Abstracts

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.

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.

Abstracts

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.

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.

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.

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.

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 paper 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.

Abstracts

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 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, **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.

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.

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.

Abstracts

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.

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.

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. 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).

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 paper 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. Our 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.

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 see who can be 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.