks first and foremost. The prudential requirements applied to banks have greatly improved their ability to stand up to crises, making them an island of stability in the payments system. This special position needs to be preserved at a time when the economics of the system are changing.

Last but not least, regulatory requirements designed at the European level and transposed country by country could lead to increased market fragmentation. The fact is that despite SEPA and the PSD, the European payments market remains extremely fragmented. For example, there is no bona fide pan-European operator. The two entities that could potentially lay claim to such a title are Visa and MasterCard. But these two US groups do not cover all payment services. Fragmentation can be reduced only by two things: shared requirements on consumer disclosures and harmonised and coordinated authorisation and oversight procedures for participants.

The emergence of a European payments industry would be good for the system's stability and security. This would entail changes to the doctrine of the European Commission's Competition Directorate, which is ill-suited in this regard.

3| Conclusion

The retail payments system is undergoing deep-seated changes. The arrival of new entrants that are not all subject to the same regulations and supervision, greater uncertainty over profitability, and the swift deployment of new technologies increase the system's vulnerability. Weak links are appearing, and systemic risk is growing. To properly control these developments, the supervisory system needs to extend in practice to all participants and be conducted on a closely coordinated basis within Europe.

12 *Pauget and Constans (2012).*

References

Autorité de contrôle prudentiel et de résolution (2014)
ACPR Position, P-01 29 January.

Edgar, Dunn & Company
Pôle Finance Innovation (2014)
« *La filière des moyens de paiement, le fleuron caché de l'industrie française* », April.

Edgar, Dunn & Company(2015)
"Payment innovation trends and implications for the schemes", Speech by Peter Sidenius, Mobey Forum, Warsaw, 9 December.

European Central Bank (2015)
"Systemic risk, contagion, and financial network", *Financial Stability Review*, November.

Financial Stability Board (2015)
Reports describe progress in implementing OTC derivatives market reforms, and highlight where further work is needed, 4 November.

Financial Stability Board, International Monetary Fund and Bank for International Settlements (2009)
"Guidance to assess the systemic importance of financial institutions, markets and instruments", "Initial considerations", "Report to G20 Finance Ministers and Central Bank Governors", October.

Ministère des Finances et des Comptes publics (2015)
Assises des Paiements, June.

Pauget (G.) (2012)
Banques : le grand saut ? Éditions de la Revue Banque, June.

Pauget (G.) (2016)
"*Europe-Afrique : les facteurs clés de succès des systèmes de paiement. Analyses et perspectives*", in D. Saidane and A. Lenoir. Banque et Finance en Afrique. Éditions de la Revue Banque, January.

Pauget (G.) and Constans (E.) (2012)
"L'avenir des moyens de paiement en France", Report to the Minister of Economy, Finance and Industry, May.

Financial institutions and cyber crime
Between vulnerability and security

Quentin GAUMER, Stéphane MORTIER and Ali MOUTAIB
Club cybersécurité – École de Guerre économique, Paris

In the current world, financial institutions, like other companies, have become increasingly dependent on their information systems. These systems allow them to conduct business transactions (transfers, account management, withdrawals, etc.) and at the same time exercise control over the information exchanged.

More and more, information is becoming the target of cyber attacks from different groups of cyber criminals. They use strategies such as social engineering (human intelligence, manipulation) or more sophisticated techniques (such as advanced persistent threats – see the case of Carbanak). 2015 was a major year for cyber security actors. The cyber crime events of that year were highly instructive for the banking sector, enabling them to adjust their defence tactics and increase their resilience.

Despite the efforts of security companies and the evolution of CISOs' (Chief Information Security Officer) strategies, cyber criminals are constantly updating their fraud methods. Security actors now have to increase their awareness of cyber crime techniques and enhance their monitoring in order to face the new threats to corporates, including those targeted at the banking sector.

As observed last year, hackers have started to shift towards a strategy where they target financial institutions instead of end-users. There were many examples of attacks on point-of-sale systems and ATMs with a significant financial impact for the banks. The trend should be maintained over the coming years, with hackers increasingly trying to find breaches in stock markets and payment systems.

In addition, cyber criminals are already shifting their focus to smartphones due to the growing use of smart mobile devices. On the one hand, alternative payment systems such as Apple Pay or Google Pay will push hackers to monetise fake stolen credit cards. On the other hand, the spread of transactional malwares on mobile devices is likely to increase markedly.

Improving resilience is a major financial stability issue, as it is vital to prevent cyber attacks or IT failures from escalating into systemic crises. However, creating the best possible protection for financial institutions will never reduce to the risk of a cyber attack to zero. Financial institutions also need to have the best possible plans to resume their activities as quickly and efficiently as possible after a breach in their IT systems.

States, institutions, companies and the general public are facing new kinds of vulnerabilities due to the sharp increase in the size, importance and scope of digital activities:

- actions violating international treaties or national laws made in cyberspace or via a computer system (cyber crime);

- hacking into public institutions, corporations or personal files to gain access to confidential information. The aim is to collect personal or economic advantage (cyber espionage);

- acts of terrorism using computer systems or computer technologies as a weapon or target. Cyber terrorism can be motivated by political, social or religious concerns. The aim is to induce fear, provoke panic or destabilise a population, an institution, a company or an army, etc.

- risk of information or computer warfare in relation or not to a real armed conflict. This would take the form of a cyber conflict involving cyber attacks and consequently the implementation of a cyber defence.

"Cyber" is the key prefix to be used whenever topics of risk and crime are discussed. All types of digital activities are potentially affected. Cyber crime is one of the major issues for financial and banking institutions, but also for any large organisation. The executive management and CISOs are under constant pressure to ensure information and internal data are secured, while at the same time making sure that business needs are appropriately covered.

Securing banking systems' assets requires prevention and anticipation, with processes to measure and react to different risks and threats. The financial industry faces different challenges today, mostly linked to the merging of classical cyber crime threats (carding, phishing, etc.) and targeted threats (APT,[1] data leaks, etc.). Cyber criminal groups have turned their attention away from end-users as they see more opportunities in attacking the financial institutions themselves and looking for valuable data to steal, or hacking directly into their point-of-sale systems and ATMs. The Carbanak campaign, identified by Kapersky Lab, is one of the biggest cyber attacks ever discovered. The operation targeted financial organisations and led to the theft of hundreds of millions of dollars.

We could also see a rising trend where cyber criminals focus directly on stock exchanges using subtler means of interference, such as attacks on high-frequency trading (targeting algorithms) in order to generate long term and stable gains with less chance of getting caught.

1| From cyberspace to cyber security

First, why use the word "*cyber*"? The Greek word "kubernan" means "to guide and govern". Yet cyberspace is to a great extent a territory without frontiers, or at the very least appears to be without controls and without rules. The word cyberspace was coined in 1984 by the novelist William Gibson, one of the leading figures of the cyberpunk movement.[2] His novel *Neuromancer* depicts cyberspace as a dystopian and abstract world where information flows freely, and the lines between reality and fiction are sometimes blurred. In real life, cyberspace is where dematerialised flows are stored and traded (Chawki, 2006). John Perry Barlow, the founder of the Electronic Frontier Foundation, went so far as to issue the following Declaration of the Independence of Cyberspace in February 1996: "*Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather*."

In this sense, cyberspace is a kind of utopia, without government and without controls. But cyber crime also thrives in cyberspace. Indeed, it is clear that cyberspace is used by all sorts of criminals for all sorts of purposes, and even if it is not without rules, it is extremely difficult to control it, to track down criminals and to impose sanctions. Moreover, the issues related to cyberspace cannot always be adequately understood and tackled at national (i.e. State) level.

1 *APT: advanced persistent threat (a network attack in which an unauthorised person gains access to a network and stays hidden and undetected for a long period of time, monitoring the network and/or stealing data.*
2 *Cyberpunk is a current of science fiction set in a near future, in a highly technologically advanced world.*

During the last decade, a lot of progress has been made in the implementation of international or regional instruments to fight cyber crime. These instruments are vary in effectiveness, but show an increasing level of awareness.

All of these instruments are essentially inspired by the Council of Europe's Convention on Cyber Crime (2001). This convention was the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security (UNODC, 2013).

Most national policies on cyber security were founded after this convention. In France, the *Agence nationale de la sécurité des systèmes d'information* (ANSSI – the National Agency for Information Systems Security) defines cyber crime as follows: "*Acts that are violations of international treaties or national laws, using networks or information systems as ways of committing an offence or a crime, or having them for a target*."

Because there are cyber criminals, we need to find ways and means to enforce rules and provide protection, hence cyber security. Cyber crime and cyber security cover a wide range of fields. Sieber (1998) defines the following fields: protection of privacy, economic criminal law, protection of intellectual property, illegal and harmful contents, criminal procedural law and security law.

Although the real purpose of Sieber's list is to make a classification of legislative initiatives, the first four fields provide a typology of cyber crime offences: acts which undermine personal data, economic IT offences, acts undermining intellectual property rights, harmful and illegal content.

Other specialists, like Professor David L. Carter (1992) from Michigan State University, divide cyber crime into two categories:

- acts where the computer system is the target of the offence;

- acts where the computer system is the vector of the breach. The computer system is merely a tool for a more traditional offence.

Regardless of the type of offence, financial institutions, as any other major corporation, are vulnerable – and not just financial institutions as such, but also financial transactions, information heritage, the personal data of workers and customers, insider trading, financial transfers, ATMs, etc.

2| Overview of cyber crime in financial institutions

2|1 Where are we now?

Regulatory authorities have taken various steps to ensure the security of financial institutions' systems. These actions are designed to provide security standards and enforce internal security processes.

According to the recommendations of these authorities cyber security risk management should cover different areas such as audits, regular tests and the periodic evaluation of cyber security monitoring.

The financial industry also has to focus on developing different actions that limit their risk of being hacked to as great an extent as possible:

- identity and access management: prevention and control of any attempt by an unauthorised entity to access the system and its data (remote access, logins, and passwords, help desk protocols to address customer login problems and direct access);

- data leak prevention (management and protection of sensitive documents and storage in the system);

- awareness campaigns and training: training programmes for employees in order to raise their awareness of how to apply internal security processes within the institution;

- incident response planning: definition of incident responses to ensure that the reaction to a major attack on the system is adequately managed (planning, training of an incident response team and crisis management plans);

- security governance: definition of a clear management plan to ensure fluid communication between the CISO, the security department and the top management.

2|2 What are the current trends?

Despite the fact that they have defined strong security processes, and bearing in mind that total protection will always be impossible and that cyber criminals' capabilities are constantly evolving, financial institutions will have to face different and rising threats to their business in coming years. One of the most important relates to the increasing use of mobile devices, which will certainly lead to the development of financial malwares targeting smartphone users.

Additionally, the main threat to financial institutions will be from the inside, in the form of intentional leaks of sensitive and strategic information to competitors or to a cyber crime organisation.

Focus on mobile malware

Driven by the sharp increase in smartphones and tablet users, fraudsters and cyber criminals are adapting their schemes to target financial apps and building new patterns to monetise their fraud operations. As the infection rate is on the rise, security measures on mobile channels should be reinforced, especially for the financial industry.

What kinds of mobile malware are most prominent? Transactional malware remains the main threat on the mobile channel, with approximately 30 per cent of the distinct variants targeted at stealing financial information.[3] These malicious programs can perform many operations on smartphones and other similar devices, like stealing personal data, reading and sending SMSs, keylogging and stealing sensitive information.

How does it work concretely? A user working in a financial institution could receive a spear phishing e-mail and then download the Trojan horse malware onto his/her device. The Trojan is then activated to retrieve system administrator permissions. It can then perform as many malicious acts as needed (such as setting new passwords, storage encryption, etc.) The hacker can then access sensitive documents, financial information or personal data and sell them on the black market.

In the underground market, demand for mobile hacking kits is rising as hackers are increasingly focusing on mobile technology, to carry out infection campaigns by loading Trojans onto users' devices.

Mobile infection is consequently a major and rising threat against end users, but also for financial organisations. Numerous processes are being deployed to ensure mobile security within financial companies. However, the risk of human error still exists, even if a Master Data Management (MDM) system can control the mobile equipment of the company. In addition, many users actually jailbreak or root their devices in order to access unofficial app stores or get free applications and, in doing so, open a breach for hackers and fraudsters.

Data leaks and insiders

Information dissemination is a major issue for companies, especially for financial institutions. Despite the protections put in place by these institutions against external threats, recent studies[4] show that insider threat remains a serious risk to their security schemes. The increasing number and complexity of devices and systems, and constant changes in their usage, make these threats more difficult to detect.

The main goal of these types of internal attack is still to gain some form of financial advantage, and industrial espionage.

Companies should notice and detect any employee's intent to harm, or lead training campaigns to avoid unintended mistakes by employees. The methods used can differ and can have a serious impact on the activity of the company. Below are some examples of actions that fraudsters can take:

- social engineering: collection of sensitive data by manipulating an employee in a targeted company (e.g. phishing, malware, phoning);

- data leakage: exfiltration of sensitive information from a sensitive company via an inside employee, using a profitable reward.

3 *IBM (2015).*
4 *Vormetric (2015).*

3| The main risk is human error and malicious behaviour

3|1 Social engineering – An updated modus operandi

Over time, the modus operandi and attack capabilities of cyber criminals have evolved, and so too have their goals. The hackers of the early days of the internet were motivated by ego, by the thrill of the challenge and the desire to prove their computer abilities. Today, their motivations are different. Cyber criminal organisations are now highly organised. Some take the form of criminal groups, like the mafia, and some, perhaps the most impressive, operate as a form of IT service company. Indeed, it is possible to use the services of one or more hackers to attack one or more targets. These outfits are organised like a real company and can offer a new breed of after-sales service.

Hackers use technical skills, but not only in the field of computer science. They also become skilled in exploiting human frailties to launch cyber attacks (e.g. phishing), and have developed social engineering capabilities to achieve their goals. Hackers do not hesitate to get in touch with their target (human target) by e-mail, telephone or via a real meeting in order to build trust and manipulate their victim's behaviour.

As part of the fight against social engineering attacks, there are two main issues within financial institutions and especially banks. Indeed, banks and other financial institutions can be the primary target of an attack; but they can also be a secondary-level target through their customers, especially in retail and corporate banking. The best way to reduce the risks of such an attack is staff awareness (all staff need to be trained: chairman, directors, managers, secretaries, accountants, switchboard operators, etc.). Like all companies, financial institutions need to carry out simple awareness programmes:

• about phishing: not to trust emails, being as vigilant as possible, checking addresses and spelling mistakes, being careful with mail.com or gmx (global message exchange);

• about attacks by telephone: ensuring caller authentication, not transmitting sensitive information (login, password, personal telephone number, private information, etc.), establishing a callback procedure, etc.

For a few years now, an attack named "false international transfer order fraud" has been affecting companies, notably in France. The modus operandi is traditional phishing to obtain the logins and passwords used by the company to connect to its bank website. After obtaining these pieces of information, hackers can order money transfers to their own bank account. As time passes, the modus operandi is becoming increasingly complex. Generally speaking, cyber criminals (specialists in human intelligence) make a telephone call, apparently originating from the chairman of the company to an accountant. The hacker asks to make a money transfer within the framework of a confidential foreign merger and acquisition operation. Often a second call is made by a fake business lawyer (also a specialist in human intelligence) to give more details about the transaction. The accountant then makes the money transfer because he/she has been manipulated into making it. The effective breach is human frailty and not a computer intrusion or lack of cyber security. This case raises very serious legal questions about the bank's responsibility in authorising the transfer. In France, legal responsibility can be attributed to the bank in some situations. Indeed, banks have to verify all signatures on the transfer order and warn their customers if there is any doubt over a document or a transaction (case law of the French *Cour de Cassation*).

To avoid problems, financial institutions have to run awareness programmes for their customers.[5] However, awareness programmes alone are not sufficient and additional security measures are needed. For example, many banks don't send e-mails to their customers and prefer to use internal mail posted on the bank's website. Responses to social engineering are human but also technical.

5 *Examples :* 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
Different public administrations make awareness for companies (Intelligence service, police, Gendarmerie nationale*, etc.).*

3|2 Social engineering – A first step towards compromising information systems

As described above, social engineering is one of the first possible steps towards initiating a more complex cyber attack, such as an APT. These targeted attacks implement all possible techniques in order to compromise a computer system. Human intelligence via social engineering is used to obtain technical and technological information about the target and its environment. This modus operandi was particularly used in the case of the Carbanak attack.

Carbanak is a textbook case studied by numerous cyber-security specialists. At the end of 2013, several banks and financial institutions around the world were the target of a major cyber criminal organisation, which has yet to be identified. The total financial damage could be up to USD 1 billion. Kapersky, one of the leaders in information system security, published a detailed report on this case[6] after having been involved in identifying the attack and helping clients to sanitise their IT systems. According to the report, about 100 banks were targeted and approximately 50% of them suffered financial losses. Most of victims (financial institutions) were located in Russia, the United States, Germany, China and the Ukraine. To infiltrate banks and commit a new type of burglary, hackers used the technique of spear phishing. First, information system administrators were personally targeted: they received an e-mail with a malware in an attached document. Second, the malware was executed on sensitive computers (those of system administrators). Third, hackers were able to study the bank's information systems over time (they remained dormant within the systems for several months), identify established security measures and therefore discover vulnerabilities, the security breaches. This left the door open for the burglary, which was carried out using the following methods:

- use of the bank system to make money transfers to the hackers' own bank accounts;
- wrongful crediting of accounts and transfer of the overpayment to the hackers' own bank accounts;
- reprogramming of ATMs to distribute money to an accomplice standing in front of the machine (no need for a bank card or pin number). It was actually because of a dysfunctional ATM in Kiev that the Carbanak attack was identified.

This kind of cyber attack is a new type of hold-up without guns, violence and hatred, and foreshadows the future of crime against financial institutions: human intelligence, technical operations, burglary.

Financial institutions have reached a certain stage of maturity in the field of cyber security and are able to measure the technical level of a malware by themselves or using a service provider. But the first vulnerability, in particular in the case of Carnanak, is human frailty. So awareness will always be necessary, whatever the level of technology.

4| Going further: ensuring financial stability in the face of cyber crime

At the international level, cyber crime has been taken on board by the Committee on Payments and Market Infrastructures (CPMI) and a first report was published for consultation in November 2015.[7] Market infrastructures are critical to the functioning of the financial system and could generate significant systemic consequences if they were affected by cyber attacks.

The work on financial institutions and banks in particular, is not as advanced. The Financial Stability Board has identified and regularly updates a list of global systemically important banks (so called G-SIBs)[8] and a list of global systemically important insurers (G-SIIs).[9] A list of non-bank non-insurance systemic financial institutions is also currently being considered. The financial

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

institutions identified as systemic have to meet specific requirements in order to take into account the consequences of their potential failure for the markets.

As regards financial stability, the worst-case scenario would be a cyber attack targeting systemic financial institutions and making them go to resolution. It makes no sense for a burglar such as the criminal organisation behind the Carbanak case to go for such an extreme attack. In order to steal money, the attack has to be as discreet and limited as possible, to avoid counter-measures. So is there a risk? Two possibilities:

- an attack initiated by a competitor or a group of competitors in order to modify market shares and gain importance: an unlikely move from a financial institution considering the consequences if it were made public, but not impossible. It's a case of economic warfare;

- a politically or religiously motivated cyber attack launched to create a diversion or financial mayhem.

The awareness programmes already mentioned and the technical IT protection implemented by financial institutions are not sufficient to guarantee that such an extreme scenario would never occur. More work is needed at international level; not only to prevent the attacks as far as possible, but also to maintain resilience in the event of successful attacks. Financial institutions have to be able to maintain their vital functions and their basic services even if their IT system is shut down, and public authorities have to be prepared to react and provide support if need be. Synergies between financial institutions and public authorities are needed more than ever.

Combining strong defences and strong resilience is the best way to ensure financial stability in this context.

Conclusion

In the real world, financial institutions are increasingly shifting their operations to cyberspace, and this new world reflects today's society. No country, no company, no organisation, no financial institution, no one can escape this reality. And, as in the world around us, there are criminals lurking in cyberspace. Just as a sovereign state is required to protect its territory and guarantee the security of its residents, so an entrepreneur must protect his/her company by taking the necessary steps to defend its information systems and make them resilient to cyber attacks.

Financial institutions are no exception to this rule. Cyber attacks against financial institutions generally take advantage of a mix of technical and human vulnerabilities. Most financial activities are dematerialised but carried out by human beings. And humans use computers, smartphones, social networks, etc. and the internal information systems of their employers. In addition to the technical aspects of cyber attacks, there are human frailties. The need for sensitive information in order to launch a technical attack involves human intelligence. Both are intimately linked.

Fighting cyber crime requires the involvement of all financial institutions. This means organising awareness campaigns for employees and management staff, so that they can detect suspicious activities. The dissemination of information and good practices on cyber security is crucial. In this regard, we can highlight a number of government initiatives.[10] Financial institutions are taking steps in the same direction. For example, clubs such as Luxembourg for Finance organise conferences on digitalisation, financial technology and security. There is a real awareness of the issues at stake, but more can still be done. In particular, putting human beings back at the centre of things and keeping them there is absolutely crucial. At international level, more work is needed to coordinate efforts towards resilience.

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

References

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, July.

De Villenfagne (F.) and 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*, No. 1.

IBM (2015)
Security Trusteer Report.

Sieber (U.) (1998)
"*Legal aspects of computer-related crime in the information society – COMCRIME Study*", prepared for the European Commission.

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, February.

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

Where are the risks in high frequency trading?

Thierry FOUCAULT
Professor of Finance
HEC Paris

Progress in information and trading technologies have contributed to the development of high frequency traders (HFTs), that is, traders whose trading strategies rely on extremely fast reaction to market events. In this paper, the author describes HFTs' strategies and how they rely on speed. He then discusses how some of these strategies might create risks for financial markets. In particular, he emphasises the fact that extremely fast reaction to information can raise adverse selection costs and undermine incentives to produce information, reducing market participants' ability to share risks efficiently and asset price informativeness for resources allocation. The author also discusses recent extreme short-lived price dislocations in financial markets (e.g. the 2010 Flash crash) and argues that these events are more likely to be due to automation of trading and structural changes in market organisation rather than high frequency trading per se*. Throughout he argues that regulation of high frequency trading should target specific trading strategies rather than fast trading in general.*

A very important role of financial markets is to facilitate risk sharing among investors. To this end, the finance industry constantly innovates, by creating new financial instruments or new ways to trade (see Allen and Gale, 1994). Changes in trading technologies over the last thirty years offer a very good example. Trading has become increasingly automated, first in stock markets and more recently in derivatives, foreign exchange, and bond markets. Exchanges have replaced their trading floors by automated matching systems[1] and human traders (brokers or proprietary trading desks) are progressively replaced by machines and algorithms. This evolution also led to changes in the way information is disseminated to traders and gave rise to new forms of trading. In particular, automated trading allows extremely fast reaction to events and some trading firms' business models (so called high frequency traders) exploit this feature.

As other financial innovations, this evolution and high frequency trading raise many questions. For regulatory purposes, one must understand what are economic forces driving the growth of high frequency trading and their effects on the ability of financial markets to efficiently perform their functions (in particular risk sharing). In this paper, I discuss these points in light of recent academic findings regarding high frequency traders. My goal is not to provide an exhaustive survey of the quickly growing literature on this topic but rather to identify sources of risks associated with high frequency trading that deserve regulatory attention.[2]

1| Algorithmic and high frequency trading

Algorithmic trading encompasses a wide variety of strategies. For instance, brokers use algorithms to optimally slice and dice their orders over time and across different trading platforms (using so called smart routers) to reduce their price impacts and therefore execution costs for their clients. These strategies often call for frequent order submissions and cancellations, resulting in a sharp increase in the traffic on electronic trading platforms (see Chart 1).

Chart 1
The evolution of the quote-to-trade ratio
(nr. orders/nr. trades)

Source: Foucault, Kozhan, Tham (2015).
The figure shows the evolution of the quote-to-trade ratio around the introduction of Autoquote API on Reuters D-3000 (a trading platform in currency markets) in July 2003. Autoquote API allow computers to automatically enter orders on Reuters D-3000 without human intervention. Its introduction marks the beginning of algorithmic trading on Reuters D-3000.

Some proprietary trading firms' strategies rely on extremely fast reaction to market events, very broadly defined. For instance, a market event might be the arrival of news about a stock, a quote update for this stock, or a trade in assets with correlated payoffs (e.g. an option on the stock or a futures on a market index). To be fast, these firms invest in technologies that help them to minimise their trading "latencies", i.e. the time it takes for them to receive messages from data providers (e.g. trading platforms or data vendors such as Bloomberg, or Thomson-Reuters), process these messages, make a trading decision (e.g. the submission of a market order, a limit order, or the cancellation of orders previously submitted to the market), and finally implement this decision. For instance, they will invest in high speed connections to markets and data vendors, e.g. by buying the right to locate their servers in very close geographical proximity to trading platforms' own data servers (a practice known as "co-location") or by subscribing to direct data feeds to receive market data a split second before other market participants.[3]

These firms are usually called "high frequency traders" (HFTs). HFTs are one type of algorithmic traders because their strategies are computerised.

1 *For instance, the Paris Bourse switched to electronic trading in 1986 and the Chicago Mercantile Exchange closed its pit in July 2015.*
2 *See Biais and Foucault (2014) and SEC (2014) for more detailed surveys of the literature on high frequency trading.*
3 *For instance, in the United States, trading platforms must transmit their data to plan processors (the Consolidated Tape Association and Consolidated Quote Association), which consolidate the data and distribute them to the public. As this process takes a few milliseconds, market participants with direct access to the trading platforms' data feeds can obtain market data even faster than participants who obtain the data from plan sponsors (for a discussion, see SEC 2010, §IV.B.2). In Europe, there is yet no consolidated datafeed for stocks traded in multiple platforms.*

However, another defining characteristic of HFTs, not common to all algorithmic traders, is the very high speed at which they operate. For instance, using data on orders submitted by 15 HFTs on Nasdaq OMX Stockholm, Baron *et al.* (2015) find that the average minimum time elapsed between the submission of orders by the fastest traders in their sample is below one millisecond (of the order of one microsecond for the fastest trader). Well known independent trading firms with high frequency operations include KCG, Virtu, Flow traders, or Tradebot. Broker dealers and banks (such as Goldman Sachs, Morgan Stanley or Deutsche bank) or hedge funds (e.g. Citadel or Renaissance) also have high frequency trading desks.

There is so far no clear legal or regulatory definition of high frequency trading, which creates difficulties to analyse their effects on financial markets and regulation.[4] They are usually defined as being characterised (see SEC, 2010) by: (i) the placement of a large number of orders, (ii) the use of very high speed and algorithms to generate and execute their orders, (iii) the use of co-location services and individual data feeds provided by exchanges, (iv) the entry and exit of positions over very short time frames, (v) a high cancellation rate for their orders, and (vi) small end of the day positions.

Researchers rarely have access to datasets that "flag" orders with an identifier allowing them to distinguish orders placed by high frequency trading desks from orders placed by other market participants. Thus, they have often relied on indirect methods to identify those orders (see SEC, 2014 for a review of empirical studies on high frequency trading and the datasets used in these studies). Hence, one must be careful in interpreting existing empirical findings about high frequency trading. In particular, empirical regularities uncovered in these studies might in fact be due to strategies of participants that in fact are not HFTs.

Keeping this caveat in mind, estimates indicate that HFTs account for a significant share of the trading volume in electronic markets. For instance, for US equities markets, a report from the Tabb Group estimated that HFTs accounted for 51% of the number of shares traded in the United States. For twelve European trading platforms and 100 stocks, a study from the ESMA (2014) finds that pure HFT firms (i.e. excluding high frequency trading desks of investment banks) account for 24% of the value traded. HFTs are also present in foreign exchange markets, treasury markets, or commodities markets.

2| High frequency traders' trading strategies

The effects of HFTs on market quality are likely to depend on their trading strategies. Hence, before discussing these effects, it is useful to describe these strategies. They can be broadly classified in three categories: high frequency market making, high frequency arbitrage and high frequency directional trading.

2|1 High frequency market making

Market-makers post bid and ask quotes at which they stand ready to buy or sell shares of an asset. Thus, they are intermediaries between final sellers and buyers of an asset. For instance, a market maker might buy a stock from one investor at some point and then resell it after a while to another one. Alternatively, when the same asset is traded in multiple trading platforms (as in United States and European stock markets), a market maker can buy the asset on one platform (e.g. BATS in Europe) from one investor and resell it on another platform (e.g. Euronext).

Market makers are exposed to various risks (see Foucault, Pagano, and Röell, 2013): (i) the risk of fluctuations in the value of their positions ("inventory risk"), (ii) the risk of trading with better informed investors ("adverse selection risk") and (iii) the risk of trading at stale quotes when news arrives ("picking off risk"). Their bid-ask spread (the difference between the price at which they sell and the price at which they buy) is a compensation for these risks and therefore increases when they are higher. Bid-ask spreads are often used as measures of market illiquidity.

In principle, fast reaction to market events can alleviate some risks inherent to market making. First, by allowing market makers to turn around

4 *MIFID II defines high frequency trading as* "algorithmic trading that relies on computer program to determine the timing, prices or quantities of orders in fractions of a second."

their positions more quickly, speed can help them to reduce their inventory risk.[5] Second, speed allows market makers to update their quotes faster when news arrives, which reduces their exposure to the risk of trading at stale quotes.

Thus, speed can be a way for market makers to reduce their costs and thereby to post more competitive bid-ask spreads. In line with this idea, Brogaard *et al.* (2015) find that traders who subscribe to the fastest co-location service on Nasdaq OMX Stockholm have characteristics of market makers and that an upgrade in this service reduced their exposure to the risk of being picked off and their inventory costs.

2|2 High frequency arbitrage

Arbitrage opportunities between related assets are pervasive at the high frequency. For instance, consider an exchange traded fund (ETF) on a stock index. In theory, the price of the ETF must be equal to the value of the index (the value of the portfolio of constituent stocks of the index) at any point in time. If instead, the price of the ETF is above (below) the value of the index, an arbitrageur can immediately buy (sell) the portfolio of constituent stocks and sell (buy) the ETF, at a profit. In practice, such arbitrage opportunities appear frequently in ETF markets for two reasons. First, large buy or sell orders in the ETF (or constituent stocks) exert transient price pressures on the ETF, creating an arbitrage opportunity. Second, when information arrives, quotes for ETFs and constituent stocks are not updated at the same time (e.g. quotes in underlying stocks tend to be updated with a lag relative to quotes in the ETF market). This lack of perfect synchronisation in the adjustment of prices to information also give rise to arbitrage opportunities. The same type of opportunities arise more generally between derivatives assets (CDS, futures, options, etc.) and their underlyings, in currency markets (e.g. so called triangular arbitrage), between stocks traded on different platforms etc.[6]

These arbitrage opportunities are extremely short lived: they disappear as soon as market makers update their quotes or an arbitrageur exploit the opportunity. For instance, Budish *et al.* (2015) find that the median duration of arbitrage opportunities between the SPDR S&P 500 ETF (SPY) and the E-mini S&P 500 future from January 2005 to December 2011 varies from 250 milliseconds (in 2006) to about 10 milliseconds (in 2011). They also find on average 801 opportunities per day that deliver a potential profit of USD 98.01 per opportunity. Thus, a trader can exploit these small but frequent fleeting opportunities only if he is very fast. This has been another major impetus for the development of high frequency trading (see, for instance, Chaboud *et al.*, 2014 for a discussion in the context of currency markets).

2|3 High frequency directional trading

HFTs can also take position in anticipation of future price movements. This type of strategy is called "directional" because traders take a position in an asset in the direction of their expectation of a future price movement (e.g. they buy a stock if they expect its price to increase). Speed might be useful for this type of strategy because it enables traders to react faster to news.

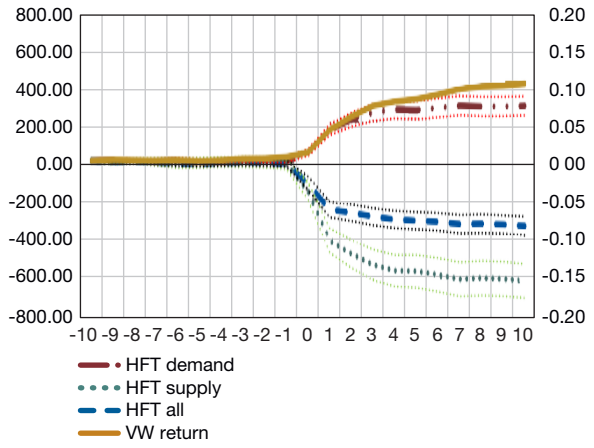
For instance, consider Chart 2 (taken from Brogaard *et al.*, 2014). The bold plain line shows the average price change over the ten seconds following the arrival (date 0) of "positive" (i.e. higher than expected) macroeconomic announcement for a sample of 120 Nasdaq stocks over the 2008-2009 period. On average, macroeconomic news in their sample moves prices by about 10 basis points in the 10 seconds following the news. Hence, a trader who reacts fast enough (say, in 10 milliseconds) to the release of positive macroeconomic news can expect to make a small profit on average by buying the stock. Brogaard *et al.* (2014) show that this is what some HFTs do. The dashed dotted line in Chart 2 shows the aggregate cumulative (over time) difference between

5 *For instance, consider a market maker with a long position in a French stock that trade on multiple markets (e.g. Euronext and BATS). If one particularly high bid price for the stock is posted on one market, a fast market maker can take advantage of this opportunity to unwind his position before other sellers take advantage of this bargain.*

6 *See, for instance, Ben-David* et al. *(2015) for evidence on arbitrage opportunities in ETF markets, or Chaboud* et al. *(2014) and Foucault, Kozhan and Tham (2015) for evidence of arbitrage opportunities in currency markets.*

Chart 2
Positive macro news

(x axis: seconds around macro news announcements)
HFT order flow USD 10,000 *Returns in %*



Source: Brogaard, Hendershott and Ryordan (2014).

"aggressive" purchases and sales (i.e. executed with marketable orders) by HFTs in Brogaard *et al.* (2014)'s sample. Similarly, the dotted line shows the aggregate cumulative difference between "passive" purchases and sales (i.e. executed with limit orders) by high frequency traders in this sample.[7]

Clearly, some high frequency traders quickly accumulate a significant long position (by placing buy market orders) just after the arrival of the positive macro news, presumably in anticipation of the price rise that materialises in the subsequent 10 seconds. Interestingly, other HFTs (those who trade with limit orders) sell shares just after the announcement, as the dotted line shows. The symmetry between the dashed dotted line and the dotted line suggests that in fact the latter do not have time to revise their quotes after the news arrival and get adversely executed ("picked off") by HFTs who are fast enough to take advantage of the macro announcement before prices adjust (see Dugast, 2015 for a model of price adjustments after news that formalises this scenario).

Macroeconomic announcements only constitute a small fraction of all "news" in a given day. In fact, progress in information technologies enable traders to react to a myriad of signals that in principle could move market prices. Accordingly, some information providers (such as Thomson-Reuters, Bloomberg, or Dataminr) now provide buy and sell signals extracted from raw information available in social medias such as tweeter.[8] Moreover, market data (quotes, trades, order submission etc.) themselves constitute a piece of information about future price movements.[9] Having access to these data faster is another way to anticipate price movements in the short run. Consistent with this idea, Brogaard *et al.* (2015) find that lagged one second returns of futures contracts on the OMXS30 index forecast the direction of market orders submitted by fast traders in their sample (30 Swedish stocks constituents of the OMXS30 index), suggesting that these traders use information in future returns to forecast impending price changes in constituent stocks (see also Zhang, 2012 for similar findings).

Another source of advantage for high frequency traders might stem from their ability to process vast amount of data quickly due to their massive investments in computers and efficient algorithms. This capacity might be useful in particular to better filter out noise from market data and thereby obtain more accurate signal to forecast future price movements. Foucault, Hombert, and Rosu (2016) derive the optimal trading strategy of an investor who reacts faster to news and filters out noise from news more efficiently than other market participants. They show that speed matters: the equilibrium trading strategy of the investor is significantly different from that of an investor who is just skilled at processing information (as in traditional models of trading with asymmetric information).

In addition, HFTs' computing power (and sophisticated data analysis techniques) might help

7 *A limit order is an order to buy or sell a given number of shares at a given price. In general, this price is such that the order cannot be filled immediately. In this case, a limit order is stored in a limit order book until another investor accepts to trade at its price or until the limit order submitter cancels his order. "Marketable orders" are orders to buy or sell a given number of shares at a price such that they can be filled upon submission against other limit orders standing in the limit order book. Trading platforms often refer to marketable orders as "aggressive" orders in the sense that their submission triggers a trade. Limit orders are "passive" in the sense that their execution can only be triggered by the arrival of a marketable order.*

8 *See "Mining for tweets of gold",* The Economist, *June 7, 2014, or "How investors are using social medias to make money",* Fortune, *December 7, 2015.*

9 *This is in fact consistent with theories such as Grossman and Stiglitz (1980) or Blume, Easley, and O'Hara (1994) that predict that market data such as stock prices or trading volume contain information that can be used to forecast future returns.*

them to detect footprints left by other traders when the latter execute large orders (see Hirshey, 2013 and van Kervel and Menkveld, 2015 for evidence). Indeed, such large orders are often split in a chain of smaller orders (called "child orders") to reduce their impact on prices. The detection of early child orders in this chain might then be useful to forecast the arrival of later child orders.

This "order anticipation" strategy might be profitable for at least two reasons. First, traders placing large orders might themselves be informed. Thus, their buys (sales) forecast a price increase in the future (decrease). In this case, it is optimal for order anticipators to mimick these trades (see Yang and Zhu, 2015 for a theoretical analysis). In this scenario, order anticipators compete away informed traders' profits. Second, traders placing large orders might be forced to liquidate a large position because of funding needs (e.g. an hedge fund might liquidate a large position to meet margin calls). Such forced liquidation by distressed traders generally occur at discounted prices. As shown by Brunnemeier and Pedersen (2005), traders who correctly infer the presence of such a distressed trader have an incentive to (i) initially trade in the same direction as the distressed trader to amplify the downward price pressure due to the distressed trader's orders and (ii) eventually buy the asset at a deep discounted price (Brunnermeier and Pedersen, 2005 refer to this strategy as "predatory trading").

Using data on HFTs' orders and institutional investors on Nasdaq OMX, Menkveld and van Kervel (2015) do not find evidence that HFTs in their sample engage in predatory trading around large institutional trades. Indeed, they appear to trade against early child orders from institutional investors, thereby dampening their impact on prices. However, HFTs eventually turn around their position and start trading in the same direction as early child orders. This behaviour might be consistent with either optimal risk management by HFTs or the "order anticipation hypothesis" according to which HFTs "mimick" institutional investors' informed trades, once they have inferred the presence of such investors from past trades.

High frequency traders have also been accused to engage in price manipulation. In particular, two strategies ("momentum ignition" and "spoofing") have attracted attention. "Momentum ignition," consists in placing buy market (or sell market orders) in the expectation that this behaviour will induce other traders to do the same. The flurry of buy orders that ensue might then push prices up, allowing the "momentum ignitor" to liquidate his position at a profit. "Spoofing" consists in entering, say, buy limit orders and cancelling them quickly in the hope that this will induce other traders to buy the asset and allow the manipulator to gain from execution of sell limit orders at inflated price. This practice is banned by the Dodd-Frank act and, recently, several traders have been charged of "spoofing" in the United States.[10]

Defining price or market manipulation is difficult, both in legal and economic terms (see Fishel and Ross, 1991 and Kyle and Viswnanathan, 2008). In particular, as Kyle and Viswanathan (2008) point out, it is difficult to distinguish between trading strategies that undermine both price informativeness and liquidity (which Kyle and Viwanathan, 2008 view as manipulative) from trading strategies that might look manipulative, but which just consist in rational exploitation of market power and private information. Several models show that the optimal behaviour of informed investors can be complex and counter-intuitive and yet their trades make prices more informative and do not intend to be manipulative.[11] The same problem arises for interpreting the intent of HFTs' order submission patterns.

Market making, arbitrage, directional trading, order anticipation, and manipulative strategies have a long history in financial markets and they have all been extensively analysed by economists. What is novel is the intensive use of information technologies to implement these strategies and the way they are implemented. On this, very little information is available because high frequency trading desks see this implementation as the source of their competitive advantage and naturally make all efforts to protect their "secret sauce."[12]

10 *See "Flash crash: trading terms and manipulation techniques explained",* Financial Times*, April 22, 2015 and "Regulators step up efforts to stop spoofing",* Financial Times*, November 5, 2015.*

11 *For instance, Back and Baruch (2004) show that randomising between buy and sell orders can be a way to minimise trading costs for an informed investor.*

12 *A good example is Alexei Aleynikov's case. He was charged of stealing high-frequency trading code from Goldman Sachs (see "Ex-Goldman programmer guilty of stealing code",* New York Times*, May 2015).*

As different strategies leave different footprints in the data, it is possible to infer – to a limited extent – HFTs' strategies. For instance, market makers tend to mainly use limit orders (so called passive orders) while directional traders who seek to profit from very short term price changes should predominantly use marketable orders (as limit orders take time to execute and might not execute at all). In a recent survey of the empirical literature, the SEC notes that: "*Perhaps the most noteworthy finding of the HFT Dataset papers is that HFT is not a monolithic phenomenon but rather encompasses a diverse range of strategies. In particular, HFT is not solely, or even primarily, characterized by passive market making strategies that employ liquidity providing orders [...] Moreover, the level and nature of HFT activity can vary greatly across different types of stocks*." (SEC, 2014).

