CHAPTER 20

The role and contribution of innovation for payment instruments and market infrastructures

Updated on 17 December 2018

Technical innovation is salient to market infrastructures and most non-cash payment instruments (the direct result of technological innovation), enabling them to meet market requirements in terms of transaction reliability, execution speed and service diversification.

The 1960s to 1980s saw exponential advances in information technology and are a prime example of financial technological innovation, specifically in the field of market infrastructures. Until then, financial market infrastructures' (FMIs) role had been to physically centralise transaction-related documents in order, as far as possible, to clear the transactions in question (by calculating net balances from their gross amounts) and then exchange the physical documents needed to complete them. Securities were thus physically transferred, in paper form, from seller to buyer as proof of ownership. Computing power and the concomitant development of information technologies then made it possible to replace the physical holding of securities in the form of paper certificates by computer records. This paperless technology enabled market infrastructures to evolve towards the modus operandi with which we are familiar today.

Thus, while these infrastructures have existed since the early 1950s, technological developments have enabled considerable progress in the way they process transactions, making it possible for example to switch to so-called real-time processing, which in the early 1990s was still difficult to imagine in this industry. Thanks to computerised processing, market infrastructures have thus been able to accelerate, expand and systematise their traditional centralisation services, and round them out with new, post-market processing services.[1]

Indeed, this development of real-time processing has been spectacular in the case of payment systems, which have evolved from deferred net settlement (DNS) to real-time gross settlement (RTGS – see Chapters 6 and 7). The same is true for settlement and delivery systems, which have gone from having a single settlement session a day to real-time settlement.

Developed in the 1990s in G10 countries, RTGS systems offer the advantage of finalising payments in real time, reducing settlement risk. Until now, they were reserved for urgent, large-value payments. However, thanks to the maturity of the associated technologies, retail payments can now also be made in real time and at low cost; the key lies in the instantaneous nature of transfers, as illustrated in the European Payments Council (EPC) scheme that has been in force since November 2017 and in the instant payment settlement service TIPS, operational since November 2018 (see Chapter 2, Section 3 and Chapter 7, Section 6).

In another area, today's most widely used non-cash payment instruments (payment cards, credit transfers and direct debits) are based on electronic features that have evolved constantly in recent decades, from the development of chip card and PIN code functionality to that of instant credit transfer processing capabilities, including for retail banking, and the use of artificial intelligence for credit scoring. Cash-based payment instruments have also evolved as a result of cutting edge innovations, aimed particularly at combating counterfeiting. Banknotes, for example, are designed using highly sophisticated anti-counterfeiting techniques such as watermarks and holograms.

In the space of a few decades, therefore, market infrastructures and payment instruments have undergone profound change, combining compliance with stringent risk management requirements with exponential IT performance. In this chapter we look at recent initiatives in this field, which are marked by the dynamism of the current wave of new technologies such as blockchain and big data and the arrival of new players. In this context, and in constantly changing markets, central banks play an important role in terms of the

1 Norman P., *Plumbers and Visionaries, Securities Settlement and Europe's Financial Market*, Wiley, 2007.

financial system's stability and the security and efficiency of payment instruments and market infrastructures.

1. Payment instruments and innovation

The surge of innovation in payment instruments is the result of two concomitant phenomena:

- on the one hand, the arrival in the payments field of technological players, from small start-ups to internet giants (GAFA, large telephone operators, etc.) seeking to assert themselves as innovators and commonly referred to as 'fintechs', derived from 'finance' and 'technology';

- on the other hand, the emergence of innovative technologies, within a framework extending beyond the financial sphere and with potentially promising prospects for application in the area of payments. Specific examples here are blockchain and technologies combining big data and artificial intelligence.

1.1. Fintechs and payment services

In the area of payment services, the term 'fintech' currently covers three main categories of activities.

The first of these essentially concerns client relations. It is illustrated in particular by the provision of mobile applications or websites offering enhanced interfaces for viewing accounts and managing payments, for example making it possible to aggregate information from different banks, automatically manage the rebalancing of funds between accounts or even offer users value-added services based on an analysis of their account activity, such as a different banking package or payment instrument, or access to an overdraft facility or a loan based on future expenditure, etc..

This category of players notably covers account information aggregators, which fall within the payment services provision scope defined by the second European Payment Services Directive (PSD 2: see Chapter 3).

A second category of fintechs focuses on developing solutions aimed at facilitating exchange by providing additional services, in support of the banking system but without seeking to change it structurally. These innovations include new payment initiation methods, for example mobile phone or web-based, such as Paylib, Apple Pay and Paypal, which in themselves are not new payment instruments but an innovative way to initiate payments based on existing instruments (card, transfer, electronic money, etc.). Depending on their nature, the services offered by these fintechs may fall within either the PSD 2 payment services provision regulatory framework, which requires fintechs to be authorised, in France, by the *Autorité de contrôle prudentiel et de résolution* (ACPR – French Prudential Supervision and Resolution Authority - see Chapter 3), or that governing the provision of technical services to authorised payment service providers such as banks.

Finally, a third category of fintechs, sometimes referred to as 'neobanks', offers account-keeping and payment services equivalent to those of traditional banks but sold differently, for example on the basis of lower service costs, the limitation of risk by exclusion of authorised overdrafts and the provision of payment instruments with systematic authorisation (which can only be used after checking the balance in the account), a digital interface designed for mobile application use, ease of access and use, etc.. As these activities are governed by European regulations (see Chapter 2), this type of service provider must be authorised as a payment institution or an electronic money institution.

1.2. The emergence of crypto-assets

Crypto-assets such as bitcoin and ether emerged in the early 2010s following the global

Box 1: Crypto-assets: the example of bitcoin

Bitcoin is a virtual asset stored on an electronic medium which allows a community of users that accept it as payment to carry out transactions without having to use legal currency.

Bitcoin was created by a community of internet users, also called 'miners', each of whom has installed free software on their online device or computer that uses an algorithm to generate bitcoins, which the miners then receive in recognition of their contribution to the system's operation.

