# Enabling technologies in financial market infrastructures and payment services innovation : An overseers' perspective on opportunities, risks and policy

Filip Caron

Nimble technology firms are eating the lunch of traditional financial institutions, a recurrent statement in the financial press, literature and at conferences. But while FinTech is often considered as a collective noun for (start-up) disrupters in the financial industry, the concept was originally coined to describe the intersection between finance and technology.

Belgium-based financial market infrastructures (FMIs), custodians, payment service providers (PSPs), as well as critical service providers (CSPs) have a long tradition of technology-driven innovation in their business processes. At the same time, disruptors and digital giants have demonstrated significant interest in revisiting traditional business processes. This trend is partially driven by the rapid development of enabling technologies, the need for operational excellence and expectations for customer intimacy.

Two approaches to business process innovations are generally being distinguished : improving the efficiency and/or effectiveness of existing business processes and extensive business process redesigns. Increasing the speed, transparency and tracking of transactions without changing the processing flow are examples of the former (observed in e.g. SWIFT's Global Payments Innovation Initiative, see section 4 on SWIFT). Disintermediation like in Bitcoin, on the other hand, is an example of a significant business process redesign as it renders certain functions obsolete.

This article points up technology-induced paradigm shifts with a potential impact on FMIs and payment services in the longer run (section 1). Focus is on the future stable section of the hype curve, which follows the peak of inflated expectations and the trough of disillusionment[(1)]. The article discusses the most important risk drivers (section 2) in the technology (r)evolution and concludes with the overseers' main policy principles (section 3).

## 1. The potential of enabling technologies

Technological innovation and finance have long since gone hand in hand. The next wave of financial technology has been triggered by the abundance of recent technological advances such as the ubiquity of the internet, the availability of high-speed computing, cryptographic progress and innovations in data analysis.

(1) The Gartner Hype Curve or Cycle represents the maturity and adoption of new technologies in five key phases. After the initial stages of new technologies (technology trigger, peak of inflated expectations, trough of disillusionment), the technology's life cycle enters a phase where more deliverables benefiting the industry start to crystallize (slope of enlightenment) and, finally, where mainstream adoption or implementation starts to take off (plateau of productivity). Focus of this article is put on the last phase of the Gartner Hype Cycle.

Ingenious combinations of technologies could lock in interesting benefits and process improvements for the financial industry. For example, Bitcoin combined a variety of technologies such as digital signatures and peer-to-peer practices to develop an electronic payment system based on cryptographic proof instead of trust.

While these ingenious combinations are commonly referred to as enabling technologies (e.g. distributed ledger technology, see below), they are in their early stages of development. A series of important design decisions still need to be made and unsolved problems tackled before the full potential of these technology combinations can be realised. Consortia of various stakeholders are currently working on standard proposals.

This section describes three categories of promising enabling technologies: (1) distributed ledgers, (2) application programming interfaces, as well as (3) big data and artificial intelligence. For each enabling technology, the prospective benefits and potential impact on FMIs and financial services will be discussed.

### DISTRIBUTED LEDGER TECHNOLOGY

Finance professionals, venture capitalists and regulators have been struck by the potential of distributed ledger technology (DLT), which focuses on providing access to trustable and complete data in networks without centralised data storage. A distributed ledger can be defined as a consensus on data replicated, shared and synchronised over a network. Replications of the data can be geographically spread and dispersed over multiple entities.

These ledgers could record ownership of a broad variety of assets. Typically, a distinction is made between digital assets that originate on the ledger (i.e. native assets such as virtual coins) and digital representations of physical assets (i.e. tokenised assets like unallocated gold). Hence, a multitude of potential use cases has been put forward; including global (wholesale) payments and securities, collateral management and corporate actions.

DLT has the capacity to open up considerable opportunities for efficiency gains. Primarily, DLT has the potential to disintermediate the trusted middlemen with a notary function. All entities participating in a DLT network can acquire real-time access to complete and accurate ledger data, which potentially reduces the frictions related to information sharing and reconciliation. Consequently, faster end-to-end processing of transactions becomes possible. As a network can comprise globally dispersed participants, these efficiency gains could also apply for cross-border transactions without a notary function as intermediary.