This observation is important because the effects of high frequency trading on market quality are more likely to depend on the type of strategies that fast traders use (see below) than speed *per se*. In practice large high frequency trading firms are likely to be opportunistic and use a strategy as long as it is profitable (and, hopefully, legal) and exit it when it becomes unprofitable. The data however suggests that there is some degree of specialisation among high frequency trading firms, some appearing to be more specialised in market making while others more specialised in arbitrage or directional trading (see Hagströmer and Norden, 2013).

3| High frequency trading: risks and benefits

High frequency trading has attracted a lot of media and regulatory attention, with claims from popular writers that high frequency trading could harm other market participants and threaten the integrity of financial markets (see, in particular, Michael Lewis, 2014). A key issue is whether high frequency trading enhances or undermines (i) market liquidity for risk sharing and (ii) pricing "accuracy", i.e. the informativeness of asset prices for resources allocation since risk sharing and information production are two important functions of financial markets. Another concern is that high frequency trading may jeopardise market stability. I discuss these points below.

3|1 Private vs. social benefits

As explained previously, HFTs massively invest in trading technologies and information. This suggests that they individually benefit from these investments. The social benefit of these investments is less clear, however. Indeed, they give an edge to HFTs in accessing to information and reacting fast to it, which is a source of adverse selection for other participants.

For instance, consider Chart 2 again. It shows that some HFTs place buy market orders just after the arrival of positive macroeconomic news and slightly in advance of a price increase due to these news. The gain made by these traders on their buys is a loss for their counterparties, who are "adversely selected" by better informed parties. More generally, empirical evidence on high frequency trading (see, for instance, Baron, Brogaard, and Kirilenko, 2014 or Brogaard, Hendershott, and Riordan, 2014) suggests that market orders from HFTs are informed (anticipate on future price movements) and thereby generate adverse selection costs for their counterparties (including HFTs specialising in liquidity supply). For example, Brogaard, Hendershott, and Riordan (2014) write (on page 2268): "*We show that HFTs impose adverse selection costs on other investors*."

One might argue that this is not a problem because fast trading on information is just a monetary transfer from fast to slow traders, i.e. a zero sum game. This redistribution can be perceived as unfair (for slow traders) but there is no welfare loss in aggregate. Biais, Foucault, and Moinas (2015) show that this argument is incomplete for two reasons. First, adverse selection implies that all traders bear larger impact costs when they trade. As the cost of trading gets larger, investors with small gains from trade (relative to the cost of trading) trade less (e.g. hedge risks less efficiently) or stop trading. Second, investment by HFTs must be accounted for in computing the social gains and benefits of this activity. If this activity just serves to play a zero sum game then its social cost is equal to the resources allocated to it. These resources are significant. For instance, the Project Express by Hibernia Atlantic drew a new fiber optic cable across the Atlantic, to increase by 5 millisecond the time to connect Wall Street to the City at a cost USD 300 million. Eventually, the cost of this project has to be covered by fees charged to firms using this cable to get fast access to information. For 2013 alone, the Tabb Group estimates the investment in

fast trading technologies at USD 1.5 billion, twice the amount invested in 2012 (see *The Wall Street Journal*, 2014).

Not all HFTs are directional traders, however. As explained previously, some use their fast access to markets and information for market-making. If, in this case, trading speed reduces the cost of market making (inventory costs and the cost of being picked off by faster traders) or if it intensifies competition among market makers then HFTs should reduce transaction costs for investors. Moreover, if high frequency market-making reduces the cost of intermediation then this reduction is a social benefit.

It has been difficult so far to separately measure the effects of various type of trading strategies used by HFTs. Indeed, empiricists often observe HFTs' actions (order submissions, trades etc.), directly or indirectly, but not the strategies that command these actions. Yet these are the strategies that matter for observed effects. For instance, Brogaard *et al.* (2016) analyse the evolution of liquidity measures (e.g. the effective bid-ask spread) for 30 stocks on Nasdaq OMX around an up-grade in colocation services provided by Nasdaq OMX. They find that this up-grade results in an improvement in liquidity (smaller bid-ask spreads). Decomposition of this effect shows that the upgrade has two effects: (i) it results in smaller "realised bid-ask spreads" (a measure of per trade profit net of adverse selection costs for market makers) and (ii) larger price impacts (a measure of adverse selection costs borne by market makers). The decrease in realised spreads is consistent with investment in speed intensifying competition among market makers while the increase in price impacts is consistent with investment in speed increasing exposure to adverse selection for market makers.

The decrease in realised spreads more than offsets the increase in price impacts in Brogaard *et al.* (2016)'s sample so that, in net, investment in speed (co-location up-grade) appears beneficial. This analysis however shows the importance of measuring separately the effects of various strategies (maybe the benefit of co-location up-grades could have been even stronger if co-location could not be used to implement directional strategies).

Regulatory interventions about high frequency trading should therefore target specific trading strategies rather than high frequency trading in general. Indeed, regulation should not discourage high frequency trading when it serves to decrease trading costs for investors. In contrast, it should discourage strategies that exploit small differences in the speed of access to information about future price movements.

Consider for instance the proposal to tax traders when their order-to-trade ratio exceeds a certain threshold (as planned by MiFID II). Such a tax makes cancellations of their orders more costly for traders who mainly use limit orders, i.e. those who most likely are market makers. These traders need to frequently cancel their limit orders to (i) optimally control their inventory risk (cancellations can be part of an optimal inventory management strategy), (ii) reduce their exposure to the risk of trading at stale quotes, (iii) account for information contained in trades in other trading platforms (see van Kervel, 2015). If canceling orders become more costly, high frequency market makers must therefore raise their bid-ask spreads because their costs of market making increase. In contrast, directional traders (those trading on information) mainly submit market orders. Thus they naturally have smaller order-to-trade ratios. Hence, a tax on order-to-trade ratios is rather counterproductive: it discourages high frequency market making (which is likely to improve liquidity) while having no effect on directional HFTs (who harm liquidity). A more effective tool would be to add a very small random delay to the execution time for market orders. Indeed, this delay should reduce HFTs' ability to pick off stale quotes while leaving the possibility to traders submitting limit orders to revise their quotes.

3|2 Foreknowledge vs. discovery

In addition to facilitate risk sharing and the realisation of gains from trade, another important function of financial markets is to produce information. That is, asset prices aggregate informed investors' signals and thereby convey information for real decisions, e.g. investment (see Bond, Edmans, and Goldstein, 2012).[13] Thus, one potential benefit

13 *For instance, Fama and Miller (1972, p.335) write:* "An efficient market has a very desirable feature. In particular, at any point in time market prices of securities provide accurate signals for resource allocation; that is firms can make production-investment decisions."

of informed trading is that by making prices more informative, it also makes real decisions more efficient.

A natural conjecture is that by trading faster on information, high frequency directional traders accelerate the speed at which prices reflect information. Brogaard *et al.* (2014) find supportive evidence. They show that HFTs trade in the opposite direction to transitory pricing errors and in the same direction as permanent changes in asset value. In other words, HFTs' make prices closer to a random walk, as should be the case in an informationally efficient market. There is also evidence that the growth of algorithmic trading is associated with more short-lived arbitrage opportunities (see Budish *et al.,* 2015 for evidence about cross market arbitrage in ETFs and Chaboud *et al.,* 2014 for triangular arbitrage).

It does not follow however that HFTs make prices more *informative* as signals for resources allocation.[14] Hirshleifer (1971) distinguishes "foreknowledge," i.e. information about a state that, in due time, will be known to all, from "discovery," i.e. the production of information that would not be known without active human intervention. This distinction is very relevant to think about the effect of high frequency trading on price informativeness. Indeed, consider again the case of positive macroeconomic announcements in Chart 1. By observing macroeconomic news slightly faster than other traders, some HFTs obtain foreknowledge of an information that will be evident to all in a few seconds. By trading fast on this information, they accelerate the speed at which prices reflect this information, making markets more informationally efficient. However, they do not "discover" information: the macroeconomic announcement takes place whether or not some traders observe it very fast. In contrast, an analyst that combines various data about a firm to assess its value produces information that would not be available otherwise. By trading on this information, the analyst incorporates in prices information that would not otherwise be available.

There is no evidence so far that HFTs contribute to incorporate in asset prices information that otherwise would not be available. In fact, to the extent that HFTs reduces profits from discovering information, they might make asset prices less informative. For instance, Dugast and Foucault (2016) consider a model in which investors can choose to trade on raw information (e.g. buy or sell signals based on the content of tweets; see *Fortune*, December 7, 2015.) or on processed information (information processing is a form of discovery). Processed information is more accurate but processing information takes time. Thus, trading on raw information is a form of fast trading. They show that a reduction in the cost of access to raw information can discourage the production of processed information and thereby make prices less informative in the long run. Interestingly, Weller (2016) finds empirically a negative relationship between measures of algorithmic trading in US stocks and the extent to which prices contain information upon forthcoming earnings announcements. This suggests that the incentive to produce information about firms' fundamentals is smaller in stocks with a high level of algorithmic activity.

3|3 Fragility vs. reliability

In recent years, US financial markets have experienced several severe but short price disruptions. Three events are particularly noteworthy.

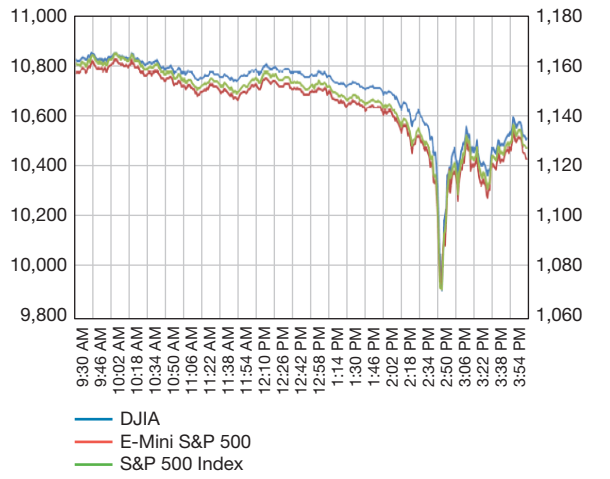
- **The flash crash of May 6, 2010 (see Chart 3)**. Over an interval of 30 minutes starting at 2:32 p.m. (Eastern Time), US stock indices, exchange traded funds, and index futures experienced very large upward and downward price movements. In particular, the Dow Jones lost about 6% in about five minutes, with stocks trading at very distorted prices (e.g. Accenture at one penny per share or Apple at USD 100,000 per share). The crash affected stock markets, exchange traded funds and futures markets. By 3:00 p.m., prices had reverted to levels close to their pre-crash level.

- **The Treasury flash crash of October 15, 2014 (see Chart 4)**. Between 9:33 and 9:40 a.m., the yield on the US 10-year Treasury bond fell by

14 *The reason is that the notion of informational efficiency is defined with respect to the "stock" of available information. It says nothing on amount of available information itself. If there is no information available, asset prices will be completely uninformative, even if they are informationally efficient.*

Chart 3
End-of-minute transaction prices of the Dow Jones Industrial Average (DJIA), S&P 500 Index, and the June 2010 E-Mini S&P 500 futures

(contract on May 6, 2010 between 8:30 and 15:15 CT)



Source: CFTC/SEC Staff Report, "Preliminary Findings Regarding the Market Events of May 6, 2010", 2010.
Note: This figure presents end-of-minute transaction prices of the Dow Jones Industrial Average (DJIA), S&P 500 Index, and the June 2010 E-Mini S&P 500 futures contract on May 6, 2010 between 8:30 and 15:15 CT.

Chart 4
10-year Treasury yield in cash market on October 15

Source: US Department of the Treasury, Board of Governors of the Federal Reserve System, Federal Reserve Bank of New York, SEC and CFTC, Joint Staff Report (2015), Chart 2.1.

16 basis points. The entire Treasury bonds and futures yield curve was affected as were, to a lesser extent, interest swaps and equity markets. By 10:00 a.m., yields were back to their level before the outset of the crash.

- **The exchange traded fund (ETFs) flash crash of August 24, 2015**. At the opening of the market, at 9:30 a.m. on August 24, 2015, the price of several exchange traded funds in the United States declined significantly relative to the indices that they track. For instance, the SPDR S&P 500 ETF (SPY) opened for regular trading hours at a discount of 5.2% relative to its previous day closing. This discount deepened further by 7.8% by 9:35. The SPY price then quickly reverted above the opening price. The drop in price for the SPY relative to the previous day price was one of the largest in the last decade (see SEC, 2015). The 50 largest exchange traded products (about 40% of all these products) experienced a decline in prices by more than 10% (SEC, 2015). Moreover, from 9:30 a.m. to 9:45 a.m., a large number of large capitalisation stocks on the NYSE and Nasdaq experienced drop in prices larger than 10%.

All these events share some common features. First, the extreme price movements observed during these events are accompanied by a sharp decline in liquidity of the affected markets (see Joint Staff Report, 2015 for the Treasury flash crash and CFTC/SEC Staff Report, 2010 for the 2010 Flash crash). Thus, these crashes are both price and liquidity crashes. Second, they happened without apparent changes in fundamentals. In fact, in each case, the quick price reversal that follows the initial high drop or spike in prices suggests that these price movements are not due to a change in fundamentals. Third, multiple assets are affected, maybe due to spillovers effects between asset classes linked by no-arbitrage relationships.

In addition, market participants claim that "mini flash crashes" (sudden drop or spike in prices followed by a price reversal in few seconds in one asset) happen routinely in today's markets.[15] These flash crashes are labeled "mini" because they do not simultaneously

15 *For instance, according to an article from the* Huffington Post*: "*[…] mini-flash crashes happen all of the time now. Just Monday, shares of Google collapsed briefly in a barely noticed flash crash of one of the country's biggest and most important companies." *(See* Huffington Post*, 2004). Similarly, Nanex (a financial data provider) reports more than 18,000 mini flash-crashes from 2006 to 2010 in US equity markets, that is, about USD 195 per month (Nanex defines a flash-crash as an up or down price movement greater than 0.8% in less than 1.5 second). See* http://www.nanex.net/FlashCrashEquities/FlashCrashAnalysis_Equities.html

affect a wide number of assets, in contrast to the three crashes discussed above. Yet, these events are potentially problematic because they might potentially be a catalyst for wider market disruptions.

In the aftermath of the 2010 Flash crash, several commentators suggested that high frequency trading might have played a role in the crash and that high speed trading was making markets more fragile. For instance, in September 2010, speaking before the Security Traders Association, Mary Schapiro, then Chairman of the Securities and Exchange Commission (SEC), said: "*Given their volume and access, high frequency trading firms have a tremendous capacity to affect the stability and integrity of the equity markets. Currently, however, [they]…. are subject to very little in the way of obligations either to protect that stability…. in tough times, or to refrain from exacerbating price volatility…. An out-of-control algorithm…. can also cause severe trading disruptions that harm market stability and shake investor confidence*."

Yet, it is far from clear that HFTs played a role in flash crashes and detailed reports by public agencies on these events do not show or even suggest that HFTs were directly responsible for these events (see, for instance, SEC, 2015, Joint Staff Report, 2015 or CFTC/SEC Staff Report, 2010). In fact, the cause(s) of flash crashes (or mini flash crashes) and the mechanisms for propagation of shocks across asset classes are still far from being well understood. It is likely that these events are due to a combination of factors and that automation, rather than speed of trading alone, might have played a role.[16]

In fact, it is useful to recognise that the automation of trading creates new operational risks.[17] Consider first the growth of algorithmic trading. Several recent events show that errors in the design of these algorithms can be a source of serious failures in financial markets. For instance, the IPO of BATS Global market failed on March 23, 2012 because the algorithm used to run the electronic auction for this IPO went wrong.[18] Another example is the loss by Knight Capital (a major broker-dealer in the United States until 2012) of 440 million in 30 minutes on August 1, 2012 due to an ill-designed algorithm, leading to the acquisition of Knight by one of its competitor (GETCO).

Trading platforms' matching systems and data feed used to disseminate information on market conditions can also experience technical glitches. For instance, on July 9, 2015, a computer glitch (due to the rollout of a new software) led to a trading halt of two hours on the NYSE. Automation might also leverage people ability to engage in market manipulation or deliberate attempt to affect the integrity of financial markets (for terrorism purpose for instance). For example, in April 2015, an independent London-based trader (Mr. Navinder Singh Sarao) was charged by US authorities of directly causing the Flash crash using a "spoofing" strategy (see Section 2).[19] Another example is "quote stuffing", a strategy that consists in deliberately increasing the number of messages (e.g. limit order submission followed by cancellations) sent to a trading platform to slow down other traders (e.g. the speed at which they receive information from exchanges' datafeed).[20]

The race for quick access to trading platforms or market data can also be a source of operational risk when it leads to traders to bypass safety checks. For instance, for risk management purpose, trading firms usually embed in their algorithms automated checks of their orders, to guarantee that they do not expose the firm to too large risks. Yet, these checks take time and therefore conflict with economic incentives to be fast for HFTs. Similarly, brokers usually impose automated risks limits on their clients. However, high frequency trading firms often bypass these automated limits by requiring so called direct market access (DMA) to again increase the speed at which they can submit orders to markets.

Given the automation and increasing complexity of financial markets, it should not be surprising that technological mishaps sometimes happen as it is

16 *Other possible factors might be market fragmentation (see Madhavan, 2012) or changes in the nature of liquidity provision, in particular the disappearance of designated market makers.*

17 *The Basel Committee on Banking Supervision (2001) defines "operational risk" as:* "The risk of loss resulting from inadequate or failed internal processes, people, and systems or from external event."

18 *Ironically, BATS operates one of the major electronic trading platform in the United States and in Europe.*

19 *The case is not settled. It is unclear whether Mr Sarao's orders were manipulative and unclear whether, if so, they could alone have triggered the Flash crash (see* Financial Times*, 2015).*

20 *See Ye, Yao, and Gai (2013) for evidence on quote stuffing.*

the case in other industries (e.g. transportation). Kumiega, Sterijevski, and van Vliet (2016) argue that one should therefore use notions from industrial engineering such as "reliability", which is an estimate of the probability of a mishap event, to evaluate the performance of financial markets and their fragility. They claim that from this perspective financial markets are on par with other industries. For instance, Gao and Mizrach (2015) have measured the frequency of large but transient price movements during the day (which they call "breakdowns" or "breakups") in US stocks.[21] They find that the frequency of such events has decreased since 2000 to less than 1% per stock-day in recent years, in contrast to the perception that they are more frequent. More empirical work is needed to assess the reliability of current market structures.

Several recent regulatory initiatives aim at reducing operational risks due to algorithmic trading (including high frequency trading) and automation. For instance, according to the SEC's Regulation Systems Compliance and Integrity rule (SEC, 2013), exchanges and traders using computerised trading systems must "*establish written policies and procedures reasonably designed to ensure that their systems have levels of capacity, integrity, resiliency, availability, and security adequate to maintain their operational capability and promote the maintenance of fair and orderly markets, and that they operate in the manner intended*" (p. 3). The rule would also require exchanges and traders to regularly test their systems and have disaster plans in place. MiFID II in Europe has qualitatively similar provisions for the algorithms used by HFTs. For instance, according to MiFID II, HFTs will have to develop effective systems and risk controls and to report their algorithmic strategies to regulators.

As mentioned previously, the May 2010 Flash crash or the Treasury flash crash were accompanied by a sudden evaporation of liquidity. This evaporation suggests that one source of fragility stems from a change in the nature of liquidity provision in electronic markets. In particular, one concern is that high frequency market makers do not have the ability to provide significant liquidity in times of market stress or might even withdraw from the market in such times. Again, academic evidence on this issue is scarce and does not particularly support the view that liquidity provision by high frequency market makers is particularly more fragile than that of human market makers. Using Nasdaq data, Brogaard *et al.* (2015) find that, on average, HFTs in their sample trade against extreme price movements, whether these movements correspond to permanent (e.g. due to information arrival) or transient price changes. In contrast, non HFTs' orders are positively correlated with the direction of extreme price movements. These preliminary findings suggest that HFTs dampen rather than exacerbate extreme price movements.

The nature of liquidity provision in financial markets might have changed in recent years. In particular, it is possible that liquidity provision is less resilient in case of large shocks. However, again, there might be multiple causes for this evolution and, so far, there is no evidence that HFTs are a direct cause. In fact, banks have cut the amount of capital that they allocate to market making activities in various markets (due to the financial crisis and new regulations such as the Dodd-Frank act in the United States). New players (including HFTs and hedge funds) might replace banks as liquidity providers but these are probably more lightly capitalised and therefore have a smaller risk bearing capacity. This evolution in itself might make liquidity in financial markets more prone to sudden evaporation than in the past.

21 *They define a "breakdown" (resp., breakup) for a stock as a larger than 10% drop (resp., increase) in its price relative to its level at 9:35 a.m. with a reversal of at least 2.5% by 3:55 p.m.*

References

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

Back (K.) and Baruch (S.) (2004)
"Information in securities markets: Kyle meets Glosten-Milgrom", *Econometrica*, 72, pp. 433-465.

Baron (M.), Brogaard (J.), Hagströmer (B.) and Kirilenko (A.) (2015)
"Risk and return in high frequency trading", available at: *http://dx.doi.org/10.2139/ssrn.2433118*

Ben David (I.), Franzoni (F.) and Moussawi (R.) (2015)
"Do ETFs increase volatility?", *Working paper*, Ohio State University.

Biais (B.) and Foucault (T.) (2014)
"HFT and market quality", *Bankers, Markets and Investors*, January-February.

Biais (B.), Foucault (T.) and Moinas (S.) (2015)
"Equilibrium fast trading", *Journal of Financial Economics*, 116, pp. 292-313.

Blume (L.), Easley (D.) and O'Hara (M.) (1994)
"Market statistics and technical analysis: the role of volum", *The Journal of finance*, 49(1), pp. 153-181.

Bond (P.), Edmans (A.) and Goldstein (I.) (2012)
"The real effects of financial markets", *Annual Review of Financial Economics* 4, pp. 339-360.

Brogaard (J.), Carrion (A.), Moyaert (T.), Riordan (R.), Shkilko (A.) and Sokolov (K.) (2015)
"High frequency trading and extreme price movements", available at: *https://www.rsm.nl/fileadmin/home/Department_of_Finance__VG5_/LQ2015/Ryan_Riordan.pdf*

Brogaard (J.), Hagströmer (B.), Norden (L.) and Riordan (R.) (2015)
"Trading fast and slow: colocation and market quality", *Review of Financial Studies*, forthcoming.

Brogaard (J.), Hendershott (T.) and Riordan (R.) (2014)
"High frequency trading and price discovery", *Review of Financial Studies*, 27, pp. 2267-2306.

Brunnermeier (M.) and Petersen (L. H.) (2005)
"Predatory trading", *Journal of Finance*, 60, pp. 1825-1864.

Budish (E.), Cramton (P.) and Shim (J.) (2015)
"The high frequency trading arms race: frequent batch auctions as a market design response", *Quartely Journal of Economics*, 130, pp. 1547-1621.

Chaboud (A.), Chiquoine (B.), Hjalmarsson (E.) and Vega (C.) (2014)
"Rise of the machine: Algorithmic trading in the foreign exchange market", *Journal of Finance*, 65, pp. 2045-2084.

Commodity Futures Trading Commission and Securities & Exchange Commission (2010)
"Preliminary findings regarding the market events of May 6, 2010", *Staff Report*, May 18.

Commodity Futures Trading Commission and Securities & Exchange Commission (2010)
"Findings regarding the market events of May 6, 2010", Staff Report, September 30, available at: *https://www.sec.gov/news/studies/2010/marketevents-report.pdf*

Department (US) of the Treasury, Board of Governors of the Federal Reserve System, Federal Reserve Bank of New York, SEC and CFTC (2015)
Joint Staff Report, available at: *https://www.treasury.gov/press-center/press-releases/Documents/Joint_Staff_Report_Treasury_10-15-2015.pdf*

Dugast (J.) (2015)
"Unscheduled news and market dynamics", *Working paper*, Banque de France.

Dugast (J.) and Foucault (T.) (2016)
"Data abundance and asset price informativeness", available at: *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2398904*

ESMA (2014)
"High frequency trading activity in EU equity markets", *Economic Report*, 1, pp. 1-30.

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

Financial Times (2015)
"Ex-SEC economist to testify on flash crash", October 22.

Fishel (D.) and Ross (D.) (1991)
"Should the law prohibit 'manipulation'", *Harvard Law Review*, 503.

Fortune (2015)
"How investors are using social medias to make money", December 7.

Foucault (T.), Hombert (J.) and Rosu (I.) (2016)
"News trading and speed", *Journal of Finance*, 71, pp. 335-382.

Foucault (T.), Kozhan (R.) and Tham (W. W.) (2015)
"Toxic arbitrage", available at: *http://dx.doi.org/10.2139/ssrn.2409054*

Foucault (T.), Pagano (M.) and Röell (A.) (2013)
Market liquidity: Theory, evidence and policy, Oxford University Press.

Gao (C.) and Mizrach (B.) (2015)
"Market quality breakdowns in equities markets", available at: *http://dx.doi.org/10.2139/ssrn.2153909*

Grossman (S.) and Stiglitz (J.) (1980)
"On the impossibility of informationally efficient markets", *The American Economic Review*, 70(3), pp. 393-408, June.

Hagströmer (B.) and Norden (L.) (2013)
"The diversity of high-frequency traders", *Journal of Financial Markets*, 16, pp. 741-770.

Hirschey (N.) (2013)
"Do high frequency traders anticipate buying and selling pressure", *Working paper*, London Business School.

Hirshleifer (J.) (1971)
"The private and social value of information and the reward to inventive activity", *American Economic Review*, 61, pp. 561-574.

Huffington Post (2004)
"Twitter causes a flash crash, highlighting market' structural problems", February 23.

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

Joint Staff Report (2015)
"The US treasury market on October 15, 2014", available at: *https://www.treasury.gov/press-center/press-releases/Documents/Joint_Staff_Report_Treasury_10-15-2015.pdf*

Kumiega (A.), Sterjevski (G.) and van Vliet (B.) (2016)
"Beyond the flash crash: Systemic risk, reliability, and high frequency financial markets", *Working paper*, University of Illinois.

Kyle (A.) and Viswanathan (S.) (2008)
"How to define illegal price manipulation?", *American Economic Review*, 98, pp. 274-279.

Lewis (M.) (2014)
Flash boys – A Wall Street Revolt, W. W. Norton & Company.

Madhavan (A.) (2012)
"Exchange traded funds market structure and the flash crash", available at: *http://dx.doi.org/10.2139/ssrn.1932925*

Security Exchange Commission (SEC) (2010)
"Concept release on equity market structure".

SEC (2013)
"Regulation systems compliance and integrity".

SEC (2014)
Equity market structure literature review, Part II: High frequency trading, staff of the division of trading and markets, pp. 1-37.

Van Kervel (V.) (2015)
"Competition for order flow with fast and slow traders", *Review of Financial Studies*, 28, pp. 2094-2127.

Van Kervel (V.) and Menkveld (A.) (2015)
"High-frequency trading around large institutional orders", *Working paper*, Vrije Universiteit.

Wall Street Journal (2014)
"High-speed stock traders turn to laser beams", February 11.

Weller (B.) (2016)
"Efficient prices at any cost: does algorithmic trading deter information acquisition?", *Working paper*, Northwestern University.

Yang (L.) and Zhu (H.) (2015)
"Back-running: Seeking and hiding fundamental information in order flows", *Working paper*, MIT.

Ye (M.), Yao (C.) and Gai (J.) (2013)
"The externalities of high frequency trading", *Working paper*, University of Illinois.

Zhang (S.) (2012)
"Need for speed: An empirical analysis of hard and soft information in a high frequency world", *Working paper*, University of Manchester.

Regulation and policies to address these new risks

Making Europe's financial market infrastructure a bulwark of financial stability

Yves MERSCH
Member of the Board
European Central Bank

Europe's financial market infrastructure has proved to be resilient through bouts of financial market volatility, supporting the liquidity and stability of financial markets in times of stress. The European Central Bank and the Eurosystem, in conjunction with European legislators and market participants, have made Europe's financial market infrastructure into the bulwark of financial stability it is today. Looking ahead, besides a further deepening of integration, the focus in the further development of market infrastructure is on the impact of technological innovation such as distributed ledger technologies. To deal with the technological and strategic challenges, the Eurosystem has developed three key action points it will work on in the run up to 2020: 1) explore synergies between TARGET2 and T2S, 2) support the development of a pan-European instant payment solution, and 3) review the harmonisation of Eurosystem arrangements and procedures for collateralisation.

Europe's financial market infrastructure, including systemically important payment systems, central counterparties (CCPs) and securities settlement systems, has proved to be resilient through bouts of financial market volatility, supporting the liquidity and stability of financial markets in times of stress.

An abrupt reversal of global risk premia, weak profitability prospects for banks and insurers in a low nominal growth environment, debt sustainability concerns in the public and non-financial private sectors, and the risk of stress in a rapidly growing shadow banking sector have been identified in the European Central Bank (ECB)'s most recent review as major risks to financial stability.[1] While those aspects rightly take the centre stage in the financial stability debate, it is also worth recognising that, behind the scenes, the ECB and the Eurosystem, European legislators and market participants have made Europe's financial market infrastructure into the bulwark of financial stability it is today. Furthermore, despite the achievements, financial market infrastructure is not in a steady state. There are still further integration efforts to be made and, in particular, the challenges emerging from technological innovation such as distributed ledger technologies (DLTs) and their potential future use in financial services will have to be addressed.

Against this background, this article will discuss the challenges of the digitalisation of financial services and the emergence of DLTs. It will also present the Eurosystem's ideas on how to respond to these challenges in its vision for 2020.

1| The impact of digitalisation and technologies in financial services on Europe's market infrastructure

Technical innovations in financial services, including DLTs, will be among the key focal points for the Eurosystem over the next few years as they will shape the way financial market infrastructures evolve.

In the domain of retail payments, digitalisation is paving the way for product and service innovation. In the past year, the development of **pan-European instant payments** has taken centre stage. Instant payments are electronic retail payment solutions available 24 hours a day, 365 days a year and result in the interbank clearing of transactions and crediting of the payee's account with confirmation to the payer within seconds of the payment being initiated. This is irrespective of the underlying payment instrument used (credit transfer, direct debit or payment card) and of the underlying arrangements for clearing (bilateral interbank clearing or clearing via infrastructures) and settlement (e.g. with guarantees or in real time).

The Euro Retail Payments Board (ERPB), which is a high-level entity chaired by the ECB and set up to facilitate the further development of an integrated, innovative and competitive market for euro retail payments in the European Union (EU), has decided on the development of an **instant payment scheme** (i.e. a set of agreed rules and technical standards to execute instant payment transactions). By November 2016 the European Payments Council (EPC) is to develop an instant payment scheme for euro payments based on the Single Euro Payments Area (SEPA) credit transfer. Implementation of the scheme is foreseen by November 2017. By that time, end-user solutions for instant payments in euro should be made available at the pan-European level by the payment service providers.

This means that by November 2017 the European financial market infrastructure has to be ready to **clear** and **settle** instant payments on a pan-European scale. In line with the objective of an innovative, integrated and competitive retail payments market, the clearing industry is expected to adopt a pan-European approach to instant payments, i.e. scheme participants should be able to reach and be reached by any other participant in the EU. Where there is more than one clearing infrastructure, it will be enough for a payment service provider to participate in one and be reachable at the pan-European level. This consequently requires infrastructures to adopt fair and open access policies vis-à-vis both payment service providers and other infrastructures. They also need to ensure full technical and business interoperability. Finally, the clearing industry is expected to ensure appropriate risk mitigation.

1 Financial Stability Review, *November 2015*.

As an operator of market infrastructure, the Eurosystem will support the settlement of pan-European instant payments with its TARGET2 services. Instant payments are consequently one of the key components of the Eurosystem's vision for 2020, which will be discussed later.

Another innovative service whose provision will impact the underlying financial market infrastructure is **person-to-person (P2P) mobile payments**. In 2015 the ERPB endorsed the vision of allowing any person to initiate a pan-European P2P mobile payment safely and securely. It said that existing and future local mobile P2P solutions should cooperate to ensure pan-European interoperability.

One component of pan-European P2P mobile payments should be a standardised proxy lookup (SPL) service, i.e. a database service that can link the mobile number (or other proxies, e.g. email addresses) of the payment recipient to the destination bank account (i.e. the IBAN). This mapping (between proxy and IBAN) would greatly add to the convenience of mobile payments as it would free users from having to know and use the IBANs of the payment recipients.

Such database services are already available at the national level. The ERPB has called on the market to develop a pan-European solution, a task which the EPC is currently facilitating. Any such solution should, of course, respect existing data protection legislation.

The potential for the provision of innovative retail payments products and services, in conjunction with European legislation on the activities that regulated non-bank payment service providers (or "payment institutions") can carry out (the revised Directive on Payment Services or PSD2), has opened the doors for a wave of **new market entrants**. These are often start-ups making use of new information technology applied to financial services ("fintech" companies), as well as established internet companies (social media or e-commerce platforms, the so-called GAFA[2]). Whereas the first tend to be very agile and quick to leverage new technologies as they emerge, the latter pay a great deal of attention to the customer experience, exploit network effects and have the capital to buy the new solutions developed by fintech start-ups. In most cases, they do not offer banking services other than the initiation of payments or access to account information and thus do not require a banking licence.

Established internet platform companies already have a large customer base and see payments as a logical component in their value chain. Their motivation often comes from the fact that they view traditional payment methods as not very user-friendly or too slow for the e-commerce environment and/or because they already have a large network and the technology for transmitting large amounts of data between customers. Their payment services are also usually viewed as a secondary revenue stream, which means they do not necessarily expect to gain a huge profit from them, if any profit at all. Often, they simply offer payment services to make their core business more attractive.

While these new product and service providers might present a challenge to the traditional market incumbents' revenue streams, their impact on the underlying financial market infrastructure will be more limited if the clearing and settlement of payments and securities transactions still take place between the incumbent account-holding entities.

What may have a much more profound impact on the financial market infrastructure in the years to come is DLTs. DLTs allow the verification of financial transactions in a decentralised way and thus have the potential to reshape the mechanisms for making such transactions. Instead of settlement occurring in a centralised market infrastructure (such as a payment system, a central counterparty, a securities settlement system, a clearing house or a custodian), strong cryptographic and verification algorithms allow all participants in a DLT network to have a copy of the ledger and give authority for managing and updating that ledger to multiple participants.

In its capacity as operator of, catalyst for development in and overseer of payment systems, the Eurosystem needs to reflect on the possible impact and use of DLTs.

- As far as the market infrastructure services operated by the Eurosystem – i.e. TARGET2 and TARGET2-Securities (T2S) – are concerned, discussions are currently ongoing in the context of the Eurosystem's vision for 2020.

2 *Google, Apple, Facebook, Amazon.*

• In the Eurosystem's catalyst function, discussions with market participants have already been initiated in the T2S governance framework (through the T2S Harmonisation Steering Group). Although the work is still in its infancy, it appears that the range of potential improvements stemming from the new technology is vast, from the execution of corporate actions on securities to the automatic margining of cash accounts.

In its role as overseer, the Eurosystem needs to arrive at a common understanding as regards the developments which potentially affect the continuity of overseen infrastructure. Discussions are needed on whether the existing frameworks can continue to apply or require adaptation. For example, the ongoing work in the field of CCP recovery and resolution needs to take account of the possible impact of DLTs. The possible benefits of a decentralised ledger also need to be studied in the context of the activities surrounding cyber resilience of market infrastructure services.

2| The Eurosystem's vision for 2020

Europe's financial market infrastructure has been built on the basis of a collective approach driven jointly by the public and the private sector, supported by strong governance. Achieving this required both a sound regulatory basis and technical action. The past decade provides some examples where the creation of an integrated financial market infrastructure for payments and securities has been supported by regulatory action aimed at removing barriers and overcoming European fragmentation. Establishing the appropriate governance involving all relevant stakeholders has proven efficient as it has led market participants to drive integration and innovation by bringing in their strategic considerations.

In the domain of retail payments, one example of the complex collaboration of regulation and technical action supported by strong governance is the creation of the (SEPA). In the post-trade area, T2S is another example.

While T2S migration is still under way, the Eurosystem is addressing the need for Europe's financial market infrastructure to continuously evolve in order to keep pace with market developments and technological progress. In particular, the challenges emerging from the digitalisation of financial services and DLTs will have to be addressed. To deal with the technological and strategic challenges to the infrastructure, the Eurosystem has developed three key action points it will work on in the run up to 2020.[3]

The first is to **explore synergies between TARGET2 and T2S, potentially even merging them into a single platform** in the future, with the goal of achieving a consolidated market infrastructure for large-value payments and securities settlement. Both platforms have key functions supporting financial stability in Europe.

TARGET2, the platform that is used Europe-wide to settle large-value payment transactions in euro, including central bank monetary policy operations, contributes to financial stability in the euro area by enabling participants to move money throughout the market extremely quickly and efficiently. Since payments are settled in central bank money with immediate finality, recipients are not subject to any credit risk. Liquidity risks are also carefully managed. The platform is regularly tested to ensure business continuity, and its users know they can rely on TARGET2 to always be available, even in abnormal circumstances (last year it again registered a technical availability of 100%).

T2S, the integrated IT platform which processes the real-time settlement of securities transactions against central bank money across Europe, is also an important benefit for financial stability as it makes liquidity crises less likely. It allows banks to manage their collateral and liquidity needs more easily, as they can hold a single pool of collateral in T2S, rather than it being spread across several different systems. This makes it quick and easy for them to move collateral anywhere it is needed across Europe, thereby balancing out shortfalls in one market and surpluses in another, something which was time-consuming and costly before. In addition, the platform's advanced standards of

3 *Read more about the Eurosystem's vision for 2020 at* https://www.ecb.europa.eu/press/key/date/2015/html/sp151014.en.html

resilience, availability, business continuity and security contribute to greater financial stability in Europe.

Consolidating some components of the technical infrastructure of TARGET2 and T2S and potentially even forming a single platform will allow TARGET2 to benefit from some of the state-of-the-art features of T2S, such as the implementation of ISO 20022 standards. Migration to ISO 20022 in TARGET2 was originally planned for November 2017, but upon the banks' request it was postponed and moved under the umbrella of the Eurosystem's vision for 2020, so as to find the most appropriate method and timing for migration.

The enhancements envisaged for Europe's financial market infrastructure will benefit users from a technical perspective in that they will have access to all available services via a single gateway. Moreover, these enhancements will provide an opportunity to further increase the resilience of the system, which is also beneficial from a financial stability perspective.

As regards the business benefits for users, it is planned to enhance the services currently provided by TARGET2, for example by further optimising liquidity-saving mechanisms. In addition, it could be possible to add statistical tools to support banks in their regulatory reporting.

The second action point of the Eurosystem's vision for 2020 is to consider new service opportunities that the closer integration of TARGET2 and T2S would bring. In particular, the Eurosystem is considering **enhancing the TARGET2 services with instant payments,** at least in the settlement layer. Currently, business requirements for the settlement of instant payments and credit risk management across systems are being gathered from market participants. We also need to assess how far the adoption of a single settlement model in TARGET2 by all systems would facilitate settlement and credit risk management across systems.

Third, there are plans to review the harmonisation of Eurosystem arrangements and procedures for **collateralisation**. The correspondent central banking model (CCBM) is a cross-border mechanism which ensures that collateral can be accessed by all Eurosystem counterparties, regardless of where in the euro area they or the collateral may be located. Alongside the CCBM, links between central securities depositories (CSDs) have been used as another way to move marketable assets across borders.

As the euro area's banking and financial markets become increasingly integrated, demand for more efficient collateral management arrangements is increasing. This is something the Eurosystem will seek to address. It will also consider the business case for a common Eurosystem collateral management system, particularly since the market is becoming increasingly reliant on cross-border collateral flows for secured funding and treasury management operations.

In all three of these action points, the Eurosystem will continue to work closely with the market in order to benefit from its knowledge and experience as well as to ensure that Europe's future financial market infrastructure fully meets the needs of its users. This requires efficient governance. Against this background, the Eurosystem's internal governance set-up for market infrastructure is currently being streamlined. In the light of the positive experience gained with the T2S governance arrangement, there are concrete plans to establish a Market Infrastructure Board in charge of operations and projects in the area of Eurosystem market infrastructure. In addition, the interaction with market participants is being reviewed with the aim of ensuring that the Eurosystem services meet market needs.

In its three roles as operator, overseer and catalyst, the Eurosystem is not only helping to create a more integrated financial market – moving us closer to the goal of a true Single Market in Europe – but is also contributing to greater financial stability by ensuring a strong and efficient European market infrastructure. Looking to the future, the Eurosystem remains committed to these objectives and will seek to exploit technological advances and innovation while maintaining safety, reliability and, ultimately, confidence and stability.