Once created, bitcoins are stored directly in an electronic safe on the user's computer, tablet or laptop, or remotely (on the cloud, for example). They can then be transferred online, anonymously, between members of the community.

While bitcoin is the most widely known and highly valued crypto-asset, at the beginning of 2018 there were over 1,300 such assets worldwide. Other crypto-assets such as ether and ripple are also experiencing strong growth and function based on concepts similar to those underlying bitcoin.

development of so-called virtual communities, which bring together internet users through digital interaction tools such as chat apps and forums. Often incorrectly referred to as 'virtual currencies' or 'crypto-currencies',[2] these assets do not fulfil or only very partially fulfil the three functions assigned to currency (unit of account, means of exchange and store of value), are not recognised as legal tender or payment instruments and offer holders no guarantee of security, convertibility or value. That is why it is preferable to refer to them as 'crypto-assets'.

1.2.1. Crypto-assets are highly speculative

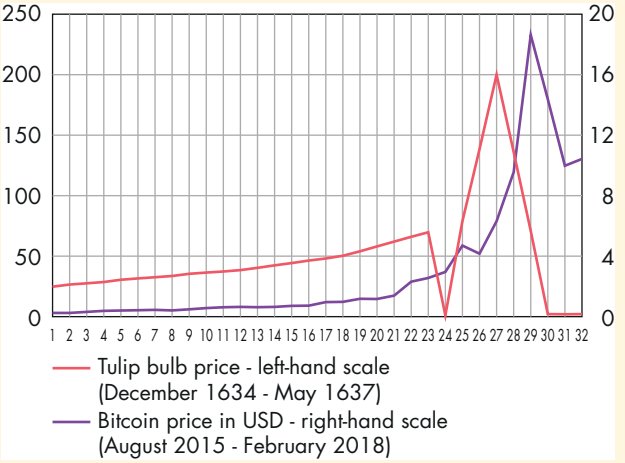
No centralised body guarantees the convertibility of crypto-assets into different currencies. Investors can therefore only recover their funds in currency if other users wish to acquire the same crypto-assets. As a result, the price of a crypto-asset can collapse at any time if investors wishing to unwind their positions find no buyers and end up holding illiquid assets.

In the particular case of bitcoin, the process of issuing units – which is dependent entirely on electronic computing power – is time-capped. This limitation fuels a shortage phenomenon which, given the strong demand for bitcoin resulting mainly from speculation, leads to very sharp price fluctuations. Bitcoin's historical price movement is reminiscent of that of tulip bulbs[3] between 1634 and 1637, as shown by the graph below.

2 See Chapter 1.

3 The tulip mania of the 17th century, which originated in the flower's use for decorative and artistic purposes, led to a sudden increase in tulip bulb prices in the north of the United Provinces (now the Netherlands), amplified by a surge of speculation. At the height of the speculative bubble, in February 1637, pan-European demand inflated the price of a forward tulip bulb sale contract to 15 times the annual salary of a specialist craftsman, or the equivalent value of five hectares of land. The sudden collapse of prices in the spring of 1637 bankrupted a large number of investors and shook the Dutch economy – the result of what is now considered to be one of history's first speculative bubbles.

Chart 1 – Bitcoin price compared with tulip bulb price



Sources: Earl Thompson (tulip bulb price), bitcoin.com (bitcoin price).

1.2.2. Crypto-asset stock remains limited compared with the stock of currency in circulation

The outstanding amount of crypto-assets in circulation came to around EUR 220 billion at end-December 2018, and comprised mainly bitcoin (35%), ether (20%) and ripple (10%). This sum needs to be considered, however, against the stock of currency in circulation: at end- 2017, the M1 aggregate, which corresponds to the sum of banknotes and coins in circulation and sight deposits of non-financial agents, stood at more than EUR 7,500 billion in the euro area and nearly USD 3,500 billion in the United States.

1.2.3. Use of crypto-assets is broadening

Crypto-assets are raising the public's interest outside their original communities, i.e. from users and merchants, or non-crypto-asset miners, with no operational role in the asset management and issuance network. This is leading to the development of multiple services, organised along the lines of existing, traditional financial services.

In the area of market infrastructures, for example, trading platforms have been created to buy and sell crypto-assets for currency such as EUR and USD. These platforms thus enable users who have not participated in the creation process to acquire crypto-assets, or to convert crypto-assets received as payment into legal tender currency. Increasing numbers of crypto-asset custody services – akin to depository activities – are also emerging on the heels of this trading activity.

Linked to this exchange activity, services in financial information and data supply, investment advice and trading are being developed. These activities encourage the creation of investment instruments backed by crypto-assets, such as funds or derivatives, with initiatives launched by the Chicago Board Options Exchange and the Chicago Mercantile Exchange, for example.

The financing business has also benefited from the development of crypto-assets, in the form of initial coin offerings (ICOs). ICOs are in some respects the transposition into crypto-assets of the crowdfunding concept: in this type of arrangement, internet users who make a financial contribution to a project (in crypto-assets or currencies) receive digital assets (or tokens) in exchange. In practice, these tokens represent a form of economic interest in the project. They give their holders certain rights, such as to first use of the financed platform or application (as in traditional crowdfunding), receipt of part of the profits generated by the company or the exercise of voting rights (as with shares). Management of the tokens issued in ICOs is itself assured through the blockchain used for the ICO, and based on exchange mechanisms similar in all respects to those of crypto-assets. ICO tokens can therefore be seen as another type of crypto-asset, enhanced by the specific rights referred to above. The limitations and risks of crypto-assets described in this chapter also apply to the exchange and custody procedures for tokens.

1.2.4. Crypto-assets are a vector for money laundering and terrorist financing, cyber attack, and also have an environmental cost

Crypto-assets' anonymous nature facilitates the financing of terrorism and criminal activities and the circumvention of anti-money laundering rules.

