Blockchains:
The concept, techniques, interested parties and uses

Côme Berbain, assistant manager of expertise, Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

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

Abstract:
Blockchains are a fad. This hard-to-ignore word is frequently used with varying acceptations! To make sense of this new phenomenon, we must define it, identify its structural characteristics and inquire into the pertinence of its properties and promises. Does the word "blockchain" relevantly apply to the many experiments being conducted in various branches of the economy? What motivates various parties to take interest in this phenomenon? Far from being merely technical, the fundamental issues related to blockchain technology have to do with organizing, governing and finding solutions for trustworthy transactions, for securing confidence in human interactions. In this sense, this new technology will play a part in the digital transition in several fields, especially in the legal professions.

A single concept but several forms of technology

Trust between the parties to a transaction is usually grounded on a centralized system. The parties, unable to trust each other, prefer placing their confidence in an entity recognized by both of them, such as the state, a bank or notary.[1] This trusted third party keeps a ledger (or register) to vouch for the regularity of transactions. Depending on the type of transactions, access to the ledger may be open to anyone or restricted to certain agents. To avoid risks of fraud, the trusted third party always holds a monopoly over updating the ledger.

The concept of a blockchain proposes extending this centralized model so as to allow for joint management of a "distributed ledger", thus obviating the need for a trusted central authority. This concept has two characteristics:

- The ledger is distributed as a "chain" of the data blocks used to record transactions. These blocks are chained via cryptographic procedures for regulating access to the ledger, which is usually decentralized.
- Any user may add information to the ledger. What is added is assembled in blocks; and a procedure definitively validates them as they are added to the chain. This procedure purposes to keep the ledger from being falsified. It is usually public, and performed in a decentralized manner.

Several cryptocurrencies (among them: Bitcoin, Ethereum and Ripple) have been designed on this paradigm and use existing techniques: distributed ledgers, electronic signatures, asymmetrical cryptography, proof-of-work, virtual machines, etc. What is innovative is the way that these techniques have been put together.

[1] This article has been translated from French by Noal Mellott (Omaha Beach, France).

In fact, there are four major building blocks in current forms of blockchain technology:

- THE LEDGER AND ITS CONTENTS. The ledger takes the form of a distributed storage of information. Various sorts of information can be recorded there. Most such ledgers are used to record transactions; but files and communications can also be stored there. Smart contracts (code stored on a blockchain that is executed automatically once the preset conditions are met) extend the idea of distributed storage to the capacity for distributed computing.
- ACCESS TO THE LEDGER. The principal parameters are: openness (public vs. private chains, chains in a consortium); the parties authorized (natural persons, or legal entities); and their identification (real or pseudonymous) to be displayed. These parties have two functions, as users or validators.
- VALIDATION OF THE LEDGER BY CONSENSUS. The procedures chosen for validation determine whether all or only some parties are allowed to take part in forming this consensus or to express disagreement. What all parties do agree on is the state of the ledger. There are various, distinct methods of distributed validation: proof-of-work, proof-of- stake, shared consensus, etc.
- REGULATION OF THE PARTIES INVOLVED. To motivate users to contribute to the "community" (in particular by providing computer processing time) and to keep the system in equilibrium, a regulatory procedure is needed. It usually relies on a "currency" linked to the blockchain.

Each form of blockchain technology is characterized by the decisions made about how to cope with these four problems. Whether or not a blockchain will meet up to its promises depends on these decisions, and can be evaluated only for that given form of the technology. Table 1 presents the decisions made by three blockchains.

Three applications of blockchain technology			
	Bitcoin	**Ethereum**	**Ripple**
Contents	Monetary transactions	Transactions, smart contracts	Financial transactions
Access	Open (public)	Open (public)	Restricted to financial circles (private). Public notice of transactions but not of payments.
	Pseudonym	Pseudonym	Real identity
Validation	Proof-of-work	Proof-of-work moving toward proof-of-stake	Vote among validators (supermajority of 80%) on correcting transactions
Regulation	Production of new bitcoins (BTC) Adjustment of the difficulty of the proof-of-work system	The currency: ethers (ETH) Consumption of "gas" as a function of the quantity of distributed computing in smart contracts	The currency: ripples (XRP)

Structural properties and limitations

Blockchain technology promises mainly to decentralize trust services and, consequently, eliminate the trusted third party who keeps the ledger. This promise can be kept only if the ledger is not falsified and its data are neither deleted nor modified. A blockchain keeps the information added onto it in the chronological order of validation. Inherent in this structural impossibility of falsifying data is a limitation with regard to litigation: even illegal or dubious transactions cannot be deleted; their effects can only be corrected by new transactions.

The validation procedure, intended to guarantee that the ledger has not been falsified, is the cornerstone of any blockchain. Its function is to produce a consensus among all validators about each new block — in spite of the possible presence of uncooperative or malevolent users. This brings to mind the well-known mathematical problem of the Byzantine generals, who, forced to communicate via messages written using an algorithm, have to win the battle even if there are traitors among them. By the way, there is no provable link between this theoretical problem and the solutions put to use by blockchains.

Since the ledger is distributed, its information is transparent and can be audited. In the case of open (public) blockchains, this property significantly augments the confidence, or trust, in the ledger; but it entails restricting the information (*e.g.*, personal data) that may be manipulated. Methods exist for implementing this restriction. The zero-knowledge protocol, for example, allows for manipulating data without revealing their contents. In the case of private blockchains, only the parties with permission benefit from the system's transparency.