Beyond technology – adequate regulation and oversight in the age of fintechs

Andreas R. DOMBRET
Member of the Executive Board
Deutsche Bundesbank

With the number of financial technology firms, or fintechs, increasing steadily in the age of digitalisation, banks as well as regulators must learn to deal with them. Supervisory authorities must ensure that their supervisory approach produces financial stability and establishes a level playing field for banks and technological innovators. In Germany, a risk-based regulatory approach ensures that no relevant risks remain unregulated – neither those stemming from traditional banks nor those created by fintechs. Traditional established banks, meanwhile, must face up to the challenges posed by these new competitors and ensure that their business models remain profitable. The following article presents the status quo *in terms of the regulation of fintechs under the German regulatory framework, assesses challenges for regulated institutions and sheds light on potential future risks.*

In light of the fundamental impact of digitalisation, the existence of growing numbers of innovative financial technology firms, commonly referred to as "fintechs", has alarmed traditional banks as well as regulators. New players have introduced innovative solutions to many aspects of conventional banking and finance. For example, the lending business of banks is complemented by platforms enabling peer-to-peer or peer-to-business lending and funding. Investment advice is on offer from social trading platforms, where users exchange their investment experiences and strategies. Payment services are enriched by convenient applications like mobile payment solutions or electronic wallets. Still other services offer personal finance solutions, data and analytics and other financial software.

Even existing infrastructure is being challenged: crypto protocols, which promise near-real-time, manipulation-proof transaction mechanisms, could in principle be established in an entirely decentralised environment by using distributed ledger technologies and without the involvement of banks. Once successfully implemented, this mechanism is likely to be a disruptive threat to existing providers of financial infrastructure for transactions in currencies, securities, contracts and certificates. As a result, the fintech industry, though not as homogeneous as this term may imply, is evolving dynamically. For 2014, global investment in fintechs was estimated at USD 12.2 billion (Accenture, 2015). In Germany, for instance, over 250 fintechs have emerged within a few years, according to the statistics provider Statista.

At the moment, most new services probably add little value to the financial sector. But significant growth rates and disruptive potential demand our attention. Banks are being compelled to rethink their strategies in the face of this wave of innovation. For regulators, stability and regulatory considerations about fintechs are gaining momentum as their innovations may involve a broad range of risks. Quite commonly, such risks entail cyber and IT-related issues as well as threats to consumer protection like the potential for fraud, misleading information or mis-selling. Depending on the concrete business model, fintechs may – like credit institutions – also face credit and liquidity risks (see EBA, 2015). Thus, the initial question should be quite straightforward: Is our regulatory and prudential framework able and adequate to cope with these innovative market entrants? Or does the new wave of digital finance call for an enhanced or even entirely new regulatory regime?

The current debate about regulatory concerns regarding fintechs is fairly unstructured. This is partly due to a pervasive confusion about the notion of fintechs themselves. In public and media narratives, they are mostly perceived as launching a concerted attack on classical banking. Moreover, new lines of business like peer-to-peer lending and crowd funding, mobile payment services, automated investment advice and distributed ledger applications are often portrayed as an entirely new form of banking and finance applications which cannot be captured by existing regulation. Those descriptions influence the public perception of fintechs, yet are misleading, because they inaccurately describe fintechs as a group of similar, possibly disruptive competitors to traditional banks or other long-established intermediaries (e.g. asset managers, insurers). While some radical concepts exist under which fintechs could, in principle, have a disruptive impact on financial services, the vast majority of start-ups do not have their eye on the entire value chain of lending, payment or fee business at banks, but rather seek to improve specific services. Apart from their "fintech" label, innovative and IT-based financial firms do not share a common business model or economic foundation. Thus, a differentiated take on fintech businesses and their regulatory and stability implications is called for.

Here, policy objectives are a second source of confusion. As a yardstick for regulatory responses to fintech business, some highlight potential sector instability or the existence of an uneven playing field in the financial industry, while others cite the huge potential benefits that fintechs may bring and that cry out for innovation– and newcomer – friendly regulation. Political concerns therefore include various issues, in particular microprudential regulation, macroprudential oversight, consumer protection and also innovation development aids. This might lead to erroneous implications in terms of regulatory and supervisory responsibilities. To identify areas for regulatory action on the digital financial industry, this article therefore presents the *status quo* in terms of the regulation of fintechs under the German regulatory framework as an example of a technology-neutral regulatory approach (section 1), assesses challenges for regulated institutions (section 2) and sheds light on potential future risks (section 3). Results are summarised in section 4.

1| *Status quo*: does current regulation capture fintechs adequately?

The presentation and self-perception of fintechs as opponents to banks has led to the erroneous but widespread belief that their business ideas commonly fall through the cracks of financial regulation. In fact, looking at regulation in Germany,[1] the existing logic of financial regulation is equally applicable to any innovative, IT-based business. The main reason is that regulation is rigorously built on risk orientation and a definition of financial business activities that codifies the principle of "same business, same risk, same rules". Technical implementation issues are not taken into consideration when defining permissions and responsibilities. In Germany, new enterprises in the financial sector are either classified as credit institutions, financial services institutions or payment services providers or they remain unregulated. As an example, a crowd funding platform – just like any other fintech business – may be subject to permission on various grounds. It is typically not considered a credit institution as long as it neither takes deposits or other repayable funds from the public nor grants credits for its own account. This is consistent with the idea of risk-orientation, as it is investors who take the credit risk. A business classification as payment service or financial service institution, both entailing different financial risks, has to be assessed independently. As far as platforms in Germany are concerned, money transactions are settled by a supervised credit institution; this means that no relevant risk remains unregulated. In principle, such an assessment calls for a case-by-case analysis of innovative business ideas. A similar logic is in place for virtual currencies like bitcoin: since virtual currencies are classified as financial instruments in Germany, trading bitcoins is subject to permission by the financial authorities.

The above summary of German regulation reveals that if a fintech business remains unregulated, this will not be due to regulatory ignorance. Rather, that business does not, for good reason, qualify as a financial institution. Conversely, any fintech business that tries to evade justified regulation will be prosecuted. Financial regulation systematically addresses all of a financial institution's relevant risks. Banking without banks – in the sense of a financial intermediary providing all the services of a bank without being treated as a bank by supervisory authorities – is therefore irreconcilable with existing financial regulation.

As a systematic framework for financial regulation whose rules are also applicable to any IT-based business, existing regulation is bound to serve as a starting point for discussing other political objectives relating to fintechs. An obvious implication can be drawn with respect to the "level playing field" objective. Fair competition may certainly be measured using multiple standards. In light of the above, equal treatment of equals must be understood in terms of risk-oriented regulation. This may undoubtedly encourage new market entrants with scant regulatory experience to concentrate on unregulated fields of the banking business. On the other hand, incumbent market participants have an equal opportunity to engage in these business lines. However, activities in *per se* unregulated business fields might still merit supervisory attention in regulated institutions. For example, non-financial risks in innovative applications may impair a bank's viability, thus legitimising targeted supervisory responses. I am convinced that in the hierarchy of regulatory objectives, risk-orientation must therefore have priority. This certainly gives regulators an incentive to look out for new dangers to financial stability that may emerge in unregulated firms.

As a competing policy goal, it is often hoped that digital innovators will prove to be a source of qualitatively enriched banking and economic growth. Indeed, innovations frequently aim at improving banking convenience, increasing efficiency, targeting previously unprofitable banking segments and intensifying competition. An innovation-friendly regulatory environment is thought of as an alternative orientation for rule-setters. The EU digital strategy comprises several initiatives in this direction that aim at facilitating digital innovation throughout the European Union. Some countries have initiated special programs to foster growth in the fintech sector with the aim of intensifying currently low competition in their national market. However, in Germany, competition in the banking market is already intense, and German authorities focus on the risk perspective

1 *In other European countries, relevant definitions are not entirely congruent.*

when it comes to regulation. From this perspective, there is far less scope for support. The mandate to ensure financial stability implies neutrality towards financial innovation as long as innovations do not unleash the potential to create new or exacerbate existing systemic risks. New mandates for financial regulation and supervisory authorities that promote innovation-related services may produce a conflict of interest. Faced with a trade-off between helping achieve innovation and ensuring risk-adequate regulation and supervision, institutional safeguards must be put in place to guarantee that the latter maintains categorical priority. An institutional separation of supervision and innovation support is appropriate. Furthermore, support instruments have to be selected with caution, given that they could magnify emerging side-effects. As was the case with previous financial innovations, we are again presented with potential efficiency gains and benefits in terms of customer surplus, while unable to forecast all the negative consequences, side-effects and potential instability as a result of the fundamental socio-financial change through digitalisation.

2| Challenges for the supervised sector

While maintaining the present regulatory framework, stability concerns still emerge to challenge both microprudential supervision and macroprudential oversight. In the face of technological and social transformation, the guiding principle for microprudential supervision is not that of rigid sector composition. On the contrary, market forces must be allowed to help discover better solutions. Instead of preserving the *status quo*, the primary concern must be to safeguard the smooth and appropriate adaptability of those financial institutions that perform vital tasks for the financial sector and the financial architecture (Dombret, 2015a). For that purpose, supervisory authorities have to monitor the ability of supervised institutions to transform their business in addition to their ultimate solvency and liquidity risk profiles.

Adaptability is closely affiliated with future earning power. Profitability is therefore bound to be a chief indicator of banks' ability to withstand the wave of digital transformation. The impact of innovative competitors on banks' business strategies is certainly remarkable. Fintechs – for the sake of the argument, confined here to unregulated market entrants – increase pressure on banks' business models. But the direction of market developments is by no means straightforward. An indisputable economic driver of fintechs is their ability, to 'skim the cream' of lucrative services by targeting the most profitable elements of banks' value chain. The innovative use of IT enables convenient solutions for customers and cost reduction through automated processes. Moreover, specialising in specific services often means less complex organisations and flat hierarchies, which in turn facilitates innovation. While these aspects benefit the disaggregation of value chains, other aspects favour services from a single source. These include economies of scale, reputation, synergies among services and experience with regulatory issues. After all, IT-based innovations promise more than a zero-sum game among new entrants and traditional banks: some innovations are targeted at previously untapped market segments like big-data-driven lending to demographic groups which were previously difficult to rate or convenient extra services. Long-established banks may themselves discover profitable new lines of business. Through innovative IT they, too, may save administrative costs and improve their risk management. While the above list of driving forces is not exhaustive, it does demonstrate that technological change should lead to a heterogeneous landscape in which competition and cooperation among traditional and innovative credit institutions, investment firms, payment services and non-regulated fintechs exist side by side.

Innovative services that target the entire value chain of bank lending, payments and fees business represent an altogether different challenge. What most of these new visions have in common is a network effect which possibly leads to monopolistic market structures. Taking the internet and smartphones as the given infrastructure, a sufficiently large enterprise could reap the benefits of low per-unit costs and vast synergies in terms of, for example, cross-selling and big-data usage. The current IT giants are commonly thought of as highly capable invaders. But for the reasons mentioned above, any all-encompassing financial institution will not be beyond regulatory and supervisory reach. New players' competitive edge is rooted in their technical advance, not in their exploitation of a regulatory loophole. Incumbent banks have to remain attentive regarding any of those potential impacts on their long-term profitability.

The digitalisation of banking does not only matter for the profitability of banks' business models, it also leads to specific operational risks in the institutions. The need for business continuity and reliable services puts pressure on IT transformation processes. In addition, IT-based services and processes are prone to error, just as humans are. Data confidentiality, integrity and availability will continue to grow in importance, and new sources of operational risk such as manipulation of algorithms could become more relevant. The latter is an example of counterintuitive risk. While IT applications are perceived as rendering banking more transparent and as treating every customer in the same way, computer algorithms could facilitate the manipulation of results or open the door to unreflected biases. Quite frequently, these issues will not be confined to individual institutions. The increase in cyber risks has shown the need for both national and international cooperation among banks as well as among regulatory and supervisory authorities. The network character of IT-related phenomena also pertains to this risk category. Attackers seek to profit from worldwide access to targets, their swift learning capability and even the division of labour. The onus is on financial institutions to counter the rising menace of attacks on financial IT by engaging in voluntary mutual knowledge building and developing ways to overcome reputational fears.

3| Threats beyond current regulation and supervision of financial institutions

Regulation and supervision are at present equipped with instruments and powers to address risks presented by the emergence of IT-based banking. To support this framework, new regulatory objectives in the field of innovative banking need to be closely aligned to the existing rules. Otherwise, we risk artificially segregating related issues. This becomes clear when we consider that, in principle, banks could themselves provide any business offered by fintechs. Subjecting fintechs to special regulatory treatment may lead to a distorted playing field and hamper market forces.

In order to safeguard the stability of the financial system, supervisors have to closely monitor developments in the entire financial system. It is in the nature of things that we cannot trust markets to internalise systemic risks stemming from externalities. These issues played a significant role during the last financial crisis. An important insight was that we cannot stop at merely patching loopholes in regulation after they have been exploited. Thus, technical innovations will have to be monitored in terms of their potential systemic risks (Dombret, 2015b). Crucially, it seems difficult to draw up a complete list of the associated risks because of the large spectrum of fintech businesses. With respect to crowd funding and crowd lending, for example, unless effective control mechanisms are put in place, asymmetric information on creditworthiness may encourage moral hazard on unregulated platforms in the same way as originate-to-distribute schemes did during the crisis. For many innovations, consumer protection issues might become important because these innovations are put into effect at the interface with the customer. As an example, the Joint Committee of the European Supervisory Authorities (2015) has analysed the risks entailed in automated investment advice, frequently referred to as *"robo advice"*, which has attracted a great deal of attention as a banking innovation. The premise here is that even in a highly computerised world, consumers usually have only limited access to information and limited ability to process that information. The Committee points to risks related to flaws in the functioning of the tool as well as to risks stemming from the widespread use of automated financial advice. As a case in point, consumer protection issues indicate that automated financial advice tools may have an indirect adverse effect on the stability of the financial sector. It is not only banks that can offer *"robo advice"* in their banking applications, but these tools may – under certain circumstances, depending on each specific business model – *per se* remain unregulated. Monitoring emerging problems is therefore valid to protect consumers.

The vast array of innovative products and business models that are being introduced into the financial industry calls for a prioritisation strategy. Regulation cannot be built on theory alone. Any innovation may entail critical side-effects, but in terms of financial stability implications we need to assess whether any new product or business is likely to become significant enough to cause system-wide effects especially regarding funding, liquidity and credit risk as well as complexity and transparency

issues. Monitoring the impact of innovations can be a feasible compromise that leaves room for innovative experiments on the one hand while allowing an immediate response to significant threats on the other. However, this monitoring should also target, early on, those innovations that are likely to bring disruptive change to entire business fields, even if they are, at the time, considered insignificant.

In dealing with these issues, which have only just started to emerge, prudential actors will have to find suitable responses which may involve either adapting and enhancing financial regulation to new business models or creating a new sphere of regulation. To ensure a consistent regulatory framework, interventions have to be thoroughly risk-oriented and follow the principle of "same business, same risk, same rules". For example, the privacy of customer-related data is not an issue that is confined to financial institutions alone – hence the current European approach of defining harmonised economy-wide standards to combat targeted data privacy breaches. Artificially drawn regulatory lines between businesses that entail the same risk ought to be avoided.

4| Avoiding regulatory pitfalls

While innovative players and new technologies are entering the financial industry with impressive rapidity, regulation should not aim for an artificial separation between fintechs on the one hand and traditional banking on the other. Such a dichotomy is neither consistent nor appropriate with regard to the present regulation and sector composition: while there may be good reasons for fostering an innovation-friendly environment for fintechs, these should be addressed independently of supervisory and regulatory concerns. Also supervisory authorities risk a conflict of interest between those dissimilar mandates.

Many innovative ideas are still in their infancy and their impact is still small, meaning that side-effects and risks have not yet been adequately identified and established. With regard to financial stability, fintechs do not call for special treatment, but for an appropriately structured response. By the same token, authorities are advised to adopt a neutral position with respect to sector transformation. Banks as well as their supervisory authorities need to examine banks' responsiveness to innovations to ensure that banks offer a banking package that is unfailingly sound.

Also, in dealing with emerging risks, future regulation will need to build on the existing, risk-centred regulatory framework, which is to say treatment according to risk, not according to technology *per se*. Hence, I argue that digital innovations might create new risks that call for early monitoring. Despite the apparent transparency and neutrality of computerised banking, digital business inside and outside regulated institutions may still be prone to issues of asymmetric information, misaligned incentives and other risks that might become systemic if their frequency rises. Overall, the seemingly homogenous group of fintechs and their innovations is found to require a multifaceted response by financial authorities. Furthermore, this response needs to be consistent with the current regulatory framework in order to ensure a risk-adequate level playing field with regard to the most suitable and convenient financial innovations.

References

Accenture (2015)
"The future of fintech and banking. Digitally disrupted or reimagined?", available online at: *http://fintechinnovationlablondon.co.uk/media/730274/Accenture-The-Future-of-Fintech-and-Banking-digitallydisrupted-or-reima-.pdf*

Dombret (A.) (2015a)
"Digital Darwinism and the financial industry – A supervisor's perception", speech at the EBS Symposium (9/18/2015), available online at: *http://www.bundesbank.de/Redaktion/EN/Reden/2015/2015_09_18_dombret.html*

Dombret (A.) (2015b)
"Banking on big data – Different policy issues?", statement at the Third Frankfurt Conference on Financial Market Policy "Digitizing Finance" (11/6/2015), available online at: *https://www.bundesbank.de/Redaktion/EN/Reden/2015/2015_11_09_dombret.html*

European Banking Authority (EBA) (2015)
"Opinion on lending-based crowd funding", available online at: *https://www.eba.europa.eu/documents/10180/983359/EBA-Op-2015-03+(EBA+Opinion+on+lending+based+Crowdfunding).pdf*

Joint Committee of the European Supervisory Authorities (2015)
Joint Committee Discussion Paper on automation in financial advice, available online at: *https://www.eba.europa.eu/documents/10180/1299866/JC+2015+080+Discussion+Paper+on+automation+in+financial+advice.pdf*

Statista (2016).
"Zahl der in Deutschland tätigen Fintech-Unternehmen im Jahr 2015 nach Geschäftsbereichen", available online at: *http://de.statista.com/statistik/daten/studie/436311/umfrage/fintech-unternehmen-in-deutschland-nach-geschaeftsbereichen/*

The rise of fintechs and their regulation

Serge DAROLLES
Professor
Université Paris-Dauphine

The 2008 financial crisis led to a loss of confidence and gave rise to a new financial sector landscape. The emergence of the fintech phenomenon is attracting interest from new generations who are turning their backs on traditional players. The digital adjustment of the banking and financial sector at large is based on a move towards greater productivity through the use of new tools that reduce distribution costs. These developments raise questions as to their impact on banks, the reaction of the latter, and the risks incurred with the emergence of new practices. Regulators are facing new challenges that involve ensuring a level playing field for the different players and protecting users.

The term "fintech" is a contraction of the words "finance" and "technology". It refers to the technological start-ups that are emerging to rival traditional banking and financial players, and covers an array of services, from crowdfunding platforms and mobile payment solutions to online portfolio management tools and international money transfers. Fintechs are attracting interest both from users of banking services and from investment funds, which see them as the future of the financial sector. Even retail groups and telecoms operators are looking for ways to offer financial services via their existing networks. This flurry of activity raises questions over what kind of financial landscape will emerge in the wake of the digital transformation. What role will the traditional banks play? Will fintechs expand with or in spite of the banking sector? And what new risks do they pose for users of banking services?

This article addresses all of these issues, focusing in particular on the role of financial regulation and how it can contribute in the future. The first part looks at the reasons behind the rise of fintechs. These include supply-side factors, with the onset of the digital revolution, and demand-side factors, with the emergence of new modes of consumption. The 2008 financial crisis also played an important role, by prompting tighter regulation of traditional players and a growing sense of mistrust among consumers towards the banks. In the second part of this article, we analyse the responses of the large traditional players, and examine the various strategies that are open to them. We look at how incumbent firms and new entrants are creating links that could offer a foretaste of the future structure of the financial sector. We then go on to look at the challenges faced by regulators, and explore different approaches they could adopt to ensure a level playing field for incumbent firms and newcomers and protect users of financial services.

1| The emergence of fintechs

In this first section, we look at three aspects of the recent changes in the banking and financial sectors. We start by discussing the impact of the 2008 financial crisis, both on the regulation of incumbent players and on the trust placed by customers in their banks. We then go on to examine changes in the behaviour of banking service users. Lastly, we look at the digital transformation, the true catalyst behind the fintech phenomenon.

1|1 The financial crisis, regulation and trust

The 2008 financial crisis triggered a series of major upheavals in the financial and banking sectors. The first was the realisation that the activities of the major financial institutions generate systemic risk. This led to the development of different measures designed to quantify that risk.[1] Bank financial regulation was tightened. In particular, the notion of a financial entity's contribution to systemic risk led to the definition of systematically important financial institutions (SIFIs). The Basel Committee on Banking Supervision (BCBS) increased banks' regulatory reserve requirement in order to take account of individual contributions to global risk. This regulatory tightening placed a dual burden on banks: directly, by forcing them to set aside greater reserves and therefore scale back their activities; and indirectly, in that they were singled out as the main culprits behind the financial crisis.

As the global economy emerged from the crisis, it became clear that many customers, and notably the younger generations, had lost all faith in banks. How could they trust the very economic agents that caused the trouble in the first place? And to make matters worse, those agents had only managed to avoid bankruptcy thanks to massive injections of public money. If the banks themselves were incapable of managing the risks they took, why should anyone take their advice or trust them with their savings? New generations of clients are only too willing to turn their backs on the traditional players, and are keen to see new companies emerge who played no part in the recent crisis and can offer an innovative approach to finance.

1|2 From consumers to users of financial services

As well as taking a dimmer view of the banks, younger generations have developed very different consumer habits from their elders. They have grown up used

1 *See Benoit (S.), Colliard (J.-E.), Hurlin (C.) and Pérignon (C.) (2016). "Where the risks lie: a survey on systemic risk",* Review of Finance, *forthcoming.*

to having access to personalised solutions, tailored to their needs, in stark contrast with the mass marketing approach of the banks and other traditional financial players. The conventional model of the customer who consumes whatever he/she is offered has been left behind and replaced by the "user" of financial services. The old customer was passive, content to choose from a finite selection of products or pre-defined services, while today's user is active, expecting to be provided with the tools he/she needs to construct a personalised solution. The example of asset management is a case in point. Whereas a banking network offers the same savings product to a maximum number of clients in order to generate economies of scale, the user-client expects a flexible solution that can be adapted to his/her individual needs and investment objectives. Matching products and services to the expectations of the user requires close interaction, and this is only possible via online platforms.

From the outset, fintechs have targeted younger generations who are used to interactivity and to bespoke solutions. Yet this strategy is not without risks. On average, younger generations own fewer assets than the rest of the population, and the gap is particularly wide with respect to the oldest generations who tend to have substantial financial wealth. In order to be economically viable, newcomers quickly need to attract large quantities of assets. And there are two pivotal factors for this: the number of clients and the average amount of assets per client. Even if they attract large numbers of young clients, fintechs will still struggle to turn a profit as long as younger generations' wealth remains low. Will fintechs have time to grow in parallel with younger generations' assets, and eventually become profitable? Even if the answer is yes, there is no guarantee that they will be able to retain these clients. As younger generations age, they will face increasingly complex savings challenges, and robot-advisers only offer basic solutions that are not really suited to these demands. There is a clear difference between robot-advisers, which are ideal for clients with few assets who mainly want to avoid high bank charges, and traditional firms whose clients tend to have more assets and require much greater expertise. Fintechs will struggle to make money if they lose their clients as soon as the latter become profitable.

Conversely, if the traditional players are to attract profitable clients, they will have to evolve and offer the same level of interactivity as their fintech rivals. Today's robot-advisers are just one example of the way incumbent firms are innovating in order to transform their client relationships and offer new approaches to banking. For the time being, this type of service is reserved for private banking clients. However, in the future it will be opened up to a broader range of clients in the traditional banking networks. This is the only way the sector giants can survive the transition from consumers to users.

1|3 The digital transformation

Digital transformation is nothing new in the banking and financial sectors. High-frequency trading and related arbitrage strategies are good examples of the impact new technologies have already made. It has become common practice to monitor changes in market prices over tiny fractions of a second, construct arbitrage strategies based on statistical rules and move in and out of positions at high speed to profit from very short term fluctuations in prices. In this case, the most important aspect of the digital transformation is the ability to process a sequence of repetitive tasks at speeds previously unknown in trading. However, for a long time, the high cost of implementing these systematic approaches prevented their widespread use. The acquisition and processing of information in particular were extremely expensive, raising a barrier to entry for new players. In addition, in the asset management sector in particular, this first digital transformation only really affected the production side of the business, and not distribution. Investors who purchased a share in an investment fund from their banking network continued to receive standard quarterly reports on the performance of their savings, but these took no account of their specific investment objectives (retirement funding, investment for a future real-estate purchase), or of any other holdings in their portfolio.

The second stage in the digital transformation, linked to the emergence of fintechs, has been more far-reaching, and began with the dissemination of tools that could simultaneously improve the entire value chain. Recent IT developments have brought solutions both for the production side (databases, decision-making tools) and for distribution (digital channels, knowledge of clients, flexibility of client offerings). These advances are enabling new entrants to find a place in the industry, by developing niche

offerings based on the interactivity and customisation sought by younger generations, all at a much lower cost than conventional firms.

In banking and finance, client relationship management was for a long time thought to be the preserve of the major networks, due to the high cost of client acquisition. Now, however, both newcomers and other non-financial agents (telecoms operators, retail chains) can use emerging technologies to offer new services to their existing client base; they can also build up new client bases more easily, as consumers are eager to buy services rather than ready-made products. In the asset management industry, this second digital transformation has affected both production and distribution simultaneously. On the production side, investment managers increasingly use sophisticated data-analysis and risk-management tools to create new products. But the biggest change this time has been in distribution, with clients – or service users – now receiving offerings that are adapted to their needs. To achieve this, distributors need to know as much as possible about their clients; hence the widespread use of metrics, quantitative information that distributors collect by closely analysing their clients' overall consumption trends. By statistically inferring the level of a client's income, for example, as well as his/her monthly outgoings, an asset manager can calculate the monthly saving capacity and offer suitable investment strategies. These analytical approaches are particularly effective with large client bases, where the behaviour of new clients can be simulated on the basis of the past behaviour of existing clients belonging to the same group. It is also possible to predict the future behaviour of a client based on his/her particular characteristics, and use this to provide a personalised approach.

2| The response of traditional players

The traditional sector players have not remained idle in the face of the rising threat from fintechs. Their digital strategy can be summed up in one simple question: make or buy? In this section, we look at these two alternatives and then describe a third path, midway between the other two, which could form the basis for a new business model, whereby traditional players combine their skills in core banking systems with the agility of new entrants.

2|1 The challenges of making

In the previous section we discussed the in-depth digital transformation currently changing the face of the financial industry. As in other industries that are being affected, this revolution is being spearheaded by market newcomers and not by incumbents. In the financial industry in particular, fintechs have a competitive advantage due to the technical debt accumulated by traditional players, notably the banks. The concept of technical debt is directly linked to that of financial debt: developing an IT system generates future costs, which can be likened to a form of interest payment, and the total amount of these costs makes up the technical debt. The more complex a system becomes, the more frequently it needs to be upgraded and the higher the associated debt. A good example of this is a large banking group created through the merger of several different banks: the overall information system has had to integrate various pre-existent components; as a result, it reflects the history of the bank and the major stages in its construction, but it will never be as efficient as a comprehensive IT system, built to cover the current scope of the bank's activities. Asset management is another good example. Financial innovation has created increasingly complex tools, requiring the development of more and more sophisticated storage and control systems. The introduction of tighter regulations has also had a similar effect. Indeed, the vast majority of the IT resources deployed in recent decades have been in response to these two phenomena. Today's IT systems are like a "*millefeuille*", built of multiple versions that have been layered on top of each other as new financial innovations or regulations have emerged. For a long time, this complexity was a barrier to entry for new participants. But all that is changing. Fintechs now have access to technical solutions enabling them to integrate the impact of financial innovation and regulation from the outset, all at a much lower cost. There seems to be no holding them back. In contrast, incumbents firms have more limited room for manoeuvre due to their technical debts, leaving fintechs ideally placed to take the lead.

The industry incumbents have responded by trying to expand the technical skills of their IT teams, and by changing the way they are structured. The digital transformation has thus led to changes in the way projects are managed, with large groups adopting more agile IT development methods, similar to

those used by tech start-ups. It is still important to know the business, notably due to its regulatory complexity, but the key factor now is the ability to develop interactive tools that match new user habits. Traditional players have all the elements they need to succeed in this transformation: knowledge of the business, a network, a track record in client relationship management, transaction security and financial resources. It is easy, therefore, to imagine them launching a digital version of their conventional banking model, drawing on their existing industry expertise to offer a different client experience. A number of traditional players have already tried this, albeit with mixed results. There are various reasons why they have struggled: fear of cannibalising their existing activities, the failure of previous attempts or difficulties in effectively mobilising staff – all these can explain why traditional players have been reluctant to invest massively in the digital transformation. Banks will only succeed if they can encourage their staff to adopt new working methods, while at the same time capitalising on their main strength: knowledge of their clients. This synthesis will not be easy to implement.

2|2 The temptation to buy

The traditional banking and financial players have not been very active when it comes to investing in or acquiring fintechs. Indeed, banks have made almost no investments at all in this segment, despite regularly taking indirect capital stakes in start-ups via investment funds. The few cases where they have taken a stake have been for a set purpose: to modernise an existing service offering, acquire a new technology or foster the development of a specific fintech. Indeed, for fintechs, having a bank as a stakeholder can reassure the regulators and make it easier to get a licence for their activity.

Acquisitions of fintechs by traditional players are even rarer. Banks seem to be afraid they will slow their target's momentum, or will struggle to merge the new entity with their existing development teams. The main motive for purchases by incumbent firms seems to be, again, to acquire a new technology or development team that can help them upgrade their offering as quickly as possible. Combining a fintech with conventional banking services is a way of developing new services in the short term and makes it easier to shift traditional client relationships towards a more interactive and personalised model.

2|3 A possible synthesis

A third method of collaboration is emerging, specifically in the banking and financial sector. In order to sell their financial services and products, fintechs need to have access to partners who know how to operate a core banking system; banks in turn can provide this service, and can sell their products to third parties in unbranded form. A number of banks have opted for this solution in order to create ties with fintechs, positioning themselves as a service-provider and giving guidance on their core banking business. Some payment fintechs, for example, operate using existing platforms, while a number of platforms for the distribution of savings products sell solutions constructed using bank products. In return, the partner bank can directly observe how the client relationships evolve, and adapt its offering to suit the needs of the fintechs, and ultimately of the final users.

This type of relationship is raising fundamental questions about the way the distribution of financial products is currently structured. It is possible to imagine a new distribution model with the banks operating as product design platforms, selling unbranded solutions to captive or non-captive fintechs, and capable of adapting more readily to changes in user needs. In this case, acquiring a fintech as a subsidiary would make sense as it would enable banks to secure their distribution channels. The only risk with this model is that the fintech, which is in charge of the client relationship, might outgrow the platform supplying the financial products. Do financial institutions really have the capacity to keep pace with the fintechs' growth?

3| The role of the regulators

Faced with these profound changes in the banking and financial sectors, regulators need to take care to avoid two pitfalls. The first is overprotecting incumbents by erecting barriers to entry for newcomers. Doing so would discourage financial innovation and stifle competition in the very sector they are supervising. The second potential pitfall is choosing instead to

favour newcomers by regulating them less stringently than incumbents. These challenges can be illustrated by two examples: client identification in internet payments and in bank account aggregation services. In the case of payments, clients now have access to a range of different options, and the trend is towards using simpler and more user-friendly identification solutions than the standard login and password approach. However, these solutions differ starkly from the traditional approaches used by banks, raising concerns about security. The same problem occurs with bank account aggregation services. These applications need to retrieve information from the banks on their clients' banking activity. The client thus has to send credentials for his/her different accounts to the aggregator, who in turn uses them repeatedly to construct an overview of the client's finances. Again, this raises the issue of security. Regulators can respond by issuing recommendations on the security of cashless payment systems or online access to bank accounts, but ultimately it is the users who decide whether or not to adopt a technology.

The European directive on access to banking information[2] covers the range of new uses and innovative services that are positioned between the banks and their clients. Under the directive, new payment service providers are subject to the same rules as other payment institutions. However, in return, banks are obliged to give service providers access to information on their clients. This means, for example, that a bank cannot prevent an aggregator from accessing its clients' details by advising the latter not to give a third party access to their accounts. This poses the question of who should pay for the infrastructure needed for this kind of interconnectivity. The most crucial issue it raises, however, is that of security, as the sharing and use of client identification details heightens the threat of cyber-attacks. If a payment services provider is hacked, it could unintentionally propagate the attack to all its clients' banks. Banks are thus calling for tighter security regulations for newcomers and raising concerns about the authentication systems they use. Banks are constantly receiving requests for data using client identification codes, without knowing whether they come from the client or a third-party operator. Clearly, the first step would be to improve the traceability of these connection requests. However, the banks think more needs to be done and are also demanding the use of strong identification systems. In this case, third-party operators would need to request authentication each time they send a request to the bank. But an account aggregator that needed to ask its clients to re-enter their credentials each day, for each of their accounts, would soon lose its appeal. These examples demonstrate the difficulties regulators face in reconciling innovation and security.

3|1 Equal treatment and competition…

Regulators have a difficult role to play as their decisions have both a direct and indirect impact on competition between incumbent firms and newcomers. They have to provide a level playing field for all participants, but at the same time foster an innovative, secure and competitive financial market. The Swiss regulator's action against money laundering is an interesting case in point. The Financial Market Supervisory Authority, or FINMA, has modified its Anti-Money Laundering Ordinance to directly reflect changes in technology, and the revised version covers internet payments and identification procedures. Online authentication is now permitted, but FINMA has defined specific thresholds below which clients do not need to formally identify themselves. This is a good example of how regulation can evolve to avoid hampering new technologies and new ways of using financial services.

In addition to the regulation itself, rule-setters need to look more generally at the incentives offered to market agents, and how these lead them to modify their behaviour. They also need to keep a harmonised set of rules in place and avoid applying different regulations to specific categories of player. This would have the effect of compartmentalising the financial industry, preventing the emergence of new players and discouraging financial innovation. Keeping newcomers out would distort the market in favour of existing players. Conversely, authorities might tend to regulate existing players more tightly as they know their business well, while taking a laxer stance towards market entrants whose activities are new, and who have not been through sufficient crises to fully understand the risks they pose. Clearly regulators face a difficult task in finding the right balance, one that allows existing players to survive

2 See the European Banking Authority's revised Payment Services Directive or PSD2, (2015).

but also facilitates innovation by new entrants, and ultimately promotes healthy competition in the financial market.

It is possible, however, to outline a number of general principles. Obviously, the first should be to maintain a neutral stance with regard to technological advances. Regulations should foster healthy competition between players, regardless of whether they offer conventional approaches or use new technological solutions. We need to make sure we remove all obstacles to growth for new entrants. The second principle is that we keep in place a harmonised set of rules, covering all players simultaneously, rather than treating players differently according to their characteristics, an approach that would artificially segment the market and hence limit competition. Whether a transaction is processed online or using conventional methods should not affect how it is seen by the regulator. Only the risks related to the transaction itself should be taken into account, and not the manner in which it is performed. Lastly, the third principle should be protecting the users of the financial system as well as the system itself. Regulators must act in the interests of users, protect them in a changing environment that can pose new, unanticipated risks. Respecting these principles will clearly be difficult, and giving one principle priority could undermine the others. The role of the regulator is to find the right balance. To remain neutral with regard to technological progress, for example, regulators need to assess the potential benefits of financial innovation and identify existing rules that could hamper those advances. In the introduction, we discussed the example of client authentication. Numerous technologies are now available to simplify this step, each entailing very different risks. Rejecting the notion of online identification outright would stifle innovation and prevent new solutions from emerging to tackle problems already identified. In contrast, allowing online identification for transactions below a specific threshold would encourage the development of new solutions, and eventually give rise to more efficient tools that limit the – minimal – risk of fraud. This approach would allow regulators to meet two of the above-listed principles, despite them being hard to reconcile.

It is also difficult to see how we can treat fintechs – which are often highly specialised – in the same way as traditional players – which are much more generalist. The solution here could be to create new categories of financial intermediary, subject to less stringent requirements than banks. Certain rules could be relaxed under specific conditions, for example if the entities in question are not exposed to liquidity mismatch. A market newcomer does not really qualify as a bank if it has no liquidity mismatch, and its clients are less exposed to risk; as a result, it does not need to be regulated in the same way as a bank.

3|2. … without ignoring the new risks

Technical progress fosters innovation, but it also entails new risks, as shown in the two examples described above. At the same time, the primary mandate of the regulator is to protect the users of financial services and the stability of the financial system. In this section, we analyse two issues the regulator needs to focus on: the threat of cyber-attacks and the risks related to the outsourcing of certain traditional bank activities.

Companies in the banking and financial sectors are prime targets for cyber-attacks, and the emergence of online services, designed to be simple and interactive, only heightens this risk. In a worst case scenario, it is possible to imagine a wave of concerted attacks triggering a liquidity squeeze in the markets and threatening the solvency of sector participants. For regulators, however, the difficulty is knowing how to evaluate these new risks. There are no historical examples that can be used to construct realistic scenarios. All regulators can do is take a pragmatic approach, defining plausible attack scenarios and testing the defence mechanisms put in place by digital enterprises. This task is made difficult by the lack of historical data and the fact that ongoing financial innovation is constantly opening up new possibilities of attack. Only by developing in-depth expertise in this field can the regulators effectively fulfil their role.

The second source of risk is the outsourcing of certain tasks in the financial transaction processing chain. Before the technological revolution, it was usual for banks to carry out all tasks in the value chain internally, so that only one overall entity was subject to regulation. These days, this is increasingly rare, both for conventional players and new market entrants. In the case of conventional banks, cost pressures have pushed them to offload some

traditional tasks, such as computerised transaction processing, onto external service providers. In the case of tasks with a high technological content, there is a particular temptation to outsource them to new and more nimble players, who are better at using new technologies and more likely to be cost-effective. The value chain is thus split between the regulated bank and other players that are not necessarily subject to oversight. This creates holes in the supervision system, and makes it hard to predict how the relationship between the bank and its service providers would evolve if a crisis threatened the bank's solvency. Would the service provider agree to continue processing transactions if the bank were in trouble? Although economically viable in normal times, outsourcing clearly raises a new risk of coordination in times of crisis. Similarly, would a default by a service provider with a monopoly position create a new systemic risk?

The question of outsourcing also concerns newcomers to the market. In the previous section, we saw how many fintechs use the services of traditional banks in core banking systems. In some cases, this helps them obtain the licences they need to launch their activity. It also allows them to concentrate on adding value, via client relationship management, without having to pay to develop their own service production tools. These new players are therefore highly likely to use outsourcing. They have also evolved in today's sharing and virtual economy, so will always feel the need to look for efficient and low-cost solutions to handle the least profitable tasks in the value chain. Today, it is the traditional banks that provide these services. But what about tomorrow?

For regulators, outsourcing has many different consequences and, in this case, the challenges of technological innovation affect both historical and new market players.

Conclusion

Up to now, the traditional players have responded largely by collaborating with fintechs rather than seeking to acquire them. As a result, a number of partnerships have emerged between major institutions and newcomers, a trend that could shape the future of the banking and financial sectors.

The digital transformation offers huge growth potential for the financial sector. However, we need to make sure that the necessary regulatory changes do not stifle innovation, and at the same time provide the stability the sector needs to meet client expectations.

The migration to online lending and the rise of private regulation of online financial transactions with business customers

G. Philip RUTLEDGE
Chairman
Bybel Rutledge LLP
Visiting Professor of Securities Law and Regulation
LL.M. Programme, BPP Law School

Regulation of online banking services may be viewed in both a public and private context. The public context concerns governmental regulation of the banking sector and focuses primarily on issues relating to safety and soundness of national financial systems and adequate levels of consumer protection. The private context concerns financial institutions individually and focuses on the allocation of liability between the financial institution and its customers through written agreements pursuant to which it provides banking services.

While governments have been focused on increasing prudential measures for regulated financial institutions in light of the recent financial crisis, less attention has been given to the developing "fintechs" that act either as intermediaries in the online provision and distribution of credit or as online non-depository lenders.

Although government consumer protection regulation has imposed requirements on consumer electronic banking, most of these regulations do not apply to business banking where the bulk of transactions occur. Although these transactions may be subject to national commercial law, many of the terms and conditions are set forth in banking agreements. These agreements become the basis for allocation of liability between the customer and the financial institution, particularly when unauthorised transactions occur due to the security of electronic banking systems being compromised.

This article will focus on the rise of private regulation of online banking services enforced through contractual agreements and the various factors giving rise to this development, including, but not limited to, the lack of effective government regulation of "fintech" providers and the wide variance of security procedures utilised by business customers of financial institutions.

This article focuses on the increasing use of "private regulation" to govern online financial transactions effected by deposit-taking financial institutions and non-depository lenders on behalf of business customers, particularly small to medium sized enterprises (SMEs). As used in this article, private regulation describes the contractual terms contained in service agreements whereby financial institutions seek to allocate risks between the business customer and the financial institution with respect to it providing specific financial services. It is argued that the rise of "fintech" firms will accelerate this trend to increasingly sophisticated private regulation through contract.

Financial technology firms (i.e. "fintechs") use proprietary algorithms and software that can sift through enormous amounts of data to arrive at decisional points to which the fintech has associated specific terms. In context of loans, the crunching of data culminates in a decision point to which specific pre-determined terms apply, such as maximum loan amount, maturity of the loan, interest rate, principal and interest payment schedule and permitted flexibility in the terms. All relevant applicant data is collected from an online application and other online sources, such as social media posts. The time in which a fintech can deliver a loan quote to an applicant is measured in minutes, not days.

