Blockchains,
the Bank of France and the ACPR

Nathalie Beaudemoulin,
coordinator of Pôle FinTech Innovation (Autorité de Contrôle Prudentiel et de Résolution),
Didier Warzee,
engineer from the Corps des Mines, expert at Pôle FinTech Innovation (Autorité de Contrôle Prudentiel et de Résolution),
&
Thierry Bedoin,
chief digital officer (Banque de France)

[special issue of *Réalités Industrielles*, August 2017]

Abstract:
The ACPR (Autorité de Contrôle Prudentiel et de Résolution), which oversees the banking and the insurance industry, and the French central bank are coming to grips with the technological revolution under way in financial services. Blockchains are among the techniques that can modify, or even optimize, the processing and delivery of financial transactions. However this not-yet-mature technology must cope with four major dilemmas before being used for financial operations.

A blockchain or blockchains?

The word "blockchain" (or similar terms) is sometimes used inappropriately to refer to computerized arrangements that differ significantly both in their design and underlying principles.[1] Beyond the question of terminology, a regulatory authority endeavors, above all, to justify its position by examining the essential characteristics of propositions. For instance, the phrase "timestamp server" was initially used to refer to the Bitcoin protocol, until the word "blockchain" cropped up soon afterwards. Given the pioneering combination of the technological procedures that went into creating Bitcoin, "blockchain" is now regularly used for systems that present similarities with Bitcoin; but it is also often used for systems that differ significantly from Bitcoin. The initialism DLT (distributed ledger technology) is also sometimes used to mark a difference (mainly for reasons of image) with the cryptocurrency, bitcoins (BTC).

[1] This article has been translated from French by Noal Mellott (Omaha Beach, France). The translation into English has, with the editor's approval, completed a few bibliographical references.

Not considered to be legal tender, bitcoins are intrinsically and highly risky for their bearers due to volatility and the corroborated risks of fraudulent practices. They also hamper the fights against money laundering and the financing of terrorism, since the anonymity of bearers violates the fundamental principle in the financial world about identifying the parties to a contract. As a consequence, public authorities, both French and European, have justifiably taken up strong positions on bitcoins in order to inform the public and warn against the risks as best possible.[2]

Some promoters of technological procedures of a blockchain type have subsequently tried to protect themselves from being assimilated with bitcoins. Nonetheless, they are still advocating a fully decentralized method that they claim — owing to the hoped-for elimination of intermediaries and even of a central authority — will be a major vector for overhauling financial services or even society. This technology is thus placed at the service of a philosophy that we might qualify as libertarian: it promises the return (as primitive as digital) to direct financial transactions between individuals through a fully decentralized procedure for generating "trust".

Apart from these rather utopian claims, blockchain technology has sufficiently remarkable characteristics for financial agents (whether new or established) and financial authorities — including the Bank of France and the ACPR (Autorité de Contrôle Prudentiel et de Résolution, which oversees the banking and insurance industry in France) — to take a closer look.

What potential for open, decentralized blockchains in the financial sector?

Apart from bitcoins as a virtual money, what has aroused enthusiasm for blockchains is its proposed system of confidence. This is what has whetted the creativity of financial agents, in particular the many start-ups that see this technology as a way to compete with financial establishments.

Bitcoin's creator(s) designed the original blockchain as a decentralized system that, without a trusted third party, relies on cryptographic techniques to ensure all at once: the transparency, security and anonymity of direct peer-to-peer electronic transactions. Distributed over a considerable number of nodes in a network, the completely transparent ledger of these transactions is claimed to be indestructible. Its integrity is guaranteed by a procedure that entails, for each validation of a new block of transactions (secured via a proof-of-work consensus protocol), the integration of the hash value of the preceding chain of blocks.

A quality often vaunted by this technology's promoters is that the distributed database cannot be altered. This is intended to inspire confidence in the ledger, a confidence that serves as the grounds for their plans for ledgers (or registers) of information or transactions (via the use of tokens) in the real world.

Beyond these advantages however, significant limitations soon appeared, to name but two: the volume of transactions that can be processed and the time needed to do so. Other procedures have been worked out to make up for these shortcomings, whence the creation of open blockchains, such as: Ethereum, which provides for smart contracts, which will be automatically executed once an external piece of information (an "oracle") pulls the trigger; Hyperledger (designed for businesses); or Tangle/IOTA (specialized in connected devices).