Additionally, DLT-based systems have the potential to strengthen data quality in the financial sector. Encryption technology can ensure the authenticity of the ledger data without recourse to central institutions and could guarantee the immutability of the data. Block chain is an oft-cited data organisation approach for DLT that focuses on cryptographically guaranteeing data immutability. Providing participants and trusted third parties (e.g. regulators) with access to full and immutable data, enables these parties to trace ownership and transaction history.

At the same time, DLT's near real-time data replication could assist financial institutions in reducing their operational and credit risk exposure. The pervasiveness of transaction data ensures strong data resilience, which is highly desirable in the event of a local system failure at an FMI or payment system provider. Additionally, this close-to-real-time data replication might ensure faster end-to-end processing.

The extent of these potential benefits might largely be determined by the proposed technology implementation, e.g. the scalability of the proposed implementation will likely impact the end-to-end processing speed. Currently, no convergence towards a generally accepted DLT implementation has been observed. As part of its technology assessment, the Bank has identified the governance arrangements, the data access restrictions, the synchronisation mechanisms and the underlying data structures as critical influencers for the quality of a DLT implementation. The Committee on Payments and Market Infrastructures (CPMI) recently published an assessment framework for DLT implementations[(1)].

(1) CPMI (2017), *Distributed ledger in payment, clearing and settlement – an analytical framework*, BIS (www.bis.org/cpmi/publ/d157.pdf).

In a scenario in which the core players were to adopt market-wide distributed ledgers, at least some peripheral players could be disintermediated[1]. This would be a significant process redesign. While this process could theoretically also render the settlement function of Central Securities Depositories (CSD) redundant, their disintermediation could be rather difficult from a legal point of view. Under the legal requirements of the Central Securities Depositories Regulation (CSDR)[2], securities subject to a transaction on a trading venue must be recorded in the books of a CSD prior to or at the latest on the intended settlement date. More generally, the potential efficiency gains of DLT can only materialise when its implementation matches fully within the existing legal environment. This might be achieved by adapting implementation, and where expedient from a public policy perspective, adapting the legal framework. While disintermediation of FMIs may result in less friction for end-to-end processing, it may also result in an abolition of certain risk reducing functions (e.g. netting), thereby reintroducing financial risks for participants.

### APPLICATION PROGRAMMING INTERFACES (APIS)

Interoperability will be a key requirement for institutions wishing to benefit from a wealth of innovative solutions or aiming to connect to existing financial infrastructure, which is typically the case for respectively incumbents and start-ups. Structured interaction will be needed for information systems to invoke services from (e.g. creditworthiness assessments based on data from social media) and/or exchange data (e.g. account balances) between each other. The application programming interfaces (APIs) of an information system facilitate standardised access to the services and data offered by that system, and thereby enable automated interaction between systems.

APIs could unlock important opportunities for the creation of a new ecosystem. Contemporary financial institutions record a wealth of information on the behaviour of their customers that could be highly relevant for other organisations. By providing access to the data in a financial information system, for which consent and authorisation by individual customers will always be required, institutions could monetize the data. At the same time, APIs enable the integration of complementary services. Institutions can partner up with others to offer a more holistic and innovative product portfolio through their online platform. Similarly, they can take advantage of the API infrastructure of other institutions to broaden their distribution network.

Furthermore, FMIs, custodians, PSPs and CSPs could harness opportunities for reducing the regulatory cost and improving compliance assessments. The in-house development and maintenance of compliance tools (e.g. screening against sanction lists and anti-money-laundering services) can be notoriously complex and typically does not generate a competitive advantage. APIs enable institutions to invoke the services of externally developed and maintained compliance tools, sometimes referred to as regulatory technology or RegTech. Alternatively, institutions could use APIs to automatically collect sanction lists and/or collect know-your-customer details from a central depository.

Opening up the information systems to third-party service providers may result in an important increase of the cyber attack surface. Adequate mitigation measures will need to be put in place to ensure that access is restricted to trusted (authorised) third-party service providers. Furthermore, financial institutions will have to develop sound governance and risk management processes to ensure that the cyber security measures adopted by third-party service providers are appropriate. Any cyber event at a partner with a direct or indirect impact on the financial institution will likely have an impact on the institution's reputation.