One fintech advertises that, for a loan to a SME, all the SME needs is to be in business for 24 months, have at least USD 75,000 in annual sales, have no recent history of bankruptcy or liens, have a principal who owns at least 20% of the business and have a principal who has fair or better personal credit. Not needed is collateral for loans or credit lines under USD 100,000, business plans or projections, an onsite visit, appraisals or title insurance.

Deposit-taking financial institutions have found it difficult to match the fintech lending model as their lending procedures operate to a large degree in the offline world and are subject to more regulatory scrutiny. However, many of today's entrepreneurs grew up in an online environment which makes them gravitate toward lenders that will allow them to apply for loans online from wherever they may be (think mobile devices) and get fairly instant feedback so they either can lock-in the loan quote or use the quote to compare loan terms with other lenders. While some prospective fintech customers may be interest rate sensitive, others may feel the speed of obtaining a loan and placing the loan proceeds to work quickly justifies paying a higher interest rate than the interest rate which might be offered by a deposit-taking financial institution at the culmination of its loan application process.

Some deposit-taking financial institutions, particularly large ones, may not be organised to effectively serve the SME loan market which involves smaller credits. Banks such as JP MorganChase recently decided to provide funds to OnDeck, a fintech platform in the United States, for a programme that will focus on credits of USD 250,000 or less. With respect to the OnDeck venture, Jamie Dimon, head of JP MorganChase, was quoted as saying that it is "the kind of stuff we don't want to do or can't do." Although the size of the deposit-taking financial institution may be relevant (e.g. JP MorganChase versus a community banking institution in the United States), government regulation also may affect the lending policies and procedures of deposit-taking financial institutions holding insured deposits.

In the United States, a deposit-taking financial institution holding insured deposits is subject to regulation by at least two separate governmental entities. State-chartered banks generally are subject to supervision and examination by the relevant state banking regulator and the Federal Deposit Insurance Corporation (FDIC). National banks are subject to supervision and examination by the Office of the Comptroller of the Currency (a division of the US Department of the Treasury) and the FDIC. Many deposit-taking financial institutions have a bank holding company which is supervised and examined by the Board of Governors of the Federal Reserve System (FRB) which is the US central bank. Additional regulation will apply if the financial institution has been determined to be a systemically important financial institution (SIFI) by the federal Financial Stability Oversight Committee (FSOC). SIFIs may have representatives of government regulators embedded in their compliance and business operations.

By definition, non-depository lenders are not banks and are not subject to the same regulatory regime as deposit-taking financial institutions, primarily because non-depository lenders do not rely on insured deposits as a source of funding for loans. However, loans made to consumers by non-depository lenders

generally are subject to federal and state consumer protection legislation which provides, among other things, for specific consumer disclosures, a "cooling off" period whereby a loan agreement may be rescinded by the consumer without liability, caps on interest rates and fees, prohibition on mandatory use of other service providers (e.g. appraisal services or title insurance), and penalties for discriminatory or predatory lending policies. Non-depository lenders that provide loans to consumers may be required to register with a government regulator and may be subject to examination by such regulator.

As to consumer mortgage lending, the financial toll taken on the balance sheets (and share prices) of many US deposit-taking financial institutions by defending and settling numerous class action lawsuits and paying significant regulatory fines in connection with various alleged transgressions related to subprime mortgages and home foreclosures have led them to adopt more conservative consumer mortgage underwriting criteria.

This trend has been validated publicly by the chief financial officer of Wells Fargo, a US money-centre bank, where, in talking about consumer mortgage loans made by non-depository lenders, he said that Wells Fargo was not interested in making loans to riskier borrowers, even those who met US Federal Housing Administration guidelines; saying "those are the loans that are going to default, and those are the defaults we are going to be arguing about 10 years from now; we are not doing that again." Furthermore, the new consumer mortgage suitability obligations imposed by the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank Act) have incentivised deposit-taking financial institutions to concentrate on offering consumer mortgages meeting the definition of a "qualified mortgage" for which there is a presumption of borrower suitability.

Based on fear of repeating a pattern of consumer mortgage lending that proved extremely expensive to deposit-taking financial institutions and the advent of new borrower suitability obligations imposed by Dodd-Frank Act, it should not be surprising to see a migration in consumer mortgage lending from deposit-taking financial institutions to non-depository lenders. The *Los Angeles Times* has reported that 42% of all mortgages in 2014 were issued by non-depository lenders as compared to 10% in 2009 and non-depository lenders now account for 4 in 10 home loans.

Although lending to business customers is not as highly regulated as consumer lending, business loans made by deposit-taking financial institutions are subject to regular examination by banking regulators and mandatory reserves of capital to allow for potential losses on those loans. The allowance for loan loss and the methodology used by deposit-taking financial institutions is a separate category on which US deposit-taking financial institutions are evaluated by regulators under the 5-step CAMELS evaluation system. A CAMELS rating of "3" or more after a regulatory examination more likely than not would lead to corrective enforcement action against the deposit-taking financial institution by the relevant government banking regulator.

Not surprisingly, deposit-taking financial institutions in the United States generally organise their lending operations around what government regulators want to see during their regulatory examinations. Even where a deposit-taking financial institution has been given a CAMELS rating of "1" or "2," the bank examiner still may identify "Matters Requiring Attention" (MRA) by the board of directors and executive management. These MRAs could include criticisms of the policies and procedures employed by the deposit-taking financial institution in its credit analysis and decision-making for business loans.

For example, the previously mentioned fintech stated that, for credits less than USD 100,000, it would not require a business plan, appraisal or onsite visit with the loan applicant. If a deposit-taking financial institution made a business loan on a similar basis, it might be criticised by a bank examiner for not requiring a business plan or appraisal or failing to meet face-to-face with the loan applicant. Again, the difference is that monies funding loans made by a deposit-taking financial institution come, in large part, from insured deposits held by the deposit-taking financial institution.

Non-depository lenders, and especially fintech non-depository lenders, generally receive their funding for loans not from depositors but from institutional sources (e.g. pooled investment vehicles, insurance companies, pension funds, family offices and money-centre banks such as JP MorganChase) as well as individual or institutional investors purchasing debt instruments of the lender in private placement transactions or securities offerings registered with the US Securities & Exchange Commission (e.g. Lending Club).

Overreliance by deposit-taking financial institutions on wholesale funding through commercial paper and senior debt has been cited as a major contributor to the recent financial crisis when the financial markets' appetite for both short and long-term debt instruments issued by deposit-taking financial institutions suddenly dried up. The regulatory reaction has been to significantly increase mandatory capital reserves, mandate minimum five year "no call" provisions for certain instruments which may be treated (in whole or in part) as regulatory capital, require ring-fencing of retail operations and encourage the use of debt instruments which would convert automatically to equity in the event of a significant erosion of regulatory capital or catastrophic loss of share value.

Higher regulatory capital requirements, a visceral aversion to making consumer loans that could result in a repeat of the massive penalties and settlements that ensued from the subprime mortgage debacle and the additional regulation imposed on US financial institutions by Dodd-Frank Act may have a cumulative effect of reducing returns to investors in US deposit-taking financial institutions.

Hence, with investors chasing yield in a worldwide low interest rate environment, it is not unexpected that investors would reallocate their capital from deposit-taking financial institutions to less regulated non-depository lenders, particularly fintech non-depository lenders, which has allowed these lenders to raise substantial funds. However, institutional funding often is viewed as "hot" money which is not as "sticky" as consumer or business deposits and is apt to be more readily reallocated to other uses, especially when those alternatives offer better returns and where the risks are viewed as being equivalent.

Therefore, the regulatory concerns raised by the drying up of credit available from deposit-taking financial institutions when their sources of wholesale funding abruptly disappeared could be repeated in the context of non-depository lenders as they have no deposits upon which to rely if their institutional funding would disappear on a similar scale and time frame. With more consumers and businesses relying on credit extended by non-depository lenders, a future credit "freeze" affecting non-depository lenders could have a significant negative effect on the economy as deposit-taking financial institutions may not be able or may not want to fill any resulting credit void.

Notwithstanding the trend of reallocation of lending from deposit-taking financial institutions to non-depository lenders, each is operating more and more in an online environment and many fintechs operate exclusively in an online environment. Deposit-taking financial institutions and non-depository lenders providing financial transactions to business customers (which are not subject to the same level of government regulation as consumer lending) have begun using what this article refers to as "private regulation" to govern the financial services provided to these customers. The principal aim of private regulation is to allocate risks based upon contractual terms entered into between the business customer and the deposit-taking financial institution or non-depository lender for the provision of specific online financial services.

Although private regulation may have applications to both deposit-taking financial institutions and non-depository lenders, this article will focus on efforts made by deposit-taking financial institutions due to the sheer volume and value of transactions which they process daily, particularly in context of treasury management services utilised by business customers ranging from SMEs to multinational corporations. These provisions focus on systems and data security, reliance on properly authorised and authenticated transaction requests, fraud detection and prevention and liability and indemnification.

1| Systems and data security

Contractual provisions relating to systems security focus on the security of the IT systems used by the customer to transmit instructions to the financial institution and the processes it maintains with respect to individuals authorised to initiate online transactions with the financial institution. With regard to IT systems, financial institutions contractually will require the customer to maintain minimum system requirements set forth in the service agreement as amended from time to time by the financial institution and adopt policies and procedures requiring an annual risk assessment, review and testing of the customer's IT systems which also may include submission of the results thereof to the financial institution.

Since customer IT systems will be interfacing with the IT systems of the financial institution via internet connections to transmit instructions to the financial institution, financial institutions also will require customers to maintain security procedures specified by the financial institution with respect to hardware, software, and communication devices and facilities and agree to update, maintain and keep them current. Customers are obliged to maintain commercially reasonable security features on their computers, computer systems and electronic networks designed to detect and prevent willful or malicious destruction of computer programs, content, instructions or other electronic data stored in their computer systems and electronic networks or the introduction of unauthorised computer code or programs.

Mandatory use of security procedures such as codes, usernames, passwords, PINs or security tokens (collectively "access devices") also has become a standard provision in service contracts for business customers of financial institutions. In this regard, financial institutions are requiring customers to acknowledge in their service agreements that security of all access devices, whether created by the customer or the financial institution, are the sole responsibility of the customer. Furthermore, financial institutions are requiring that the customer develop, maintain and enforce policies and procedures with respect to issuing, re-issuing, changing and safeguarding access devices which may include prohibiting (i) sharing of access devices, (ii) storing of access devices within browsers, (iii) use of access devices for purposes other than services made available to the customer by the financial institution under the service agreement and (iv) using letters, digits and symbols that may constitute an access device for any purpose other than accessing the services made available by the financial institution under the service agreement.

With the rising use of mobile devices by customers to transmit instructions to the financial institution over the internet, financial institutions are requiring customers, when using mobile devices, to use only secure internet connections, ensure that the mobile devices meet certain security standards (including encryption) and scan such devices periodically to detect and remove any viruses, malicious programs or other harmful components.

Given the ever increasing sophistication of hackers, financial institutions also are placing in their service agreements various statements that they are not providing the customer with any warranty that websites, servers, networks and similar communication facilities that deliver online services to the customer by the financial institution or a third party service provider to the financial institution are free of viruses, malicious programs or other harmful components.

Financial institutions also are requiring customers to adopt and implement commercially reasonable policies, procedures and systems to ensure that the receipt, storage, transmission and destruction of data is accomplished in such a manner as to prevent loss, theft or unauthorised access to such data. These policies, procedures and systems include, but are not limited to, physically and electronically securing computers, mobile devices, paper documentation and backup media from unauthorised physical or electronic access and following guidelines for appropriate destruction of paper and electronic media so that the information cannot be read or reconstructed.

2| Authorised persons

Equal to the security of computers, computer systems and electronic networks of its customers is the scope of individuals at the customer authorised to initiate instructions to a financial institution on behalf of the customer (Authorised User) and individuals authorised by the customer to authenticate instructions sent by an Authorised User to the financial institution when either the customer or the financial institution requires authentication measures (Authenticator). In this regard, a customer may designate different individuals as Authorised Users for different types of transactions (e.g. payroll versus wire transfers) or level of transaction (e.g. less than USD 100,000 versus more than USD 100,000) or when a separate authentication measure is required (e.g. foreign wire transfers).

In this regard, there are two major issues of concern to financial institutions. The first is that the documentation from the customer to the financial institution identifying Authorised Users and Authenticators and their respective levels of authorisation be kept current at all times. Failure by a customer to alert its financial institution about the termination (whether voluntary or involuntary) of an Authorised User or Authenticator or a change

in the level of authority of an Authorised User or Authenticator creates a critical breach in the security of online financial transactions as the financial institution otherwise is unaware that the customer no longer deems the credentials of the Authorised User or Authenticator to be valid for issuing instructions on behalf of the customer to the financial institution. Notification of such changes is crucial in order for the financial institution to delete the identity of an Authorised User or Authenticator from its IT systems and invalidate, change or re-issue any access device.

The second major issue is the effectiveness of the customer's internal security policies and procedures applicable to access devices used by Authorised Users and Authenticators. Particularly, financial institutions are concerned that lax customer security procedures (e.g. storing usernames, passwords and PINs on a browser) easily could result in an unauthorised individual obtaining use of an access device, impersonating the Authorised User and initiating an online instruction to the financial institution which, in fact, was not authorised by the customer but appeared to the financial institution as being a valid instruction from the customer. Alternatively, an Authorised User could improperly obtain an access device from a co-worker and initiate an online financial transaction for a purpose or in an amount for which the individual did not have requisite authority from the customer (e.g. an Authorised User for payroll obtains an access device from the individual authorised to make vendor payments and initiates a payment from the customer to the spouse's company based on a fraudulent invoice).

3| Fraud detection and prevention

Financial institutions are becoming more vigorous in imposing mandatory fraud detection and prevention responsibilities on its customers through contractual obligations contained in its service agreements. Not only are certain contractual monitoring and reporting obligations imposed on the customer but the customer also agrees that the financial institution may suspend or terminate a specific service or all services covered by the service agreement under certain circumstances without prior notice to the customer.

For example, a customer may agree that the financial institution may take such measures as are necessary and appropriate to prevent any of the services being provided by the financial institution from being used to perpetrate a fraud on the financial institution or the customer. This agreement would permit the financial institution, where it has in good faith formed a reasonable belief that the customer, an Authorised User, Authenticator or a third party is effecting or attempting to effect a transaction using any service provided by the financial institution to the customer that may operate as a fraud on, or cause a loss to, the financial institution or the customer or would be illegal where performed, to suspend one or more services immediately without prior notice and for such time as it deems necessary or terminate such service altogether.

Where a financial institution has suspended a service to a customer, the customer further will acknowledge and agree that the financial institution, as a condition precedent to restoring the suspended service, may require the customer to provide such information, documentation, assurances or other matters which the financial institution deems appropriate. In a "real world" context, the financial institution may suspend a service due to the detection of an unauthorised transaction by an unauthorised person using an Authorised User's access device due to a lapse of internal IT security of the customer. In this instance, the financial institution may not want to restore the suspended service to the customer until it is satisfied that the customer has revised its internal IT security policies and procedures. This may take the form of the financial institution requiring an independent audit of the customer's internal IT security policies and procedures and being satisfied that the customer has implemented all recommendations made by that audit.

Data breaches have become all too commonplace and have expanded beyond financial institutions to other participants in global commerce. With respect to data breaches, the three important elements are notification, remediation/prevention and preservation/cooperation.

Notification. In its service agreements, financial institutions may impose an obligation on the customer to notify the financial institution within a specific time period (e.g. no more than 24 hours from discovery) when a customer knows or has reason to suspect that its access devices, computers, computer systems or electronic networks have been compromised which resulted or may result in the loss, theft,

manipulation, mis-characterisation, unauthorised access or any other threat to the security of such data, information or access device. After discovery and reporting, the customer may be obliged to take all reasonable measures, including retaining competent forensic experts, to determine the scope of the data breach and identify transactions affected by such breach which were not authorised by the customer.

Remediation and prevention. Upon discovery and notification of a data breach, a customer will be obligated to immediately commence remediation of the data breach and keep the financial institution apprised of its progress. To prevent further damage, the customer will agree that, upon delivery of a data breach notification to the financial institution, the financial institution immediately may suspend one or more services to the customer without prior notice or terminate any service to the customer. Restoration of a suspended service may require the customer to provide the financial institution with a high level of assurance that the cause of the data breach has been adequately remedied.

Preservation and cooperation. In data breach cases, it is important to forensically preserve equipment or programs that might have been involved in the data breach. Particularly, the device or program that might have been compromised should be isolated, taken offline and preserved for investigation by law enforcement and IT personnel from the financial institution. The customer also will agree to cooperate fully with law enforcement and personnel representing the financial institution with respect to the investigation of the cause of the data breach. This would include providing access to relevant employees of the customer.

4| Liability and indemnification

The fourth way financial institutions seek to use private regulation to govern online financial transactions is through the allocation of risk. This is accomplished by specifying those instances whereby the customer agrees that the financial institution will have no liability or limited liability and also the circumstances under which the customer will indemnify the financial institution for losses suffered or expenses incurred by the financial institution in connection with transactions effected by the financial institution upon instructions initiated by the customer.

Since there are a plethora of regulations in the United States addressing allocation of risk with respect to consumers, the risk allocations discussed herein are applicable only to business customers. Furthermore, these risk allocations generally do not alter the liability provisions of the Uniform Commercial Code as adopted by state jurisdictions in the United States which apply to business customers.

The four main categories in which customers will agree that financial institutions will have no liability generally include (i) negligence by the customer in allowing an unauthorised person to obtain an access device to initiate instructions to the financial institution; (ii) failure of the customer to maintain the specified computer, electronic network and internet security requirements; (iii) failure or interruption of service by an internet service provider and (iv) suspension or termination of a service by the financial institution without prior notice under circumstances permitted by the service agreement (e.g. actions necessary to prevent a fraud being perpetrated on a customer or the financial institution).

Perhaps the most common problem that arises with a business customer is that the customer negligently has allowed a person to initiate instructions to the financial institution on behalf of the customer who is not an Authorised User, not an Authorised User at the level of the service accessed or is a person who, in reality, is not an Authorised User but is posing as an Authorised User, whether or not using such Authorised User's access device. Under these circumstances, the customer agrees that the financial institution will have no liability for any loss which the customer may suffer as a result thereof or that a third party may suffer as a result of the customer's action, inaction, delay in action, negligence, misconduct or recklessness.

In service agreements with business customers, a financial institution will have a customer agree to limit the liability of the financial institution to those instances where the financial institution has engaged in activities constituting gross negligence or willful misconduct. Furthermore, the maximum amount of damages may be fixed using a specific formula such as all the fees paid by the customer to the financial institution under the service agreement

for the preceding twelve month period. In addition, the customer will waive any right to reimbursement of attorneys' fees and expenses, expert witness fees or forum fees as well as to any special, incidental, punitive, exemplary, compensatory, multiple or indirect or direct consequential damages of any kind, including but not limited to, lost profits or opportunity or investment, suits against the customer by the customer's employees, agents or representatives or any suit against the customer by a third party.

To protect financial institutions from suits by third parties that may have suffered loss or expense due to action taken or not taken by a financial institution for services covered by the service agreement, the customer will be obligated to indemnify and hold harmless the financial institution and its officers, directors, employees, shareholders and representatives for any and all losses, expenses, liabilities and costs resulting from (i) the negligence, error or omission of the customer to observe and perform properly each and every material term and condition of the service agreement, (ii) other wrongdoing of the customer (e.g. customer using a service offered under the service agreement to engage in unlawful activity) or (iii) any action taken or omitted to be taken by the financial institution in reliance upon information provided to the financial institution by the customer, unless it is proven that the activities of the financial institution constituted gross negligence or willful misconduct in the performance or non-performance of services to the customer in accordance with the terms and conditions of the service agreement.

5| Mandatory mediation and arbitration

Financial institutions, through forum selection clauses in service contracts, may require customers to resolve disputes in connection with the financial institution providing online financial services through mediation and arbitration. With respect to business customers, the designated situs of the arbitration most likely will be convenient to the financial institution.

6| Some policy questions

Thus, this article returns to its thesis that deposit-taking financial institutions offering online treasury management services to businesses as well as online non-depository lenders which are increasing their share of business lending, particularly to SMEs, are using contractual provisions as a form of "private regulation" to govern their online financial transactions with their business customers. If more and more financial transactions move into the online world, it is expected that this form of "private regulation" by contract will expand and become ever more sophisticated.

A policy question arises as to whether a SME should be treated similarly to a large corporation and imputed with the same level of commercial sophistication to understand and appreciate the ramifications of all of the terms and conditions similar to those described herein that are becoming prevalent in service agreements with financial institutions relating to the provision of online financial services. With respect to mandatory arbitration provisions in service agreements for online transactions, is it appropriate to require SMEs to arbitrate disputes at a situs that may be extremely inconvenient to them?

Based on the foregoing, is there a case to be made to develop consumer protection type regulation applicable to SMEs as it is expected that they increasingly will be consumers of online financial services with both deposit-taking financial institutions and non-depository lenders but may not have the business sophistication to understand that the protections they take for granted as individual consumers generally do apply in the business world in which their start-up businesses now operate?

The digital transformation of the financial sector: some concrete examples

Money and payments in the digital age: innovations and challenges

François VELDE
Senior Economist and Research Advisor
Federal Reserve Bank of Chicago

Virtual currencies like bitcoin are protocols that maintain consensus among participants about legitimate ownership of assets; ownership is transferred by modifying the consensus appropriately. In monetary applications the asset is a chain of transactions in scarce supply because the initiation of valid chains is restricted. Similar protocols, using a variety of methods to establish consensus, could facilitate simple or complex transfers of financial assets and reduce transaction and record-keeping costs, but doing so will require costly changes. Distributed ledgers replace trust between counterparties with trust in the protocol. Regulators will need to adapt their frameworks to ensure that the actors in payments and markets abide existing rule and do not create new risks, but also to protect the trust in the new protocols.

NB: The views expressed here do not necessarily represent those of the Federal Reserve Bank of Chicago or the Federal Reserve System.

The emergence of digital currencies in recent years has opened up a number of important questions. Unfamiliar technology, based on cryptography, is being put to unexpected use and holds the potential to alter the way payments are made. This article reviews some of these questions.

As the subject is new and complex, I will use the most prominent example of digital currency, bitcoin, as a guiding thread. I will first present how it works, then highlight its key features, before describing the developments that bitcoin spurred and conclude on the implications for financial stability.

1| The bitcoin protocol

It is important to keep in mind that bitcoin is a protocol, that is, a set of rules which users follow to send and receive information over the Internet. The information, however, is very structured and the purpose of the protocol is very specific: it is to disseminate authenticated transactions. Being the object of such transactions is what makes bitcoins money-like.

1|1 A description

Let us describe the protocol.[1] The best way to do so is recursive: suppose for now that *A* is the verified owner of a bitcoin. How does she transfer ownership to *B*? This takes place in several steps. First, note that to each individual corresponds an address, managed by a "wallet," an application residing on the individual's device and controlled with a password.[2] To transfer funds to *B*, *A* only needs *B*'s address. *A*'s wallet forms a transaction message proving that *A* indeed controls *A*'s address and declaring the funds transferred from *A* to *B*. At this stage, the message is somewhat like a check, or a payment order. In traditional banking the order is sent to a payer (e.g. a bank) who executes it. In the decentralised world of bitcoin, there is no payer. The order is, in effect, sent to everyone else, saying "please accept that *B* is now the owner of this bitcoin." This is the second step: the transaction message is broadcast to the network of participants, or nodes, in the protocol. Nodes receive transactions from other nodes and pass them on after checking that they satisfy certain rules; in particular, that each spender is a valid owner of the funds. They do so by checking that *A* was on the receiving end of an earlier transaction recorded in the list of all valid transactions, the "blockchain."

At this point, *A*'s payment to *B* is still not valid. To become valid, it will have to be authenticated by inclusion into the blockchain. Bitcoin is decentralised, so there is no custodian of the list. Every participant can have a copy of the list and can modify it, but they must follow the protocol's rules. This is the third step. Nodes of the network that wish to add to the list (we will see shortly why they would) gather up recently broadcast transactions into a block and start "mining," that is, solving a numerical problem. The problem involves a formula (called a hash algorithm) that combines texts of arbitrary length and produces a string of letters and numbers of fixed length (256 bits). It is relatively easy to compute the formula but it is virtually impossible to invert it, that is, to find the inputs that will produce a given output. The numerical problem is to find a number (called the nonce) that, combined with the last block on the blockchain and the proposed block, will produce a string beginning with *N* zeros. The only way to do so is to randomly try different values of the nonce until the resulting string satisfies the requirement, a process that requires computing power. The larger is *N*, the harder it is to satisfy it, or the more computer power is needed, which is why *N* is called the difficulty.

The first miner who finds a nonce broadcasts his block, with the nonce, to the network. The other nodes easily compute the formula with the proposed nonce and add the block to the blockchain. The nonce serves as proof that miners expended effort to solve the problem (so-called "proof of work"). But why did they expend that effort? Because they are allowed to include into the block a special transaction (called a coinbase) with no spender and themselves as recipient of a specific amount: in other words, a reward that creates new bitcoins and attributes

1 *See Antonopoulos (A.) (2014): "Mastering bitcoin: unlocking digital cryptocurrencies", O'Reilly Media, for a technically precise but readable account.*
2 *Strictly speaking, A knows a private key from which A's address was generated. With the private key A can generate "signatures", outputs of a mathematical function. The function is such that anyone, without knowledge of the private key, can verify that the signature was generated from the same private key as the address. The signature therefore serves as pubic proof that A knows the private key: ownership is knowledge of a private key.*

them to the lucky miner. Of course, this would induce new miners to enter the network. But the difficulty is periodically adjusted by the protocol, as a function of how long it took to solve the previous 2016 blocks, so as to maintain an average rate of six new blocks per hour.[3] As for the reward, it is halved every 210,000 blocks, approximately every four years (it is currently 25 bitcoins and due to halve in the summer of 2016).

Because mining is decentralised, the blockchain is not a pure straight line. Two miners may well find a solution within short time of each other and not know about the other's success. As a result, there may be two valid blocks serving as endpoint of the blockchain, and part of the network will try to add to one block while the rest tries to add to the other. The protocol dictates that the longest blockchain is always accepted as the valid one. Branches are usually resolved fairly quickly, because another coincidence of a valid block at each endpoint within a short time is unlikely to recur. Soon one branch will be shorter than the other and be ignored.

This, however, opens up the main (and well-known) risk of the protocol. A transaction could be included as valid in a block that is later discarded. The chances of being discarded diminish quickly as blocks are added and are nil after six new blocks. But a malicious miner could try to "double-spend" funds by voluntarily including a first transaction in a valid block and then creating another branch that includes a second transaction with the same funds. For this to work, the miner needs to mine faster than the rest of the network, which he would, on average, if he has more than 50% of the mining power.[4]

1|2 Features of the protocol

We can now understand how the blockchain is validated. In the bitcoin protocol, it is a combination of the consensus rule (the longest chain is the valid chain) and the proof of work (a valid block includes proof that work has been expended). The only way to alter the blockchain is to come up with a longer valid chain, and doing so requires effort. Moreover, the further back in the past (the deeper in the chain), the more costly it is to create another longer chain, since the network is constantly adding blocks in the meantime.

Mining creates the incentive to expend the work required for authentication; authentication is its own reward, and being honest is less costly than cheating. Mining also regulates the bitcoin supply. Bitcoins are only produced by mining at a rate that declines geometrically over time, so that the total sum of bitcoins converges to a fixed number.

What is the object of value in the bitcoin protocol? It is a sequence of valid transactions, starting from a coinbase and ending with its current owner. This is similar in some way to a land registry, but the entries in the blockchain don't link the owner to some object of value like land, they are themselves the object of value. They are similar to the entries on a central bank's ledger, except that there is no central bank. What makes bitcoin into a potential currency is that bitcoins are artificially scarce and are, by design, easy to transfer.[5]

But, unlike any previous currency, it has no alternate use (like precious metals), it has no government sanction (like legal tender), it is no one's liability (like a bank note). It is worth pointing out in passing that the term "mining" can lead to incorrect analogies. Bitcoin is not a commodity-based currency like gold. Mining refers to the resources expended in ensuring the safety of the protocol, which are analogous to the resources spent on anti-counterfeiting devices and armored trucks to ensure the safety of cash. The proper analog for a gold-based currency would be the expense of refining gold and minting it into coins, thereby certifying its authenticity. If gold ceases to be used as currency, the content of coins can be melted down and converted to other uses. For bitcoin there is no such physical asset.

Bitcoin can be seen as a claim: I own bitcoins if I have the password to a wallet whose address appears on

3 *The rate of one block every ten minutes is only an average; the length of time it takes to mine a block is a Poisson process, and can be as little as a few seconds. One's chances of mining the block are proportional to one's share of the total computing power applied to mining.*
4 *Technically, he needs less than 50% if he refrains from broadcasting his mined blocks until he has constructed a longer chain than the rest of the network.*
5 *They are also fungible, in that any two bitcoins are treated identically and any two sums can be combined. That need not be the case, however: users could treat differently coins with different histories (this is the idea behind "colored coins").*

the blockchain as entitled to transfer those funds. But it is a claim, not on a single entity, but on all participants: by using the same protocol as me they stand ready to accept my choice of the next owner of the claim. Put another way, a bitcoin is the ability to transfer a bitcoin. Of course the claim has value only to the extent that there are participants to honor it; but in this respect bitcoin is no different than fiduciary currencies, which, even backed by the State, only have value if others think they do.

Bitcoin thus does not eliminate the need for trust, but it places it elsewhere: *A* and *B* do not have to trust each other (or the State) to transact, but they do have to trust the protocol.

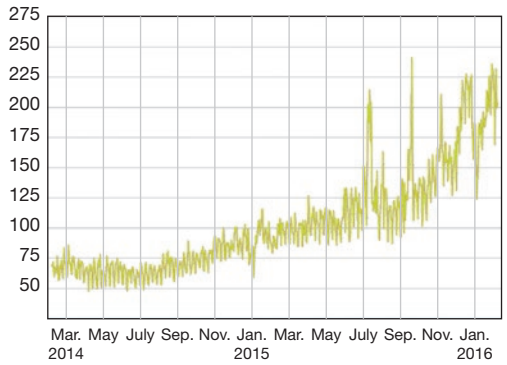
1|3 Bitcoin today

The bitcoin protocol is undoubtedly elegant. It has also proved viable, in the narrow sense that it is traded and has value. Launched in 2009, it came into notice in early 2013 and has remained in the news. The number of users is difficult to estimate, because any individual can have as any number of addresses, but probably numbers in the hundreds of thousands or low millions. The number of transactions has been steadily increasing over time, from a few per hour to two per second: a lot for a computer science experiment, but three orders of magnitude less than Visa (Chart 1). The USD/BTC exchange rate, which for the first few years languished below 10 dollars, has been above 200 dollars for more than two years, nearing 1,000 dollars in November 2013 and now (February 2016) around 380 dollars. At this price the 15 million bitcoins in existence have a total value of about 5 billion dollars, which is again a lot for an experiment, but four orders of magnitude less than fiat currencies in the world. Moreover, if something has value it is worth stealing, yet the bitcoin protocol has proved so far resistant to hi-jacking. It has also retained its primacy over hundreds of competitors and imitations.[6]

Bitcoin is still not a currency in the usual sense of a generally accepted medium of exchange. That is in part due to its unstable value. Chart 2 shows the price of bitcoin in US dollars over the past two years. The volatility remains tremendous: at 36%, it is higher than commodities or the more unstable currencies. To this day the use of bitcoins for retail purchases remains limited, and much of the activity is speculative in nature. Those merchants who do accept bitcoins do not quote prices in bitcoins, and tend to convert their receipts into their local currencies immediately, leaving it to investors to hold the currency. This will continue as long as the price of bitcoins remains as volatile as it has been: I am willing to accept a currency in exchange for goods because I expect to do exchange it for goods in the future, and I will only do so if I can depend on its value.

Chart 1
Number of bitcoin transactions per day

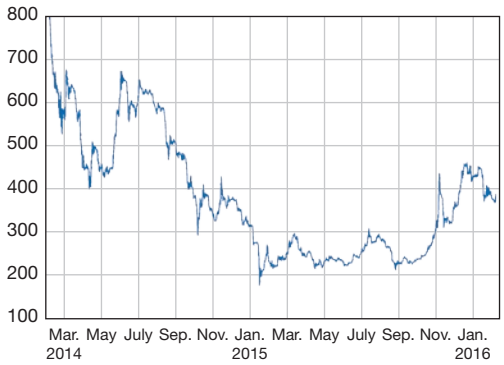
(Thousands)



Source: blockchain.info

Chart 2
Value of 1 bitcoin

(USD)



Source: blockchain.info

6 *See market capitalisations of various cryptography-based currencies at* http://coinmarketcap.com/all/views/all/

Bitcoin has also had its share of bad publicity, between the failure of a major exchange called Mount Gox and the use of bitcoin by participants in the illegal Silk Road operation; the latter attracting regulatory scrutiny. But the failure of a particular operator should be kept distinct from the performance of the protocol itself, just as the failure of one financial institution does not, of itself, invalidate a currency. The protocol guarantees a mechanism of transactions, but it is up to users to manage their wallets and save their passwords. As for the use of bitcoin for illegal activities, that is a bit of a red herring. Cash is well suited for illegal activities too, and in some ways better suited. After all, the blockchain keeps a record of all transactions. It is true that wallets are not necessarily linked to physical identities, but if they are, they can provide damning evidence in court, as the Silk Road prosecutions have shown.

1|4 What next? The future of bitcoin

The future of bitcoin remains an open question. It is unlikely to replace, or seriously compete with, any of the major currencies, but it has demonstrated its viability and usefulness.[7] It faces a number of challenges, although none seems overwhelming.

If bitcoin does become more broadly used, scalability will become a concern. The number of transactions per second has doubled over the past year, but the block size is limited in the current protocol to 1 megabyte, which translates into seven transactions per second. Increasing the block size poses no major technical difficulty, but raises the more general issue: how are changes made to the bitcoin protocol?

Bitcoin is what bitcoin users use; they use it because they find it in their interest to do so. The protocol is open-source: owned by no one, it is curated by a small number of programmers who seek to maintain consensus among users, but there is no formal mechanism for establishing consensus on the consensus. Proposals to raise the block size have created much debate within the community, raising the risk of a "hard fork", that is, a split in the community of users.[8]

More generally, any element of the protocol could be changed (including, for example, the limit on bitcoin creation), at the risk of splintering the currency. Bitcoin has survived outside competition, most of which consisted in attempted improvements upon the basic protocol, but could succumb to internal schisms. If bitcoin continues to grow, tensions about its nature and purpose will grow, and so will the need for a way to resolve them.

Aside from governance, another question is concentration of mining. As the size of the blockchain increased the (slightly utopian) original vision of bitcoin as a network of peers has, perhaps inevitably, been replaced by a world in which light nodes free-ride on the work of full nodes that verify proposed transactions and broadcast them and mining becomes a highly specialised activity. Indeed recent years have seen the advent of application-specific integrated circuits (ASICs), chips designed only to run bitcoin's hash algorithm. Mining is big business, currently mostly located in China, with large fixed costs (designing chips and building computers) and marginal costs entirely driven by the price of electricity. Whether features of the protocol (including block size) promote concentration is an open question. A self-interested miner would probably not want to become too large since excessive concentration opens up the possibility of double-spending, undermines trust in the protocol, and ruins the miner's investment. But a malicious miner might have the motivation and (in the case of state actors) the resources to reach a large market share.

Finally, as bitcoins move from an experiment in cryptography to transferable assets with real value, it inevitably comes into contact with the law, because the transfer of value is a highly and multiply regulated area.

7 *Ali (R.), Clews (R.) and Southgate (J) (2014): 'The economics of digital currencies',* Bank of England Quarterly Bulletin, *Q3, pp. 276-286.*
European Central Bank (2015): "Virtual currency schemes: a further analysis", February.
Bank for International Settlements, Committee on payments and market infrastructures (2015): "Digital currencies", November.

8 *In a soft fork, the new protocol restricts the blocks it accepts, but as long as 51% of miners switch it will naturally overtake any chain that follows the old protocol, whose followers recognise the blocks generated by the new protocol. In a hard fork, the new protocol accepts blocks that the old doesn't, so a chain will continue under the old protocol unless 100% of miners switch. Increasing the block size would accept blocks that were previously not accepted.*

As means of transferring value, bitcoin comes into contact with a host of regulations designed to prevent the financing of illegal activities. As a transferable asset bitcoin falls under the purview of regulations designed to promote fairness in asset markets. As an easily held but risky asset (with fluctuating value) it becomes an object of concern both for consumer protection agencies and for those who regulate entities that are both critical to the economy and very sensitive to risky assets, namely financial institutions and in particular banks. I will return to the question of regulation later.

While bitcoin faces challenges, it also poses challenges. The fact that bitcoins can be easily transferred over the Internet makes it a prime vehicle for payments, in particular cross-border transfers. Of course, the protocol only provides one leg of a transaction: *A* transfers bitcoins to *B*, but what *A* receives from *B* is outside the protocol, and it can be goods, services, or some currency. To use bitcoins in a cross-border transfer requires *A* to exchange her local currency for bitcoins and *B* to exchange bitcoins for his local currency. The potential of digital currencies nevertheless presents a threat for the incumbent financial system, including banks (and, perhaps, central banks). How this plays out will depend in part on the response of regulators, as banks have cause to complain that digital currencies' competitive advantage stems in part from their elusion of compliance costs. It also depends on which characteristics of digital currencies are valuable: the fact that they bypass the existing financial system, or rather the convenience of use over the internet, a feature that could be replicated by banks (and central banks) issuing their own digital currencies.

2| Beyond virtual currencies

Bitcoin has been a successful experiment, proof-of-concept that a decentralised digital currency is possible. It has done so by combining various existing elements of cryptographic technology into a coherent whole. The success of bitcoin has brought attention to these elements, some of which might be picked up on their own for uses that are related to, but distinct from, digital currencies.

2|1 Smart contracts

Recall that bitcoin is based on sequences of authenticated transactions. A bitcoin can be thought of as a chain of authenticated transactions ending with the current owner; the current owner has the ability to extend that chain with one more transaction. From a technological point of view, the transactions that form the links in that chain are pieces of code, instructions executed by applications that implement the protocol. Some of these instructions are conditional: for example, the transaction will be valid only if it is signed with the current owner's private key. More complex conditional statements are possible, either in bitcoin itself or in other protocols. The transaction might require multiple signatures, or might be made conditional on the prior occurrence of certain events that can be verified on the blockchain: *A* pays *x* to *B* at date *T* only if *C* has paid *y* to *D* before date *T*–*K*. More broadly, the conditions might be events outside the blockchain: the temperature in New York, the value of the S&P 500, the result of an election.

The term "smart contracts" to designate these transactions is rather unfortunate, since they are neither contracts nor smart. Rather, they automate the performance of contracts, such that neither the contract nor its performance can be disputed, because they are embedded in the immutable and public blockchain.

To some extent bitcoin can support smart contracts, although it was not its primary purpose. Other protocols, such as Ethereum, are designed with smart contracts in mind.

2|2 Distributed ledgers

Another element of the bitcoin protocol that has received a lot of attention during the past year is the blockchain, or the distributed ledger (DL).[9] The key property of the blockchain is that it secures among a set of participants a permanent and verifiable agreement on data (in particular, who owns what) in a decentralised manner. Various actors in the financial system, such as banks and exchanges, have

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

started investing resources in exploring the potential of blockchains for their own purposes.

There are some important differences with the bitcoin protocol. One is intent: the point of bitcoin is to create a transferable digital asset that can be used by anyone and is controlled by no single entity. For banks or exchanges, the point is not to create a new asset or to allow unlimited participation, but to record transfers of existing assets among a set of identified owners. As a consequence the means by which consensus is achieved among participants need not rely on proof-of-work as in bitcoin, and indeed in some applications other mechanisms are used (for example, the Ripple protocol relies on participants maintaining individual lists of trusted partners and on successive rounds of voting to validate additions to the blockchain). More broadly the set of participants who would be allowed to read from or write to the ledger could vary depending on the application.

What the blockchain may offer is an immutable record that is automatically and safely updated. This holds attraction for situations in which recording and altering ownership is done through disparate infrastructures and cumbersome processes. DLs could arguably simplify and speed up transfers, and also enable more complex transactions (such as smart contracts). They could also be safer, since the records are kept in multiple locations and are difficult to alter. Such advantages would be greater in contexts where it is easier to trust a protocol than to trust a single entity, although DLs might be an efficient way to coordinate activities within a single institution as well.

But applying DLs to bank settlements or securities exchanges is not straightforward. First, what makes them attractive (their simplicity, relative to existing systems) is also what will make them difficult to implement: existing systems will have to be adapted to, or replaced by, the ledger. Second, there remains the problem of the interface between the ledger and the "real world". Whereas bitcoin is self-contained (at least for one side of each transaction, the transfer of bitcoins), in broader applications the ledger's entries refer to pre-existing assets (bank deposits, securities) whose ownership is recognised, but not defined or regulated, by the protocol. If ownership of the assets resides "off the blockchain" then events on the ledger must be validated by the legal and regulatory system under which banks and exchanges operate. Of course, this interface problem would be greatly simplified if the relevant legal structures recognise the ledger itself as the authentic record, or if the assets being transferred were defined on the blockchain, but such changes will not happen soon.

