Why standardize blockchains?

Olivier Peyrat,
managing director of Association Française de Normalisation (AFNOR);
& **Jean-François Legendre**,
in charge of development at AFNOR

In J.P. Dardayrol, editor of the special issue *Blockchains and smart contracts: The technology of trust?* of *Réalités industrielles*, 2017

Abstract:
Blockchain technology has a considerable growth potential given the many uses that have been imagined, some of them now being rolled out. It will be potentially disruptive, and probably become strategic in several industries. However blockchain technology must first mature, whence the need for standards to offer the necessary reassurance about the processes being used.

Given the digital transformation of society, the need has been expressed for traceability in the records of various transactions (not just financial ones).[1] This traceability is necessary for setting up and using trust services. It, in a way, transposes the principles applied in several business services prior to the digital era.

Distributed ledger technology (DLT) was invented in 2008, when a programmer (or group of programmers?) called Satoshi Nakamoto published under a free MIT license the blockchain protocol for software written in C++.[2] A year later, Bitcoin, the first cryptocurrency platform using this protocol, was launched. DLT has aroused lively interest in recent months, partly because the digital transition in society and corporations is accelerating. Blockchains are now a topic at the "peak of inflated expectations" in Gartner's "hype cycle" of the maturity of a technology![3] As a consequence, the list of potential uses is becoming longer day after day: the financial industry, including insurance companies, pharmaceuticals, energy, agribusiness, not to mention for managing intellectual property rights, land registries, inheritances, etc.

A blockchain promises to be a sure, robust, open, public system for authenticating records without resorting to a centralized, trusted third party. For this, reason, we have dubbed it, herein, "distributed notarial system".

[1] This article has been translated from French by Noal Mellott (Omaha Beach, France).
[2] NAKAMOTO S., "Bitcoin: A peer-to-peer electronic cash system", 9p., October 2008. Available at https://bitcoin.org/bitcoin.pdf

[3] www.gartner.com/technology/research/methodologies/hype-cycle.jsp

What is a distributed notarial system?

It is a decentralized system for an exhaustive chronological record of all “transactions” made since its creation. It is referred to as a ledger, by analogy with the longstanding business practice of keeping track of receipts and expenses by entering them in a daybook. In such a system, transactions are recorded in the ledger in consecutive blocks, each block containing a set of validated transactions — the necessary condition for the block to be added to the chain.

The fundamental characteristic of this decentralized record-keeping system is that the ledger is shared (and the job of updating it is distributed) over a network. Each node in the network has its own, permanently updated copy of the ledger. Various procedures, not to be explained herein, ensure this system’s security. The following characteristics have an impact on the specifications and standards to be used for blockchain technology:

- Anonymity between the sender and recipient of a transaction is ensured via digital multisignature techniques.
- The knowledge is minimized that each node in the network needs to calculate the validity of a transaction.
- The bookkeeping procedures shared by the nodes in the network rely on a “consensus” system whereby a majority of the nodes is required for validating a transaction;
- The ledger is fully transparent, as are the transactions.
- In the case of Bitcoin, a specific arrangement provides for remunerating the nodes in the network that verify transactions.

The term “transaction” is to be understood in a broad sense.

The first blockchain application was the virtual money bitcoins (BTC). However it was soon imagined that blockchains could serve other purposes. In 2013, Vitalik Buterin, a student, had the idea of a blockchain protocol fully incorporating a programming language such that instructions for any software could be written in the chain. After one of the biggest crowdfunding operations in the history of information and communications technology (ICT), the platform Ethereum, based on this idea, started operating in 2015.

This conception of “smart contracts” for placing executable software instructions in the blockchain set in motion a dynamic system for entering all sorts of “intelligent data” to be made secure in the ledger and tracing them — data about, for example diplomas to be validated under certain conditions, elections, lots for a land registry or issues of financial securities. Furthermore, the blocks in the chain can contain instructions to be automatically executed once the preset conditions are fulfilled (*e.g.*, trigger the conveyance of an inheritance once a person dies).

This system allows each party to potentially know everything that takes place in this digital world, to make a record of the occurrence of given events and to trigger actions associated with these events — all this very naturally, without disclosing confidential details about the transaction or the parties concerned.

The issues to be addressed and voluntary standards

Standards are documents for voluntary application drawn up by a recognized standardization organization that respects principles having to do with the plurality of the representation of stakeholders, and with openness and transparency in matters related to the management of intellectual property rights.

A blockchain protocol is a set of techniques released under a widely documented open-source license.[4] The security functions that are used are well known: hashing, electronic signatures, etc. None of this seems to require any particular action in terms of international standards! But this opinion will have to move if this technology is to enter anytime soon the phase of maturity, as it should.