The anonymity that characterises the issuance and transfer mechanisms of most crypto-assets increases above all the risk of these assets being used for criminal purposes (online sale of illegal goods or services, payment of ransoms, etc.), including money laundering and terrorist financing.

The French agency combating illegal financial circuits, Tracfin (*Traitement du Renseignement et Action contre les Circuits FINanciers clandestins*), identifies

the use of crypto-assets, particularly bitcoin, as being the source of a specific risk in terms of money laundering and terrorist financing.

Custody of crypto-assets is subject to significant cyber risks and offers no security or protection for these assets.

There have been a number of cases of hacking of electronic wallets used to store crypto-assets. In case of theft of assets, wallet holders have no recourse against the hackers. Repeated, large-scale incidences of fraud (the USD 534 million hacking of Coincheck in January 2018 and the high-profile bankruptcy in 2015 of MtGox, the world's first bitcoin trading platform[4]) illustrate the vulnerability of the crypto-asset ecosystem and – in the absence of guarantee mechanisms – the high level of associated risks.

The use of crypto-assets is also associated with an environmental cost.

The computerised validation of crypto-asset transactions has also a considerable environmental impact linked to the energy it uses: in December 2017, the validation of a single bitcoin transaction was estimaed at 215 kWh of electricity, being the equivalent of six months of uninterrupted PC use. This energy consumption increases constantly due to the important competition associated with the expansion of the transaction validation (mining) network. However, it should be noted that certain crypto-assets rely on less energy-intensive procedures, depending on the issuance and validation procedures of the associated transactions.

1.2.5. To control the identified risks, the public authorities are exploring crypto-asset-specific regulatory solutions

Regulation of crypto-asset-related activities is desirable for four main reasons: the high-priority fight against money laundering and terrorist financing, investor protection, the preservation of market integrity, including against cyber risk, and, lastly, if these activities continue to grow strongly, financial stability concerns.

At national level, the Banque de France and the Autorité de contrôle prudentiel et de resolution *(ACPR) partially supervise crypto-asset-related services as part of their payment service provider-related remit, and plan to extend this framework to the various types of crypto-asset intermediation platforms.*

The activity of the platforms that offer conversion into legal currency, which act as an intermediary between buyers and sellers, is considered a payment service requiring authorisation as a payment service provider. However, this requirement arises from the management on behalf of third parties of accounts held and denominated in a legal currency, and not from the crypto-asset-related service.

In addition to this approach, the Banque de France and the ACPR advocate an extension of the regulatory framework applicable to services associated with crypto-assets, through the introduction of a crypto-asset service provider status.

This regulatory change could follow on from the revision of the fourth anti-money laundering and terrorist financing directive currently being adopted by the European Union (the so-called fifth AML-CFT Directive). This directive's provisions are applicable to players offering (i) services to convert crypto-assets into legal currencies, and (ii) custody, on behalf of their clients, of private cryptographic keys that make it possible to hold, store and transfer crypto-assets.

As well as contributing to the fight against money laundering and terrorist financing, which is a priority, a crypto-asset service provider status would submit its holder submit to rules relating in particular to

4 Following an internal fraud leading to the misappropriation of 650,000 bitcoins with a monetary value of around USD 360 million.

transaction security and client protection. This status could also cover services concerning transactions between different categories of crypto-asset.

The regulatory framework for crypto-asset service providers could be supplemented by a limitation of the possibility for certain regulated companies (banks, insurance companies, management companies, etc.) to work with crypto-assets.

The first step would be to ban crypto-asset deposit taking and loan granting. With regard to savings products, the question of banning all related marketing through retail collective investment vehicles should be considered, with the aim of reserving these instruments for the most experienced investors. These products should also be made subject to stringent client protection rules. Lastly, as regards the proprietary investments of regulated entities, in the absence of a complete ban on investments in crypto-assets, strict control of these investments, for example by deducting them completely from capital, should be considered. These provisions presuppose changes to national and European legislation.

European and international coordination would be desirable in order to ensure more effective regulation in this area.

Given the paperless nature of crypto-assets and the use of internet-related technologies that facilitate the provision of cross-border services, the heterogeneity of national regulations could prevent full control of the resulting risks.[5]

With this in mind, on 7 February 2018, France and Germany's economics and finance ministers and central bankers placed the subject on the G20 agenda. The meeting of G20 ministers and governors held in Buenos Aires in March 2018 gave accordingly impetus to a common international commitment to reflect in depth on the subject, as recorded in the summit's official communiqué.[6]

1.3. Big data and artificial intelligence technologies

The development of real-time data analysis technologies is a key driver of innovation in the payments sector, which by definition conveys large volumes of flows on a continuous and permanent basis.

The main application of these technologies to payment services relates to the identification of risky transactions, for the purposes of combating fraud or terrorist financing and money laundering, by using transaction and/or user profiling techniques and the capacity to simultaneously process data relating to all ongoing transactions.

In addition to the strong authentication solutions deployed by issuers of payment instruments (see Chapter 3), transaction risk-scoring techniques are used to determine whether the transaction should be blocked, suspended or executed. Scoring tools generally use rules based on known fraud scenarios. In a credit transfer context, for example, rules may take into account the transfer data (type of account to be debited, amount, new account to be credited or not, etc.), the account holder's profile and the data that the institution has collected on the account holder's habits (frequent or non-frequent use of the communication channel in question, previous transfer amounts, intensity of use of the payment instrument, etc.).

The regulatory technical standards associated with the second European Payment Services Directive (PSD 2: see Chapter 3) notably stipulate the following criteria as being usable for risk analysis purposes:[7]

- the identification of abnormal behaviour or expenditure;
- the detection of unusual information about the device or software used;
- the identification of a virus during a session that required client authentication;

5 See Beau D.: *https://www.banque-france.fr/intervention/conference-de-la-banque-de-france-liae-de-rouen-le-31-octobre-201*

6 "We acknowledge that technological innovation, including that underlying crypto-assets, has the potential to improve the efficiency and inclusiveness of the financial system and the economy more broadly. Crypto-assets do, however, raise issues with respect to consumer and investor protection, market integrity, tax evasion, money laundering and terrorist financing. Crypto-assets lack the key attributes of sovereign currencies. At some point they could have financial stability implications. We commit to implement the FATF standards as they apply to crypto-assets, look forward to the FATF review of those standards, and call on the FATF to advance global implementation. We call on international standard-setting bodies (SSBs) to continue their monitoring of crypto-assets and their risks, according to their mandates, and assess multilateral responses as needed."