To a large extent, then, the touted advantages of DL technology stem not so much from the technology itself but from the changes that its application presupposes.

2|3 The internet of value

The more enthusiastic supporters of digital currencies like to draw an analogy between the beginnings of the world-wide web in the early 1990s and the present time. Some go so far as to see bitcoin as the last missing piece of the internet, a protocol to transfer value like TCP/IP (Transmission Control Protocol/Internet Protocol) is a protocol to transfer data. What made it difficult to understand the potential of the Internet was the lack of easy ways to connect the real world to the internet, and convert the information we cared about into data. Both hardware and software have improved to the point that I can share a picture of my meal with thousands of people around the world in a few seconds. Perhaps the same will happen with the internet of value, once the interface between assets and the internet is improved.

The key question remains: will these innovations allow us to do things we already do, only better, or will they enable us to do things we couldn't do before, like smart contracts?

If we think back to the traditional parable about the birth of money out of a double coincidence of wants, money enables transactions that would otherwise not have taken place (as does credit). As our lives and the objects we have and use become increasingly connected to the internet, so payments may become easier and transactions may take place that couldn't before. In particular, one virtue of digital currencies is their almost unlimited divisibility (the smallest amount of bitcoin is 1e-8, or less than 1-e03 cents), enabling "micro-payments" for very small services, which could themselves be provided automatically. The notion of smart contracts is another intriguing possibility. Finally, the blockchain is more than a ledger, because it records not just the current state of ownership but

the complete histories as well. The implications of this richer information set have yet to be fully explored.

3| Stability and disruption

Whether it is virtual currencies, blockchains, or the Internet of value, change is bound to happen. The challenge for regulators and policymakers is to respond to it.

3|1 A threat to existing currencies?

It is perhaps not a coincidence that bitcoin emerged in 2009, soon after the financial crisis. Although the original paper describing bitcoin[10] cited the costs of financial intermediaries as a main motivation, some of its early proponents were concerned not only by the stability of the existing financial system, but also by response of the main central banks to the crisis and the increase in their balance sheets. The autonomy of bitcoin from political pressures and human error and its money-supply rule enshrined in the code seemed to promise incorruptible stability. In addition, the emergence of a currency unconnected to any State seemed reminiscent of Friedrich Hayek's conceptions of currency competition. Finally, the open-source code and peer-to-peer structure appealed to those who saw the Internet as a template for equality between citizens.

Six years later bitcoin is nowhere near displacing the US dollar, and few of its supporters expect it to. Decentralised digital currencies like bitcoin may yet provide alternatives in economies with unsettled monetary systems, and people may turn to them as they turned to foreign currencies during past hyperinflations. But they have not yet disrupted existing payments systems in advanced economies and are unlikely to do so any time soon.

For one thing, the democracy of equal nodes has given place to a fairly concentrated mining industry, and, as discussed above, managing the protocol has proven difficult. Furthermore, the performance of existing currencies, in terms of the stability of their value, has been much better than anticipated by some. Quantitative easing has not devolved into hyperinflation. In this context, digital currencies like bitcoin offer no fundamental improvement. There is no active monetary policy in bitcoin: the money supply rule is mechanical and based on calendar time only, with no feedback from its current market value. Even Milton Friedman, who once advocated a k% rule for money growth, might not have gone so far as to set k to *0* forever. An asymptotically fixed supply of bitcoins can be an advantage compared to the uncontrolled money supply of a hyperinflation, but does it improve over an already stable currency? And if digital currencies offer competition among currencies, it is not the kind of competition that Hayek envisaged: he thought of entrepreneurs, not robots, competing to offer better currencies.

3|2 Regulatory responses

Monetary policy won't be the first victim of digital currencies, but regulators have already taken notice of the innovations they bring.

Regulators will either find ways to fit the innovations into the existing framework, or else adapt the framework to fit the innovations. The first response is easier and quicker, and naturally the one followed until now. One of the most urgent needs was to ensure that the innovations were not allowed to offer new tools to evade money-laundering and anti-terrorism laws, and one of the earliest determinations in the United States was the applicability of regulations on money transmitters to digital currencies in March 2013. A money transmitter receives funds from one person and transmits to another person, and the regulator decided that such funds could take the form of digital currencies. Another important dimension of regulatory scrutiny has been the prevention of fraud and the protection of consumers and investors.

In the United States regulators have defined a virtual currency as a commodity, others as a currency, yet others as an investment; mainly in order to bring it under their respective purviews. This is not necessarily a sign of incoherence; rather, it shows that in order to fit digital currencies into the framework

10 *Nakamoto (S.) "Bitcoin: a peer-to-peer electronic cash system"* (https://bitcoin.org/bitcoin.pdf). *As is well known, Nakamoto is a pseudonym and the author's identity remains unknown.*

it was not necessary to determine their nature. Regulations are designed to prevent certain actions, and if those actions can be performed with digital currencies then the regulations apply.

Regulating bitcoin itself is thus difficult, because it is a protocol, not anyone's asset or liability; but regulating users of bitcoins, on the basis of their purpose, is possible. Banks are regulated on the basis of the contractual and fiduciary relation they have with their customers, and this can apply to bitcoin banks or bitcoin exchanges, all the more as bitcoin resembles money and allows to do better something we already do. And even if regulating an open-source protocol is not easy, the protocol itself, or code that relies on the protocol, can adapt to regulatory pressures if needed to survive.

The regulatory response will be more difficult if the innovation allows us to do something new, in which case the framework may have to adapt. It is difficult to predict how that might take place, but in conclusion a few simple points can be made.

At a basic level, regulators will need to scrutinise the safety of ledger technologies if they are to be used extensively by banks, as with any IT innovation. But to the extent that distributed ledgers are a common tool used by important players, they have systemic implications.

Digital currencies and DLs don't replace trust, they place it elsewhere: in the protocols. This is another area which guardians of financial stability will have to monitor closely. In the United States, the presumption has generally been that innovation is good and best left to the private sector, but finance is an area where consumers (and voters) have expected government oversight to ensure trust, whether through deposit insurance or securities markets supervision. The global financial crisis has reinforced, not diminished, this expectation.

Finally two important questions will arise for policymakers. One is that virtual currencies and ledgers, based on peer-to-peer technology, mark a shift away from centralised trading. The other is the extent to which their use will reduce the need for liquidity by increasing net settlement. Both trends, if they materialise, would run counter to the developments that have taken place since the global financial crisis began.

Future evolution of electronic trading in European bond markets

Elizabeth CALLAGHAN
Director, Market Practice and Regulatory Policy; Secondary Markets
International Capital Market Association

Bond market trading is going through unprecedented change today and will continue to do so over the next years. The traditional bond trading model, mostly reliant on market makers and voice broking, is being eroded. This is partly due to a natural evolution of bond trading, driven by technological progress and the strive for cost efficiencies, resulting in an increasing electronification of markets. The traditional trading model is, however, also being undermined by regulatory pressures which are reducing the capacity for broker-dealers to hold, finance or hedge trading positions, and thus provide liquidity as market makers. The upcoming implementation of Europe's new trading rules under MiFID II will be another key component exacerbating the scale of the transformation. There are signs of the new market structure to come but no one can predict exactly how the secondary bond markets will look in 5, 7 or 10 years. We can only take an educated guess. What is certain is that bond trading must adapt and innovate in order to endure. This will involve all facets of trading including people, technology and a redirection of business strategy. The change will affect the entire market place: sell-sides and buy-sides, but also trading platforms and other trading technology providers. The bond trading ecosystem will see new (and possibly disruptive) entrants, innovative incumbents and adaptive trading protocols and venues. Although often referred to as an equitisation of fixed income, the changes will take a different shape from that of previous developments in equities given the structural differences between equity and fixed income trading. Overall, the transformation will be painful as regulation and technology are disrupting established market structures, presenting serious challenges for many industry participants. However, the transformation will also create opportunities through innovation for market participants.

The focus of this paper is the "future" evolution of electronic trading in European bond markets. The purpose is to complement the Bank for International Settlements (BIS) paper on the current state of electronic trading in fixed income markets,[1] taking note of the Banque de France's contribution. The following will hopefully provide a market practitioner's perspective on how the changing fixed income trading model will progress. A glossary is available at the end of this article for reference to some of the more technical electronic trading terminology used.

Electronic trading in fixed income is often referred to as the "equitisation" of fixed income. However, this is an oversimplification. Bond market electronic trading will take a very different path from that of equities. This is due to the vast differences in both these markets:

- equity instruments – 6,810 shares admitted to trading on regulated markets in the European Union, on average trade 400 times per day;

- fixed income instruments – over 150,000 debt securities (contained in Xtrakter's Computer Updated International Database or CUPID), on average trade 1.5 times per day.[2]

Customarily, fixed income markets have been a combination of voice market making and intermediation (using inter-dealer brokers and hybrid voice-electronic systems to source liquidity), organised largely around banks (broker-dealers) and a relationship-based network of clients. The model has primarily been:

- broker-dealer to client, i.e. bank to asset manager or pension fund manager (the buy-side);

- broker-dealer to dealer, i.e. bank to bank or bank to inter-dealer broker (IDB);

- but not client to client, i.e. asset manager to asset manager.

The market practice has traditionally been based on market makers, who are mostly broker-dealers who provide two-way pricing to their clients in a range of bonds, regardless of their ability to find an opposite seller or buyer at the same time, not least since the simultaneous "coincidence of want" is highly improbable in bond markets. Where clients are sellers of a bond, the market maker will show a bid and take the bond onto their own book, which they will hedge and look to sell, either to another client or another broker-dealer, at a later time. Where clients are buyers of a bond, the market maker will show an offer and sell the bond, which they will cover via the repo market if it leads to a short-sell, hedge and look to buy back in the market at a later time.

In addition, a broker-dealer requires three interdependent components in order to offer market making to counterparties. This is made more difficult due to prudential capital adequacy and leverage rules causing balance sheets and derivatives markets to become far more expensive. Market making needs the following to be successful:

- ability to hold inventory on balance sheet;

- a liquid repo market in order to fund long positions or cover short sales;

- the capacity to hedge in the derivatives markets.

As regulatory pressures reduce the capacity for broker-dealers to hold, finance or hedge trading positions, the traditional source of bond market liquidity is being eroded.

Lastly, it is important to note that the market structure in fixed income for dealer-to-client has always been identified as quote-driven (versus "order-driven" in equities). Prices are only offered in response to a counterparty request for quote (RFQ). Because this is unidirectional, details of price formation (including actual volume and size) are not shared with the public. Therefore, quotes and trade prices for an individual bond can contrast widely depending on the broker-dealer.

Bond market structure has been described as glacial and resistant to change. However, markets are

1 *See* BIS report (2016), *"Electronic trading in fixed income markets", January.*
2 *See Biais (B.), Declerck (F.) (2007), "Liquidity, Competition and Price Discovery in the European Corporate Bond Market", IDEI Working Papers 475, Institut d'Economie Industrielle (IDEI), Toulouse (August); and 2009 figures from ICMA http://www.icmagroup.org/Regulatory-Policy-and-Market-Practice/Secondary-Markets/Bond-Market-Transparency-Wholesale-Retail/So-why-do-bonds-trade-OTC-/*

currently undergoing a transformation due to natural evolution (such as technological advancement and cost efficiencies) as well as the impact of regulations. The old-style bond trading model is breaking down. There are signs of the new form to come but no one can predict exactly how the secondary bond markets will look in 5, 7 or 10 years. We can only take an educated guess.

The future & darwin's "survival of the fittest"

In order to endure, bond trading must adapt and innovate. This will involve all facets of trading including people, technology, and a redirection of business strategy. The bond trading ecosystem will see new, possibly disruptive entrants, innovative incumbents and adaptive trading protocols and venues.

Many market participants agree that 80% of revenues come from 20-30% of clients. This fact is more in focus now than ever before. Broker-dealers are identifying priority clients and assessing the clients by opportunities to cross-sell rather than single-product (or region) sales strategies, e.g. clients need to be a "client" for more than one business line such as derivatives, emerging markets, equities or possibly even a revenue producer in other global regions. Hence, for many, the old market-making model is disappearing.

This is having a knock-on effect. Banks are restructuring and redirecting their strategies. They are becoming agency brokers, niche players or getting out of certain areas of the bond business altogether, as evidenced in many of today's news headlines.

Some wonder if the traditional model of capital commitment and monetisation of the bid-ask spread is becoming a less appropriate method of bond trading, suggesting the market could move to a more commission-based model. With a commission-based model, overheads relating to regulatory change (e.g. IT costs) might be passed on to clients more easily through commission rates (which are more standardised).

Buy-sides as well as sell-sides are restructuring and redirecting their business strategies. The costs involved in meeting regulatory requirements are escalating dramatically. The industry's view is that, when MiFID II comes into effect, many smaller buy-side firms will not have the resources to build the IT facilities required by the law. A further risk is that they may be de-selected as clients by broker-dealers. So, what are market participants doing? The smart ones are adapting to the future (including modifying portfolio construction based on expected liquidity, reviewing broker coverage and service levels and reviewing regulatory impacts on trading).

1| Strategy redirection: firms reshaping business strategies due to lack of returns in fixed income

Niche brokers are already starting to appear. They are the smaller sell-side dealers consolidating their businesses, relying on reduced trading and sales teams while using electronic trading platforms to reach more investors. These participants are becoming the new specialists in certain sectors or segments within the bond markets, particularly credit. They are combining electronic trading and sourcing with a directed balance sheet.

The new entrants, or indeed incumbents, who will be here in the next 5 to 10 years, will be innovative and most likely use technology based solutions to face market challenges.

1|1 New entrants

New entrants will not be hindered by the fragmented IT legacy of large incumbents, so they may be more agile in solving challenges for the industry. These tools, solutions and new business ventures will use advanced technology. Below is a description of potential new entrants, along with an explanation of why they might emerge successfully onto the electronic trading landscape:

Order management systems and execution management systems (OMS/EMS) – Provide straight-through processing (STP) connecting internal systems across the institution. The benefits are: smooth, efficient, seamless integration

interconnecting risk management, credit-checking, and position management – ensuring trades are within risk limits and meet client obligations. Basically, OMSs and EMSs connect the front office to the back office, achieving efficiencies, cost-reduction and risk-mitigation. They also use Financial Information eXchange (FIX) messaging technology (buy-side/sell-side communication protocol), enabling dealers to send out orders and support multiple protocols such as RFQs, request for stream (RFS) and indicative pricing with other market participants. FIX also distributes liquidity to platforms and interacts with the trading infrastructures of other market participants.

Transaction cost analysis (TCA) – TCA lets a firm analyse the cost of a decision to trade over a specified time period with respect to various benchmarks. Traditionally, TCA is heavily used on the equities buy-side desks. Fixed income TCA has been viewed as one of the most difficult areas in which to offer performance measurement, due to a lack of market transparency and of available data. There is a split between vendor-provided TCA and internally built solutions, in what little is available in fixed income markets today. In the coming years, with the data that will be generated by MiFID II, TCA for fixed income will grow.

Data analysis tools (of any kind) – Unstructured data such as voice/e-mail/chat creates problems for evidencing best execution. Deep trading history along with sophisticated data processing tools will increase the level of granularity and allow an almost forensic approach to data analysis. This will enable better price formation for both the sell-side and buy-side. Moreover, the buy-side will benefit from better visibility and traceability of end-investors. Again, due to the reams of data that will be produced for MiFID II compliance, any tools that analyse data for optimised performance measurement will rise to the top.

Algorithmic trading in fixed income – Algorithmic trading (complex computer-based programs following defined sets of instructions) is usually thought of in terms of equity trading. However, algo traders from equities now see an opportunity to leverage their existing investment in fixed income trading. As more technology is introduced into fixed income trading and it gets easier to acquire datasets (MiFID II data) for back-testing, fixed income traders will use algos for low-touch trading in order to assist with the consequences of regulations, such as margin compression due to increased costs. The growth of algorithmic trading will primarily be seen in certain liquid fixed income products, such as government bonds (we are seeing this already today). However, it is expected that algos will become more attractive for other fixed income instruments as data becomes available under MiFID II.

"False positives" (FPs) IT tools – Technology tools that identify false positives (bonds that are labelled as liquid but in fact are illiquid; i.e. incorrect liquidity classification). FPs are a key quirk that is a side effect of MiFID II liquidity calibrations. This is probably one of the biggest issues raised by MiFID II. The sell-side is concerned about false positives as they affect market-making capabilities, and the buy-side is concerned as they can impact perceived portfolio liquidity. Therefore, any tool that can accurately identify false positives will be highly valued.

Regulatory tech services – Any technology-based service or consultancy firm that can assist with keeping market participants (buy-side, sell-side and platforms) on the right side of compliance and best execution will do well in the years ahead. The successful providers will identify for firms the necessary data to meet regulatory obligations while managing downstream IT implications of regulations.

Internaliser engines – Firms that operate multiple trading desks, across different time zones or subsidiaries will require an advanced technology system that provides the ability to internalise order flow automatically. This will enable them to execute trades in-house and thus save brokerage fees.

Information networks (INs) – Sourcing and aggregating liquidity. IN firms provide an aggregation layer, providing the trader with two key sets of functionality: a global view of liquidity and a choice of trading protocols and execution mechanisms from which to select. The trader uses this layer to obtain an accurate, timely view of available liquidity across markets. INs use a high degree of technology embedded in buy-side and sell-side's internal systems, e.g. Algomi, B2Scan.

Consortium-owned networks between buy-side and sell-side – Collaborative efforts between the buy-side and sell-side, where market participants

are coming together to attempt to create liquidity in the bond markets. The hope is to enable greater transparency of trading interests across the marketplace between buyers and sellers of bonds. The relationship is made up of banks and asset managers, e.g. Neptune.

These collaborative-based firms use open standard technology, allowing participating sell-sides to send pre-trade indications to their clients (asset managers) across the network. Consortium networks provide flexibility of connectivity options. The buy-side can receive pre-trade indications from multiple banks in a standard format using a single connection (i.e. FIX protocol).

1|2 Innovative incumbents

Price-maker hedge funds – Hedge funds are not new entrants but they will adapt to the new landscape. While traditional buy-sides will most likely not step in as "price makers" on central limit order books (CLOBs) or other agency-only trading venues, hedge funds may step in (providing it suits their trading strategies) and provide larger illiquid pricing, bolstering liquidity. This is because hedge funds do not have the same legal structure and mandates as asset managers.

Independent market making firms – Independent market makers will start to emerge, focusing on market making in specialised instruments or sectors. Less expensive, improved and widely used technology will help to facilitate these market making firms as advanced technology is lowering the barrier to entry, e.g. XTX Markets.

Niche trading – Banks will also develop specialised expertise and be known for trading and making markets in certain asset classes or regions. This will notably be the case for emerging markets as this sector can, in certain circumstances, return greater yield. Technology can also connect clients to regional experts around the globe.

Multi-asset trading – As banks and buy-sides review their bottom lines more, it will become obvious that some IT and skill sets can be shared. It is too expensive to have totally separate infrastructure carrying out trades that would ultimately benefit from sharing of knowledge between asset classes. There are a few multi-asset trading desks today on the buy-side but we will see more emerging in the next 5 to 10 years and even on the sell-side too.

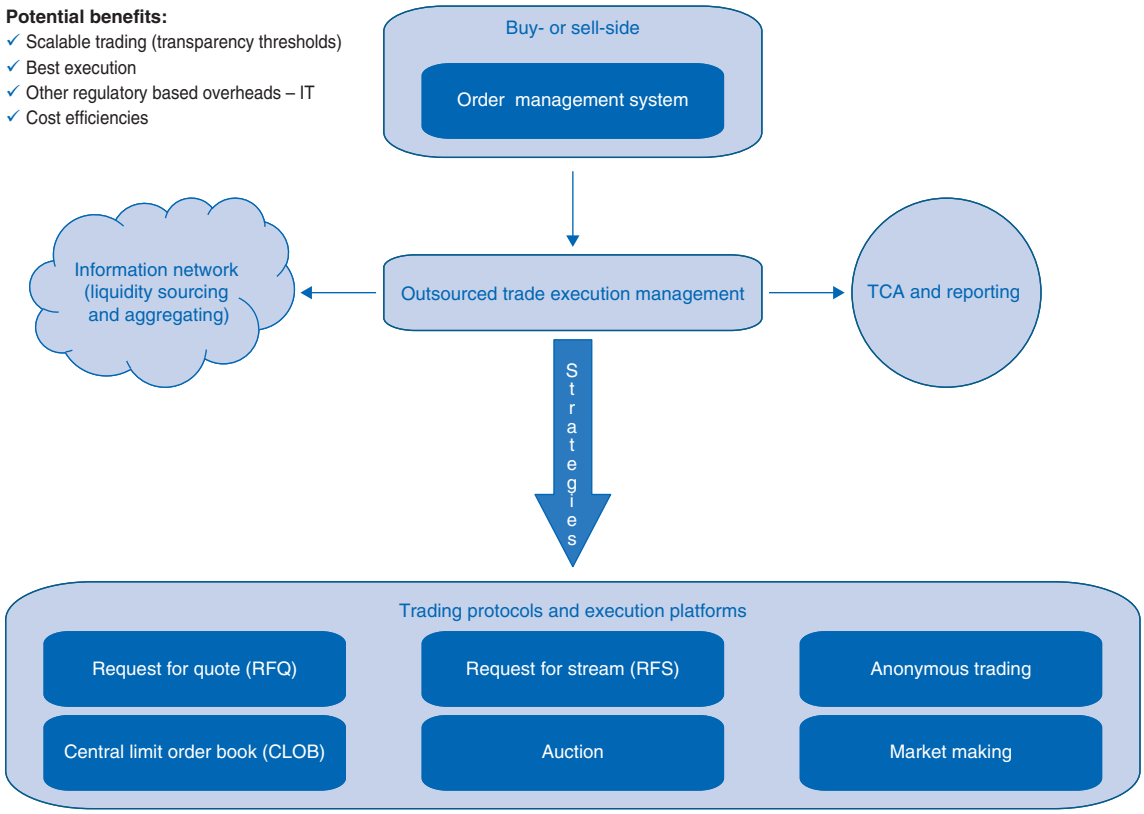
"Super trading desks" or "outsourced trading" – Large regional sell-sides and buy-sides will create centralised super desks which have extensive market making capabilities and global reach. We are already seeing signs of larger buy-side desks offering trading services to smaller firms to provide the benefits of economies of scale, e.g. BNP Paribas Dealing Services.

The level of spend for anything relating to connectivity such as platform access, compliance, legal, risk and IT may be so great that Tier 2 and 3 asset managers and smaller sell-sides may investigate alternatives. Outsourced trading may become a very viable option. This is already in use today, although it is still in the early stages. However, it should develop more fully in the coming years and become a centralised source for regulatory management (although regulatory obligations cannot be outsourced) and scalable trading. In some operations it may end up as a multi-asset offering. In addition, the outsourced provider will be able to evidence best execution to regulators and trade report to the public on behalf of its clients. Another service that outsourced providers could offer clients (using TCA) is the ability to report back on broker performance measurement.

It is expected that a greater degree of access to and response from market makers will create higher levels of liquidity and, overall, should improve portfolio performance through enhanced trading performance. In addition, due to economies of scale, these "super trading desks" will more frequently hit MiFID II's large-in-scale (LIS) waivers and deferrals (regulatory thresholds requiring forced transparency for both pre- and post-trade activity) due to trade combining. It is important to note that this outsourced "serviced" trading could be set up for routine routing of business, ad-hoc requests or it could even be an independent firm offering a centralised consolidated service.

Lastly, outsourced trading desks of the future will be able to cope with a diverse set of protocols and apply them based on targeted trading strategies and the universe of market structure in high or low liquidity situations: RFQs, RFS, exchange traded or CLOBs, OTC market making, anonymous trading and all potentially global or local.

Outsourced trading scenario



Source: ICMA.

2| Evolving market structure – trading protocols and venues

One thing is certain, electronic trading (including trading venues and protocols) is at the core of senior management planning for market structure redesign. Traditional trading protocols and platforms will also evolve and adapt to the new world of electronic trading in cash bonds. MiFID II, particularly in combination with other regulations, will be the biggest driver of radical change in market structure. Some are prophesising the disappearance of protocols we have used for years, such as OTC voice-based broking. However, most believe this is not the case. Current platforms and protocols will still exist but the usage weightings will shift and, over time, shift quite dramatically. Further down the line, today's platforms and protocols will be joined by new innovative platforms and protocols.

The platforms and protocols are split between the categories below. It should be noted that organised trading facilities (OTFs) and systematic internalisers (SIs) will join the "multilateral" category of platforms and protocols once MiFID II comes into effect on 30 January 2018.

- Bilateral: RFQ, RFS, OTC including market making.[3]

- Multilateral: CLOBs, exchanges, multilateral trading facilities (MTFs) and post MiFID II, SIs and OTFs, crossing platforms (anonymous or semi-lit) and auctions (time-based bid/offer multilateral trading).

In all probability there will be a staged approach to how protocols and platforms evolve in the coming years. It does not seem unfeasible that the initial introduction of MiFID II could prompt a reversion to off-venue trading as the market tries to ascertain

3 *Acronyms are defined in the glossary.*

the implication of a more "lit" (transparent) market. Progressively, it is expected that as the market gets used to the new MiFID II trading landscape, more electronic protocols and platforms will be used. For example, there may be an increase in buy-side to buy-side electronically traded volumes for large or illiquid trades.

All electronic platform and protocol usage will increase, to some degree or other. Even bilateral protocols will take on more electronic characteristics. For example, the market is already seeing a rise in automated RFQs, where buy-side traders seek quotes from brokers in a more controlled, auditable environment compared to what is offered via traditional voice broking (pure OTC).

While agency-only and multilateral trading will increase, it is a matter of "horses for courses". Not all of the multilateral protocols and platforms are suited to all types of trades. Below are some examples of how they are used and how they may possibly evolve.

All-to-all – This is the true definition of multilateral trading (connecting dealers, investors and other market participants on a centralised all-to-all platform). CLOBs are an example of "all-to-all" with built-in electronic limits (while CLOBs are the most prominent examples of all-to-all, anonymous trading protocols and platforms, hybrid RFQ protocols and even auctions might also, at times, be described as all-to-all).

CLOBs will increase but only in retail-size flow. This is due to the buy-side not having the mandate to make prices and post on platforms.

Also, no one (buy- or sell-side) will want to leave a large/illiquid price available to be picked off on a CLOB. Therefore the price on the CLOB will not be a representative price if it is large or illiquid.

Interestingly, many believe the volume of these limited-size trades will increase as it did in equities.

RFQs (request for quote, bilateral, one-to-one) – Only protocols that can create believable and consistent pricing will have the best chance of success. The price has to be an "acceptable" current price in order to trade and be competitive. While there will be an increase in multilateral trading, bilateral RFQs will not disappear. A trusted conversation between a buy-side and sell-side trader about the nuances of a trade will always be valued.

The downside to RFQs from a buy-side perspective is that, once information about a potential trade is discussed, it can be acted upon. This "information leakage" can lead to a market impact (the price going against them). Hence, the rise of electronic crossing platforms (anonymous trading platforms).

OTC market making – While market making may be choosier in the future, it will always be necessary, particularly when a buy-side trader requires size.

The risk for the buy-side is that they might be unable to get a market maker to make a ready, "executionable" price on a particular bond as and when they need it. The sell-side is becoming more discerning as to which clients they offer balance-sheet.

Anonymous trading platforms (multilateral) – Anonymity is attractive to market participants who want to complete large transactions without drawing attention to their trades, since such attention could impact market prices. These trading venues are anonymous and/or semi-lit, and can be buy-side to buy-side or buy-side to sell-side. Price formation is in the dark (non-transparent) as the anonymity protects participants.

The anonymous trading venues, particularly buy-side to buy-side, will follow the equities model and become successful. However, as with equities there will only be one or two successful venues as most believe that only 6-10% of trades will be carried out on this type of platform (results based on voting carried out at a trading-based conference held in late 2015).

The risk for these trading venues or platforms is that a trading venue can match a buyer and a seller in the dark but they need to have an idea of a mid price to trade successfully.

Systematic internaliser (SI) – The rationale for the SI regime is to move "dark", off-venue trading, onto "lit" venues by creating a level playing field and greater price transparency between OTC and venues (basically, SIs prevent activity moving off "lit" venues onto dark ones, i.e. they "light up" the more active OTC markets). The key requirement of an SI, compared to a non-SI, is that it is subject to similar pre-trade transparency obligations as a regulated

market (RM), MTF or OTF, as this is expected to aid price formation for investors.

MiFID I introduced the SI regime, but for equities only. MiFID II extends the SI regime to bonds. The SI regime under MiFID II requires an investment firm which, on an organised, frequent and systematic, and substantial basis, deals on its own account by executing client orders outside an RM, MTF or OTF.

SIs for bonds are required to provide firm quotes to clients on request (standard market size) for liquid bonds. However, SIs are able to limit the number of transactions a client may enter into, and the clients to whom the quotes are provided, so long as their commercial policy is set in a non-discriminatory way. Thus, SIs are able to manage their trading activity and the associated costs and risks.

From a market-making perspective there are no obvious benefits to an SI, as there is no guarantee of competitive pricing. The purpose of the SI regime is not to provide pricing or liquidity; rather it is to provide transparency in the OTC market. It could be possible that some investors, as part of their best execution policy, may require quotes from SIs for specific instruments when trading OTC. Alternatively, whether a bond has a certain number of registered SIs, could be a component of an investor's internal liquidity scoring.

Multilateral trading facilities (MTFs) – In MiFID II, requirements for MTFs have been aligned with those of RMs in order to create a more level playing field. Most agency trading platforms will be classified as MTFs.

Organised trading facilities (OTFs) – Alongside MTFs, this will be a third type of multilateral system (regulated markets or exchanges, MTFs and now OTFs) in which multiple buying and selling interests can interact in a way which results in contracts. OTFs do not apply to equities. They will come into force with MiFID II.

The execution of orders on an OTF is carried out on a discretionary basis. There are two different levels of discretion for the operator of an OTF: (i) when deciding to place or retract an order on the OTF, and (ii) when deciding not to match a specific client order with another order available in the system at a given time, provided it is in compliance with specific instructions received from a client and best execution obligations.

An OTF will not be permitted to trade against its proprietary capital and this ban also applies to the capital of any entity that is part of the OTF operator's corporate group.

Most believe that post MiFID II IDBS, where they execute "name give-up", will be the only trading venues classified as OTFs.

3| Evolution and staff restructuring

When looking at the evolution of trading and market structure, it is often easy to overlook the "people" who trade. How will they evolve to meet the needs of the future? There is a great deal of staff restructuring going on at sell-side firms today. This is due mostly to performance-related issues in the fixed income business. In several cases, what might have been a solid fixed income business in the past is now not performing or looking likely not to in the near future. Fixed income businesses have recently published declines in activity ranging from 20% to 30 %, and in some cases much more. In addition, many industry participants have declared that bank balance sheet availability has been reduced by approximately one-third. There is not enough business to support a large staff of bond traders and sales people. In 2015, we routinely witnessed staff downsizing or "re-sizing" as it is often referred to. This trend looks set to continue as firms react to changing landscape of bond trading.

One of the ways to cut costs and rationalise business is to lay off older, more experienced sales and trading staff. However, this is creating a culture of "juniorisation" where not only are the trading and sales teams becoming smaller, but banks are relying more on younger, less experienced staff. Buy-sides are complaining about young traders on desks making execution errors and increasingly becoming incapable of making prices or managing positions. There is also a reduction in proactive sales people bringing trade ideas to the buy-side traders.

There are unintended consequences to this trend of "juniorisation" and the disappearance of "go to" traders and sales people. Now more than ever, investment

managers are following "the knowledge" rather than the "firm name". The danger for the sell-side is that previously reliable clients are reviewing their broker lists and leaving.

These major moves on the chessboard are causing anxiety amongst older, experienced sales and trading staff. However, it is not all necessarily doom and gloom. While the sell-side are downsizing, the buy-side is "upsizing". Experienced sales people and traders who were made redundant are now moving to the buy-side to bring "the knowledge" directly onto asset management desks. Furthermore, many of these redundant "chess pieces" are now the ones turning up as heads of the various new electronic trading initiatives. It is important for the industry to note that this "sell-side to buy-side" chessboard move may help out former sell-side players, but it does not mean these players are bringing traditional capital commitment along with them.

The only possible exception to the "juniorisation" phenomenon and the demise of voice brokering is seen in repo trading. In the repo market, older, experienced traders are still seen as adding value, and providing something that the inter-bank CLOB cannot: knowledge, flow, colour, experience and discretion.

Lastly, many of the roles that were traditionally carried out in the equities world are now finding their way over to fixed income markets. A few years ago, no one in fixed income trading had ever heard of market structure or market structure strategy. Today in fixed income, we can see evidence of these roles emerging with the hiring of "global head of credit market structure strategy", "head of liquidity strategy & market structure" etc. In these challenging times for profits, these roles are proving vital in the decision-making around business rationalisation and overall competitiveness.

Conclusion

Bond market trading is going through unprecedented change today and will continue to do so for the next 5, 7 to 10 years. Much of it will be painful as regulation will not be a smooth course. The outcome of MiFID II and other regulations will likely impact staffing, bond availability and potentially future buy-side investment strategies.

However, regulation and technology are creating new market structures. While this will present challenges for some industry participants it will also create **opportunities through innovation** for others. Those participants will become Darwin's electronic trading "survivors" in the future.

Emergence of big data: how will it impact the economic model of insurance?

Thierry DEREZ
Chairman and CEO
Covéa

Improved knowledge of one's clients, new pricing models based on greater risk segmentation, the recent wave of connected objects which paves the way for new personalised services, etc.; the exact contours of the "big data" phenomenon and its potential consequences may appear fuzzy and definitions differ from one person to another. However, there is a unanimously shared feeling that this technological revolution will not spare the insurance sector, and that in a few years business models will probably be widely different to what they have been in the past.

This perception is often associated with the prospect of a demutualisation, resulting from the differentiation to an extreme degree of insurance offers and prices from one person to another. While the development of new technologies and the exacerbation of competitive pressures could actually result in much finer segmentations than what is now the case, this fear must however be put into perspective. Besides the regulatory constraints that are present and do not appear to be on the decline, an extreme segmentation would go against the very interests of insurers, creating excess risk and profit volatility.

Structural changes will also arise from the new types of relationships between insurers and their policyholders (when taking out a policy and, even more so, throughout the life of the insurance contract). In the longer term, the changes in the actual underlying risks could constitute structural breaking points of economic insurance models. The announced development of the driverless car is a perfect example.

In this context, access to data will be of decisive importance and may eventually have an impact on financial stability. It therefore seems essential to define clear rules for accessing these data, based on self-determination and individual freedom of choice.

The big data phenomenon refers to the emergence of data sets that are so large that they cannot be processed with conventional data processing tools. This development covers both the emergence of the data themselves (in practice digital data, which are increasingly vast and varied) and the ability to store and process them through new and alternative methodologies, both aspects being completely inseparable one from the other.

Big data: a multifaceted phenomenon

For several years, big data have served increasingly diverse purposes in all fields of knowledge (biology, environment, aeronautics and space research, etc.) and in all sectors (automotive, retail, financial sector, etc.). However, the development prospects are probably still largely unknown. The scope of analysis is extremely variable, depending on whether one sticks to a strict definition of the phenomenon, or whether one considers all the uses that can indirectly arise from this new capacity to process massive datasets. The boundary of this second definition is likely to shift as it can include examples of platformisation (Uber) or the future introduction of the driverless car. These latest developments have indeed been made possible, or at least fostered, by the new data processing capacities. In the case of Uber, the quality of the service depends to a large extent on the geolocation of customers and vehicles, and the ability to measure demand in real time in order to adjust prices and encourage supply. In the case of the driverless car, technical developments also depend on the instantaneous analysis of the information collected, from both the other users and the transport infrastructures.

Of course, the insurance sector has not been spared by the wave of big data, even though objectively the economic model of insurance has so far not been disrupted. Examples of application are, here also, extremely diverse. They may notably concern customer relations (better knowledge of policyholders and their needs, simplification of the insurance process, etc.), the development of new price offers or models ("pay how you drive", connected bracelets, etc.) or, in a less visible manner to the customer, the improvement of operational efficiency (portfolio steering, fraud detection, etc.). These fields of development are multifaceted and concern all departments of insurance companies; it is therefore difficult to analyse the phenomenon of big data and its potential impact on the insurance sector as a whole. Although the different aspects are somewhat interconnected, we will look at successively the impact on offers and price segmentation (Part I), on customer relations (Part II) and the impact of the change in the underlying risks themselves (Part III).

I A MORE PRONOUNCED PRICE SEGMENTATION RATHER THAN A DIFFERENTIATION OF PREMIUMS

One of the comments often made is that policyholders now want to pay the "real price of their risk," i.e. the insurance premium that corresponds exactly to their characteristics and their behaviour. This wish, combined with the growing ability to compare prices – thanks to online quotes and aggregators –, with the growing competition between economic players and especially with the ability for insurers to have a better understanding of each client could, according to this logic, eventually lead to a complete differentiation of prices. This differentiation based on individuals would mean the end of what is the very basis of insurance: risk pooling, between policyholders, between generations, between geographic areas.[1]

This consideration should not be ruled out entirely, but analysed with great caution

In general, a client wishes to obtain the best service at the best price. In insurance, this corresponds to the most protective guarantees possible given his/her profile, together with efficient services and a fluid user experience, all at the lowest price. However, should this premium correspond, at least in the eyes of the policyholder, to the "real price of risk"? If so, the insurance business would be a singularity, different

1 *However, it is important not to confuse the concepts of solidarity and pooling. Indeed, it is in principle possible to pool heterogeneous risks (the law of large numbers applies if the variables are independent, but without necessarily being identically distributed). Insurance of industrial risks for example is a pooling of tailored contracts and prices, thus individually differenciated.*

from all other economic activities. In most economic approaches, the client sets the price that he/she considers legitimate – i.e. the price that he/she is willing to pay – according to the use that he/she makes of the good or service, to the balance of supply and demand in the market, but also to regulation. The latter may prohibit certain pricing methods, under a social consensus or in the name of a public policy objective. The willingness to pay may therefore differ very substantially from the actual cost of the good or service. This explains why a consumer may agree to buy goods with high margins (luxury goods, smartphones, etc.) or, conversely, may not be aware of sometimes paying a price that is below the production price in the case of highly subsidised goods or services (transport, certain agricultural products, etc.).

Just as fundamentally, in the field of insurance, the very notion of "real price of risk" does not correspond to an intangible mathematical reality. It does not stem from an unquestionable measure perceived in the same manner by the insurer and the policyholder, or even by all insurers. Insurance is based, in its very foundation, on heterogeneity calculations, a notion that is often wrongly likened to that of hazard. While the policyholder is exposed to a number of hazards, it is not these hazards that the insurer can directly assess, but the heterogeneities between policyholders in the occurrence of accidents, which are the ex-post manifestation of these hazards.[2] Whatever the actuarial sophistications used or the expert judgments, pricing grids are all based on averages drawn up on populations considered as homogeneous and sufficiently large for the application of the law of large numbers to make statistical sense. This improper assimilation between hazard and heterogeneity can also sometimes lead to misunderstandings, and make one lose sight of the fact that purely quantitative risk measures (for example Solvency II) result primarily from an indirect risk assessment, and can therefore in essence meet their objective only imperfectly (VaR of 99.5% at a 1 year horizon for the above example). However, it must above all make us aware that the "real price of risk" does not exist, and is by its mere construction a subjective notion which differs from one insurer to another. Indeed, the "real price of risk" is the average cost of the category of policyholders considered but, besides the fact that two insurers may have slightly different statistics on a given category, the categorisation itself is not univocal. Advances in medicine which isolate one risk factor will result for example in a category breakdown. Access to such and such information using a smartphone or connected object will also result in a category breakdown, but a different one. Two different insurers will assign a different "fair price" to a given policyholder based on the data at their disposal. Similarly, a given {insurer; policyholder} pair, immersed in two societies with different levels of technology or imposing different data processing constraints, will display a different "real price of risk".

Nevertheless, this should not lead to the conclusion that big data will not result in any changes to pricing. Instead, it raises the question of segmentation: what level of detail can we reach to build homogeneous groups of policyholders, which are fine enough for pricing to be tailored to individual situations (and therefore be competitive), yet large enough to obtain statistics that make sense? The answer is a technical one, and as such big data can be an important development, but it is also and very fundamentally a social and regulatory one.

We are currently witnessing a strong trend towards the segmentation of policyholders, with greater price differentiations between "good" and "bad" risks. This movement is likely to continue in the coming years. Today it is more commercial than technical: the strong competitive pressure, coupled with the right to cancel a contract at any time introduced by the Hamon Act, may lead some players to focus on certain insured populations deemed more profitable. And technical developments could further reinforce this trend. For example, if it is possible to model individuals' driving behaviour with sufficient accuracy, this information could become a central element in the pricing of car insurance, thus increasing price segmentation compared to the current situation.

But how far can this segmentation go? It is difficult to give a definitive answer to the question but many elements go against the complete individual differentiation of prices, a controversial issue often brought up. As already mentioned, there are technical constraints: an excessive segmentation would result

2 *See Frezal (S.) (2015):* « Aléa et hétérogénéité : l'amalgame tyrannique ».

in such a breakdown that statistics would no longer be relevant. This would therefore lead to excessive volatility in claims in each homogeneous risk class, the cost of which would probably exceed the marginal gains in terms of pricing. Excessive segmentation would therefore run completely counter to the very interests of insurers,[3] and thus ultimately of policyholders. Furthermore, the temporal aspect should not be overlooked: in insurance, prices are usually set for a relatively long period (usually one year, with at best a monthly adjustment), which reduces the relevance of taking account of instantaneous data. Overly segmented prices could further expose insurers to a poorly controlled change in risk during the guarantee period, related for example to a change in the behaviour of certain policyholders.