Not being falsifiable and being transparent are characteristics that imply an additional property about the resilience of a blockchain. In case of a major incident or attack, any party to the blockchain is capable of generating the blockchain anew from a state of the system on which a consensus was reached. However this depends on a significant number of users and validators accepting to switch to the new system. In the few cases where this situation has arisen, these parties tend to divide — on the one side, those who stay with the chain and, on the other side, those who adopt the new one — as a function of their self-interests.

Beyond these inherent properties, a key question is how the performance of this new technology compares with conventional systems. This performance varies widely depending on the sort of blockchain. It is improving for financial transactions: the time needed to validate a block is from ten to twenty minutes for Bitcoin, a few minutes for Ethereum, and a few seconds for newer cryptocurrencies. However blockchains with proof-of-work systems require a high number of computations, which makes them less energy-efficient.

Abundant services for specific uses

Protocols or platforms based on blockchain technology are being used to design services in demand for specific uses. Some services, though not financial, rely on Bitcoin, which was initially designed exclusively for monetary transactions. There are now thousands of services based on techniques built up from blockchain technology; and variants are regularly being invented.

The fields of application and uses are quite variable. Beyond the financial sector, busy using bitcoins (an estimated $210 billion invested in 2016), services exist in: energy, commerce (diamonds, artworks), transportation and logistics, digital property rights (music, films, video games), health and public administration (land registries). The main use of this technology is to monitor and trace transactions and curb fraud.

As these services have grown, four major issues have cropped up. They can be used to evaluate the match between a specific use, the specific form of this technology and the service rendered:

- GOVERNANCE. The rules organizing users and validators and the blockchain's regulatory procedures are decisive for the durability of the service.
- TECHNICAL EFFICIENCY. Comparisons with conventional techniques, which use distributed data bases accessible via application program interfaces (APIs), seldom turn out in favor of these new services. This gap, unfavorable to blockchains, cannot be too wide lest this new technology fail.
- INTEGRATING EXISTING SERVICES AND MANAGING DISPUTES. Currently, many services have overlooked this eventual but inevitable issue.
- DIGITIZING PROCEDURES INVOLVING PHYSICAL ASSETS OR COLLATERAL. In some services, the counterpart to the digital data in the blockchain has to be "physical" (a diamond, a painting or the electric current generated by a windmill). This forces us to look beyond the blockchain as such. However this technology has come up with several efficient solutions offering varying degrees of warranty. One involves using "oracles" (*i.e.*, a specialized trusted third party chosen by users) for smart contracts.

Players with varying motives

The enthusiasm aroused by blockchain technology and its potential applications soon led to the growth of a lush environment. Blockchain technology is definitely on the "peak of inflated expectations" in Gartner's "hype cycle".[2] These proliferating initiatives betray a fad. They are also evidence of this technology's immaturity and of users' efforts to learn through trial and error.

Several sorts of economic agents are involved in blockchains: start-ups (including in consultancy); the conventional trusted third parties who are conducting their own experiments (such as notaries who are trying to adapt to the changing times for their profession); big industrial groups, especially in finance (banks, insurance companies, etc.), who are experimenting through partnership with start-ups or with R&D establishments; and public authorities (like the Caisse des Dépôts et Consignations and France Stratégie in France or the Government Office for Science in the United Kingdom), who are trying to keep abreast.

These agents have different motivations. Their top-ranking motive is to learn. Many of these experiments are mainly intended to test technical and organizational models, and obtain feedback so as to better understand concepts and gain a degree of control.

Blockchains, since they are decentralized, generate a network effect. The result is a race between several players who want to offer the landmark service platform in this business and obtain a dominant position (a winner-takes-all strategy). Also running in this race are the conventional trusted third parties, their client firms (who now want to eliminate these middlemen), and newcomers (who want to shake up the whole business). A few startups are devoting as much effort to being bought out by a big group as to making their business prosper.

[2] http://www.gartner.com/technology/research/methodologies/hype-cycle.jsp

A step forward in the digital transition

Blockchain technology has emerged out of a new, decentralized approach based on computer science. Its full impact will be felt only in the long run.[3] By opening an approach that leads beyond the mere "dematerialization" of transactions and contracts, blockchain technology bears the possibility of changing our conception of how to manage trust, or confidence, in human relations and organizations. By boosting the digital transition in whole sectors of the economy, this technology raises questions that are not just technical.

Smart contracts, in particular, are going to deeply change legal professions. Bitcoin, the first blockchain application, is centered on payments, the simplest form of a contract. An attorney's major task is to translate the intentions of the parties to a transaction into legal clauses and contracts. Besides eliminating intermediaries, smart contracts are pushing legal professionals into the digital transition. They translate into computer code the intentions of the interested parties and see to the automatic execution of engagements. They illustrate the principle that "code is law". This is reason enough for the legal professions to take an interest in them. Even though the drafting of smart contracts is a complicated, poorly controlled process, and even if the question of litigation is not yet settled, new jobs will, we expect, emerge for the drafting of smart contracts. Standardized forms for smart contracts will be exchanged.

Once again, blockchains have consequences that extend beyond the technology itself. They have legal and organizational effects. Experiments are more than ever needed to understand these new technological tools, imagine applications, and envision the new forms of organization associated with them.

[3] It is hard to determine whether it is worthwhile making a comparison with TCP/IP (transmission control protocol/Internet protocol) in the 1980s.