Through the adoption of the Second Payment Services Directive (PSD2)[3], the European Commission has mandated account holding institutions to provide payment initiators[4] and account information services providers[5] access to the following services: the balance inquiry, credit transfer initiation and account identity verification services. Furthermore, the European Banking Authority (EBA) will develop a standardised specification for the APIs that need to be opened up

(1) Pinna, A. & Ruttenberg, W. (2016), *Distributed ledger technologies in securities post-trading*, ECB, Occasional Paper Series No 172 (https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf).

(2) Regulation (EU) No. 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012, OJ. 28 August 2014, L. 257, 1-72 (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0909&from=en).

(3) Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ. 23 December 2015, L. 337, 35-127 (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN).

(4) Third parties facilitating the use of online banking to initiate internet payments from the user account to the merchant account by creating a software "bridge" between these accounts, fill-in the information necessary for a transfer (amount of the transaction, account number, message) and inform the merchant once the transaction has been initiated.

(5) Third parties collecting and consolidating information on the different bank accounts of a consumer in a single place. These services will typically allow consumers to have a global view on their financial situation and to analyse their spending patterns, expenses, financial needs in a user-friendly manner.

under PSD2. In contrast, the technical specification for additional APIs may vary considerably. This would require financial institutions to adopt different interaction scenarios for different partners, which could be costly and therefore limit the overall interoperability in the industry.

APIs that allow organisations outside the financial industry to connect to PSPs will be crucial to facilitate automated payments in the Internet of Things context, e.g. cars automatically paying an insurance premium in a pay-as-you-go model, objects automatically paying for the energy they consume, refrigerators sending shopping lists along with payment credentials to an online grocery delivery store, or in pay-per-use object-sharing models.

FMIs and CSPs generally publish API specifications to enable direct connections between their clients' back office systems and their own information systems. These direct connections could lead to greater transaction processing efficiency, including enabling straight-through processing.

### BIG DATA AND ARTIFICIAL INTELLIGENCE

The digital revolution has led to a huge increase in the scale of collection, processing and sharing of personal data. Hence, institutions seeking an information advantage have been collecting a wealth of data. Some of them start facing big data issues as it becomes computationally infeasible to process the datasets using traditional tools. These scalability issues are likely to arise in situations where the volume, velocity, variety and veracity of the data are considered high.

Artificial intelligence (AI) is being looked into to conduct data and behaviour analyses in a timely manner. AI is a set of advanced data analysis techniques that aim to mimick the cognitive functions of the human mind, e.g. deducing facts, reasoning, creative problem-solving for issues, representing knowledge, planning and social intelligence. Fintech start-ups are aiming at even further enriching the analyses by compiling data from different sources.

A variety of use cases for AI has been presented in FMIs and payment services, including obtaining detailed customer insight and fraud detection. Typical customer insight analyses relate to individualised and enhanced product offerings, upselling and churn prediction. Card scheme operators have successfully experimented with the identification of fraudulent transactions through behaviour analysis.

While data and behaviour analysis might result in clear competitive advantages, institutions must be cautious not to violate basic privacy principles. General legitimacy and purpose limitation principles dictate that data can only be processed for transparent predefined (or compatible) purposes. Big data projects, on the other hand, tend to focus on finding hidden relations between data variables and therefore could benefit from the reuse of data collected for other projects. While data anonymisation might allow for compliance with some basic privacy principles, there is often still the risk of re-identification based on data compilation.

## 2. Risks in a disrupted financial environment

The current wave of disruptive technologies and start-ups may pose significant opportunities for the financial industry. The right strategical decisions (e.g. ecosystem or utility provider visions) could well make the difference between the incumbents' survival and their demise. At the same time, innovations come with their own set of risks and challenges, including the usual set of operational (information and cyber), third-party, governance, legal and financial risks.

### INFORMATION AND CYBER RISKS

Information and cyber security focus on reliable service delivery in a networked environment, i.e. guaranteeing the confidentiality, integrity and availability of information. In addition to the traditional cyber security threats, the particular characteristics of the FinTech ecosystem cause additional challenges.

FinTech solutions are often based on relatively immature internet-facing technologies, which may contain unforeseen vulnerabilities and other issues. Any failure has the potential to significantly undermine market confidence. Technology-testing scenarios must closely reflect real-life situations, and could be complemented with extensive penetration testing.

Furthermore, setting up effective (mature) authorisation and fraud detection mechanisms will be crucial in reliable service delivery.