There are also a series of regulatory constraints. Already, regulations lay down strict limits designed to avoid discrimination and to create solidarity. This solidarity is often intergenerational (for example the system of coefficients for reducing/increasing premiums in car insurance, which tends to reduce the premium for young drivers relative to the real cost of risk; or conversely the capping of the price differentials between the young and the elderly in referenced complementary health insurance policies, which reduces the premium of the latter). These restrictions do not seem ready to subside, quite the contrary, as evidenced by the ban introduced in late 2012 on making any price differentiations between men and women. In this same logic, increased segmentation, if it ends up by reducing the solidarity between policyholders and intergenerational solidarity, and even more so if it results in situations of insurance exclusion, will inevitably raise the question of its social acceptability and therefore of its regulatory framework.

2| Changes in customer relations

Another aspect of the changes in the economic model of insurance brought about by big data concerns customer relations. Indeed, big data has the faculty of altering two fundamental aspects: the knowledge of one's clients, and the nature and frequency of the relations that may be established with them. The phenomenon is however not unique to insurance and covers most sectors.

In terms of the knowledge of one's clients, the dynamics generated by the big data phenomenon in the insurance sector are not new, and are based on the simple idea that the more one knows one's policyholders, the better one is able to offer the right products at the right time. Beyond the simple obligations of collecting customer needs and providing advice, these dynamics have already led to a strengthening of the information requested when taking out a policy or notifying a claim, or to a more efficient use of this information (development of customer relationship management). Big data can amplify this phenomenon by combining these specific data with third-party data (social networks, connected objects, etc.).

Marketing is probably the field where big data opens up the most development prospects. Thanks to the nature and the exponential frequency of available digital information (internet searches, cookies, etc.), it is possible to identify the needs of customers much more precisely than in the past and therefore to address them at the most appropriate moment. This will enable insurers to offer their customers a perfectly targeted package when taking out a policy, and more personalised services throughout the life of the contract. This change is not without dangers for market participants, and in particular creates an intermediation risk (or "uberisation" according to the meaning generally associated with this word). A new player, which is better capable of capturing these information flows than others, could thus intermediate between insurers and policyholders as broker and capture a significant share of the operating margin. However, this phenomenon offers at the same time real opportunities to improve the relationship with policyholders.

These phenomena are, again, not specific to insurance but probably affect this sector with particular acuity. Because it is a service activity, this service being a promise only exercised in the event of a claim, and because insurance is in many cases perceived by the policyholder as an obligation as much as a protection. Insurers have largely understood the need to change this perception, and have worked for several years

3 *See Charpentier (A.), Denuit (M.) et Elie (R.) (2011):* « Segmentation et mutualisation, les deux faces d'une même pièce ».

on extending their role and developing new types of relationships with policyholders (prevention, development of new services). Digital developments, and big data in particular, can contribute to this extension by leading to more and better targeted interactions. The development of connected objects may be interesting in this respect, as it offers policyholders the possibility of transmitting more information to their insurers, and the latter the possibility of permanently stepping out of a simple role as claims settler.

All this is possible only if insurers manage to fully reassure their policyholders on the use made of their data. This requires in particular demonstrating that the data freely provided will be used to tailor offers or services more effectively to individual needs and not to abusively select risks. The current regulatory framework is already very restrictive in terms of personal data protection and respect for customer privacy – with even stricter rules in the health sector. However, a certain distrust unquestionably remains, which can only be lifted through better communication on the part of insurers, on the framework in which data is transmitted and used.

3| The mutation of underlying risks, a potential upheaval for insurance

A third aspect related to the new capacity to capture and understand data concerns the changes in the very nature of risk. While it is less immediate than the previous two, this development appears particularly structuring as certain insurance activities could purely and simply disappear, giving rise to new risks and thus new insurance opportunities.

We will not discuss in detail the issue of cyber-risk, which deserves to be examined separately. While cyber insurance, whose market is still limited – total premiums of EUR 2.5 billion in 2015, collected mainly in the United States – is likely to increase significantly in the coming years, its development is conditioned by the ability to really measure risks in a rapidly changing world. Furthermore, companies are still faced with the choice between a technical solution (securing of data and infrastructures, backups, etc.) and an insurance solution.

The emergence of the driverless car is, however, a particularly interesting example of a possible (if not probable) mutation in uses and risks, impacting the insurance sector with full force. This development is here again closely linked to the new ability to process ever-increasing data flows in real time: data picked up from other vehicles and from the infrastructures themselves, in the future data transmitted from the latter, etc.

The maturity and even more so the speed of deployment of this technology are uncertain and depend on many parameters: technical developments of course, the regulatory framework, the ability to convince users on a wide scale which requires demonstrating a low risk of accidents, etc. It is therefore difficult to define at what horizon driverless cars will account for a significant share of the car fleet. But the phenomenon itself seems unavoidable.

It is clear that these developments will have a highly structuring impact on the car industry and, by extension, on the car insurance sector. There are several studies on the subject, which attempt to quantify these phenomena. One of them[4] concludes that the emergence of the driverless car, together with new uses that might ensue, could lead to a decrease of more than 50% in the car fleet by 2040. Indeed, a number of households could decide not to have their own vehicles (or at least reduce their number) and to have recourse instead to rental services, if it becomes possible to have access almost instantly to an autonomous vehicle at a desired location. This choice would result from a cost comparison between buying a car and renting an autonomous vehicle even on a regular basis. By implication, this could lead to a general decline in claims – and therefore insurance premiums paid – and a substantial switch in the car insurance business, from an individual insurance to a fleet insurance. Not to mention the thorny legal issue of who is liable in the event of an accident: the car manufacturer, the operator or the supplier of IT solution?

As the authors of these studies readily acknowledge, all these expectations or estimations are to be considered with caution. In addition to the uncertainty about the speed of deployment mentioned above, the change in uses will depend on the very perception that

4 *See Johnson (B.A.) (2015): "Disruptive mobility", Barclays Research Department.*

future generations have of the car. But this example clearly shows how a technological breakthrough, born of data processing and advances in IT, can alter the very nature of a risk and represent an upheaval for the insurance business.

Conclusion: access to data, the decisive point in the competitive battle and a potential issue for financial stability

All of these aspects raise the fundamental issue of access to data. Indeed, a player that manages to capture certain key data sources better than others will unquestionably have a competitive advantage. The phenomenon will clearly be tenfold greater if it obtains an exclusive access to the information flow. This highlights how a good "customer experience" is more than ever a key aspect. In all the areas where an intermediation phenomenon has been observed, these intermediaries (Uber, Airbnb, but also Google for mobile telephony) have made a name for themselves thanks to a simple, fluid and efficient service offer that has convinced users. This offer has enabled them to have privileged access to their customer data and consolidate their position, and not the reverse. The commercial battle is not won with data, but with an unassailable customer experience, which in turn provides access to data. In this respect, it is worth mentioning a certain discrepancy between the expectations of customers, which expect an ever-increasingly fluid and instantaneous offer, especially through digital channels, and the regulatory framework (for example on distance selling of financial services) which does not always allow these expectations to be met.

However, there may be cases where the excellence of the customer experience is not sufficient to ensure access to specific data. The most convincing illustration is that of the automobile, if autonomous vehicles based on a single technology are developed or even, in the shorter term, if a few manufacturers or OEMs control all the data gathered by the "intelligent vehicles". However, this phenomenon can potentially be extended to other private insurance sectors (for example home insurance thanks to connected objects), the business insurance sector being, for some time at least, less concerned. This obviously has major potential commercial consequences. We previously mentioned intermediation risk. There is also the risk for insurers of being played one against the other by third parties which would have exclusive access to certain technologies or key data.

Even if this does not really represent a short-term threat, it can also have consequences in terms of financial stability. If major players are likely to lose a significant share of their business and profitability overnight, because they lose access to key data, this could weaken the system as a whole. The very existence of this risk would probably alter, by implication, the investment strategy of insurers to reflect this increased uncertainty (reduction of risky assets, reduction of asset duration, etc.). Given the sums involved, and the fact that this phenomenon would occur across world markets, the impact on the financing of the economy would be very significant. Today these risks appear rather theoretical and diffuse. This aspect should not however be completely ignored in future discussions.

In the shorter term, it is important to define a clear framework for accessing data. In order to guarantee healthy competition and, more importantly, an adequate protection of individuals' personal data and privacy, this framework should proclaim the principle of self-determination, i.e. the right for each individual to decide how his or her personal data are used. In this way, each individual could decide to freely transmit these data to a third party and, symmetrically, to later ask it to remove them. In a world where access to information will more than ever occupy a central place, it is essential to create the conditions of confidence, which requires first and foremost a great degree of transparency.

Big data challenges and opportunities in financial stability monitoring

Mark D. FLOOD
Research Principal
Office of Financial Research
US Department of the Treasury

H. V. JAGADISH
Bernard A. Galler Collegiate Professor of Electrical Engineering and Computer Science
University of Michigan

Louiqa RASCHID
Professor of Information Systems
University of Maryland

The exponential growth of machine-readable data to record and communicate activities throughout the financial system has significant implications for macroprudential monitoring. The central challenge is the scalability of institutions and processes in the face of the variety, volume, and rate of the "big data" deluge. This deluge also provides opportunities in the form of new, rapidly available, valuable streams of information with finer levels of detail and granularity. A difference in scale can become a difference in kind, as legacy processes are overwhelmed and innovative responses emerge.

Despite the importance and ubiquity of data in financial markets, processes to manage this crucial resource must adapt. This need applies especially to financial stability or macroprudential analysis, where information must be assembled, cleaned, and integrated from regulators around the world to build a coherent view of the financial system to support policy decisions. We consider the key challenges for systemic risk supervision from the expanding volume and diversity of financial data. The discussion is organised around five broad supervisory tasks in the typical life cycle of supervisory data.

NB: Views and opinions expressed are those of the authors and do not necessarily represent official Office of Financial Research or US Department of the Treasury positions or policy. The authors acknowledge helpful comments from Greg Feldberg, Julie Vorman, and David vun Kannon. Comments are welcome, as are suggestions for improvements, and should be directed to the authors.

1| Background

"Big data" means more than simply larger storage requirements, or collecting data from social media platforms with millions of participants. "Bigness" is a symptom of scalability issues in one or more dimensions — the four *Vs* of volume, velocity, variety, and veracity (IBM, 2016). "Big data" is a misnomer, suggesting that "bigness" is an intrinsic characteristic of a dataset. Rather, bigness describes the relationship between a dataset and its usage context.[1] A dataset is too big for a particular use case when it becomes computationally infeasible to process the dataset using traditional tools (MongoDB, 2016). Scalability is a binding constraint for any process, of course, if extrapolated too far. Big data can create an inflection point where differences in scale imply transformational differences in the costs and benefits associated with using the data.

Big data is not the only challenge facing financial stability monitors, who potentially have the entire financial system in scope and face data scalability challenges on many fronts.[2] Fundamental economic factors, such as macroeconomic uncertainty, credit conditions, market volatility, liquidity, and contagion risk, remain core concerns. On the measurement front, the salient supervisory challenge is often too little information to integrate, analyse, and make actionable, rather than too much. Some official pronouncements, such as the Office of Financial Research's recent *Financial Stability Report* (OFR, 2015), focus on the first-order task of filling data gaps: do supervisors lack adequate data coverage, data quality, and data access to achieve their mandates? The existential questions of data availability must take priority over the scalability questions of data management. The Bank of England's recent One Bank Research Agenda (BoE, 2015) identifies big data, including news feeds, social media, and transaction-level trading data, as potentially important untapped lodes of information for central banking research.

The proliferation of measurement technologies in all sectors of society, much of it captured through our interactions with the Internet and cellular networks, means that many industries are confronting big-data scalability issues simultaneously. These challenges are revolutionising a diverse array of fields, including official statistics (Kitchin, 2015), scientific research (Hey *et al.*, 2009), retail sales (Manyika *et al.*, 2011), health care (Horvitz, 2010), and even the arts (Somerset House, 2015). The financial services sector is not immune. Casey (2014) identifies six general types of data that are coming together to compose the big data inventory for central banks: macroeconomic, survey, financial institution, third-party, micro-level, and unstructured (examiner reports, social media, etc.). We focus on official data collections of macroprudential supervisors, but many of the issues discussed extend to other data types.

The upshot is that new datasets are emerging from a variety of sources, including official collections such as stress-test exposure details, third-party vendors such as market intelligence and social media platforms, and search tools on the public internet. One characteristic common to all these new sources is a large increase in data requirements. Trading activity, for example, is growing exponentially, and at an increasing rate (Flood, Mendelowitz, and Nichols, 2013, Figure 1; Kirilenko and Lo, 2013, p. 51). Given the persistent growth in computing power and the automation of finance, supervisors have reoriented toward "data-driven" regulation; see, for example, Stein (2015), CFPB (2013) and FRB (2015).[3] A prominent example of data-driven supervision is the collection and analysis of detailed contractual terms for bank loan and trading books for stress-testing programs in the United States and Europe since the 2007-09 financial crisis. The scale of the problem is inexorably outstripping the capacity of certain legacy processes that rely significantly on human examiners and analysts. "You can't solve exponential problems with linear solutions; one must fight computation with computation."[4]

1 *Diebold (2012, p. 4) notes, "…someone reading this in twenty years will surely laugh at my current implicit assertion that a 200 GB dataset is large," further observing that the Large Hadron Collider, the world's largest particle accelerator, today generates a petabyte (10^{15} bytes) of data per second.*

2 *We are more concerned with data management issues rather than specifics of legal supervisory authority. We use the following terms interchangeably to avoid cluttering the text with clarifying language: "financial stability supervisor (or monitor)", "macroprudential supervisor," and "systemic risk supervisor;" these refer to national or international authorities responsible to maintain awareness of and respond to financial-sector stresses and crises.*

3 *Pattison (2014) offers an interpretation of this trend from the perspective of industry. Recent conferences on big data in financial supervision include those hosted by the Bank of England (Bholat, 2015), Sweden's Riksbank (Hokkanen,* et al.*, 2015), and European Central Bank and International Institute of Forecasters (IIF, 2014).*

4 *Attributed to Prof. Banny Banerjee (Chase, 2015, p. 72).*

Exploiting the new resources will require novel approaches to data management and statistical analysis, and financial stability supervisors have taken notice. These challenges can arise in the most inconvenient circumstances — for example, in the midst of a financial crisis. The potential uses for big data apply to routine situational awareness, as well as occasional spike loads on analytical resources during episodes of market stress. An effective response requires an appreciation of the underlying forces at work.

Experience in numerous sectors shows that the transition point, at which scalability begins to bind, is likely to arise in one of four general directions, often referred to as the four *Vs* of big data. Macroprudential examples include the following:

• **Volume** – Roughly speaking, the simple size (in bytes) of a dataset, which can place a strain on storage and computational resources. Modern economic datasets often outstrip the query-processing capacity of relational databases such as structured query language (SQL), creating a market for so-called "NoSQL" tools, according to Varian (2014). In some cases, one can attenuate this burden through data aggregation or compression. One example of a financial monitoring task that will experience significant increases in data volumes relative to legacy practice is the move toward data-centric audit analytics for forensic analysis of financial accounting records (AICPA, 2015).

• **Velocity** – The rate at which data arrive, which can strain network bandwidth and stream analytics (O'Hara, 2015). An example from macroprudential supervision is real-time monitoring of high-frequency data streams during a flash crash (Berman, 2015). By design, high-frequency trading firms deliver quote and transaction messages at the technical limits of network latency, creating a significant throughput burden for any downstream process.

• **Variety** – The diversity of schemas, or formal structures, for data arriving from different sources, which can strain data integration processes (Halevy, *et al.*, 2006). This applies to the integration of legacy systems after a bank merger, and also to systemwide integration. An example is aligning and synchronising legal entity identification schemes across a wide variety of independently managed datasets (Rosenthal and Seligman, 2011). Without coordination, the alignment of identifier registries across n back offices requires $(n^2\text{-}n)$ mappings between them; for example, 10 back offices implies 90 mappings (Flood, 2009).

• **Veracity** – An elevated error rate in the data can strain data validation, data integrity, and data curation processes (Dong and Srivastava, 2013). An example is maintaining data quality for detailed and granular portfolio data in bank stress tests (Hunter, 2014). Because data integrity is often assessed by reconciling data points against each other, the veracity burden can rise exponentially with data volumes.

The remainder of this paper connects these big data scalability problems to particular data challenges facing financial stability supervisors. The OFR's *Financial Stability Report* (OFR, 2015, ch. 4) organises these issues around three dimensions: scope, quality, and access. Roughly, these address what data to collect, how best to manage and use the data, and who should get to see the data.

In the following sections, we address these same questions of what, how, and who, but organise the discussion around the five significant phases in the usual lifecycle of big data (Jagadish *et al.*, 2014), considering them in the context of financial supervision. Figure 1 depicts these steps: acquisition, cleaning, integration, analysis, and sharing.

Figure 1
The lifecycle of supervisory data

Source: Office of Financial Research.

2| Data acquisition

The front end of data-driven supervision is the collection of information about participants in the financial system. Data collection is an exercise in instrumentation of the system, and a key design consideration is the appropriate measurement resolution. Measurement is necessarily a projection from a deeply nuanced financial system into a discrete measurement space, and important details may be lost in the process. One way to address the lossiness (i.e. the degree of information loss) of the projection is to provide for resolution enhancement within the measurement process, allowing users to drill down into additional detail. For financial stability data, resolution involves four key dimensions: coverage, frequency, granularity, and detail.

Coverage traditionally focused on microprudential accounting data from financial firms — for example, the Securities and Exchange Commission's 10-K reports (SEC, 2014) — and price and volatility data from financial markets, such those used in Basel capital requirements, set for banks in the United States by the Federal Reserve Board and Office of the Comptroller of the Currency (FRB-OCC, 2013). However, the crisis demonstrated that vulnerabilities can arise in the blind spots not covered by formal data collections. For example, in September 2008, "regulators did not know nearly enough about over-the-counter derivatives activities at Lehman and other investment banks, which were major OTC derivatives dealers" (FCIC, 2011, p. 329). One response has been a focus on identifying and correcting these data gaps. Recently, for example, the OFR has worked with fellow regulators to collect new data on bilateral repurchase (repo) and securities lending agreements (Baklanova *et al.*, 2016). Internationally, the G20 Data Gaps Initiative is the most prominent effort to expand the coverage of supervisory information. The G20 finance ministers and central bank governors launched the Data Gaps Initiative after the crisis in 2009, endorsing 20 specific recommendations for implementation, managed by the Financial Stability Board and International Monetary Fund; see FSB-IMF (2015) and Cerutti *et al.* (2014).

Frequency addresses temporal measurement resolution. Most formal data collections involve repeated discrete snapshots of some aspect of the financial system to accumulate a regularly spaced longitudinal dataset, such as the SEC's monthly collection of money market mutual fund holdings (SEC, 2016). One typically assumes the data are sampled at regular finite intervals from an underlying continuous-time process evolving smoothly over time. Traditional econometrics provides a rich toolkit for analysing panel datasets, so that a periodic strobing of the system to collect observations at regularly spaced intervals can be extremely useful for analysis. Unfortunately, the assumption of temporal smoothness does not always hold, especially for systemic risks, where microprudential vulnerabilities may be masked by window dressing and macroprudential events can erupt abruptly, fueled by investor panic and other feedback effects. The upshot can be a sort of "sampling blindness," where the phenomena of interest occur between sample snapshots. Finer sampling frequencies do not necessarily cure sampling blindness. Microstructure noise increasingly dominates price series — and the related realised volatility and correlation estimates —as the observation frequency increases (Aït-Sahalia and Jacod, 2014).

Granularity defines the level and techniques of data aggregation, typically achieved by summing or averaging rows in a database table. This process has both costs and benefits. Because aggregation is a lossy conversion, there is an incentive to capture information at the highest resolution possible and then provide aggregated and/or filtered summaries as needed. It is easier to discard information than to recreate it. On the other hand, summing and averaging reduce raw data volumes, average away random measurement errors and can preserve confidentiality. The SEC's planned Consolidated Audit Trail (CAT) will collect and identify every order, cancellation, modification, and trade execution for all exchange-listed equities and options across all US markets (SEC, 2012). The CAT represents an unprecedented level of granularity in financial reporting. By its fifth year, the CAT is projected to generate more than 100 billion records per day, occupying more than 20 terabytes of storage daily and eventually exceeding 20 petabytes (Rauchman and Nazurak, 2013, p. 21) However, beyond the operational burden of developing and maintaining software and other routines (Rossi, 2014), aggregation introduces other challenges. Aggregation can disguise important nuances of risk exposures; it is well known, for example, that aggregate performance measures do not capture the full detail of portfolio risk (Foster and Young, 2010).

Detail refers to the specific attributes captured for each object (e.g. a firm or transaction) included in coverage — typically represented as columns in a database table. For example, the Financial Industry Regulatory Authority's (FINRA) Transaction Reporting and Compliance Engine (TRACE) for corporate bond transactions exists in two formats, confidential and public, distinguished in part by whether the dataset includes counterparty identifiers for each trade. The former allows much more detailed analysis of dealer interactions, possibly generating important insights about position concentrations and liquidity formation. Aggregation considerations, such as storage costs and privacy concerns also affect detail, but there are other scalability issues particular to detail.

It is easy for the information content of a dataset to deteriorate as downstream processes filter, normalise, and aggregate the data. Provenance documentation and other key metadata may be lost over time, or lose connection to the original context that made them meaningful (Buneman and Tan, 2007). The information content of a dataset may also grow over time, through integration with other data resources (Zhao *et al.*, 2004). It is therefore important to prepare for subsequent data curation and integration at the point of data capture.

Supervisory information requirements change over time as market conditions evolve. In consequence, data requirements are often difficult to state precisely in advance. In some cases, financial stability supervisors will want to assemble information to inform research, rather than immediate monitoring needs, or to support backtesting of models, or reconciliation of other information sources. More importantly, data requirements can change abruptly and in unforeseen ways during a financial crisis. This is a strong argument for robust data standards that enable supervisors to ingest new data sources quickly during stress episodes.

3| Data cleaning

Scalability issues also affect the next phase, data cleaning, typically achieved through a series of edits and transformations that bring a dataset into compliance with a formal list of data integrity constraints. Many official collections are highly structured and the data emerge from processes that ensure a baseline level of accuracy, such as double-entry bookkeeping or clearing and settlement. These built-in data integrity checks do not necessarily apply to raw transaction feeds, such as the CAT or TRACE. By capturing the raw transaction message stream, CAT is likely to exhibit noise in the message flow (cancelled quotes, cancelled trades, etc.). The routine realities of millions of human users — investors, traders, brokers, etc. — interacting with a diverse and dispersed financial system suggest we should expect this sort of noise will be more prevalent as data capture moves closer to the source. For example, unstructured data, such as social media feeds, are appearing in systemic risk research, using sentiment analysis to improve forecasts of financial stress.

Data quality is an important practical issue, because inaccurate signals can lead to poor analysis and misinformed decisions (Osborne, 2012). As data volumes grow, so does the magnitude of the data cleaning burden (Dasu and Johnson, 2003). There are tools available for automated data cleaning (Rahm and Do, 2000), quality assessment (Pipino *et al.*, 2000), and integration (Bernstein and Haas, 2008). These must be adapted for use with financial data, but this does not mean the task is trivial; Burdick *et al.* (2015) reveal some of the challenges in implementation. The Basel Committee on Banking Supervision (BCBS) noted that half the systemically important banks surveyed (15 of 30) are straining to implement the BCBS's 2013 Principles on risk data aggregation and rated "themselves as materially non-compliant with Principle 3 (data accuracy and integrity)." Anecdotal evidence "suggests that it will be difficult for a number of firms to fully comply with the Principles by 2016" (BCBS, 2015, p.3). The Enterprise Data Management Council is coordinating efforts within the financial industry to improve data quality along the full information supply chain (EDMC, 2015).

There are good reasons, both technical and behavioural, why data quality in financial reporting may not be a simple matter of extra diligence. Behaviourally, incentives can lead firms to subvert accurate reporting through window dressing (Munyan, 2014) or fraudulent misreporting (Benston *et al.*, 2004). Operationally, the signal-to-noise ratio can drop as granularity increases. High-frequency trading (HFT) offers an example of the limits of (temporal) granularity. Traditional price-and-time priority of order routing as the basis for best execution is in tension with the SEC's goal of encouraging

competition across trading venues under Regulation NMS (SEC, 2015). Time priority is impossible to enforce precisely when HFT trading decisions occur faster than the temporal resolution of system clocks (Lombardi, 2006).

The most recent update to the FINRA's Rule 7430 requires that trading venues "be synchronised to within one second of the National Institute of Standards and Technology (NIST) atomic clock" (FINRA, 2016, part 2-1). A one-second tolerance creates enormous latitude when trading response latency is on the order of a millisecond (Hasbrouck and Saar, 2013). In addition, operational errors in HFT systems, such as the one-sided order flow at the root of the May 2010 "Flash Crash" can generate rapid-fire actions with a large cumulative impact very quickly. Many exchanges and their HFT members have a range of techniques to clamp their systems for rapid trading halts (Clark and Ranjan, 2011), but these are not yet universally applied.

4| Data integration and representation

Financial stability monitoring frequently requires the consideration of multiple financial sectors simultaneously. A holistic view is vital, because vulnerabilities that are not apparent in individual firms can emerge at the level of the system as a whole. A comprehensive perspective can create scalability challenges in the "variety" dimension. For example, the analysis of corporate credit risk might require jointly analysing data on corporate bonds, credit default swaps, bank loans, and corporate equity. Economists are accustomed to merging datasets on a case-by-case basis, but this process does not scale well. Mortgage registration shows how integration can fail at the system level, despite enormous incentives to get it right. Data systems in US mortgage markets did not keep pace with securitisation volumes before the 2007-09 crisis, leaving the legal status of many loans unclear and contributing to a large-scale mortgage foreclosure crisis (Hunt *et al.*, 2014).

In the long run, the emergence of a globally standardised legal entity identifier (LEI) system will help greatly with many financial data alignment tasks (GLEIF, 2014). But the LEI alone is insufficient for high-quality integration. Data alignment is only a first step toward full integration, albeit a significant one. Efforts are underway to augment the simple identification of the first-generation LEI to capture complex ownership relationships (OFR, 2015, p. 70), and to map between the LEI and other common identification schemes. More advanced techniques would resolve colloquial mentions of names of financial institutions in news and social media and reconcile them with the formal identifiers. For example, Xu *et al.* (2016) resolve named entities extracted from the prospectuses of residential mortgage-backed securities against a vendor list of institution names for asset-backed securities.

In the domain of macroprudential monitoring, the OFR and NIST have funded a public Financial Entity Identification and Information Integration Challenge to develop new technologies for automated identifier alignment and entity resolution in financial datasets and text sources (NIST, 2016). The objective is a reference knowledge base — and some prototype tools — linking heterogeneous collections of entity identifiers from various sources to facilitate information integration, both within structured data such as regulatory filings, and unstructured data such as news articles and social media. Figure 2 offers a glimpse of the problem, listing a handful of commonly used identifiers for a single firm, JPMorgan Chase and Co. This is a financial holding which itself comprises thousands of additional subsidiary organisations.

Figure 2
Linking entity identifiers

Identifier	Description
JPM	New York Stock Exchange ticker symbol
0000019617	Central Index Key (CIK) assigned by the Securities and Exchange Commission
1039502	RSSD ID assigned by the Federal Reserve Board
815DZWZKVSZI1NUHU748	Legal entity identifier (LEI) assigned by the Global LEI Foundation
J.P. Morgan	Company name used in *Wall Street Journal* stories

Source: Office of Financial Research.

Entity identification is the most basic aspect of a more general problem of data representation and metadata management. Metadata most commonly appear as data dictionaries and formal schemas, which structure and describe managed datasets. The same scalability challenges that arise in the case of aligning identifiers apply to the alignment of schemas. One area where schema integration intersects with systemic monitoring is instrument type identification. Each portfolio manager is free to categorise her positions according to a self-defined schema, but financial stability monitors need to identify common exposures across many portfolios — and therefore schemas — at once. The OFR, for example, is progressing on a Financial Instrument Reference Database to fulfill a Dodd-Frank Act mandate (OFR, 2015, p. 72). Because participants and regulators have legacy typologies to meet their local needs, any instrument reference database will face challenges of schema matching and semantic integration.

All of these curation and integration activities should help improve data quality. Reconciliation of a dataset — against other aligned datasets, against the logic of its own internally consistency, and against external integrity rules — is an important technique. Conversely, data quality problems in any one of the source systems may affect the integrated whole. Within a given dataset, the cost of maintaining attribute-level metadata tends to scale linearly with the number of attributes. However, without a framework for metadata management, the costs of scaling can increase at an increasing rate when aligning metadata from multiple sources. Flood (2009) emphasises that metadata integration is intrinsically unstable for financial risk management, because innovation engenders continual evolution of financial products, risk models, and strategic priorities.

Techniques exist for automated and machine-assisted schema alignment, and the enforcement of consistency requirements, both across schemas and relative to established data integrity rules (Bernstein and Haas, 2008; Rahm and Bernstein, 2001). Formal ontologies to organise definitions and terms can be a useful tool for managing the semantic consistency of metadata across multiple schemas (Noy, 2004; Flood *et al.*, 2010, pp. 36-39). Traditionally, this semantic effort has been managed by lawyers and domain experts. Formal ontologies can lessen their burden, serve as external benchmark for reconciliation, and expose the details of their conceptual model to newcomers and occasional users who might otherwise be overwhelmed. Data standards can also help with integration (OFR, 2015, ch. 4), but effective standards require the development of good abstractions, and this is often painstaking work. An example is the OFR's collaboration with the Commodity Futures Trading Commission and international regulators to improve reporting standards and develop shared taxonomies for swap data repositories.

5| Data modeling and analysis

Analysis is a central component of macroprudential supervision, and financial stability monitors invest heavily in developing toolkits to assess financial conditions. Moreover, because the financial system is an evolving organism, macroprudential monitors themselves must innovate to maintain a collection of models adapted to current market institutions and practices. The result is that the financial system and the macroprudential toolkit co-evolve over time, with each responding to innovations in the other. The OFR *Financial Stability Report* (2015) exhibits this dynamic, for example, with two chapters covering ongoing monitoring of threats to financial stability and evaluation of current policies, followed by two chapters devoted to enhancements in data collection and research to improve the toolkit.

Data analytics are often the most prominent aspect of the big data paradigm, and many of the commonly cited approaches, such as data clustering and community detection, are well suited for data-driven pattern identification. Empirical researchers are naturally drawn to the vast and as yet unexplored data sets emerging from news archives, transaction feeds, and social media (e.g. Bholat *et al.* 2015; Mamaysky and Glasserman, 2015; Nyman *et al.*, 2014). These are early days for the exploration of these new data sources, and tantalising new empirical results have garnered research attention. However, because the underlying data-generating process in financial markets is typically endogenous, purely data-driven (i.e. model-free) empirical regularities should face additional hurdles to justify their validity. In general, if causal inference is a salient goal, as is often the case for policy analyses, then simple predictive analytics and data-driven model selection may be of limited use (Einav and Levin, 2014).

Data analysis, like the other phases of big data processing, faces scale issues that create both problems and opportunities. One challenge for traditional econometrics facing big data is model selection. Because there are few constraints on which details should be considered, feature selection on an unstructured dataset can generate an arbitrary number of potential regressors. Even structured data can yield a combinatorial explosion of specifications. Sala-i-Martin (1997), working with 62 possible explanatory variables in a traditional growth equation, famously ran two million distinct specifications. This proliferation of specifications creates the potential for data mining. What is often touted as a powerful feature of big data analytics is unacceptable to the traditional econometrician. Because many big data sources, such as news archives, are novel to financial econometrics, there are as yet few theoretical constraints to limit the set of acceptable specifications. For policy questions, the incentives are potentially very strong for an analyst to get the "right" answer, so false discovery rates are a genuine concern (Fan *et al.*, 2014; Domingos, 2012).

In some cases, a relatively straightforward Bonferroni correction is adequate to adjust for the naturally occurring rate of false positives in a large sample (Curme *et al.*, 2014); Alanyali *et al.*, 2013). In other cases, the fix is not so simple. Donoho and Stodden (2006) consider the so-called "fat regression" or "$P >> N$" problem, where the number of predictors significantly exceeds the number of observations. In these situations, the N data points are sparsely distributed in a much higher dimensional measurement space, and key elements of the asymptotic theory underlying traditional econometrics simply break down. Varian (2014) outlines some alternative approaches. Dhar (2013) emphasises the importance of out-of-sample predictive power as a model-selection criterion. The key point is that big data necessitates new approaches, not just faster hardware.

6| Data sharing and transparency

The final set of data-management tasks involves the disposition of the data once they have been collected, cleaned, documented, and analysed. The data are a resource to support decision-making, rule-making and policymaking, and to provide context for other analyses. In many cases, a supervisor openly publishes or selectively shares collected data or analytical derivations to support public accountability, transparency to investors, or industry decision making. In this role, supervisors become input-process-output engines. They take raw data (regulatory collections, market data feeds, etc.) as inputs, transform them through various analytical processes into derived artifacts (regression results, industry aggregates, financial stability reports, visualisation tools, etc.), and distribute them to targeted user groups (public or industry risk dashboards, static and interactive visualisation tools for research and decision support, archival records of system state for historical and/or accountability analysis, etc.).

The diversity of user groups, which range from senior supervisory authorities to the general public, means that data sharing takes many forms. In some cases, such as the Billion Prices Project for inflation measurement (Rigobon, 2015), researchers are using large-scale, publicly available data to develop new solutions to traditional tasks in official statistics. In the case of financial stability data, confidentiality is sometimes an added concern (Flood *et al.*, 2013). Here again, scalability affects the process. For example, the disclosure of aggregate statistics derived from sensitive underlying details is restricted. Financial supervisors and statistical agencies in the United States face a complex array of privacy and confidentiality laws and regulations governing such statistics (Flood *et al.*, 2013, Section 3 and Appendixes A and B). In Europe, the primary governing legislation is the Data Protection Act (Howell, 2014). Traditional methods of disclosure control include suppression of key fields, data "blurring" (i.e. noise addition), and data bucketing (i.e. replacing detailed attributes with coarser categories), but re-identification to match anonymised personal information back to its true owner, for example through linkage attacks involving other data sources, can often defeat these legacy techniques (Emam *et al.*, 2011). For similar reasons, the US Census Bureau no longer requests Social Security numbers for its Survey of Income and Program Participation, because respondents have gradually learned not to provide this datum (McNabb *et al.*, 2009). Ultimately, the feasibility of exposing statistics derived from confidential inputs is a difficult problem, which must consider the policy benefits, legal constraints, and technical capabilities of supervisors, target users, and potential adversaries who might compromise shared information.

Visualisation, in the ancient sense of how a picture can be worth a thousand words, is often critical to human understanding. Humans have evolved extensive capacity for visual perception and cognition, in many cases giving them a comparative advantage in pattern recognition over alternative tools. One can also supercharge these innate skills with visual analytics, which augments static images by putting a human in the loop to control the rendering interactively. Per Shneiderman's (1996) mantra, "overview first, zoom and filter, then details-on-demand," tools that offer selective resolution enhancement over huge datasets can provide the best of both worlds — depth and breadth — simultaneously. Flood *et al.* (2016) highlight four broad macroprudential tasks where visualisation can play a vital role: sensemaking, rulemaking, policymaking, and transparency. Interactive visualisation is especially valuable for sensemaking, where undirected exploration is a key part of the task.

Conclusions

Financial stability monitors clearly face big data challenges, due to the extraordinary scale of the system under supervision. The central issue is a question of scalability. Big data becomes a problem when the scale of requisite datasets overwhelms the tools available for processing, in several broad dimensions: volume, velocity, variety, and veracity. In other words, bigness is not an attribute of a dataset *per se*, but rather describes the dataset's volume, velocity, etc. *relative to* the capacity of available processes. Data describing the full financial system can be big in any of the four dimensions, overwhelming legacy analytical processes that are often fundamentally microprudential in nature.

The LEI, implemented now on a global scale, is a good example of the financial community coming together to develop a "non-linear solution to a non-linear problem." Supervisors should embrace such clearly defined, rigorously maintained (for example, via formal ontologies) shared semantics more widely. The LEI identification scheme is just the simplest and most fundamental example of shared financial meaning. When combined with state-of-the-art solutions for named entity extraction and linkage of entity mentions in financial contracts (Xu *et al.*, 2016), open standards such as LEI can provide a big-data foundation for macroprudential analysis (NIST, 2016). Macroprudential supervisors should stay alert to recognise data scalability challenges as they arise.

The financial sector and the data requirements for monitoring it will co-evolve. The industry structure responds to monitoring and vice versa. For example, Basel capital charges for concentrated mortgage exposures on bank balance sheets provided a regulatory arbitrage impetus for the migration of mortgage finance into securitisation markets (Ambrose *et al.*, 2005), where it escaped much of the intensive monitoring program that bank examiners had developed over the years. Completing the loop, data requirements for monitoring mortgage finance have grown dramatically since the crisis, at least in the United States.

The industry is generating more data and regulators are collecting more, a trend that has only accelerated since the crisis. This growth is exposing new scalability challenges, such as quality limitations that hinder the interpretation of the new, highly granular data collections. Efforts to improve data quality along the full information supply chain (e.g. EDMC, 2015) are a necessary part of the solution. At the same time, the integration of this detailed — often loan-level — mortgage information with other data sources poses new and important privacy challenges, such as linkage attacks, that can overwhelm traditional data masking techniques. New methods to assess and assure data privacy in this context are appearing, but have yet to be widely adopted as part of the supervisory toolkit. Mortgages are but one example of a more general lesson, that macroprudential supervisors should stay aware of the many techniques that are emerging to address the challenges of the big data landscape.

References

AICPA (2015)
Audit analytics and continuous audit: looking toward the future, AICPA.

Aït-Sahalia (Y.) and Jacod (J.) (2014)
High-frequency financial econometrics, Princeton University Press.

Alanyali (M.), Moat (H. S.) and Preis (T.) (2013)
"Quantifying the relationship between financial news and the Stock Market", *Scientific Reports*, 3(3578).

Ambrose (B. W.), LaCour-Little (M.) and Sanders (A. B.) (2005)
"Does regulatory capital arbitrage, reputation, or asymmetric information drive securitization?", *Journal of Financial Services Research*, 28(1), October, pp. 113-133.

Baklanova (V.), Caglio (C.), Cipriani (M.) and Copeland (A.) (2015)
"The US bilateral repo market: lessons from a new survey", *OFR Research Brief* (16-01), January, *https://financialresearch.gov/briefs/files/OFRbr-2016-01_US-Bilateral-Repo-Market-Lessons-from-Survey.pdf*

Bank of England (2015)
"One bank research agenda", *Discussion Paper*, February, *http://www.bankofengland.co.uk/research/Documents/onebank/discussion.pdf*

Basel Committee on Banking Supervision (2015)
"Progress in adopting the principles for effective risk data aggregation and risk reporting", January, *http://www.bis.org/bcbs/publ/d308.htm*

Basel Committee on Banking Supervision (2013)
"Principles for effective risk data aggregation and risk reporting", January, *http://www.bis.org/publ/bcbs239.htm*

Benston (G.), Bromwich (M.), Litan (R. E.) and Wagenhofer (A.) (2004)
Following the money: the Enron failure and the state of corporate disclosure, Brookings Institution Press.

Berman (G. E.) (2015)
"Transformational technologies, market structure, and the SEC," Remarks to the SIFMA TECH Conference, New York, *http://www.sec.gov/News/Speech/Detail/Speech/1365171575716*

Bernstein (P. A.) and Haas (L. M.) (2008)
"Information integration in the enterprise", *Communications of the ACM*, 51(9), September, pp. 72-79.

Bholat (D.) (2015)
"Big data and central banks", *Bank of England Quarterly Bulletin*, Q1, pp. 86-93.

Bholat (D.), Hansen (S.), Santos (P.) and 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*

Board of Governors of the Federal Reserve (2015)
"Enhancements to the Federal Reserve System's Surveillance program", *Memorandum*, December, *http://www.federalreserve.gov/bankinforeg/srletters/sr1516.htm*

Board of Governors of the Federal Reserve and the 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), October, pp. 62018-62291.

Buneman (P.) and Tan (W.-C.) (2007)
"Provenance in databases", In: *Proceedings of the 2007 ACM SIGMOD International Conference on Management of Data*, pp. 1171-1173.

Burdick (D.), Hernandez (M.), Ho (H.), Koutrika (G.), Krishnamurthy (R.), Popa (L. C.), Stanoi (I.), Vaithyanathan (S.) and Das (S. R.) (2015)
"Extracting, linking and integrating data from public sources: a financial case study", Working paper, September, *http://ssrn.com/abstract=2666384*

Casey (M.) (2014)
"Emerging opportunities and challenges with central bank data", presentation slides, October, *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.) and McGuire (P.) (2014)
"Systemic risks in global banking: what available data can tell us and what more data are needed?", Chapter16, In: Risk topography: systemic risk and macro modeling, Brunnermeier, M. K. and Krishnamurthy, A. (Eds.), University of Chicago Press, pp. 235-260.