A first risk comes from the proliferating uses of the blockchain protocol. If we only take cryptocurrencies into account, this network protocol now governs hundreds of platforms at various stages of development. The best known is, of course, the historical platform Bitcoin. This proliferation is a cause of concern to users. We can no longer be content with the current *de facto* standardization via the application programming interfaces (API) specific to each platform (Bitcoin, Ethereum, Nxt, etc.).

Given this proliferation of potential uses, questions arise about this technology's capacity (its scalability and the latency time for incrementing blocks in the chain). At stake are the methods for evaluating a blockchain's quality and reliability.

Additional questions concern the environment. The consensus system based of cryptography and protocols provides the basis for "decentralized confidence", the underpinnings of this technology. However it is very demanding in terms of computations, storage and, as a result, energy consumption.

Blockchains that are not limited to being cryptocurrencies might serve various uses, public, private or mixed. The stakes are not necessarily the same in each case. In the one case, the anonymity of the senders of transactions is requisite for security reasons. In another case, it would be worthwhile to identify claimants. As a result, the conditions for guaranteeing confidentiality are not the same. This also holds for the protection of personal data, the evaluation of confidence or the network's method of enrolling participants.

In June 2016, an attack that breached the code of a smart contract on Ethereum enabled a dishonest user to try to steal three million ethers (this platform's cryptocurrency, approximately $36 million). This changed the perception that some people might have had of this technology as being easy or convenient. DLT is not easy to understand, not even by experts with advanced knowledge in ICT.

This event was noteworthy because it clearly demonstrated that security procedures have to undergo an evaluation if this technology is to meet up to the criteria for being mature. Above all, it signals the end of the doxa that technology can stand on its own without any need of governance. Following this event, an intense debate took place in the Ethereum network about whether or not a blockchain could be deliberately forked in order to repair the breach and avoid making a fraudulent payment. If so, who has the right to act? The question of managing eventual conflicts of interest thus cropped up.

The European Commission, aware of the interest in, and issues related to, DLT has set up a work group on "Fintechs, blockchains and standardization". The Commission wants to rely on European organizations of standardization to evaluate the needs specific to Europe and to launch, if need be, a program.

[4] See the BIPS: https://github.com/bitcoin/bips

In this context, discussions at AFNOR (Association Française de Normalisation), where the French blockchain community (including start-ups) is represented, brought to limit the following issues related to standardization:

- the need to harmonize terminology and have a common vocabulary.
- the linkage to digital identifications for managing confidentiality (of persons and of contents) with a use case involving technical arrangements for data management in line with the requirements of the new EU regulation (GDPR: General Data Protection Regulation 2016/679) for protecting personal data.[5]
- the need for governance to facilitate a controlled rollout of blockchain technology;
- the need to organize the distribution of the work on standardization for, on the one hand, drawing up a generic list of standardized specifications applicable to any sector and, on the other hand, examining applications to specific sectors (including the financial sector, which has started devoting thought to the standardization of FinTech applications);
- the need for common specifications with regard to interoperability, portability and security.

An opportunity: The new ISO technical committee

At the request of an Australian member, the International Organization for Standardization (ISO) decided in September 2016 to set up a new technical committee (ISO/TC 307) with the assignment to draft standards for all sectors with respect to the application of "*blockchain and distributed ledger technologies*".

As the meetings held at AFNOR since the summer of 2016 have shown, French stakeholders, including start-ups, consider the ISO's initiative as an opportunity, since standardization could help address the issue of confidence and thus spur the growth of blockchains as part of the digital transition. Of course, this technology cannot, by itself, address all the issues raised by this transition.

From the discussions during the first meeting of ISO/TC 307 (held in Australia in early April 2017), we can see that international stakeholders have the same general view on this topic. A clear-cut consensus emerged, since the consolidation of confidence in new blockchain applications requires work on the following subjects: terminology; the standardization of the architecture (distinguishing the network from the service); the classification of use cases; the security and confidentiality of personal data; identification management; and smart contracts. Through this process, economic agents are trying to see to the security of their investments but without hampering the innovations brought by this technology.

In conclusion, blockchain technology was, at its origins, seen as being disruptive, and was inspired by libertarian ideas. To become mature and gain the confidence of all stakeholders however, blockchains have to fall back on a voluntary standardization process. In contrast with the offer of consortiums, which have appropriated blockchain technology to draft an overabundance of specifications, the ISO, like the International Electrotechnical Commission (IEC), has many assets for building confidence. The voluntary standards drafted by these organizations have an international scope and are durable. They can be extended, since they are maintained in the long run through a controlled process so as to be sufficiently generic. Provided that stakeholders actively contribute to this process, the ISO or IEC, by adopting a position complementary to open-source initiatives, are capable of proposing — internationally — to all stakeholders, private or public, responses to the issues that blockchains must address with regard to organization, portability, interoperability and security.

[5] The workshop CEN ISAEN has been set up at the initiative of the French association AETERNAM within a Franco-German partnership on standardization in the digital economy.