[2] Position 2014-P-01 of 29 January 2014 of the French ACPR on bitcoin operations in France. For a detailed discussion of bitcoin operations, the risks for users and regulatory issues, see: *Focus*, 10, 5 December 2013 (on the website of the Bank of France); and the warning issued on 12 December 2013 by the European Banking Authority (www.eba.europa.eu).

By interacting "intelligently" with the real world, smart contracts allow for actions more sophisticated than a simple transaction using a cryptocurrency (even one improved with a few bytes of characters as in the case of bitcoins). For example, some insurance policies relying on smart contracts propose booking policies that automatically pay an indemnity depending on the arrival times of a flight at an airport.

However the foundational characteristics of open blockchains (their being both "public" and decentralized) still raise potentially crippling difficulties for deploying this technology on a large scale in the financial sector. These difficulties can be formulated as four dilemmas;

- DECENTRALIZATION VERSUS LIABILITY. Decentralization of the method for generating confidence in the system, despite its advantages (in particular, the security of a system shared by so many persons), does not allow for identifying the party legally liable for this security, someone accountable to both customers (for outages, reimbursements, the continuity of business, etc.) and regulatory authorities .

- FREEDOM VERSUS DEPENDENCE. An open blockchain seems to be a co-managed public good to which each and everyone contributes, in principle. In actual practice however, it turns out to be heavily dependent on a few programers and, too, on mining farms that, highly concentrated geographically and economically, are induced to form pools.[3] The power of these stakeholders over the operation of an open blockchain challenges the claim to being "democratic". This can lead to literal schisms in the community, to a "hard fork" in the blockchain. This power ultimately raises the question of governance, since the trusted-third-party card, which blockchains supposedly threw out, still figures in the deck — which has been reshuffled, this card now having been dealt out to programmers and miners, power-holders that are much less transparent and accountable, and often pursue divergent goals.

- TRANSPARENCY VERSUS CONFIDENTIALITY. An open blockchain is transparent and efficient given the traceability of operations. It allows users to know about all transactions or records, like an auditing method that claims to be unique and intangible. But this characteristic soon runs afoul of trade secrecy, since a participating establishment does not want to disclose (in particular to competitors) the transactions that it makes on a blockchain.

- ANONYMITY VERSUS IDENTIFICATION: The libertarian principle underlying blockchains implies using pseudonyms to avoid identifying the parties involved. This opacity is not acceptable in affairs of money laundering and terrorism.

Given these dilemmas, it is not yet time to use open blockchains for regulated activities, not as long as we cannot imagine a blockchain built from the ground up in response to specific problems, including regulatory oversight, in the financial sector.

[3] At least up to a certain point: these mining farms ought to remain below 50% of the network's computing power lest they jeopardize the proof-of-work protocol and thus undermine confidence in bitcoins — a confidence that makes the farms rich since they are remunerated… in bitcoins.

Plans to incorporate a central authority in DLT

Drawing on blockchain technology, financial agents have tried to create systems with themselves as the centralizing authority, the trusted third party. They would thus retain a privileged position in line with their current functions while resolving some of the aforementioned dilemmas.

The case the most out of true to open blockchains is fully private distributed ledgers. In practice, such a ledger is usually a database of transactions that is reproduced at several physical sites and benefits from cryptographic procedures for guaranteeing its integrity but without recourse to mining. Mining activities are pointless since there is *a priori* a strong confidence between nodes in the network, which are completely under a single party's control. Private blockchains can be used to optimize internal procedures in groups, for example, to immediately register and share information and transactions between companies belonging to the same holding or between different units belonging to the same company. In this case, oversight means supervising the eventual operational risks (cybersecurity, the cloud, etc.) that this sort of technique has for financial establishments — just as for any other new information-management technology, even one not solely and specifically related to blockchains.

Given the limitations of private blockchains (in particular for business-to-customer activities; B2C), systems have been developed that, with an architecture close to open blockchains, confer on a central third party the governance of the blockchain and the management of codes and of access to the system. They are often called "permissioned open blockchains". However this phrase covers quite different systems, ranging from one that grants permissions to a very few agents in the peer-to-peer network (via a specific form of governance and code management — a system usually called a "consortium blockchain" when it involves companies) to a system of access that, in theory open, uses a consensus protocol that (copied after an open blockchain's) incorporates a party who centralizes permissions for access and users' data.

Depending on the uses, in particular, for generating the "confidence that exists *a priori*" among peers on the network, other consensus protocols have often been adopted that differ from Bitcoin's proof-of-work system. This substantially improves efficiency compared with Bitcoin, where the energy costs of "mining" are very high.