Chase (R.) (2015)
Peers inc: how people and platforms are inventing the collaborative economy and reinventing capitalism, PublicAffairs.

Clark (C.) and Ranjan (R.) (2011)
"How do exchanges control the risks of high speed trading?", *Policy Discussion Paper* (2011-2), Federal Reserve Bank of Chicago, *https://www.chicagofed.org/publications/policy-discussion-papers/2011/pdp-2*

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.) and Moat (H. S.) (2014)
"Quantifying the semantics of search behavior before stock market moves", *Proceedings of the National Academy of Sciences*, 111(32), pp. 11600–11605.

Dasu (T.) and Johnson (T.) (2003)
Exploratory data mining and data cleaning, Wiley-Interscience.

DeCovny (S.) (2014)
"A fair exchange", *CFA Institute Magazine*, September/October, pp. 32-35.

Dhar (V.) (2013)
"Data science and prediction", *Communications of the ACM*, 56(12), December.

Diebold (F. X.) (2012)
"On the origin(s) and development of the term 'big data'", *PIER Working Paper* (12-037), September, *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), October, pp. 78-87.

Dong (X. L.) and Srivastava (D.) (2013)
"Big data integration", In: *29th International conference on data engineering (ICDE)*, pp.1245-1248.

Donoho (D. L.) and Stodden (V. C.) (2006)
"Breakdown point of model selection when the number of variables exceeds the number of observations", In: *IJCNN '06. International Joint Conference on Neural Networks*, 2006, *http://academiccommons.columbia.edu/item/ac:140168*

Einav (L.) and Levin (J.) (2014)
"Economics in the age of big data", *Science*, 346(6210), November.

Emam (K. E.), Jonker (E.), Arbuckle (L.) and 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", technical report, *http://www.edmcouncil.org/dcam*

Fan (J.), Han (F.) and Liu (H.) (2014)
"Challenges of big data analysis", *National Science Review*, 1(2), June, pp. 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, US Government Printing Office, January.

Financial Industry Regulatory Authority (2016)
"OATS reporting technical specifications", Technical report, January, *http://www.finra.org/industry/oats/oats-technical-specifications*

Financial Stability Board and International Monetary Fund (2015)
"The financial crisis and information gaps: sixth progress report on the implementation of the G-20 data gaps initiative", Technical report, September, *http://www.fsb.org/wp-content/uploads/The-Financial-Crisis-and-Information-Gaps.pdf*

Flood (M. D.) (2009)
"Embracing change: financial informatics and risk analytics", *Quantitative Finance*, 9(3), April, pp. 243-256.

Flood (M. D.), Katz (J.), Ong (S.) and Smith (A.) (2013)
"Cryptography and the economics of supervisory information: balancing transparency and confidentiality", *OFR Working Paper* (0011), September. *http://financialresearch.gov/working-papers/files/OFRwp0011_FloodKatzOngSmith_CryptographyAndTheEconomicsOfSupervisoryInformation.pdf*

Flood (M. D.), Kyle (A.) and Raschid (L.) (2010)
"Knowledge representation and information management for financial risk management", Technical report, July, *http://irix.umiacs.umd.edu/docs/FIWreport-FINAL.pdf*

Flood (M. D.), Lemieux (V. L.), Varga (M.) and Wong (B. W.) (2016)
"The application of visual analytics to financial stability monitoring", *Journal of Financial Stability*, forthcoming, *http://www.sciencedirect.com/science/article/pii/S1572308916000073*

Flood (M. D.), Mendelowitz (A.) and Nichols (W.) (2013)
"Monitoring financial stability in a complex world", Chapter 2, In: Financial analysis and risk management: data governance, analytics and life cycle management, Lemieux, V. (Ed.) Springer, pp. 15-46.

Foster (D. P.) and Young (H. P.) (2010)
"Gaming performance fees by portfolio managers", *Quarterly Journal of Economics*, 125(4), November, pp. 1435-1458.

Global Legal Entity Identifier Foundation (2014)
"Annual report 2014", *https://www.gleif.org/en/about/governance/annual-report#*

Halevy (A.), Rajaraman (A.) and Ordille (J.) (2006)
"Data integration: the teenage years", In: *Proceedings of the 32nd international conference on very large data bases (VLDB '06)*,pp. 9-16.

Hasbrouck (J.) and Saar (G.) (2013)
"Low-latency trading", *Journal of Financial Markets*, 16(4), November, pp. 646–679.

Hey (T.), Tansley (S.) and Tolle (K.) (2009)
The fourth paradigm: data-intensive scientific discovery, Microsoft Research.

Hokkanen (J.), Jacobson (T.), Skingsley (C.) and 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", technical report, September, *http://archive2.cra.org/ccc/files/docs/init/Healthcare.pdf*

Howell (C. T.) (2014)
"Privacy and big data", Chapter 4, In: Big data: A business and legal guide, Kalyvas (J. R.) and Overly (M. R.) (Eds.), Auerbach Publications, pp. 33-54.

Hunt (J. P.), Stanton (R.) and Wallace (N.) (2014)
"US residential-mortgage transfer systems: a data-management crisis", Chapter 18, In: Handbook of Financial Data And Risk Information II: Software and Data, Brose (M.), Flood (M.), Krishna (D.) and Nichols (B.) (Eds.), Cambridge University Press, 2, pp. 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, US Senate, Washington, DC", *http://www.federalreserve.gov/newsevents/testimony/hunter20140916a.pdf*

IBM (2016)
"The Four V's of big data", web page, *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", technical report, *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.) and Shahabi (C.) (2014)
"Big data and its technical challenges", *Communications of the ACM*, 57(7), July, pp. 86-94.

Kirilenko (A. A.) and Lo (A. W.) (2013)
"Moore's law versus Murphy's law: algorithmic trading and its discontents", *Journal of Economic Perspectives*, 27(2), Spring, pp. 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), pp. 471-481.

Lombardi (M. A.) (2006)
"Legal and technical measurement requirements for time and frequency", *Measure*, 1(3), September.

Mamaysky (H.) and Glasserman (P.) (2015)
"Does unusual news forecast market stress?", *Columbia Business School Research Paper* (15-70), July, *http://ssrn.com/abstract=2632699*

Manyika (J.), Chui (M.), Brown (B.), Bughin (J.), Dobbs (R.), Roxburgh (C.) and 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.) and Puckett (C.) (2009)
"Uses of administrative data at the Social Security Administration", *Social Security Bulletin*, 69(1), pp. 75-84.

MongoDB (2016)
"Big data explained", web page, January, *https://www.mongodb.com/big-data-explained*

Munyan (B.) (2014)
"Regulatory arbitrage in repo markets", Working paper, December, *http://www.bmunyan.com/*

National Institute of Standards and Technology (2016)
"Financial entity identification and information integration (FEIII) challenge: about the challenge", web page, *https://ir.nist.gov/dsfin/about.html*

Noy (N. F.) (2004)
"Semantic integration: a survey of ontology-based approaches", *ACM SIGMOD Record*, 33(4), December, pp. 65-70.

Nyman (R.), Ormerod (P.), Smith (R.) and Tuckett (D.) (2014)
"Big data and economic forecasting: a top-down approach using directed algorithmic text analysis", presentation slides, *http://www.ecb.europa.eu/events/pdf/conferences/140407/TuckettOrmerod_BigDataAndEconomicForecastingATop-DownApproachUsingDirectedAlgorithmicTextAnalysis.pdf*

Office of Financial Research (2015)
Financial Stability Report, December, *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), May, pp. 257-270.

Pattison (J. C.) (2014)
"Data-driven regulation and financial reform: one perspective from industry on the financial crisis", Chapter 5, In: Handbook of Financial Data and Risk Information I: Principles and Context, Brose (M.), Flood (M.), Krishna (D.) and Nichols (B.) (Eds.), Cambridge University Press, 1, pp. 148-178.

Pipino (L. L.), Lee (Y. W.) and Wang (R. Y.) (2002)
"Data quality assessment", *Communications of the ACM*, 45(4), pp. 211-218.

Rahm (E.) and Bernstein (P. A.) (2001)
"A survey of approaches to automatic schema matching", *VLDB Journal*, 10(4), December, pp. 334-350.

Rahm (E.) and Do (H. H.) (2000)
"Data cleaning: Problems and current approaches", *IEEE Data Engineering Bulletin*, 23(4), pp. 3-13.

Rauchman (M.) and Nazaruk (A.) (2013)
"Big Data in capital markets", Keynote address, ACM SIGMOD/PODS Conference, New York, June, *http://www.sigmod.org/2013/keynote_1.shtml*

Rigobon (R.) (2015)
"Macroeconomics and on-line prices", Presidential address, Economia: *Journal of the Latin American and Caribbean Economics Association*, 15(2), Spring, pp. 199-213, *http://www.cid.harvard.edu/Economia/contents.htm*

Rosenthal (A.) and Seligman (L.) (2011)
"Data integration for systemic risk in the financial system", Chapter 4, In: Handbook for Systemic Risk, Fouque (J.-P.) andLangsam (J. A.) (Eds.), Cambridge University Press, pp. 93-122.

Rossi (C.) (2014)
"Portfolio risk monitoring", Chapter 3, In: Handbook of Financial Data and Risk Information I: Principles and context, Brose (M.), Flood (M.), Krishna (D.) and Nichols (B.) (Eds.), Cambridge University Press, 1, pp. 75-104.

Sala-i-Martin (X. X.) (1997)
"I just ran two million regressions", *American Economic Review*, 87(2), pp. 178-183.

Securities and Exchange Commission (2012)
"Consolidated audit trail", *Federal Register*, 77(148), August, pp. 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", Reporting form, *https://www.sec.gov/about/forms/form10-k.pdf*

Securities and Exchange Commission (2015)
"Rule 611 of Regulation NMS", Memorandum, Division of Trading and Markets, April, *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", Reporting form, *https://www.sec.gov/about/forms/formn-mfp.pdf*

Shneiderman (B.) (1996)
"The eyes have it: a task by data type taxonomy for information visualizations", In: *Proceedings of the IEEE Symposium on Visual Languages*, pp. 336-343.

Somerset House (2015)
"Big Bang Data", public exhibition, December, *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, March, *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), pp. 3-27.

Xu (Z.), Burdick (D.) and Raschid (L.) (2016)
"Exploiting lists of names for named entity identification of financial institutions from unstructured documents", Working paper, forthcoming.

Zhao (Y.), Wilde (M.), Foster (I.), Voeckler (J.), Jordan (T.), Quigg (E.) and Dobson (J.) (2004)
"Grid middleware services for virtual data discovery, composition, and integration", In: Proceedings of the 2nd Workshop on Middleware for Grid Computing (MGC '04), pp. 57-62.

Implementation of real-time settlement for banks using decentralised ledger technology: policy and legal implications

Karen GIFFORD
Special Advisor for Global Regulatory Affairs
Ripple

Jessie CHENG
Deputy General Counsel, Ripple
Vice Chair, Payments Subcommittee of the American Bar Association Business Law Section's Uniform Commercial Code Committee

A wave of innovation is occurring in financial technology, affecting products and services offered to consumers and businesses as well as financial market infrastructures such as payment and settlement systems. These innovations taken together have the potential to vastly lower the cost of financial transactions, resulting in a qualitative shift analogous to the advent of the Internet in the 1990s, supporting international financial inclusion and enhancing global systemic stability. The authors refer to both the current set of innovations bringing about the shift they describe, as well as future innovations built on these new technologies, as the Internet of Value *(IoV).*

Just as the internet ushered in an era of rapid innovation, economic growth and productivity gains, the potential promise of the IoV includes greater prosperity, financial access, stability and further innovation; however, appropriate industry, regulatory and policy support will be needed in order to achieve this promise.

This article examines one recent financial innovation, decentralised ledger or blockchain *technology, and considers the legal and policy ramifications of one of its most widely-discussed use-cases: real-time settlement in bank-to-bank payments. Authors' analysis focuses on two elements, trust and coordination, both of which are fundamental to current payments laws and rules. Decentralised ledger technology replaces certain operational and even legal elements of the current payment system; yet trust and coordination continue to be relevant considerations. Creation and adoption of appropriate policy and legal frameworks are key to optimising the potential benefits of this technology.*

That a technology-driven revolution is occurring in the global financial sector is a commonplace, repeated so often its meaning has dulled. What is this "revolution" and where is it leading us? A series of innovations, including cloud computing; open protocols and application programming interfaces (APIs); and enhanced data storage, analysis and management capabilities, among others, have vastly reduced the time and cost of an individual financial transaction, with the potential for still greater efficiencies ahead. This quantitative shift in the cost of transacting has resulted in a qualitative shift: an explosion of new companies, incubators, initiatives, and innovation labs producing new products and services at an unprecedented rate, and aimed at a broader range of businesses and individuals than the industry ever attempted to reach in the past.

In this paper, we argue that the global financial industry is witnessing a change akin to the advent of the Internet in the 1990s. We refer to both the current set of innovations bringing about the shift we describe, as well as future innovations built on these new technologies, as the *Internet of Value* (IoV). The vision of the IoV is that value movement – financial transacting, writ large – will happen as seamlessly as information movement happens over the internet today.

Understanding the implications of a systemic shift like the advent of the IoV benefits from both a bird's-eye and a snail's-eye perspective. Without specificity, the IoV remains a mere conceptual generalisation, but without a higher level view, individual technical innovations lack context. For this reason, we consider some of the practical, legal and policy ramifications of IoV generally, but also through the very specific lens of how one innovative development is affecting one particular form of financial transaction, in this case the application of the Ripple protocol to bank-to-bank funds transfers in the cross-border context.

I THE INTERNET OF VALUE

Just as the greatly reduced cost of information-sharing brought about by the Internet ushered in an era of rapid innovation, economic growth and productivity gains, corresponding reductions in the cost of financial transactions through the development of the IoV will predictably bring wide-ranging changes to the global financial system. The potential promise of these changes include prosperity, financial inclusion, stability and innovation.

Prosperity – Lowering the cost and time of transacting reduces friction and creates the possibility for many more transactions, and thus greatly increased economic activity. The truism that lowered costs can lead to more transacting can seem unremarkable, so to arrive at a concrete sense of the IoV's potential to drive economic growth, it can be instructive to consider the impact of the advent of the internet on communication. In the United States, the use of first class mail peaked in 2001, when 103.7 billion pieces of mail were sent in a single year.[1] By contrast in 2014, global email traffic averaged more than 190 billion individual emails, every day of that year.[2] A parallel evolution in the financial world would imply an increase of several orders of magnitude in the global number of financial transactions. While we are still at the very early stages of the IoV, recent developments point to the likelihood of this type of increase: for example, following the partial implementation of the Faster Payment System in the United Kingdom, the number of non-cash transactions rose significantly.[3]

Financial inclusion – Changing the cost structure and creating new rails for delivering financial products can transform financially excluded individuals and entities into potentially valuable customers. To date, many financial inclusion initiatives have structured themselves as essentially charitable efforts. While many of these programs have made impressive strides in broadening the reach of financial services, in the absence of a profitable business model, such efforts are not self-sustaining and struggle or disappear without outside funding. After investing considerable research in the question, the Gates Foundation's Financial Services for the Poor has concluded that the most effective way to significantly expand the access of people in the world's poorest regions to formal financial services is through digital means.[4] By automating and reducing the cost of processes involved in the global provision of financial services, the IoV holds out the promise of greatly expanded, sustainable financial inclusion.

1 *United States Postal Service, First class mail volume since 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 at 4.*
3 *See Greene* et al. *(2014), noting that significant increase in FPS volume did not result in decline in volumes of other non-cash payments.*
4 *See Gates Foundation.*

Stability – Greater participation in the global financial system by a wider variety of entities promotes systemic strength by reducing over-reliance on a small number of large entities. Policy makers are increasingly recognising the role that financial inclusion can play in supporting global financial stability.[5] Automating systems that were previously manual can also reduce operational risk on a systemic level.

Innovation – Lowered costs help create the conditions for the creation of new products and services, and just as industry participants and policy makers in the 1990s could hardly have predicted the advent of smartphones, GPS mapping applications or social media, we cannot know exactly how the IoV will evolve in the decades to come. What we can say with some degree of confidence is that exponential change in the global financial system's capacity to support transactions will likely fuel new sectors and industries. Already, innovations in-development that harness the IoV include applications for the integration of physical and technological systems (often referred to as the *Internet of Things*) that would permit functionalities such as enhanced collateral management and greater automation of trade finance; smart contracts that can streamline processes such as escrow arrangements and mortgage origination, and services such as payment account selection (e.g. paying with loyalty points).

We open this paper with a discussion of the promise of the IoV by intention. Its potential for expanded commerce, opportunity, economic growth and the prosperity it naturally brings about runs counter to the oft-repeated and, in our view, distorted narrative of "disruption", "disintermediation" and "winners and losers" that often frames the public discussion of technological change in the financial services world. While it would be naïve to suggest that all players will inevitably benefit from technological change, the changes we are discussing are likely to result in a rapidly growing pie, with great potential rewards for those who engage skillfully with that change, be they established players or new entrants.

2| Blockchain technology as a payments mechanism

To consider the IoV in more concrete and practical terms, let us turn to one specific manifestation of the global benefits of the IoV: the application of the Ripple protocol to bank-to-bank cross-border funds transfers. Despite rapid innovation in technology over the past several decades, cross-border payments remain a complex and imperfect experience. Fragmented payment systems limit interoperability, force reliance on a shrinking pool of intermediaries, and add costs and delays to settlement. By modernising the underpinnings of payments infrastructure, blockchain technology can reduce these structural inefficiencies and make instant, lower cost, and secure cross-border payment services accessible to a greater number of individuals and businesses.

2|1 The Ripple protocol as an example of blockchain technology

Simply put, blockchain technology is a decentralised ledger or shared public database that verifies and permanently records transactions. Transactions on this database are cleared using a *protocol*, or set of automated rules, rather than requiring a central counterparty to execute and confirm transactions. Protocols are widely used in maintaining the Internet, and most people interact with protocols on a daily basis. For example, email is sent using a protocol, SMTP, which directs the email message as it moves from the sender's outbox to the recipient's inbox.

At its heart, blockchain technology represents a mechanism for establishing trust among parties without the need for a single central authority trusted by all. The protocol developed by Ripple is one such example.

The Ripple protocol employs a shared public ledger that bilaterally clears and settles payments among banks and payment systems instantaneously. This ledger tracks the accounts and balances of participants, and new transactions are authorised and processed through a process called consensus, a process native to Ripple by which a collection of authorised counterparties validate transactions through a distributed network of servers. This process entails a supermajority of servers mutually agreeing that a transaction within the network is valid before

5 *See, e.g. Lagarde (2014), GPFI (2012) and Morgan and Pontines (2014).*

updating the ledger.[6] Servers do so by employing cryptography to securely verify transactions. It is this process of consensus that enables fast and secure settlement through decentralised ledgers.[7]

2|2 Using blockchain technology to support cross-border payments

Traditional payment systems rely on trusted, central third parties to process payments securely. Trust is imperative for cross-border payments in particular, which call for multiple parties in different jurisdictions to take a series of coordinated actions. Blockchain technologies allow a payment system to establish trust and operate in an entirely distributed way, without traditional intermediaries such as correspondent banks. The Ripple protocol can be adapted to payment systems without necessarily involving the use of a digital currency, instead using fiat currencies (such as US dollar, euro, or yen) to settle cross-border transactions.

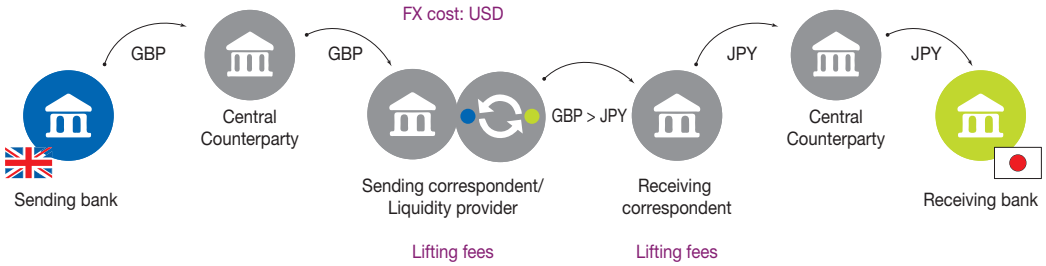
Suppose that Alpha Corp based in the United Kingdom wishes to make a payment of JPY 5,000 to Beta Corp based in Japan for products that it purchased and makes that payment by wire transfer. In a typical funds transfer, Alpha Corp (the originator) instructs its bank (Alpha Bank) to pay, or cause another bank to pay Beta Corp (the beneficiary). Thus, Alpha Corp and Beta Corp would be only two of the many parties to that payment. They likely would not share the same bank, and as a result, the transaction would also involve Alpha Bank and Beta Corp's bank (Beta Bank) and, if neither maintains an account with the other, even more intermediaries (adding still more parties). A foreign exchange transaction must also be executed, perhaps with a third-party foreign exchange dealer, in order for Alpha Corp's British Pound Sterling-denominated funds to be used to make a Japanese yen – denominated payment to Beta Corp. These parties must take a series of coordinated steps in order for the payment to Beta Corp to be made: each bank in the payments chain must credit the bank downstream and receive a credit from the bank upstream. These debit and credit entries must offset each other such that at the end of the transaction, all that remains is the increased balance in the account of Beta Corp with its bank and the decreased balance in the account of Alpha Corp with its bank.

This coordination requires trust, which payment systems have achieved through trusted third party banks, namely common correspondent banks. In the example above, Alpha Bank and Beta Bank would rely on a third party with which they both maintain accounts to settle with each other. This reliance on a common correspondent bank, let's call it Sigma Bank, requires trust that Sigma Bank will, among other things, properly authenticate the transaction and perform appropriate checks (e.g. sufficient funds), credit Beta Bank's account and debit Alpha Bank's account at the right time and in the correct amount, and do this in a secure manner. More generally, Alpha Bank and Beta Bank trust Sigma Bank to maintain a ledger that represents the definitive record of their balance of funds and that Sigma Bank will maintain this record in a reliable, accurate, and honest way. At the heart of this well-established arrangement is a central ledger, with settlement taking place on the books of Sigma Bank.

Of course this trust and coordination take place against the backdrop of the laws and rules that apply to international payments. The legal landscape surrounding international payments reflects the fragmented state of the payments networks themselves. While efforts have been made to establish uniformity in payments laws, in today's existing cross-border payment networks, different bodies of law can potentially apply to a single transaction, activity, or counterparty, possibly resulting in the application of a law different from that specified in a contract. In response to commercial pressure for greater certainty and uniformity in the legal rules governing large-value international transactions, the United Nations Commission on International Trade Law (UNCITRAL) finalised a Model Law on International Credit Transfers in 1992 for nations to consider enacting. The European Parliament and the Council of the European Union issued a directive

6 *For a more detailed discussion of the mechanics around consensus, see Schwartz* et al. *(2014).*
7 *Decentralised ledgers are not synonymous with the particular distributed ledger used by bitcoin, also known as the bitcoin blockchain, or by other digital currency protocols. For one thing, reliance on the process called proof of work (that is, "mining"), employed by the bitcoin protocol, is not necessary to validate transactions. Validation need not rely on mining, which consumes a great deal of computing power, to verify transactions, nor is the network's robustness related to the amount of processing power devoted to it.*

Chart 1



Note: The diagram above depicts a cross-border payment transaction using the traditional correspondent banking network, with the arrows depicting funds moving from the sending to the receiving bank. As can be seen from the break points in the arrows, the process is sequential and fragmented. Multiple steps involving manual processes due to the lack of interoperability between payment systems add delay, cost and risk to the transaction.

based on the principles of the UNCITRAL Model Law in 1997 (and amended in 2007),[8] with the goal of promoting efficiency with respect to cross-border payments within the European Communities. On a subnational level, the fifty States of the United States of America formulated in1989 the Uniform Commercial Code Article 4A, a comprehensive body of law with respect to the rights and obligations connected with funds transfers.

Blockchain technology can revolutionise the age-old funds transfer framework, replacing the need for the trusted third party bank (Sigma Bank) positioned between Alpha Bank and Beta Bank. Particularly given the fragmented and intermediated state of today's cross-border payment networks (as illustrated in Chart 1 above), a common global infrastructure would bring new efficiency to financial settlement, with direct benefits to international trade and financial inclusion.

Using the example above of a JPY 5,000 payment from United Kingdom-based Alpha Corp to Japan-based Beta Corp, Alpha Bank and Beta Bank would replace the trusted, central third party (Sigma Bank) with decentralised ledger technology. Alpha Bank and Beta Bank would use the Ripple protocol to simultaneously effect a foreign exchange transaction and payment transaction through any entity that maintains an account with both Alpha Bank and Beta Bank (a liquidity provider).[9] This liquidity provider can be can be any one of the many an institutional customers of Alpha Bank and Beta Bank, like a hedge fund or broker dealer, willing to act in this capacity and authorized by Alpha Bank and Beta Bank to do so. Alpha Bank would sell British Pound and purchase Japanese Yen from the Liquidity Provider at an agreed-upon exchange rate. Virtual currency such as XRP, could also be used as an intermediary asset to bridge any currency pair. Decentralised ledger technology would then be used as a payment-versus-payment system that allows Alpha Bank to both settle the foreign exchange transaction with the liquidity provider and settle its payment obligation to Beta Bank in real-time, with transparency and atomicity.[10]

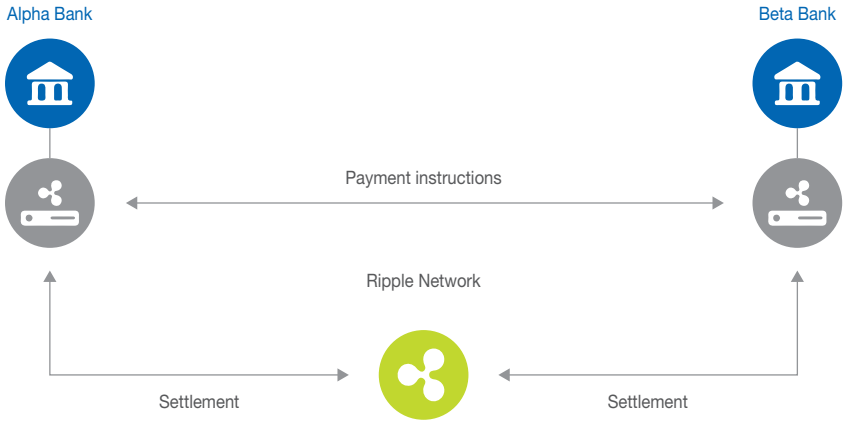
Just as with a transaction effected over the traditional correspondent banking network, described in the example above, this funds transfer would involve Alpha Bank debiting Alpha Corp's account on its books and Beta Bank crediting Beta Corp's account on its books. As between Alpha Bank and Beta Bank — instead of settling with each other through Sigma Bank, they will use the distributed ledger to coordinate certain account entries. Specifically, Alpha Bank would increase the balance it owes to the liquidity provider in the amount of British Pound it is selling to the liquidity provider and, at the same time, Beta Bank would decrease the balance it owes to

8 *Directive 97/5/EC of the European Parliament and of the Council of 27 January 1997 on cross-border credit transfers; Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market.*

9 *It should be noted that unlike certain "trustless" blockchain protocols, Ripple incorporates trust in a number of ways. In this example, trust plays a role in that (1) a liquidity provider must be an account holder at both the sending and receiving banks in order to play its role in the transaction and (2) the Ripple protocol itself contains an authorisation feature which permits participants to specify the entities with which they are willing to transact.*

10 *The term "atomicity" is a term used in the technology world to denote actions that are inherently linked. Unlike today's payments systems, which operate with delayed settlement and sequential processing, payments in Ripple are either fully and simultaneously settled in real-time or they do not occur at all.*

Chart 2



Note: The diagram above depicts a cross-border payment transaction using the Ripple protocol. Unlike today's systems, which operate with delayed settlement and sequential processing, payments in Ripple are either fully and simultaneously settled in real-time or they do not occur at all -- a process called atomic payments. This eliminates or reduces many of the risks that plague today's reliance on intermediaries for cross-border payments, including credit and operational risk.

the liquidity provider in the amount of the payment obligation (which is the amount of Japanese Yen that Alpha Bank had purchased from the liquidity provider). The Ripple protocol executes all of these transactions simultaneously. Alpha Bank and Beta Bank thus use the blockchain to communicate, coordinate, validate, and record their credit and debit to the liquidity provider's accounts.

3| Potential risks and benefits of blockchain technology in the cross-border context

In essence, this decentralised, cryptography-based payments solution cuts out the centralized common correspondent sitting between the originator's bank and the beneficiary's bank. In so doing, its overall effect is to reduce the risks inherent to any intermediated banking system. Blockchain technology eliminates the risk to Alpha Bank and Beta Bank that Sigma Bank may become insolvent with a large amount of money owed to its payment counterparties (credit risk) or not have the funds to settle a required payment at a particular moment in time (liquidity risk).[11]

By replacing dependence on a dwindling number of common correspondent banks with reliance on a diverse and robust network of many liquidity providers, blockchain technology also lowers systemic risk. The dependence of the world's financial system on a concentrated pool of private central counterparties heightens these credit and liquidity exposures arising from the existing intermediated system. The global financial system is particularly vulnerable in light of the recent "de-risking" trend in international banking — that is, the trend among certain banks to reject customers in risky regions and industries and terminate correspondent relationships with certain other banks they work with in globally sending money.[12] Rising costs and uncertainty about diligence requirements are among the main reasons cited by banks for this trend.[13] As a result, the number of banks with sufficient global reach to perform correspondent banking services is shrinking, with debilitating effects on global financial inclusion and access to international financial services.

In addition to reducing such credit and liquidity risk, blockchain technology mitigates systemic operational risk. Because blockchain technology is not dependent on a centralised party, it is more resilient to such risk. Centralised payment systems

11 *See Bank for International Settlements (BIS), Committee on Payment and Settlement Systems (CPSS) and Technical Committee of the International Organisation of Securities Commissions (TCIOSCO) (2012), Principles for financial market infrastructures (PFMI), pp. 19, 36-45, 57-63.*
12 *See Bank for International Settlements Committee on Payments and Market Infrastructures (2015).*
13 *Id.*

are susceptible to deficiencies in information systems or internal processes, human errors, management failures, or disruptions from external events that result in a reduction, deterioration, or breakdown of their settlement processes.[14] These operational failures may potentially lead to delays, losses, liquidity problems, and in some cases systemic risks and liquidity or operational problems within the broader financial system. In contrast, by virtue of being a decentralised ledger distributed across a network, Ripple and similar protocols inherently include a number of redundant backups as part of their core technology — possibly in the thousands, many more than a centralised payment system would typically operate. From a systemic risk point of view, blockchain technology has the potential to reduce risks to participants, fostering transparency and financial stability. A decentralised cross-border payments framework replaces the traditional hub-and-spoke model where a central counterparty's disorderly failure or inability to function as expected could lead to simultaneous systemic disruptions to the institutions and markets it supports. Particularly where cross-border payment services are concentrated among a small number of central counterparties for interconnected institutions and markets, these complex interdependencies raise the potential for disruptions to spread quickly, unexpectedly, and widely across markets.[15] In contrast, the blockchain connects all participant institutions to each other in a network, allowing each to promptly and effectively obtain a substitute for critical payments in the event that one fails. Moreover, the technology is designed to enables accessibility and promotes inclusiveness globally. Its neutral settlement structure supports and treats all currencies and participants equally regardless of size. The technology may also be integrated to interoperate with existing payment systems, reducing friction between participants and increasing efficiency. By giving institutions confidence to fulfill their payment obligations on time, even in periods of market stress and financial shocks, the blockchain can be an important source of strength in financial markets.

Of course, like any new technology, some residual uncertainty remains regarding the blockchain. There are always operational and technical risks involved in integrating any new financial technology; however, the principal residual risk of decentralised ledgers lies in the application of relevant laws and regulations to transactions effected using this technology. Critical to a decentralised funds transfer framework is certainty and clarity as to the parties' rights and liabilities, including when certain rights arise and certain liabilities are extinguished.[16] As we have noted, cross-border payments currently take place in an environment that includes a certain degree of legal uncertainty. Absent a globally harmonised legislative or regulatory framework, private contract and private-sector payment system rules will fill the void at this time when blockchain technology remains new and adoption is at an early stage. However, the internationalisation and greater speed of commerce and finance brought about by the IoV will lead to commercial pressure globally for greater certainty and broader international harmony in the law governing these international transactions. This process of harmonisation will call for international participation and collaboration and, in the case of treaties and conventions, a national commitment to implement.

4| Policy considerations

The IoV needs the appropriate global policy, legal and regulatory framework in order to fulfill its promise in the most positive way. Currently, as governments are looking at manifestations of the nascent stages of the IoV, some are focusing on the risks of introducing new technology into the global financial sector, or considering what steps need to be taken to limit or control it. However, considering its potential for fostering prosperity, inclusion and financial stability, perhaps the greatest risk associated with the IoV is that discordant government action or global inertia could prevent it from fully meeting its potential.

We suggest that global leadership make use of historical precedent in considering policy questions raised by the IoV. The Internet originally came about as the result of the collaborative efforts of government, academia and the private sector, and in considering the IoV, policymakers can make good

14 *See BIS, CPSS and TIOSCO, PFMI, pp. 20, 94-100.*
15 *See BIS, CPSS and TIOSCO, PFMI, pp. 9-10, 18.*
16 *See BIS, CPSS and TIOSCO, PFMI, pp. 18, 21-25.*

use of this model. Unlike the leaders of the 1990s who were dealing with the initial advent of a truly global marketplace, today's policymakers are not forced to write on a blank page. High-level policy efforts from that time that could provide useful models today include:

- Open standards

A pivotal element in the development of the internet was open standards. Open standards like HTTP and TCP/IP are the basis for the Internet as we know it.[17] Now in the area of global finance, open standards like Ripple hold out the promise that similar advances can come to the financial world.

Open standards present a host of potential benefits for the financial world. They ensure interoperability; they are key for connecting bank ledgers and payments networks that currently can't talk to each other. Open standards are also more robust than proprietary solutions, supporting greater security and fraud-prevention methods. Open standards support market competition and create an even playing field so that innovators can develop products with the greatest possible reach.

Open standards support the creation of stakeholder-based rulemaking, and to a large degree, the Internet has been successfully governed, where necessary, by private, non-profit stakeholder-based groups. While stakeholder-based groups are not the perfect solution in every case, they do have the flexibility and agility to respond relatively quickly to changes in technology and markets as compared with governmental bodies. Policy support for expanding the use of open standards to the world of financial transactions is a principal way in which global leadership can support the creation of a robust IoV.

- Policy principles for an appropriate legal and regulatory environment

We are at the cusp of a major change in the global financial industry, and a progressive harmonisation of global standards and rules is needed to realise the full potential of this wave of innovation. Global participation and collaboration are needed for international commercial law to keep pace with the innovation occurring in financial technology. Contrary to being "disruptors," many financial technology companies like Ripple are committed to working hand-in-hand with international stakeholders to clarify and strengthen consensus around the fundamental principles that can guide future policymaking efforts. In this regard, a set of principles and policy discussions that took place in the early days of the Internet provide a useful starting point.

Global leaders came to recognise the potential for economic growth that the internet could bring, and the 1990s saw coordinated efforts by policymakers around the world to ensure that the Internet would support a global marketplace for the benefit of all participants. These efforts were formalised in a Bonn declaration on global information networks,[18] as well as what was known as the Framework for Global Electronic Commerce in the United States.[19]

The aim of that initiative was to create a legal environment for commerce globally that was simple, predictable, pro-competitive, and consistent. It led to concrete, constructive efforts such as legal recognition of e-signatures[20] and the creation of the Internet Corporation for Assigned Names and Numbers (ICANN),[21] that supported the growth of the global electronic marketplace that exists today on the Internet. The basic principles outlined in the 1996 global initiative remain excellent guideposts to draw on in creating a global legal and regulatory environment for the IoV.

5| Conclusion

The potential for the IoV to bring the global economy to a new level of financial inclusion, prosperity, and systemic stability presents inspiring possibilities. Enhancements the global financial system, however, can only be achieved with the support of an appropriately harmonised global policy framework. Now is the time for policymakers to consider how best to set the stage.

17 *See Ito (2009).*
18 *See European Union (1997).*
19 *See White House, United States (1997).*
20 *See Uncitral (1996).*
21 *See Department of Commerce, United States (1998).*

References

Bank for International Settlements, Committee on Payment and Settlement Systems and Technical Committee of the International Organisation of Securities Commissions (2012)
"Principles for financial market infrastructures (PFMI)", April, available at: *http://www.bis.org/cpmi/publ/d101a.pdf*

Bank for International Settlements, Committee on Payments and Market Infrastructures (2015)
"Correspondent banking, Consultative Report", pp. 8-10, October, available at: *http://www.bis.org/cpmi/publ/d136.pdf*

Department of Commerce, United States (1998)
"Management of Internet names and addresses", Policy Statement, June, available at: *https://www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses*

European Union (1997)
"Global information networks: realising the potential", Ministerial Declaration, July, available at: *http://web.mclink.it/MC8216/netmark/attach/bonn_en.htm#Heading01*

Gates Foundation
Strategy Overview, Financial Services for the Poor, available at: *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, October 29, available at: *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.) and 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*, No. 14-5, pp. 27-35, October 10.

Ito (J.) (2009)
"Innovation in open networks", October 30, available at: *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, June 26, available at: *https://www.imf.org/external/np/speeches/2014/062614a.htm*

Morgan (P.) and Pontines (V.) (2014)
"Financial stability and financial inclusion", Asian Development Banking Institute, Working Paper No. 488, July, available at: *http://www.adb.org/sites/default/files/publication/156343/adbi-wp488.pdf*

Schwartz (D.), Youngs (N.) and Britto (A.) (2014)
"The Ripple protocol consensus algorithm", Consensus Whitepaper, available at: *https://ripple.com/consensus-whitepaper/*

Uncitral (1996)
"Model law on electronic commerce", available at: *https://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf*

White House, United States (1997)
"A framework for global electronic commerce", July, available at: *http://clinton4.nara.gov/WH/New/Commerce/*

High-frequency trading, geographical concerns and the curvature of the Earth

Fany DECLERCK
Professor of Finance
Toulouse School of Economics

For high-frequency traders, fragmentation, information, speed and proximity to markets matter. On today's financial markets each nanosecond may count; therefore, an arms race is more likely as traders, venues or investors compete to be the fastest. The theoretical literature also demonstrates that fast traders can cause more adverse selection against slower traders and can impair long-run asset price informativeness. In this set-up, regulators and empiricists are now facing major challenges. Most evidence suggests that high-speed trading has led to improvements in liquidity and price discovery. Trading on advance information is nonetheless significant. Finally, the "slice and dice" trading strategy implemented by institutional investors does not seem fully appropriate to avoid the risk of detection by fast traders. Indeed, if, during the first hour following the order submission, high-speed traders act as market makers, they then increase trading costs for the institutional trader.

"After World War II, investors held stocks for four years on average. In 2000, holding times fell to eight months. Then two months in 2008. In 2013, stocks change hands every 25 seconds on average, and sometimes in just a few milliseconds."
Alexandre Laumonier (2014)

Market microstructure focuses entirely on how to acquire and shoot out information. In the old days of the Chicago Board of Trade (CBOT), one of a trader's best asset was his shoes. Platform shoes, to be precise, that boosted his height by up to 8 centimetres.[1] It was a simple but efficient tactic to see and be seen by other traders above the flailing arms and flashing hands on the trading floor. The CBOT admitted its first female traders in 1969: the aim was not to promote gender equality, but interestingly other traders seemed to better hear their higher-pitched voices. This era of "amateurism" was followed by an incredible period of mathematical and technological innovations. This incremental process totally reshaped the financial industry.

Nine men, based in Chicago, London, New York and Santa Fe, are the primary players in this evolutionary shift. One of the first moves was Instinet, a company founded by Herbert Behrens and Jerome Pustilnik. Starting in 1969, this new, fully automated, transparent and anonymous alternative trading platform began competing with the New York Stock Exchange (NYSE). Its key advantage was to enable direct trading between banks, mutual funds and insurance companies, with no delays or intervening specialists.

In 1977, Thomas Peterffy (Interactive Brokers), a self-taught computer programmer, bought a seat on the American Stock Exchange as an individual market maker and started developing an algorithmic (or algo) trading software to replace manual processes with more efficient automated ones. In 1987, he created the first high-frequency trader, using a basic IBM computer, to trade on the Nasdaq stock exchange.[2]

In the same spirit, Josh Levine and Sheldon Maschler, who were later joined by Jeff Citron, exploited a weakness in the Nasdaq Small Order Execution System (SOES) to trade using algo software and earn large profits. These automated algos integrated inventory risk management on a continuous time basis into the SOES limit order book. As in video games, human traders simply had to click on buy or sell buttons. This eventually gave rise to Island ECN, one of the first electronic communication networks for trading equities in the United States.

Finally, in 1985, James Doyne Farmer, Norman Harry Packard and Jim McGill (The Prediction Company) combined algo trading, chaos theory and complex systems to filter out the noise component from fundamental information to forecast asset payoffs.

These nine pioneers succeeded in bringing together computer sciences, mathematics, physics and finance. The 2014 anthropological investigation *6/5* by Alexandre Laumonier is a priceless, indispensable insight into the history of the stock exchange.