7 These data are also listed in the sole authorisation system defined in France by the French data protection agency (CNIL) to provide a framework for data processing aimed at combating external fraud in the banking and financial sector (*https://www.cnil.fr/fr/declaration/au-054-lutte-contre-la-fraude-externe-dans-le-secteur-bancaire-et-financier*).

- the identification of a fraud scenario;
- the account holder being in an abnormal or a high-risk location.

In addition to the analysis of individual flows, account-holding institutions can use information concerning the aggregate flows observed on all their clients (rejection rate for direct debits, unusual beneficiaries or destinations for credit transfers, etc.). As well as facilitating the detection of fraud attempts, where appropriate this cross-referencing of information allows institutions to notify certain clients of the occurrence of transactions identified as suspicious.

The tool parameters allow the rules to be refined by modifying the influence of the input data. Once the scoring rules have been established, the system can determine, based on the 'calculated score', whether it is necessary to implement an additional authentication level or to alert the account holder for additional validation, for example by making a return call.

These technologies are also used for personal or business support purposes, to pre-identify user or client needs

Another fast-growing application of these technologies is marketing value-added account-keeping advisory applications, generally associated with account information aggregation and payment initiation services (see above), which analyse the client's behaviour with a view to suggesting rebalancing transactions and banking offers (card, overdraft, credit, investment, etc.) adapted to their profile.

As regards merchants, meanwhile, similar solutions make it possible to analyse client behaviours with a view to offering pathway optimisation (for example, by preselecting a payment method based on intended purchases), or to improve the targeting quality of promotional campaigns and loyalty programmes.

2. New technologies, a potential source of transformation of market infrastructures

Market infrastructures' activities necessarily involve a large amount of data collection, making them fertile ground for the development of new technologies.

In addition to already proven and widely implemented changes, further transformation of market infrastructures is expected with the advent of certain technological innovations. Advances in predictive analysis and artificial intelligence, for example, could not only help further improve risk models but also prevent and detect fraud attempts. They have also already been used to streamline settlement in RTGS systems.

Among recent technological innovations, blockchain is currently the focus of much attention. While market infrastructure activities seem a particularly suitable field of application for this technology, a lack of large-scale implementation has prevented it from really proving its worth. This state of transition makes it difficult to assess the changes it could bring about in the area of market infrastructures, but the subject certainly deserves consideration.

Blockchain became popular with the emergence of bitcoin in 2009. This 'chain of blocks' technology for storing and transmitting information arose from a desire to revolutionise payments and emancipate users from the centralised trusted third party system. It is libertarian in nature and introduces an organisation in which the issuance of exchange media and the management of transactions are carried out not through an intermediary (banking, legal, etc.) but directly through the user network. The blockchain's content is thus distributed in real time to all members of the network, and referred to as the 'distributed ledger' (hence DLT, an acronym of 'distributed ledger technology').

Potential blockchain applications abound, and are far from confined to the banking

and financial sector, being useable for insurance automation, diploma registration, land register security, recording of property rights for works of art, etc.

While the financial sector took an early experimental interest in this distributed ledger technology, there are as yet few cases of it being rolled out on an industrial scale.

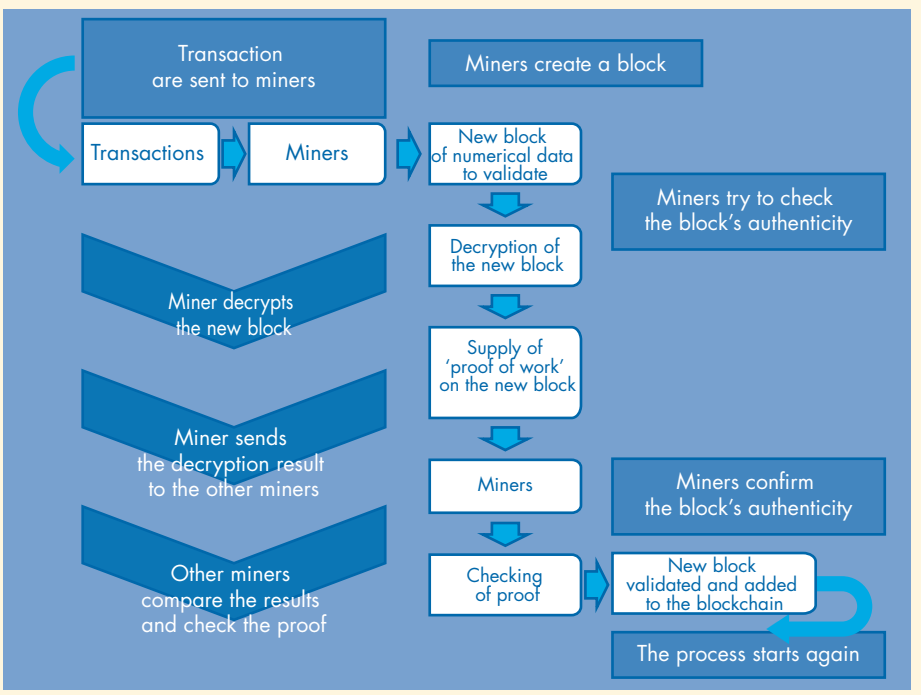
2.1. Blockchain operation: the algorithm is key to building trust between contracting parties

Blockchain technology is based on open source software, i.e. it is a computer program the source code of which is distributed under a royalty-free licence allowing anyone to read, modify or redistribute the software completely freely and legally.