There are plans for permissioned systems that would bring the ledger's properties of resilience (integrity and availability) closer to those of an open blockchain. These properties have to do with both the network's size (the bigger the network, the more copies of the ledger) and the energy spent to validate blocks in a proof-of-work consensus (the harder the proof, the more energy attackers hav e to spend to breach the system). One solution imagined — the sidechain — foresees having an open permissioned blockchain fork (we might say) into an open permissionless blockchain for reasons of security.

Most of the uses now imagined — whether by French regulatory authorities (for the registration of transactions involving unlisted securities)[4] or in the plans made for asset management, payments, transfers or insurance — are tending toward permissioned open blockchains.

[4] Article 120 de Act n° 2016-1691 of 9 December 2016 on transparency, the fight against corruption and the modernization of the economy authorizes the government to reform, in the coming year, the corpus of law on financial securities. Within the scope of this reform are the clearing, settlement and transmission (via a system of shared electronic records) of transactions involving certain financial securities, when they are not subject to operations by a central custodian.

Given that these various solutions refer to significantly different forms of DLT, we must examine case by case each proposition in order to determine how it measures up to regulatory requirements. The systems proposed have to comply with fundamental requirements about the security of transactions, consumer protection, and the fights against money laundering and the financing of terrorism. For instance, customers must always be identified, reliably, with documentation; and these identification measures must be reinforced in the absence of face-to-face contacts. Payments always have to meet security requirements (for instance, a reinforced authentication procedure). The planned-for systems will also have to comply with specific regulatory requirements (for instance, about the information to be provided prior to the signing of a contract).

Furthermore, establishments have to reckon with the applicable crosssectoral regulations, such as EU requirements relating to electronic signatures [5] or stemming from the recent EU regulation on protecting personal data,[6] among them: the customer's consent prior to data processing, the "right to be forgotten" (an apparently hard-to-meet requirement since blockchains are immutable) and EU requirements about electronic signatures.

ACPR's FinTech Innovation and the Bank of France

To fall in step with the digital revolution (in which blockchains are on the march) in financial services and to be ready to oversee an increasingly electronic financial sector, the ACPR set up in June 2016 FinTech Innovation, a laboratory devoted to financial technology and innovation. FinTech works closely with the Financial Market Authority, along with which the ACPR organizes a Forum FinTech, which brings together banks, insurance companies and other partners as well as public authorities. The topics discussed have to do with the regulation of innovation and the regulatory problems related to blockchain technology (for instance, the legal worth of operations recorded on a blockchain or in smart contracts). As an independent authority affiliated with the Bank of France, the ACPR maintains an ongoing dialog about blockchain technology with experts from the Bank.

Having soon realized how important this new technology is for the performance of certain duties (payment systems and market infrastructures, monetary policy, banking services), the Bank of France decided to run tests in order to form an opinion about its potential. The central bank's chief digital officer is in charge of several experiments using this technology. The Madre Project, conducted with investment banks, has the aim of maintaining a decentralized register of ICS identifications, which are used for direct debits in the Single Euro Payments Area (SEPA).[7] French banks currently exchange ICS information through the Bank of France, which centralizes requests, generates identifications and communicates them to the parties concerned. Thanks to DLT, the register is kept through smart contracts on a blockchain, which the banks can consult directly. The Bank of France thus manages to be an ICS service-provider since requests are automatically processed in accordance with the rules preset on the blockchain. For this system's governance, the only role still played by the Bank of France is to accredit participating banks (and thus reinforcing its position as a trusted third party).

[5] Regulation n° 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market. Full text available at: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:JOL_2014_257_R_0002&from=EN.

[6] The GDPR (General Data Protection Regulation): 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. Available via: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1478961410763&uri=CELEX:32016R0679.

[7] The ICS replaced the TIP on 1 August 2014.

This experimentation has confirmed that a blockchain is capable of handling real-life problems related to keeping a ledger. Expanding the experiment into an interbank multiservice blockchain or into uses in critical financial operations is yet to be done however. It depends on the advances to be made in: the capacity of blockchains for mass processing (scalability), the confidentiality of transactions, security and, above all, the establishment of a long-term governance.

Conclusion

Although some of DLT's characteristics are promising, applying blockchains to activities that involve processing a huge flow of financial data means that significant, technical and regulatory, issues must be addressed beforehand.