Strong cyber security measures that foster detection, containment and recovery from cyber incidents will be required for all participants of the financial industry. AI is often cited as one of the most promising technologies in cyber threat detection, whereas active defence measures should enable to limit the impact of a materialising threat[1]. Extensive cyber security guidelines have been published in a CPMI-IOSCO joint guidance report[2] and an overview of strategic, tactical and operational controls has been discussed in a previous publication of the Bank[3].

### THIRD-PARTY RISKS

Financial ecosystem strategies are based on the integration of services provided by a broad diversity of interconnected entities. Additionally, FinTech start-ups and increasingly incumbents are developing solutions based on third-party infrastructure- and software-as-a-service products as these products could result in significant cost reductions and scaling flexibility. As a result, an increasing exposure to interdependencies with third-party risk can be observed.

Adversaries might take advantage of vulnerabilities at a specific partner in the ecosystem, in order to gain access to the systems of other participants. Obtaining clear insight in the security policies and procedures, the downstream dependencies and the contingency measures of partners are commonly observed challenges in third-party relationships.

Establishing and enforcing common security baselines is considered a best practice for third party risk mitigation. Furthermore, the partners could consider to integrate their incident response processes and to put security assurance reporting models in place.

### GOVERNANCE RISKS

Governance arrangements and exception handling are increasingly captured in programming code, with the Bitcoin block chain as an extreme example. Theoretically, codes would be extremely effective in enforcing these arrangements. In practice, there are significant limitations to the automated approach that require adequate attention : emerging technology risks and misuses of the system.

Establishing a governance structure could help contain the potential negative impact of emerging technology risks, e.g. to adapt the system design, security controls and or business rules. Research has indicated that vulnerabilities in software are all too common. Additionally, the effectiveness of security controls, e.g. the strength of a cryptographic scheme tends to fall off as computing capacity exponentially increases.

Adequate incident response processes should be specified in order to deal with undesired system behaviour that is not prohibited by the code. TheDAO[4] that aimed at codifying all governance rules and the decision making processes of an organisation, was confronted with a set of vulnerabilities that enabled the draining of significant amounts of funds without violating any of the encoded rules. While patches eliminating these vulnerabilities were publicly proposed but not approved by the community, approximately a third of TheDAO's funds were "maliciously" diverted to another entity.

The CPMI-IOSCO's Principles for Financial Market Infrastructures (PFMIs)[5] prescribe the need for formal governance arrangements that are charged with establishing risk management, internal control and incident management processes. Furthermore, these arrangements should provide clear and direct lines of responsibility and accountability. Effective governance bodies consist of members with integrity that have appropriate experience and skills (including expertise in both technology and finance).

(1) Caron, F. (2016), *Cyber risk response strategies for financial market infrastructures : towards active cyber defence*, NBB Financial Stability Report, 171-185. (https : //www.nbb.be/doc/ts/publications/fsr/fsr_2016.pdf).

(2) CPMI-IOSCO (2016), Guidance on cyber resilience for financial market infrastructures, BIS (http : //www.bis.org/cpmi/publ/d146.pdf).

(3) Caron, F. (2015), *Cyber risk management in financial market infrastructures : elements for a holistic and risk-based approach to cyber security*, NBB Financial Stability Report, 169-184. (https : //www.nbb.be/doc/ts/publications/fsr/fsr2015.pdf).

(4) A decentralised autonomous organisation (DAO) codifies governance and decision-making so that the organisation can be run by a computer program without human involvement. TheDAO is currently the most prominent example of this organisational type.

(5) CPMI-IOSCO (2012), *Principles for financial market infrastructures*, BIS (http : //www.bis.org/publ/cpss101a.pdf).

### LEGAL RISKS

Two main drivers of legal risks have been identified: complexity related to determining the applicable regulation and conflicts between legal requirements and technology principles.

Start-ups may be operating in a less certain legal context, partly driven by the issue of determining the relevant jurisdiction and/or applicable regulation. FinTech solutions could, from a technical point of view, be provided globally through the internet. Additionally, determining the legal location of data can be cumbersome in a cloud environment or a DLT solution. A robust legal basis can be considered as critical to the overall soundness of new technology-enabled business models. A legal basis will facilitate the definition and enforcement of the rights and responsibilities of the relevant parties.