Yet one last ingredient was still missing: telecommunications innovation. In the days before the telegraph, in the early 1840s, information took two weeks to travel from Wall Street to Chicago. With the invention of the telegraph, the same information could be sent in just 2 minutes. Then, in September 1949, *Long Lines Magazine* announced the construction of the New York to Chicago radio relay system: a microwave system which allowed information to travel at around 3.3 microseconds per kilometre.[3] Nowadays, in order to gain a few nanoseconds in speed over the current microwave and fiber-optic links, companies like Anova, which specialises in low-latency networks for stock trading, are installing ultra-high-speed laser networks, not only between the NYSE (in Mahwah, New Jersey) and the NASDAQ (in Carteret, New Jersey), but also between the London and Frankfurt stock exchanges. If more speed is still needed, trading firms can pay to place their servers inside the exchange's data centre, a practice known as colocation.

1 *With exchange officials watching to make sure no one gets an unfair advantage, CBOT enforced shoe-height rules. A picture of platform shoes from the CBOT is available at the Chicago History Museum,* https://www.flickr.com/photos/chicagohistory/3429555190
2 *An illustration by Thomas Peterffy is available in the documentary film 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

The historical experience sheds light on the path to the high-frequency trading (HFT) revolution. Biais and Foucault (2014) define fast traders as follows: "*HFTs strive to minimise so called latencies: essentially the time it takes for them to receive messages (for instance, a quote update or the status of their orders) from trading platforms, process this information, and react to it by sending back new orders (market orders, limit orders, cancellations) based on this information.*" Speed and proximity to markets matter.

The main characteristics of HFT are as follows:[4] i) high rates of intraday messages which constitute orders, quotes or cancellations; ii) submission of numerous orders that are cancelled shortly after submission; iii) small trade size; iv) ending the trading day in as close to a flat position as possible (that is, not carrying significant, unhedged positions overnight).

1| A FEW THEORETICAL POINTS ON HIGH-FREQUENCY TRADING

Due to market fragmentation and the characteristics of HFT, investors have to collect and process very large amounts of quotes and machine-readable news (Declerck and Lescourret, 2015). One consequence of this market fragmentation is the need to invest in fast trading technologies to be able to handle information from several markets and send orders to the venue offering the best prices. Firms must subscribe to data and news vendors to feed their high-speed trading strategies.

1|1 Overinvestment

On today's financial markets, latency has become critical; each nanosecond may count and each small piece of information is important. Biais *et al.* (2015) develop a model in which fast institutions can instantaneously search across all trading venues to find attractive quotes but can also trade on advance, value-relevant information (for example asset payoffs), which generates adverse selection. Slow institutions cannot do so. Fast trading firms have no incentives to internalise these costs when making their investment decisions. In their model, the authors analyse equilibrium investment decisions in fast trading technologies, their consequences for welfare, and possible policy interventions to achieve the socially optimal level of investment in high-speed technologies. First, they demonstrate that this socially optimal investment level is, in general, not zero. Second, fast trading technology improves social welfare, and helps trading firms to deal with market fragmentation. However, fast access to market quotes generates a negative externality. As trading firms do not take into account this negative externality, they overinvest, which leads to an arms race in which all institutions end up investing in the fast technology.

Richborough (Kent, United Kingdom) is a recent example of this kind of huge investment: to be sure that even the Earth's curvature won't impede its ability to transmit data to continental Europe, Vigilant Global tried to erect a 324-metre mast,[5] 12 metres higher than the Eiffel Tower. This mega-structure was intended to beam microwaves across the English Channel for HFT firms. The project has hit opposition from members of the Ash Parish Council, who voted unanimously against Vigilant's mast. That's not the end of the story in Richborough though as New Line Networks is now planning to build its own mast in the town.[6]

With that kind of trading infrastructure, stock exchanges also need to invest in fast technologies if they want to be on the cutting edge in order to attract order flow. This is in line with Pagnotta and Philippon (2015) who demonstrate that financial markets compete for investors who choose where and how much to trade. In their model, faster venues charge higher fees and attract high-speed traders. Competition among venues increases trading volumes and efficiency, but entry and fragmentation can be too high, and excessive market investment in speed can arise. One example of this latency-based trading platform competition is the continental European Euronext data centre being built in Basildon (a suburb of London) in order to be closer to the headquarters of investment banks and hedge funds.

4 *MiFID II, Article 4(1)(40).*
5 *More information on that story is available on the* Sniper in Mahwah *blog:* https://sniperinmahwah.wordpress.com/
6 http://www.kefmast.co.uk

Finally, to improve their monitoring capacity, trading speed competition can also take place between liquidity providers and liquidity consumers, leading to socially wasteful investments. Bongaerts *et al.* (2015) focus on this liquidity provision effect of fast traders. They first highlight that the complementarity between liquidity providers and consumers increases the success rate of trading on both sides and may therefore induce underinvestment in speed if the gains from trading are large enough. However if gains from trade decrease with transaction frequency, an arms race is more likely.

1|2 Adverse selection

High-frequency traders rely on two main characteristics. First, they are highly computerised. Second, they need, very fast access to trading platforms and market information. Thanks to their fast technologies, they can observe signals and then forecast information faster than slower traders. Biais *et al.* (2015) demonstrate that fast traders are able to trade on advance value-relevant information. The theoretical paper of Foucault *et al.* (2016) considers a dynamic model of trading on public news and advance access to news content with gradual release of information over time.[7] One speculator and one competitive dealer have access to a signal about the long-run payoff of a risky asset (public news). As long as a fast speculator can trade on advance and informative private information about both the long-run value and the short-term value, she will trade first on what moves prices in the short run and then on the long-term fundamental information, even if those two pieces of information are conflicting. This model helps us to understand round-trip trades by high-frequency traders over very short time periods (from milliseconds to nanoseconds). However, the fast speculator also trades on her long-lived information and, to avoid a significant cut in the overall expected profit, she will trade more aggressively on the short-run information and less aggressively on her long-run fundamental information.

While Foucault *et al.* (2016) look at directional high-frequency traders' strategies, Aït-Sahalia and Saglam (2014) study market making by high-frequency firms in a dynamic framework. The results show higher profits, higher liquidity provision and higher cancellation rates in normal market conditions for a monopolistic high-frequency market maker. The model also predicts that liquidity supply decreases when price volatility increases. When competition is introduced between fast market makers, liquidity consumers are better off.

1|3 Trading on news and the price discovery process

Based on Foucault *et al.* (2016), we know that a fast speculator trades aggressively on her short-lived term information and more passively on her long-lived information. This behaviour implies two consequences. First, in line with Biais *et al.* (2015) fast traders can cause adverse selection against slower traders. Second, fast trades contribute to price discovery: they are more informative about short-term price variations and less informative about long-term price variations; overall the price discovery process is unaffected.

The last theoretical question that we want to address in this survey regards the quality and cost of information and its implication for the price discovery process. In today's market, information is easily, directly and electronically available to all investors, but it is still costly even if this cost has declined over time. Static models predict that, with more information, the price discovery process should be better (Grossman and Stiglitz, 1980 and Verrechia, 1982). Paying attention to and extracting a more precise signal from news is nonetheless time-consuming. In that case, Dugast and Foucault (2016) show that the reduction in the cost of accessing data can impair long-run asset price informativeness.

Two types of information stand out in their dynamic model: raw data and processed data. The former is a noisy signal and the latter is fundamental information from which the noise component has been removed. An investor can buy both raw and processed information, but since it takes time to clean up the noisy signal, she will receive the processed data with a time delay and at a higher cost. If the

7 *Information can come from company websites, financial institutions, policy institutions, newspapers, Twitter, Facebook, blogs, etc.*

cost of raw data declines, more investors trade on it, which improves the short-run price discovery process. If raw data is a poor signal, it generates mispricings, and then profit opportunities for trading based on processed data. In contrast, if the raw signal is sufficiently reliable it can lead to a crowding out effect: the expected profit from processed data is so low that the demand for processed data stops. In that case the final price will not fully reveal the asset value. Fast traders are, of course, a class of investors who are likely to trade on raw data.

2| Empirical evidence

In conducting an empirical analysis of the effects of HFT on market quality, it is crucial to keep in mind data limitations (Biais and Foucault, 2014). Empiricists can examine the impact of HFT in the United States and in Europe, but very few datasets are available.[8] This raises questions regarding the robustness of empirical conclusions. Almost all empirical papers use a data-driven definition to classify fast versus slow traders. Overall, the classifications categorise a trading firm as an HFT firm if it trades only for its own account (proprietary trading), its relative number of trades is large, its inventory is often flat, and its cancellation rate is high. By constructing samples, depending on the selection criteria, they either exclude arbitrageurs or HFT desks from investment banks or focus on HFT market makers.

2|1 Speed and market quality

High-speed trading could actually lead to an arms race, with measured liquidity as the unintended victim (Biais *et al.,* 2015, and Bongaerts *et al.,* 2016). However, most evidence suggests that high-speed trading has led to improvements in liquidity and price discovery. Using trades on the NYSE over a 5-year period, Hendershott *et al.* (2011) find a positive relationship between high-speed trading and market liquidity. They then use the introduction of autoquote in 2003 as an exogenous event to investigate causality. Following the introduction of autoquote, they observe a decline in effective spreads and in the adverse selection cost (only) for large-cap stocks. Quotes become more informative and the liquidity supply works better. Brogaard *et al.* (2014) indicate that high-frequency traders increase asset price informativeness: they use limit orders to trade in the direction of permanent price changes and use contrarian marketable orders to trade in the opposite direction of transitory pricing errors. Thus, by being able to forecast very short-run price changes, they contribute to market stability. Moreover high-frequency traders do not exit the market at time of market stress.

Using a Canadian proprietary data set for the period June 2010 to March 2011, Boehmer *et al.* (2015) rely on data-driven criteria to identify fast traders and find that HFT firms do not destabilise stock exchanges. In line with Hasbrouck and Saar (2013), they do not observe an increase in stock price volatility. Using the same Canadian data set from 15 October 2012 to 28 June 2013 on 15 large-cap stocks, Brogaard *et al.* (2015) go a step further in the study of high-frequency traders' limit orders. The authors establish that those orders are more informative and are almost twice as prevalent as non-HFT limit orders. In short, fast trading firms seem to make liquidity demand and price discovery easier for final investors.

2|2 Speed and negative externalities

A higher trading speed may reduce frictions and trading costs, but it may also generate negative externalities. Frictions are adverse selection, inventory-bearing risks, and agency/incentives issues. In 2012, the Nasdaq OMX Stockholm equity market proposed an upgrade to their existing colocation offer: each trading firm could choose (or not) to pay an extra fee to boost its trading speed. Brogaard *et al.* (2016) use a proprietary data set that allows direct observation of account-level data if the trading firm subscribed to the colocation service. Using a probit model, they show that this optional update is mainly chosen by fast market makers. Using a difference-in-differences approach, they document that the market update is associated with improved liquidity via a reduction in the inventory-bearing risk, and that the improvements benefit both fast and slow traders. Finally, the data

8 *The most well-known is the Nasdaq dataset which reports aggregated trades for 26 firms identified as high-frequency traders by the Nasdaq in 120 randomly selected stocks listed on Nasdaq and the NYSE.*

indicate that orders submitted by high-speed traders reflect advance information. This information advantage can be consistent with a higher adverse selection cost for slower traders (Brogaard *et al.,* 2014 and Brogaard *et al.,* 2015).

In line with this last result, Menkveld and Zoican (2015) show that the new trading system introduced in 2010 at Nasdaq OMX, while lowering the exchange latency, also increases spreads via higher adverse selection against slower traders. Thus, an increased speed can reduce market liquidity. Weller (2016) also finds a negative link between high-speed traders and the informativeness of prices about future earnings.

Using a unique data set from Euronext and the *Autorité des Marchés Financiers* (AMF – French Financial Markets Authority), Biais *et al.* (2016) observe the connectivity of traders to the market, and whether they are proprietary traders. They find that proprietary traders, be they fast or slow, provide liquidity with contrarian marketable orders, thus helping the market absorb shocks, even during crises, and earn profits by doing so. Moreover, fast traders provide liquidity by leaving limit orders in the book. Yet, only proprietary traders can do so without making losses. This suggests that technology is not sufficient to overcome adverse selection; monitoring incentives are also needed.

2|3 Institutional investors

One concern regularly pops up when discussing the impact of fast traders on overall market liquidity: the sharp drop in the number of shares available in limit order books and the accompanying sharp drop in trade sizes. As a consequence, institutional investors need to work their large orders throughout the day with a "slice and dice" trading strategy. We also know from the empirical literature that fast traders are more skilled in market monitoring and are able to forecast very short–term price changes (Brogaard *et al.,* 2014, Brogaard *et al.,* 2015, and Biais *et al.,* 2016). It seems that institutional traders may have to deal with detection risk by high-frequency traders. In this setup, institutional investors have expressed concerns about trading costs. Anand *et al.* (2012) have in fact captured a 33% increase in US equity markets from 2005 to 2010 for institutional investors.

The empirical analysis of Van Kervel and Menkveld (2016) supports this hypothesis. Their proprietary data set allows them to construct daily parent orders by grouping into a single order all the child order transactions. They also have direct information on high frequency trades. During the first hour following an institutional order execution, fast traders act as market makers, but they then flip for multi-hour executions, increasing trading costs for the institutional trader. Fast traders are not able to detect institutional orders immediately, but as soon as they do so they "back-run" on those orders.

Korajczyk and Murphy (2015) compare fast traders' behaviour with that of designated market makers (DMMs). They find that high-frequency traders provide, on average, far more liquidity to large institutional-size parent orders than DMMs. For the largest institutional-size orders, high-frequency traders provide less liquidity while DMMs increase their liquidity provision.

Conclusion and policy implications

Electronic trading, market fragmentation, IT improvements and regulatory enforcement have created a new entrant in stock exchanges, namely high-frequency traders. It is important to note that the results of Pagnotta and Philippon (2015) are consistent with regulations that push for more competition and fragmentation (e.g. MiFID, Reg ATS, and Reg NMS).

When one looks at the impact of fast trading on market quality, the evidence points to greater price efficiency and market liquidity. The evidence is more mixed with regard to negative externalities such as adverse selection and arms race. The secretive nature of HFT firms and their algorithms has led regulators to propose market microstructure updates to slow down trading platforms: e.g. minimum quote lives, scheduled periodic auctions, taxation. Biais *et al.* (2015) shed light on three regulator interventions to mitigate the possible adverse consequence of fast traders: a ban on fast trading, the coexistence of slow and fast markets, and a Pigovian tax on fast-trading technology. Only the latter enables a socially optimal level of investment in high-speed technology. Aït-Sahalia and Saglam (2014) also discuss three high-speed trading policy regulations in the framework of their model: a transaction tax,

minimum waiting times before limit orders can be cancelled, and a tax on the cancellations of limit orders. The first does not improve the liquidity supply, while the following two improve liquidity provision at times of low volatility, but impair it during periods of high volatility.

Regulators are also seeking to reconstruct the sequence of events across linked markets via a master clock to detect predatory or illegal trading behaviour. However, as the arms race between HFT firms has almost reached the physical limits set by the speed of light, it is simply not possible to precisely sequence such fast trades. At the finest timescales, rapid events that take place across geographically dispersed trading centres simply do not have an unambiguous sequence. Instead of trying to implement a speed bump, regulators could instead think about speeding up access to trading platforms to protect large orders and avoid disclosing information to the fast traders.

Finally, while researchers and regulators are wondering about the impact of colocation and the implementation of a master clock, several trading firms are seeking to gain a new trading advantage with high-tech snooping. For instance Genscape, Remote Sensing Metrics LLC or DigitalGlobe are at the vanguard of a growing industry that employs sophisticated surveillance and data-crunching technology to supply traders with non-public information. Their tools are a patented private network of in-the-field monitors, maritime freight tracking, infrared diagnostics, electromagnetic frequency monitors, high resolution aerial photography, and near-earth satellite imagery. They provide data and intelligence through direct data feeds into customer or third-party trading systems. Genscape's clients include banks such as Goldman Sachs Group Inc., J.P. Morgan Chase & Co. and Deutsche Bank AG, hedge funds including Citadel LLC and large energy trading outfits such as Trafigura Beheer BV.

References

Aït-Sahalia (Y.) and Saglam (M.) (2014)
"High frequency traders: taking advantage of speed", mimeo.

Anand (A.), Irvine (P.), Puckett (A.) and Venkataraman (K.) (2012)
"Performance of institutional trading desks: an analysis of persistence in trading costs", *Review of Financial Studies*, vol. 25, pp. 557-598.

Biais (B.), Declerck (F.) and Moinas (S.) (2016)
"Who supplies liquidity, how and when?", mimeo.

Biais (B.) and Foucault (T.) (2014)
"High-frequency trading and market quality", *Bankers, Markets and Investors*, vol. 128, pp. 5-19.

Biais (B.), Foucault (T.) and Moinas (S.) (2015)
"Equilibrium fast trading", *Journal of Financial Economics*, vol. 116, pp. 292-313.

Boehmer (E.), Li (D.) and Saar (G.) (2015)
"Correlated high-frequency trading", mimeo.

Bongaerts (D.), Kong (L.) and Van Achter (M.) (2016)
"Trading speed competition: can the arms race go too far?", mimeo.

Brogaard (J.), Hagströmer (B.), Nordén (L.) and Riordan (R.) (2016)
"Trading fast and slow: colocation and liquidity", *Review of Financial Studies*, forthcoming.

Brogaard (J.), Hendershott (T.) and Riordan (R.) (2015)
"Price discovery without trading: evidence from limit orders", mimeo.

Brogaard (J.), Hendershott (T.) and Riordan (R.) (2014)
"High frequency trading and price discovery", *Review of Financial Studies*, vol. 27, pp. 2267-2306.

Declerck (F.) and Lescourret (L.) (2015)
"*Dark pools et trading haute-fréquence: une évolution utile?*", *Revue d'Économie Financière*, vol. 120, pp. 113-125.

Dugast (J.) and Foucault (T.) (2016)
"Data abundance and asset price informativeness", mimeo.

Foucault (T.), Hombert (J.) and Rosu (I.) (2016)
"News trading and speed", *Journal of Finance*, vol. 71, pp. 335-382.

Grossman (S.) and Stiglitz (J.) (1980)
"On the impossibility of informationally efficient markets", *American Economic Review*, vol. 70, pp. 393-408.

Hasbrouck (J.) and Saar (G.) (2013)
"Low-latency trading", *Journal of Financial Markets*, vol. 16, pp. 646-679.

Hendershott (T.), Jones (M.) and Menkveld (A.) (2011)
"Does algorithmic trading improve liquidity?", *Journal of Finance*, vol. 66, pp. 1-33.

Korajczyk (R. A.) and Murphy (D.) (2015)
"High-frequency market making to large institutional trades", mimeo.

Laumonier (A.) (2014)
6/5, Zones Sensibles Editions.

Menkveld (A. J.) and Zoican (M. A.) (2015)
"Need for speed? Exchange latency and liquidity", mimeo.

Pagnotta (E.) and Philippon (T.) (2015)
"Competing on speed", mimeo.

Van Kervel (V.) and 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, pp. 1415-1430.

Weller (B.) (2016)
"Efficient prices at any cost: does algorithmic trading deter information acquisition?", mimeo.

GLOSSARY

Advanced persistant threat (APT)
An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g. cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organisations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organisation; or positioning itself to carry out these objectives in the future.

Algorithmic trading
The use of computer algorithms to automatically make certain trading decisions, submit orders, and manage those orders after submission.

Algos or algorithmic trading
Algorithmic trading is the process of using computers programmed to follow a defined set of instructions (most often based on timing, price, quantity or any mathematical model). Algos are frequently used to place buy and sell orders when the defined conditions are met. Algorithmic trading is systematic as it rules out emotional human impacts on trading activities.

All-to-all trading
All-to-all trading venues, where multiple parties from the buy-side and sell-side come together to make prices by displaying firm orders to each other, not just "dealer-to-customer" or "dealer-to-dealer".

Anonymous trading platform
A platform where bids and offers are visible on the market but that do not reveal the identity of the bidder and seller. Anonymous trades allow market participants to execute transactions without the scrutiny and speculation of the market. Anonymity is attractive to market participants who want to complete large transactions without drawing attention to their trades, since such attention could impact market prices.

Big data
Big data technologies describe a new generation of technologies and architectures, designed to economically extract value from very large volumes of a wide variety of data.

Bitcoin
Bitcoin is a digital, decentralised, partially anonymous currency, not backed by any government or other legal entity, and not redeemable for gold or other commodity. It relies on peer-to-peer networking and cryptography to maintain its integrity, first described in a paper by Satoshi Nakamoto (a pseudonym) in 2008.

Blockchain
Blockchain is the ledger (book of records) of all transactions, grouped in blocks, made with a (decentralised) virtual currency scheme.

Central limit order book (CLOB)
A central system that contains securities "limit" orders received from specialists and market makers. Such a system consolidates limit orders in a central location and bridges the gap in establishing a national market system. A hard CLOB executes orders immediately; a soft CLOB provides data to facilitate trading but does not include automatic executions.

Central securities depository
A central securities depository is an entity that: i) enables securities transactions to be processed and settled by book entry; ii) provides custodial services (e.g. the administration of corporate actions and redemptions); and iii) plays an active role in ensuring the integrity of securities issues. Securities can be held in a physical (but immobilised) form or in a dematerialised form (whereby they exist only as electronic records).

Cloud computing
Cloud computing is a model for enabling on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

"Dark" trading
Dark trading or dark liquidity pools are private electronic trading venues that operate separately from public exchanges. They don't publish bid and offer prices immediately and don't promptly publish transaction prices. They enable institutional traders to buy and sell large blocks of securities anonymously. This protects the privacy of an investment and reduces market impact and information leakage.

NB: The editor is very grateful to Elizabeth Callaghan for her substantial contribution to this glossary.

Data leakage
Data leakage is defined as the accidental or unintentional distribution of private or sensitive data to an unauthorised entity . Sensitive data in companies and organisations include intellectual property (IP), financial information, patient information, personal credit-card data, and other information depending on the business and the industry.

Distributed ledger
A distributed ledger is an open and decentralised record of all the transactions made by a payment system, for example. As an open, transparent and peer-to-peer technology, it disrupts traditional transaction practices based on centralised and private data. The distributed ledger is one component of the blockchain – the underlying technology of most virtual currencies, including bitcoin.

Direct market access (DMA)
Direct market access (DMA) is a service offered by some stockbrokers that enables sophisticated private investors to place buy and sell orders directly on the stock exchanges order books.

Execution management system (EMS)
Execution management systems (EMSs) are software applications used by institutional traders designed to display market data and provide seamless access to trading destinations for the purpose of transacting orders. Often they contain broker-provided and independent algorithms, global market data and technology that is able to help predict certain market conditions. One of the important features of an EMS is that it can manage orders across multiple trading destinations such as MTFs, broker-dealers, crossing networks and electronic information networks.

False positives
False positive (FP) is a term used in MiFID II to indicate "inaccurate classification of a bond as liquid, when it is in fact illiquid" (bond liquidity determination). In MiFID II the unintended consequences may be: buy-side or sell-side may not be able to liquidate a position or the price may be so disadvantageous that it corrupts performance. Behaviour will change on both the buy-side and sell-side due to perceived liquidity "false positives".

Fintechs
Fintechs, contraction of "financial technology", refers to the actors specialised in the implementation of digital and technological innovations in the financial sphere, on either external services provided to individual or professional customers (such as new payment solutions, crowdfunding, etc.) or internal processes (big data, blockchain, etc.).

FIX protocol
Electronic trading IT term for a global messaging standard which reduces connectivity costs related to links between buy-side and sell-side firms, and reduces costs due to the efficiency of integration of internal processes and external operations.

GAFA
GAFA is an abbreviation for Google, Apple, Facebook, Amazon.

High frequency trading
Subset of algorithmic trading where a large number of small-in-size orders are sent into the market at high speed, with round-trip execution times usually measured in milliseconds.

Information networks (INs)
INs provide market participants with a technology layer for a global and timely view of available liquidity across markets. A high degree of technology embedded in buy-side and sell-side internal systems is required.

"Lit" trading
Lit trading is effectively the opposite of "dark" trading. Whereas "dark" venues do not display prices at which participants are willing to trade, lit trading venues or practices do show these various bids and offers in different bonds, making "lit" trading transparent.

MiFID II
The objective of MiFID II is to increase market transparency, efficiency and safety by bringing the majority of non-equity products into a robust regulatory regime and moving a significant part of OTC trading onto regulated platforms. MiFID II will bring much of the transparency traditional in equity markets to bond trading. Europe will go further with bond transparency rules than just about anywhere in the world, including the United States. MiFID II's regulatory regime brings into effect pre-trade transparency for bonds as well as post-trade. This will result in a significant impact on the market structure of bond markets. Bond pre-and post-trade transparency requirements will be calibrated for

different types of bond market trading structures. In addition, pre-trade transparency for bond instruments will also be calibrated for voice trading systems.

Multilateral trading facility (MTF)
A multilateral system, operated by an investment firm or a market operator, which brings together multiple third-party buying and selling interests in financial instruments – in the system and in accordance with non-discretionary rules – in a way that results in a contract. The term "non-discretionary rules" means that the investment firm operating an MTF has no discretion as to how interests may interact.

Name give-up
"Name give-up broking" identifies and introduces counterparties who have indicated their willingness to trade with each other, and who have reciprocal credit or clearing, and/or where two or more customers' orders match. These counterparties contract directly with each other and/or the relevant clearing house bearing the settlement obligation, and bear the counterparty credit risk themselves. The broker-dealer aims to automate the messaging process where possible.

Order management system (OMS)
An order management system is a software-based electronic system that facilitates and manages the order execution of securities, typically through FIX protocol. Order management systems are used on both the buy-side and the sell-side, although the functionality provided by buy-side and sell-side OMS's differ slightly. On the buy-side, order management systems support portfolio management by translating intended asset allocation changes into marketable orders for the buy-side.

OMSs allow firms to input orders to the system for routing to the pre-established destinations. They also allow firms to change, cancel and update orders. When an order is executed on the sell-side, the sell-side OMS must then update its status and send an execution report to the originating firm. An OMS should also allow firms to access information on orders entered into the system, including detail on all open orders and on previously completed orders.

Organised trading facility (OTF)
OTF is a MiFID II term meaning a multilateral system which is not an RM or an MTF and in which multiple third-party buying and selling interests in bonds are able to interact in the system in a way that results in a contract in accordance with the provisions of Title II of MiFID II. Unlike RMs and MTFs, operators of OTFs will have discretion as to how to execute orders, subject to pre-transparency and best execution obligations.

Over-the-counter (OTC)
The phrase "over-the-counter" can be used to refer to debt securities which are traded via a broker-dealer network versus an MTF or centralised exchange.

Peer-to-peer (P2P)
A peer to peer network is a computer network without a central server being in-between, in which every computer acts as both a client and server, allowing every computer to exchange data and services with every other computer in the network.

Person-to-person mobile payments
Person-to-person payments is an online technology that allows customers to transfer funds from their bank account or credit card to another individual's account via the Internet or a mobile phone.

Regulated market (RM)
A regulated market is a MiFID term for an operator of a regulated market (market operator) which brings together multiple third-party buying and selling interests in financial instruments in the system, in accordance with non-discretionary rules, in a way that results in a contract.

Request for quote (RFQ)
The RFQ (from client to dealer) model has been the standard method of trading in the bond market: clients ask the dealer for a quote and can then choose whether or not to trade. Originally carried out by voice, today RFQs are mostly made through multi-dealer platforms.

Request for streaming (RFS)
Request for streaming is continually updated prices, which may be firm or may be prices where the dealer has the "last look" before agreeing to trade. The RFS model can function using either voice (telephone) or an electronic connection between trading parties.

Systematic internaliser (SI)
Systematic internaliser (SI) is an original MiFID term, used in equities. It has an increased scope in MiFID II. The SI is an investment firm which, on an organised, frequent, systematic and

substantial basis, deals on its own account by executing client orders outside an RM, MTF, or OTF. MiFID II/R level 2 will set out clearly defined thresholds for becoming an SI, based on trading volumes in respect of "frequent and systematic" and "substantial". Furthermore, the regulation specifies quantifiable definitions for "frequent and systematic", and "substantial".

Transaction cost analysis (TCA)

Transaction cost analysis (TCA) is essentially: a rating of the spread between two possible prices – and the difference between those prices is often called "slippage". More specifically, TCA refers to implementation shortfall which determines the sum of execution costs and opportunity costs, incurred in cases of adverse market movement between the time of the trading decision and order execution. The TCA program is designed for performance measurement, telling investment managers whether they are paying too much in trading costs in global fixed income markets (relatively new in fixed income). TCA has traditionally been found in equities, providing clients with quarterly monitoring of their ongoing trading process.

Virtual currency

A virtual currency is a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community.

Published articles

Below are listed all of the articles published in the *Financial Stability Review* since its inception. These studies are available on the Banque de France's website (*www.banque-france.fr*).

November 2002

- The Eurosystem, the euro area and financial stability
- Credit derivatives: a new source of financial instability?
- How much credit should be given to credit spreads?
- The development of contingency clauses: appraisal and implications for financial stability
- Post-market infrastructures and financial stability
- The CLS system: reducing settlement risk in foreign exchange transactions
- International codes and standards: challenges and priorities for financial stability

June 2003

- Stock market volatility: from empirical data to their interpretation
- Towards a "market continuum"? Structural models and interaction between credit and equity markets
- The changing incentive structure of institutional asset managers: implications for financial markets
- An analytical review of credit risk transfer instruments
- International accounting standardisation and financial stability
- Towards a voluntary Code of good conduct for sovereign debt restructuring

November 2003

- Financial stability and the New Basel Accord
- Do asset price fluctuations constitute a risk to growth in the major industrialised countries?
- Interactions between business cycles, stock market cycles and interest rates: the stylised facts
- Challenges arising from alternative investment management
- Protection of deferred net payment and securities settlement systems: the examples of SIT and Relit
- Vulnerabilities and surveillance of the international financial system

June 2004

- Market dynamics associated with credit ratings: a literature review
- Results of the French market survey of credit risk transfer instrument
- Techniques used on the credit derivatives market: credit default swaps
- Equity market interdependence: the relationship between European and US stock markets
- Goodwill, balance sheet structures and accounting standards

November 2004

- Assessment of "stress tests" conducted on the French banking system
- Insurance and financial stability
- Oversight of non-cash payment schemes: objectives and implementation procedures
- The resilience of post market infrastructures and payment systems
- Credit risk management and financial stability

June 2005

- The CDO market
  Functioning and implications in terms of financial stability
- Public debt sustainability and crises in emerging market countries: a presentation of the concepts and diagnostic tools
- Interest rate risk in the French banking system
- Interest rate risk management by life insurance companies and pension funds
- Analysis, by simulation, of the impact of a technical default of a payment system participant

November 2005

- Prudential supervision and the evolution of accounting standards: the stakes for financial stability
- Regulatory capital and economic capital
- Significance and limitations of the VAR figures publicly disclosed by large financial institutions
- The impact of stock market shocks on credit in France since the mid-1990s
- Sovereign debt (Re)structuring. Where do we stand?

May 2006

- Better capturing risks in the trading book
- Market liquidity and its incorporation into risk management
- Productivity and stock prices
- Corporate equity and financial stability:
  An approach based on net worth at risk
- Recent developments in monetary and financial integration in Asia
- Implications of globalisation for financial stability

December 2006

- Commodities: an asset class in their own right?
- Do emerging market economies still constitute a homogenous asset class?
- Capital flows and credit booms in emerging market economies
- Can risk aversion indicators anticipate financial crises?
- Bank liquidity and financial stability
- Microstructure of financial and money markets
- The Basel II framework: the role and implementation of Pillar 2

April 2007

Hedge funds

Hedge funds, credit risk transfer and financial stability
The evolution and regulation of hedge funds
Regulating hedge funds
Hedge funds and financial stability
Hedge funds and systemic risk
Hedge fund replication strategies: implications for investors and regulators
Hedge funds and prime broker dealers: steps towards a "practice proposal"
Transparency requirements and hedge funds
Risks and return of banking activities related to hedge funds
Indirect supervision of hedge funds
Hedge funds: what are the main issues?
Monitoring hedge funds: a financial stability perspective
The world of hedge funds: prejudice and reality
The AMF's contribution to the debate on alternative investment strategies
Financial conditions, alternative asset management and political risks: trying to make sense of our times
Hedge funds in emerging markets
Fund of hedge funds: origins, role and future
Hedge funds: a central bank perspective

February 2008

Liquidity

Liquidity and financial contagion
Musical chairs: a comment on the credit crisis
Market liquidity and financial stability
Ten questions about the subprime crisis
What happened to risk dispersion?
Liquidity risk management
Liquidity regulation and the lender of last resort
Liquidity shortages: theoretical underpinnings
Liquidity in global markets
The impact on financial market liquidity of the markets in financial instruments directive (MiFID)
Market liquidity and banking liquidity: linkages, vulnerabilities and the role of disclosure
Liquid assets, liquidity constraints and global imbalances
Financial innovation and the liquidity frontier
Financial market liquidity and the lender of last resort
Recent developments in intraday liquidity in payment and settlement systems

October 2008

Valuation and financial stability

Valuation challenges in a changing environment

Should financial institutions mark-to-market?

Setting the right framework for modern financial markets
– Lessons learned from the recent crisis

Revisiting valuation practices throughout the business cycle:
some symmetry is needed

Valuation and fundamentals

Taking into account extreme events in European option pricing

Fair value accounting and financial stability: challenges and dynamics

How should we respond to asset price bubbles?

Regulation, valuation and systemic liquidity

Fair value accounting and financial stability

Procyclicality of financial systems:
is there a need to modify current accounting and regulatory rules?

Valuation in insurance and financial crisis

Bringing transparency to financial reporting:
towards an improved accounting framework in the aftermath of the credit crisis

Improving fair value accounting

September 2009

The future of financial regulation

Regulating finance after the crisis

The shadow banking system: implications for financial regulation

Managing the transition to a safer financial system

Reform of the global financial architecture:
a new social contract between society and finance

Implementing the macroprudential approach to financial regulation
and supervision

Minimising the impact of future financial crises:
six key elements of regulatory reform we have to get right

On the efficacy of financial regulations

The treatment of distressed banks

Credit default swaps and financial stability: risks and regulatory issues

The future of financial regulation

The future of financial regulation: an exchange of views

Emerging contours of financial regulation: challenges and dynamics

Regulation-supervision: the post-crisis outlook

Beyond the crisis: the Basel Committee's strategic response

July 2010

Derivatives – Financial innovation and stability

Redesigning OTC derivatives markets to ensure financial stability

Credit default swaps: what are the social benefits and costs?

Fiat lux – Shedding new light on derivatives markets

Euro public debt and the markets:
sovereign fundamentals and CDS market dynamics

Derivatives: an insurer's perspective

Credit default swaps and financial stability

Credit default swaps
Financial innovation or financial dysfunction?

Is there a case for banning short speculation in sovereign bond markets?

Over-the-counter derivative markets in India
Issues and perspectives

OTC derivatives and central clearing: can all transactions be cleared?

21st century finance cannot do without a sound regulation
of the OTC derivatives markets

An industrial organisation approach to the too-big-to-fail problem

OTC derivatives: financial stability challenges and responses from authorities

Under-collateralisation and rehypothecation in the OTC derivatives markets

Silos and silences. Why so few people spotted the problems in complex credit
and what that implies for the future

Mitigating systemic risk in OTC derivative markets

What risks and challenges do credit default swaps pose to the stability
of financial markets?

OTC derivatives market structure and the credit profiles
of wholesale investment banks

What do network theory and endogenous risk theory have to say
about the effects of central counterparties on systemic stability?

Credit default swap and bond markets: which leads the other?

Concentration risk and the optimal number of central counterparties
for a single asset

February 2011

Global imbalances and financial stability

Global imbalances: the perspective of the Saudi Arabian Monetary Agency

International capital flows and the returns to safe assets in the United States, 2003-2007

The challenge of high capital inflows to financial stability: an emerging market perspective

Global imbalances: the international monetary system and financial stability

Global imbalances: the perspective of the Banco de México

Complementarity and coordination of macroeconomic and financial policies to tackle internal and external imbalances

Global imbalances: common problem to solve for both advanced and emerging market economies

Global balance and financial stability: twin objectives toward a resilient global economic system

Global imbalances: the perspective of the Bank of England

Global imbalances and developing countries

A South African perspective on global imbalances

Global imbalances, volatile capital inflows and proposed further IMF roles

Global imbalances and financial stability

Global imbalances and current account imbalances

Global imbalances through the prism of savings and investment

Global imbalances: the perspective of the Reserve Bank of India

Intellectual challenges to financial stability analysis in the era of macroprudential oversight

Securing stability and growth in a post-crisis world

Revisiting the Tinbergen Rule: use the macroprudential tools to maintain financial stability

On savings ratio

April 2012

Public debt, monetary policy and financial stability

Central banking in a context of high public debt

Fiscal outlook and fiscal sustainability risks

When Western sovereign risk is in play

The return of financial repression

A tale of two overhangs: the nexus of financial sector and sovereign credit risks

Banks, moral hazard, and public debts

Sovereign creditworthiness and financial stability: an international perspective

Stability, growth and regulatory reform

Is sovereign risk properly addressed by financial regulation?

Contagion and the European debt crisis

Monetary policy and public debt

Does monetary cooperation or confrontation lead to successful fiscal consolidation?

Fiscal challenges to monetary dominance in the euro area: a theoretical perspective

Central bank independence and sovereign default

The sovereign debt crisis and monetary policy

Sustainability of government debt: preconditions for stability in the financial system and prices

The importance of confidence in macroeconomic stabilisation efforts

Policies on sovereign debt

Hazardous tango: sovereign-bank interdependence and financial stability in the euro area

Rebuilding growth and optimism in a new fiscal era

Gaps in the institutional structure of the euro area

The euro crisis: some reflexions on institutional reform

April 2013

OTC derivatives: new rules, new actors, new risks

Foreword

Completing the G20 reform agenda for strengthening over-the-counter derivatives markets

Regulatory reforms for OTC derivatives: past, present and future

Overview of international work towards OTC derivatives markets reform and remaining challenges

International cooperation: a *sine qua non* for the success of OTC derivatives markets reform

Containing extraterritoriality to promote financial stability

International swaps market reform – Promoting transparency and lowering risk

CPSS-IOSCO Principles for financial market infrastructures: vectors of international convergence

A transparency standard for derivatives

New infrastructures for a sounder financial system

The importance of data quality for effective financial stability policies
Legal entity identifier: a first step towards necessary financial data reforms

Transparency and financial stability

Assessing contagion risks in the CDS market

Why the Greek CDS settlement did not lead to the feared meltdown

CCPs as instruments of stability and risk mitigation

Incentive compatible centralised clearing

Access to central counterparties: why it matters and how it is changing

Central counterparties in evolving capital markets: safety, recovery and resolution

Collateral and new offers for an optimised management: an industrial revolution

Collateral scarcity and asset encumbrance: implications for the European financial system

OTC derivatives market – regulatory developments and collateral dynamics

OTC derivatives: ensuring safe, efficient markets that support economic growth

Consequences of the new regulatory landscape on OTC derivatives trading

Will the new regulatory regime for OTC markets impede financial innovation?

April 2014

Macroprudential policies: implementation and interactions

Macroprudential policy: from theory to implementation

Five questions and six answers about macroprudential policy

Governance of macroprudential policy

From tapering to preventive policy

Collective action problems in macroprudential policy and the need for international coordination

A macroprudential perspective on regulating large financial institutions

The impact of macroprudential policy on financial integration

European macroprudential policy from gestation to infancy

Macroprudential policy in France: requirements and implementation

Implementing macroprudential policies: the Swiss approach

The effects of macroprudential policies on housing market risks: evidence from Hong Kong

Macroprudential policies in Korea – Key measures and experiences

Framework for the conduct of macroprudential policy in India: experiences and perspectives

Learning from the history of American macroprudential policy

Macroprudential policy and quantitative instruments: a European historical perspective

Macroprudential policy beyond banking regulation

Principles for macroprudential regulation

Macroprudential capital tools: assessing their rationale and effectiveness

The housing market: the impact of macroprudential measures in France

Three criticisms of prudential banking regulations

Macroprudential policy and credit supply cycles

Interactions between monetary and macroprudential policies

April 2015

Financing the economy: new avenues for growth

The financing of the economy in the post-crisis period: challenges and risks for financial stability

Completing the single market in capital

What does the new face of international financial intermediation mean for emerging market economies?

Financing solutions to sustain the growth of SMEs and MTEs and lay the foundations for future competitiveness

Reviving securitisation

Supporting sustainable growth: the role of safe and stable banking systems

How a supplemental leverage ratio can improve financial stability, traditional lending and economic growth

Key initiatives to unlock bank lending to the European corporate sector

The impact of the new regulatory paradigm on the role of banks in financing the economy

Impact of financial regulation on the long-term financing of the economy by banks

Global banks and the adoption of the new regulatory framework: effects on the financing of emerging markets and developing economies

The opportunity cost of collateral pledged: derivatives market reform and bank lending

Editor
Banque de France
39, rue Croix des Petits-Champs – 75001 Paris

Publishing Director
Nathalie AUFAUVRE

Executive Editor
Ivan ODONNAT

Production
Press and Communication Department

Orders
Banque de France – 07-1397
Service de la Pédagogie économique
9, rue du Colonel Driant – 75049 Paris Cedex 01

Imprint
Navis, Paris

Registration of copyright
April 2016

Internet
http://www.banque-france.fr/en/publications/financial-stability-review.html