Each of a blockchain's blocks contains data (sender, recipient, amount, etc.) relating to one or more transactions that has been encrypted, i.e. secured by computer algorithms. There are various processes for validating new blocks to add them to the chain. The one used for the bitcoin blockchain, however, is particularly representative: in this case, to add a new block of transactions to an existing chain of blocks, the new block must first be validated. To do this, certain chain participants (miners) have to solve an algorithmic problem. The first miner to find the solution validates the new block and adds it to the chain, subsequently receiving a certain amount of bitcoin in exchange (see also Section 1.2 above).

Whatever the validation mechanism used, it allows each block to be linked to the previous block and thereby ensures the data's immutability for all participants in the chain. In addition, when a transaction is validated, it is sent to a network of computers known as a 'storage node'. Each

Description of the mechanism for validating a new block:



Source: Banque de France website, *https://abc-economie.banque-france.fr/mot-de-lactu/blockchain*

'node' contains a copy of the database in which the history of the transactions carried out is recorded. All stakeholders can access it simultaneously. This decentralisation of security management aims to prevent the falsification of transactions. **Blockchain's inviolable nature is not beyond dispute, however, as it would still be possible for a coordinated majority of validators to take control of the transactions (so-called 51% attack). This is all the more significant in that there has been a trend among miners of converging on places where the cost of electricity is at its lowest**.

2.2. Blockchain, an original response to post-market issues?

Blockchain technology's decentralisation and secure ledger characteristics make it a seemingly promising technology for post-market activities. Its advocates accordingly argue that it should make it possible to organise the functioning of market infrastructures, in particular their centralised dimension, differently, the assumption being that the technology can theoretically eliminate the need for central trusted third parties and so reduce infrastructures' operating costs and further improve their efficiency.

However, market infrastructures have already, for several decades, been highly streamlined and efficient: the IT boom has meant that they have already benefited greatly from technological innovation. While admittedly they are based on more traditional technologies, blockchain technology cannot necessarily offer them significant added value. In particular, analysis suggests that the possibility of operating in a decentralised manner is not a more efficient, economical and secure solution than their current, centralised and sophisticated way of functioning. In addition, the decentralised management of financial transaction processing activities raises numerous issues related to the responsibility of the various players involved in the processing chain.

2.3. Public blockchain vs. private blockchain

Blockchain technology's dissemination beyond its original use for bitcoin has led to a substantial change in its founding principles. Elimination of the trusted third party (neutral central entity), anonymity and the open nature of the chain have given way, for example, to so-called closed or private blockchain systems, reserved for a limited number of players and controlled by a central authority playing the role of blockchain manager. Thus, instead of using a blockchain that is open to all and over which the players involved have no control, financial market initiatives are based on blockchains that are not universally accessible. Their access is limited to certain players who have to meet predefined participation criteria in terms of risk profile, activity and status. Such an organisation requires defining and verifying compliance with these criteria, which is carried out by an entity playing the specific role of 'blockchain keeper'. This clearly illustrates the non-disruptive but evolving role that this technology seems to be able to play in post-market and market infrastructure activities, since the roles of each player (participant and central entity) do not change in this scenario.

In this respect, blockchain technology is of particular interest for powering areas of post-market activity that are as yet unautomated and which have remained structured around largely manual processes.

2.4. The emergence of blockchain initiatives for post-market automation

French legislation is supportive of this movement. A ministerial order was adopted on 8 December 2017, for instance, relating to the use of a shared electronic registration system for the representation and transmission of financial securities.[8] Following on from the so-called Sapin II Law of 9 December 2016, it makes it possible to register the issue or sale of financial securities in a blockchain.

8 *https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000036171908*

Box 2: Opportunities and limits of smart contracts

Smart contracts are contracts in which certain clauses can be triggered automatically if certain predefined events occur. They are a growth area, particularly in insurance, where policies can now cover passengers for flight delays, for example. These policies are recorded in a blockchain and linked to air traffic databases, automatically triggering compensation for passengers in the event of a delay.

For post-market activities, smart contracts could be particularly useful for the execution of corporate actions, as yet a relatively unautomated area. For example, one fintech uses blockchain technology to offer smart contracts that have been programmed to carry out around 50 standard corporate actions. Such automation of corporate actions is not exclusive to blockchain technology, however, and could be carried out using other information technologies.

Smart contracts have yet to be tested for the contractualisation of more complex post-market transactions, such as the management of flows relating to collateral or margin calls. The benefits of these automation methods are therefore still open to debate.

Initiatives have already emerged, proposing a simplification and automation of certain post-market activities. A case in point concerns commercial paper, which is currently traded over the counter and for which reconciliation takes place manually in the back offices of the various parties involved in a transaction, followed by settlement and delivery. A current initiative aims to develop a commercial paper trading platform and a settlement and delivery service that will automate and streamline the entire commercial paper life cycle, from issuance and trading to settlement and delivery. It relies partly on blockchain technology, and on the T2S platform for settlement and delivery.

It is also the approach taken by another initiative to help improve access to finance for certain players, for example by promoting SMEs' access to capital markets based on blockchain technology. To achieve this, the post-market process for SMEs would have to be redesigned to simplify it by providing a lighter infrastructure than a central securities depository (CSD), comprising fewer intermediaries – specifically with no brokers and no central counterparty (CCP) – a relatively redundant entity as far as SMEs are concerned as they have little need for securities netting. The aim would also be to ensure issuers transparency on their investors and shareholders, which is currently lacking. Blockchain technology appears well placed to offer appropriate solutions in this area thanks to its original ledger functionality.

Other initiatives focus on the activity of issuing and distributing fund units, currently still a very manual process – particularly when carried out outside CSD channels. Fund management companies' challenge of finding out more about the identity of investors is also highly significant, and here too blockchain technology could provide an appropriate response.

2.5. As yet unproven technology

Despite the initiatives currently underway, questions remain about blockchain technology's translatability into real-life projects that can be deployed on a large scale.

Firstly, the question of the technology's performance and its ability to handle large volumes has not yet been answered convincingly. Indeed, blockchain technology has so far been used in niche activities or closed environments, in segments with

low-volume requirements. Depending on blockchain's public or private nature and its transaction validation methods, the performance-related questions that can be asked can vary significantly. For example, bitcoin requires the resolution of highly sophisticated algorithms for the validation of new blocks in order to guarantee the blockchain's security in an open environment with anonymous participants not bound by mutual trust. To validate a transaction, it requires miners to perform extensive calculations necessitating considerable computing power, and therefore significant IT capacity; this validation protocol uses a lot of energy for a limited performance (see above, Section 1.2.4). Conversely, under some blockchains counterparties validate transactions directly, without them being disclosed across the network and with no algorithmic resolution validation mechanism. However, such an organisation requires the use of closed or private blockchains, including ex ante control of authorised participants based on predefined participation criteria.

Generally speaking, the less burdensome the validation protocol for new transactions in terms of calculation, the easier it is to increase transaction processing speed; it is therefore a matter of striking a balance between transaction security, the open or closed nature of the blockchain and the required level of performance – high in the case of post-market activities, for example.

Secondly, the issue of transaction confidentiality and participant access management – and therefore participant identification – once again can be resolved only by using closed blockchains. Blockchain was initially based on principles of total openness to the public, anonymous participation or the use of pseudonyms, and universal access to the transactions carried out. These characteristics have proved ill-suited to the requirements of post-market activities, for which players must be known and transactions confidential. Only closed blockchains can meet these requirements.

Another current blockchain challenge relates to its ability to fulfil standardisation and interoperability conditions. This is because there is a particularly strong need for norms and standardisation if a project involves complex uses, for example linking multiple players and a number of transaction processing systems and/or integrating a process in its entirety. Standardising such a process is therefore essential to enable all its systems to interlink, regardless of the technology used (traditional or blockchain). A number of approaches have been suggested in response to the first question – one of interoperability between blockchains: (i) impose one's own standard, with the aim of becoming the norm for post-market activities, (ii) use a service provider providing all the necessary services and using the same technology, or (iii) not concern oneself with standardisation – the case of some fintechs who consider that there is no standard for blockchain technology at this stage. In this regard, it should be noted that the issue of harmonisation is a key element for post-market players (including the authorities): how can it be ensured that any developments based on this technology do not call into question the already huge efforts made in Europe to harmonise post-market activities?

Meanwhile, there has been little consideration of questions of interoperability between blockchain on the one hand and non-blockchain technologies on the other – and the research that does exist is often carried out in closed environments, for security reasons. However, this question may not represent a major challenge, insofar as blockchain relies on long-standing, reliable technical tools such as cryptographic protocols and decentralised infrastructures. In this respect, it can be considered that blockchain is less a technical innovation – since it is based mainly on existing technologies – than an organisational one, insofar as its novelty lies above all in the way it uses these existing tools to create a secure distributed system.

3. The role of central banks in this environment

3.1. The Banque de France and the Eurosystem's catalyst and market infrastructure operator roles in the context of innovation

In addition to their oversight role, the Eurosystem central banks and the ECB also play the roles of catalyst and market infrastructure operator. In their catalyst role they monitor the industry's efforts to develop innovative new services and processes, and provide support for market initiatives. As market infrastructure operators, meanwhile, the Eurosystem and the Banque de France have initiated a number of innovative programmes to improve the efficiency of the market infrastructures that they operate.

Box 3: Central bank digital currencies (CBDCs)

The possibility for a central bank to unilaterally issue digital currency, a new form of money, has often been suggested – notably in the context of reflection on the cashless society concept (see Chapter 2). This would take the form of a claim on the central bank, which would be distributed digitally and be a separate instrument to the reserves currently available to commercial banks. The idea raises two different issues depending on whether one is considering payment between businesses (wholesale, therefore) or retail payments.

As far as retail payments are concerned, the main consideration here is the public circulation of a paperless payment instrument that is a direct claim on the central bank, as opposed to traditional paperless payment instruments, which represent claims on commercial banks.

To date, most developed countries consider that there is no reason to issue this type of instrument, in that: the retail payments industry and its associated infrastructures are sufficiently efficient and secure, and payment service providers' offers meet all existing demand. Moreover, the current sharing of duties between central banks and commercial banks is adequate for responding to the challenges posed by changes in payment methods (instant payments, for example). Such is the current position in the euro area.

Issuing a CBDC does not necessarily solve the issues raised by the potential decrease in the use of cash and the need to maintain financial stability. On the contrary, there are major uncertainties about the implications of issuing this type of instrument, in particular regarding the respective roles in the economy of central banks and commercial banks, including in the event of a crisis of confidence in the banking system (heightened bank run risk).

As regards wholesale payments, issuing a CBDC would involve introducing an instrument similar to reserves, i.e. a direct claim on the central bank, which could only be held by the players currently authorised to participate in the large-value payment system.[1] The main difference would therefore relate to the technology used to issue and distribute the instrument. These considerations relate to the use of blockchain technology by the private sector, with the main objective of facilitating the interoperability of these solutions with the central bank's currency, which would also be distributed using blockchain technology.

At this stage, however, the research carried out by central banks on the possibilities of using DLTs for the infrastructures they operate (large-value payment systems and settlement and delivery platforms) is inconclusive (see 3.1.1. infra). At best, DLTs simply meet the functional requirements defined for testing purposes. They have not shown any advantages over existing infrastructures, which are critical to the economy, highly sophisticated and technologically adapted to the complexity of financial market infrastructures' activity.

1 These are credit institutions and investment firms in the case of TARGET2.

3.1.1. The Eurosystem's initiatives to promote innovation and meet market expectations

With the aim of improving the efficiency and reducing the cost of its market infrastructures while responding to new user needs, the Eurosystem seeks to take advantage of technological innovations while remaining vigilant about the associated risks, such as cyber risk.

To that end, as part of the Vision 2020 programme (see Chapter 6, Section 6), the Eurosystem has developed and launched (in November 2018) the TARGET Instant Payment Settlement Service (TIPS) for central bank money settlements. An 'instant payment' is one that can be made 24 hours a day, seven days a week, with immediate transfer of value, credit to the beneficiary's account and availability of funds. Although similar payment systems already exist in countries such as the United Kingdom ("Faster Payments"), Singapore ("Fast and Secure Transfers – FAST"), Denmark ("Express Transfers") and Australia ("New Payment Platform – NPP"), the introduction of instant payments in the euro area is a new innovation in a market of 340 million people in 19 countries. TIPS is a tangible illustration of how the Eurosystem both adapts to market developments and innovations by enabling private players to take advantage thereof, while relying on Eurosystem infrastructures capable of implementing them, and works to promote the harmonisation and interoperability of Europe's payment markets.

Lastly, the Eurosystem has also begun work to assess the potential of blockchain technology applied to financial market infrastructures. The ECB is similarly continuing work to test potential blockchain uses in market infrastructures, specifically in conjunction with the central bank of Japan as part of the Stella project.[9] During the first phase of their cooperation, the ECB and the Bank of Japan sought to analyse whether their payment systems' functionalities could operate efficiently and securely in a blockchain environment. The second phase, which ended in March 2018, focused more on implementing a delivery versus payment (DvP) system in a blockchain environment. The banks concluded that the technology was too immature to be used satisfactorily either for large-value payment systems or to manage DvP issues (particularly operational risk management).

3.1.2. The Banque de France's initiatives

The LAB is an experimental laboratory set up by the Banque de France in 2017 as a space for exchange and work with innovative players based on calls for contributions. Its objective is to review the opportunities and risks of new technologies, carry out strategic monitoring of their development and assess their potential for the Banque de France's various business lines and working methods. A concrete example of the Banque de France's action in the area of data management is the "Data Lake" initiative – a set of projects aimed at using new technologies such as artificial intelligence and big data management in the Bank's information system and thereby strengthening its ability to fulfil its financial and monetary stability role.

Meanwhile the Banque de France launched a software program using blockchain technology to manage the identifiers assigned to direct debit issuers such as EDF and the French Treasury, called the SEPA creditor identifier (ICS). This identifier is essential for issuing SEPA-format direct debits, as once it has been assigned to a direct debit issuer, the debtor's banker checks that the identifier indicated in the direct debit received is identical to that shown on the mandate signed by the client.

The software, developed by the Bank under the MADRE project, was built based on the suggestions of commercial banks, given that they are the ones who request identifiers on behalf of their direct debit issuing clients.

9 *http://www.ecb.europa.eu/pub/pdf/other/ecb.stella_project_report_september_2017.pdf*
http://www.ecb.europa.eu/pub/pdf/other/stella_project_report_march_2018.pdf

Blockchain technology was chosen for several reasons:

- it gave the banks a role in implementing the service (whereas until then it had been the Banque de France that assigned the identifiers). Once it became each account-holding institution's responsibility to decide whether or not its clients could issue direct debits – and therefore have an ICS – the logical next step was to implement decentralised ICS request input management by all the banks in the market;

- it made it possible to immediately provide the new identifier, whereas previously it took several days between the request and the allocation;

- the file containing these identifiers could be used to test this new technology in a real-life situation, whereas before, despite being the subject of numerous laboratory experiments in closed test environments, it was still rarely used for professional purposes.

The main French banks and the Banque de France worked together closely to develop this new software, and the new system went live on 15 December 2017. The partner banks joined the blockchain venture in two main phases, in March and June 2018. For its part, the Banque de France continues to process identifier requests from banks that do not participate in this project, thereby ensuring the coexistence of two systems – one traditional and the other based on blockchain technology.

3.2. Central banks' oversight role, at the intersection of innovation, stability and regulation

While the current wave of technological innovations and the emergence of new players are creating new opportunities for the financial industry in general and for market infrastructures and payment systems in particular, they also pose specific risks and challenges, particularly in operational, legal and financial terms, which it is the financial system's regulators, overseers and supervisors' job to manage.

3.2.1. Ensuring the efficiency and security of financial market infrastructures

The regulations applicable to market infrastructures reason in terms of functions performed and services provided to the market. They make no prescriptions as to the technology used to perform these functions and services. Whether the technology used is blockchain or another, all that matters from a regulatory point of view, insofar as a service such as settlement and delivery meets the definition of the central securities depositories regulation (CSDR - see Chapter 12), for example, is that it complies with the relevant rules.

Similarly, the status of the player providing the service is not taken into account. Whether it is a new entrant or an established player, if it performs functions that fall within the scope of market infrastructures, it must comply with the relevant regulations: CSDR, European market infrastructure regulation (EMIR) or the systemically important payment systems (SIPS) regulation.

Regulatory neutrality as regards technology and participants aside, the most advanced initiatives for applying blockchain technology to post-market activities[10] raise two, more specific, implementation challenges: compliance with the delivery-versus-payment (DvP) principle (see Chapters 5 and 18) and use of central bank money as a settlement asset (see Chapter 5).

As regards DvP, initiatives based on blockchain technology and offering a solution for transferring an asset in exchange for a payment should be able, if they were developing effectively, to ensure the DvP of the transactions they process. This mechanism is important because it eliminates settlement risk (or principal risk), i.e. that of not being paid despite having

10 Improvement of the commercial paper processing chain, post-market solution for listed and unlisted SME securities, solution for monitoring fund liabilities, etc.

delivered the asset, or not having the asset delivered despite having made the payment. To meet this requirement, blockchain technology-based solutions would have to be able either to have the assets and the settlement asset (money) on the same platform (integrated system) or to ensure very close interconnection between the platforms used to process the assets on the one hand and the settlement asset on the other (interfaced system).

As regards the settlement asset, the Principles for Financial Market Infrastructures (PFMI) consider that the safest settlement asset is central bank money, and that this should be used wherever possible. This would require solutions based on blockchain technology to access central bank money, and thus to meet the central bank's access criteria.

These two elements are fundamental to ensure the security and efficiency of market infrastructures. For initiatives with a securities settlement and delivery dimension, responding to these imperatives may result in use of the T2S settlement and delivery platform (see Chapter 14), which can be used for DvP in central bank money. This requires the player offering this service to have CSD status, in accordance with the provisions of the CSDR. This would both ensure the security and efficiency of post-market activities and offer the benefit of the improvements that blockchain technology potentially provides.

3.2.2. Innovation creates new threats for the financial system

Innovation can pose fraud and security-related problems due to its digital nature and the cyber environment in which it functions, combined with the rapidly increasing numbers of players involved in financial and payment processes, the greater circulation of personal data and the proliferation of potential "points of failure". These new 'cyber' risks are sparking considerable concern sector-wide, including for proven market infrastructure and payment technologies, particularly online card payments, which account for more than two-thirds of all card payment fraud in France. Moreover, the most recent technologies that have not yet been tested on a large scale, such as blockchain, are likely to create new security risks that warrant early and permanent monitoring.

Technological innovation could also threaten long-term financial stability owing to the process of increased automation. The development of high-frequency trading, for example – which, furthermore, is questionable in terms of its economic usefulness – could undermine financial markets' resilience in times of stress. New services such as smart contracts, which represent the computer coding of predefined situations,[11] can be integrated into a blockchain: this could create new channels for the transmission of shocks, or new forms of interdependence or procyclicality and, therefore, be a potential source of financial instability.

Unchecked technological innovation could also threaten market integration, particularly in Europe, where there have been considerable efforts over the last ten years to strengthen financial market harmonisation. Such efforts were evident in securities markets, for example, with the launch of T2S in 2015. At the same time, the current proliferation of new technologies, standards and protocols that are not fully interoperable, at least at this stage, poses a risk of market fragmentation. Moreover, this could result to some extent in social fragmentation if the new payment instruments are less available to the least well-off members of society.

3.2.3. Ensuring the security of payments and transactions

In this context, public authorities play a key role in making it possible to take full advantage of innovation while mitigating the threats it generates. Technological innovation is only beneficial to the economy as a whole if it is carried out in a secure environment.

11 Such as "Sell if the following price level is reached".

Technological innovation reinforces the need for cooperation and dialogue between all the parties concerned. In France, for example, in coordination with the French Financial Markets Authority (AMF), the ACPR launched the Fintech-Innovation Unit (Pôle FinTech Innovation) in June 2016 to address this need. The ongoing dialogue between regulators, supervisors and players (banks, insurance companies and fintechs) involved in innovative projects ensures that innovations are properly understood, necessary regulatory changes promptly identified and information disseminated effectively among the various stakeholders. The Banque de France and the ACPR have committed to a graduated and proportional approach to regulating and supervising fintechs. Such an approach differs from the 'sandbox' solution favoured for example by authorities in the UK, which has an associated threshold effect risk. As a reminder, the sandbox approach consists in regulators granting companies permission to experiment with new services relating to payments, money and securities transfers and financial investments within a simplified regulatory

Box 4 – ACPR's Fintech-Innovation Unit

In June 2016, the Banque de France created a fintech unit within the ACPR to support changes in the French economy. Working in close coordination with the AMF, this unit aims to be the ACPR's single entry point for fintechs, firstly to ensure they are promptly regulated at the outset and secondly to better understand their innovations in order to be able to monitor them.

The unit interfaces with the ACPR departments concerned and, where the nature of the project so requires, the Banque de France and the AMF. The Fintech-Innovation Unit also assesses the challenges that digital transformation and technological innovations pose to the banking and insurance sectors, and participates in international projects in this area.

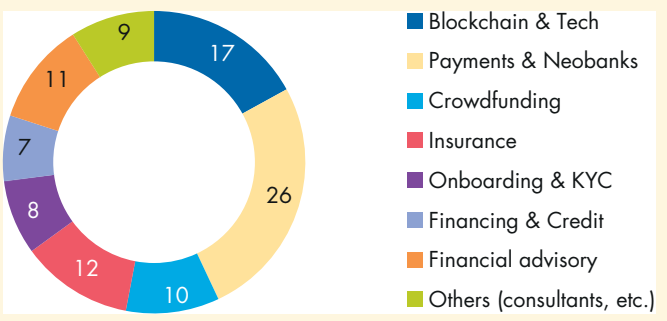
Lastly, together with the AMF's Fintech division, it coordinates the FinTech Forum, a body for monitoring, dialogue and proposals on fintech and innovation regulatory issues, which brings together fintech professionals, experts and public authorities (CNIL, the National Cybersecurity Agency of France (ANSSI) and TRACFIN).

The Forum has established four priority work areas:

- Proportionality in approval and control;
- Use of data;
- Client identification and knowledge (KYC); and
- Market attractiveness and competitiveness.

Breakdown of innovators attending the Fintech-Innovation Unit

(%)



Source: ACPR.

framework, for a predefined period and/or level of activity. While this approach has been introduced in a few other countries, such as Singapore, it raises issues of consumer and investor protection and of equal treatment between fintechs and established players who could offer the same services but do not have the light regulation advantage. It also poses a threshold effect problem in that once the trial period has elapsed or the predefined activity level has been reached, the fintech must then comply with all other applicable regulations, without checks having taken place at the sandbox stage that it will be able to do so.

These developments involve rethinking regulation in such a way as to strike the right balance between innovation and security, which must make it possible to simultaneously achieve several objectives: to take full advantage of the sources of efficiency and savings that innovations generate, to protect the consumer and deal with financial stability issues, and to ensure that innovation benefits all parties, in particular in the form of new services and lower costs. This balance can only be achieved by means of appropriate and proportional rules, based on the risk profile of the service provided and not on the supplier's nature or legal status.