A second set of legal risks originates from divergent legal requirements and technology principles. For example, an FMI should be able to reverse a transaction in response to a mistake or a legal mandate (i.e. the correctability requirement), whereas a major principle in block chain and most DLT implementations is the immutability of the data. Furthermore, a mandatory fork, which basically results in discarding part of the chain and is the proposed reversing technique, might leave participants in the network exposed to legal claims. This was for example the case in the previously mentioned TheDAO incident[1].

### FINANCIAL RISKS IN DLT

Significant uncertainty about settlement in DLT solutions remains, notably on the finality of a settlement in DLT solutions, as well as on the feasibility of implementing a genuine delivery-versus-payment (DvP) solution.

Certainty of settlement is achieved when a transaction is legally both final and irrevocable. However, in block-chain-based DLT designs, settlement is typically probabilistic, i.e. the longer a transaction is recorded in the ledger, the less likely the transaction will be reversed (or dropped) as the resources needed to change the chain of blocks significantly increases each time a block is added. Whether a probabilistic finality could comply with the requirements stipulated in the Settlement Finality Directive[2] remains untested.

A DvP securities settlement requires simultaneous finality of the transaction in both the security and cash ledger, which may imply synchronisation between DLT ledgers. Inter-ledger synchronisation is currently considered to be an important technical challenge with a legal impact.

## 3. Facilitating innovation, while guaranteeing stability

Regulators generally strive to facilitate innovation, security and competition in FMIs and payment services, while guaranteeing a level playing field for all market participants in terms of risk mitigation, prudential supervision and oversight.

### RISK-BASED REGULATORY FRAMEWORK

Risk-based regulatory frameworks that focus on the provision of reliable and secure services enable regulators to be consistent in an industry that is liable to be (radically) reshaped by technological innovators.

The Bank rigorously follows up on technological innovations and assesses their (potential) impact on FMIs, custodians, PSPs and CSPs. This setting allows for innovative experiments, while enabling adequate regulatory response to risks and threats. As overseer and prudential supervisor of these systems and institutions, the Bank continues to focus on the importance of cyber and transaction security.

(1) https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/.

(2) Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems, *OJ*. 11 June 1998, L.166, 45-50 (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31998L0026&from=EN).

### TECHNOLOGY-NEUTRAL

Regulators in general are committing themselves to the principle of tech neutrality in regulation. The actual type of technology will not be taken into account when defining the requirements for obtaining authorisations, risk mitigation and other responsibilities. These requirements are risk-based, and an implementation of a technology will be assessed on basis of these criteria.

Subjecting technology innovators to special regulatory treatment could result in a distorted playing field. The regulators should not overprotect incumbents and should enable the development of designs that are better aligned with their business models and their customers' preferences while reducing risks or maintaining low risks. An equal treatment for equals should be guaranteed.

Technology neutral regulation enables the regulators to adequately respond to technology evolutions and innovations.

### DIVERSE INTERMEDIARY TYPES

Entrants targeting a specific niche of payments, clearing and settlement services might have a different risk profile (in terms of risk types) than generalist FMIs, custodians, PSPs or CSPs. In adapting to this changed reality, regulators could introduce new regulatory intermediary types.

For example, payment initiation and account information services are two new regulatory intermediary types specified in PSD2. A risk-based differentiation from the payment institute licence has been foreseen for these intermediary types, e.g. because they do not provide account-holding services, they are not subjected to the same capital requirements as traditional payments institutions.

### SUPPORT THROUGHOUT THE AUTHORISATION PROCESS

The Belgian regulatory authorities, the Bank and FSMA, recently decided to set up a single point of contact (SPOC)[(1)] for developers of FinTech solutions and to share all relevant information on a web platform. The SPOC will provide assistance in identifying the type of licence that will be needed for the proposed solution, clarify the regulatory framework and assess the legal aspects of the business model, assist in compiling authorisation application files and follow up on the processing of authorisation requests.

### INTERNATIONAL COORDINATION

The cross-border nature of technological innovation calls for international coordination amongst regulatory authorities, which should result in a consistent, standardised and transparent regulatory environment for the providers of FinTech solutions. Examples at European level include the PSD2 and the General Data Protection Regulation (GDPR)[(2)].

(1) https://www.nbb.be/en/fintech.

(2) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ*. 4 May 2016, L.119, 1-88 (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN).