

**Research Report**

**The Blockchain**

**or distributed trust**

Author: Bertocco Thomas-Killian - #13758322

Lecturer: Sithira Vadivel

CP5603 Advanced E-Security | SP52 | 2019

27 September 2019

# Abstract

Major innovations are the result of the intersection of new technological possibilities and a favorable sociological context that transforms these technologies into uses. Thus, the blockchain was born, on the one hand, from the encounter of asymmetric cryptography and distributed systems, and, on the other hand, from an appropriate sociological ground. The latter is the result of the crisis of citizens' trust in institutions, leading them to seek new forms of governance. The advent of the Internet has demonstrated the effectiveness of a global communication system without the need for telecommunications operators. Now, it is possible to connect in seconds to any Wi-Fi network in the world. The blockchain allows the same revolution but applied to transactions. It allows people to carry out transactions, particularly financial transactions, between themselves that are guaranteed without the interaction of a trusted third party. Exchanges are faster and less expensive. As a result, the blockchain completely challenges the role of institutions, banks, notarial offices, and radically changes the administration. The first experiments, which go far beyond Bitcoin, such as autonomous decentralized organizations, show the radically disruptive nature of the blockchain.

After the introduction of some elementary techniques useful for understanding, this document presents the technical functioning of the Blockchain. Then, it identifies the key properties that give it a certain degree of confidence. Finally, it provides an overview of the risks and limitations associated with the Blockchain.

Table of Contents

[Abstract 2](#_Toc19973733)

[Introduction 4](#_Toc19973734)

[Blockchain security 5](#_Toc19973735)

[Blockchain Operation 6](#_Toc19973736)

[The enrolment phase in the Blockchain 7](#_Toc19973737)

[The transaction phase 7](#_Toc19973738)

[What is a transaction? 8](#_Toc19973739)

[What is a block? 9](#_Toc19973740)

[The mining operation to obtain PoW (Proof of Work) proof 10](#_Toc19973741)

[The simple validation operation by PoS (Proof of Stake) 11](#_Toc19973742)

[Proof of Formulation (PoF) – the future consensus model 11](#_Toc19973743)

[The different types of blockchains 13](#_Toc19973744)

[Public blockchains 13](#_Toc19973745)

[Consortium blockchains 14](#_Toc19973746)

[Private blockchains 15](#_Toc19973747)

[What is the basis of trust? 17](#_Toc19973748)

[Risks and limitations 18](#_Toc19973749)

[The future of the blockchain 20](#_Toc19973750)

[Cryptocurrency 20](#_Toc19973751)

[Data Security 20](#_Toc19973752)

[Protecting the IoT 20](#_Toc19973753)

[Bypassing censorship 21](#_Toc19973754)

[A promising future 21](#_Toc19973755)

[Conclusion 22](#_Toc19973756)

[References 23](#_Toc19973757)

# Introduction

Blockchain is a technology invented in the late 2000s. It was the Bitcoin project for exchanging cryptocurrency (Bitcoins) on the Internet that initiated it, made it popular and demonstrated its high reliability. In 2014, the non-profit foundation Ethereum, led by Vitalik Buterin, is launching a project to extend the Blockchain principle to a programmable Blockchain, thus opening the field to all types of transactions (smart contracts) and a plethora of new services. (Rosic, 2016) With the first version of Ethereum's source code made available to the general public in 2015, many manufacturers and independent developers then launched into the race to propose innovations. The Blockchain is often compared to a large book of publicly accessible and auditable accounts. Its members may add entries to it, but this operation requires validation by several members of the group, or even the majority of the group. Members act under pseudonymity, which makes it possible to trace each other's writings, without knowing their real identity.

It should be remembered that the blockchain is not a "technological" innovation; it uses technologies that are known and controlled (data storage, cryptography, distributed systems (Peer to Peer), etc.). It is the skillful assembly of these technologies that will make it possible to give birth to this concept by defining, through these technologies, an extremely innovative protocol for the exchange of information. The blockchain is, therefore, a protocol whose use can be disruptive in many sectors and which could affect all companies. Its industrial potential is important in terms of disintermediation of all actors playing a role of trusted third party, but also in terms of cost reduction, as well as in terms of security (a blockchain is considered unalterable), and speed of service (the validation time is generally low, especially in consortium cases).

# Blockchain security

The security of the Blockchain is based on standard cryptographic mechanisms, mainly public key cryptography and hash functions, a simplified description of which is provided below.

By definition, public-key cryptography assumes that each entity in the system has two keys, a public key known to all and a private key kept secret by its proprietary entity. It is this private key that allows an entity to sign a transaction request and therefore to prove that it is the originator. The public key allows another entity in the system to verify the authenticity of the signature. The level of security of a cryptosystem is measured by the difficulty of cracking its private keys. In a cryptosystem, the size of the parameters directly influences the level of security obtained, with the rule that the larger their size, the more difficult it is to crack the private key. With cheaper and cheaper computer equipment and more and more computing power and memory, it is necessary to regularly increase the size of the chosen parameters to maintain the level of difficulty. It should be noted that today, a security level 112 is considered sufficient (Naziridis, 2018), which corresponds to an attacker who is given the ability to perform 2^112 operations to carry out an attack.

In the Bitcoin project, the ECC (Elliptic Curve Cryptography) system crypto was chosen, with the ECDSA (Elliptic Curve Digital Signature Algorithm) signature algorithm. It is based on elliptical curves which have the advantage of guaranteeing, for the same level of security, reasonable key sizes compared to other crypto public-key systems such as the RSA. Indeed, for a security level of 112, where the RSA requires 3072-bit keys, ECC requires only 256bits (Naziridis, 2018).

Electronic signatures make it possible to guarantee the authenticity of each transaction injected into a Blockchain (NCCIC, 2018). Technically, the generation of a signature requires the signatory to first apply a hash function to the elements of the transaction to be authenticated, and then to encrypt the result obtained with its private key.

Hash functions are very present in Blockchains, in particular, the SHA256 function. They are also used to generate signatures to authenticate each transaction, to guarantee a strong link between a Blockchain member and its public key, to identify a transaction or block, and to link the blocks (or transactions) of the Blockchain together in order to rigidify the sequence of blocks (or transactions) and ultimately to guarantee the integrity of the Blockchain (Kotow, 2019).

# Blockchain Operation

An Internet transaction today requires certification by a trusted third party - a bank, a public body, a notary, an insurer, etc. To prevent fraud attempts, this intermediary alone keeps the transaction register. The blockchain carries out this exchange on a peer-to-peer network, i. e. without an intermediary. The transaction between two Internet users is recorded in a register (ledger) that keeps track of all operations performed. This register is not held in a centralized location but "distributed" in the computers of all participants, called "nodes". With each transaction, network members query the history to ensure that the person owns the assets they wish to exchange. Transactions are then grouped and validated in blocks - which form a "blockchain" or "blockchain". Each new block of transactions is added to the chain, linked to the previous one by a cryptographic process. The blockchain thus contains all the operations validated since the creation of the chain until today. However, it was an abuse of language that gave this first assembly process its name to the technology, because it is only one component of the protocol.

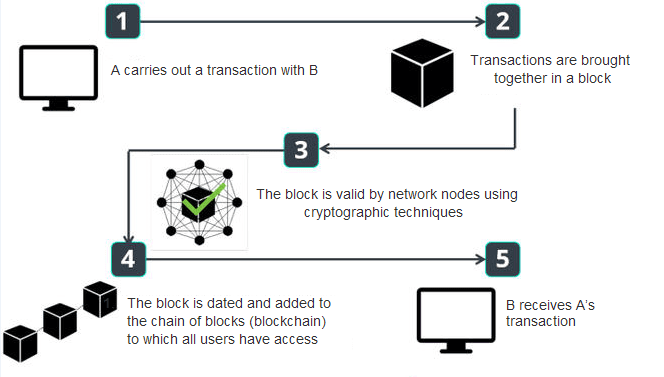


Figure 1: Blockchain operation. <https://blockchainfrance.net>, 2016

The real innovation lies more in the validation method. The blockchain promises to reach a consensus on the validity of transactions. Security and decentralization do not come from the chaining of blocks but from the distributed consensus protocol. This mechanism works by the "proof of work". This is how the blockchain succeeds in reconciling openness to the general public and maximum security. This "proof of work" or mining can be very expensive, both in terms of time and power consumption (HydroMiner, 2019). Hence the idea of using the "proof of stake", in other words, the "proof of stake" (or "proof of possession"): the Internet user must prove that he has "tokens" or a certain amount of crypto monies in order to validate an additional block of the chain. With proof of work, we talk about miners; with proof of stake, we talk about forgers.

From a technical point of view, Blockchain members are computer resources (e. g. computers) that are previously connected to the Blockchain following an enrolment phase. These resources are commonly referred to as nodes because they are networked through the Internet. Two types of nodes coexist (Evans, 2019):

* regular nodes, most of which have ordinary IT capabilities, from which individuals can issue transaction requests.
* "miner" or minor nodes, with large processing capacities, directly useful for the operation of the Blockchain and capable of issuing transactions on the same basis as a regular node.

Nodes, whether regular or minor, as long as they have large storage capacities, can store the entire Blockchain. They are called "full nodes". It should be noted that the Blockchain Bitcoin launched in 2009 reaches more than 240GB in September 2019 (Blockchain Size, 2019).

## The enrolment phase in the Blockchain

To participate in the activities of a Blockchain, a person must enroll one of its computer equipment as a node of the Blockchain. During this operation, the node, whether regular or minor, downloads software that allows it to interface with the Blockchain. This software is customized with a Blockchain account number (e. g. 160-bit Bitcoin address) and a set of public and private keys (Asolo, 2019). It is imperative that the node owner carefully keeps the downloaded software and password allowing him to unlock the private key, otherwise, he will lose access to his Blockchain account and will no longer be able to make any transactions on this account. There must be a clear and easily verifiable link between the account number and the public key. Classically, as is the case for Bitcoin, the Bitcoin address corresponds to the result of the hash of the associated public key. This allows any node to check the consistency between the ownership of an account and the signing of a transaction it is supposed to have issued. This trick avoids the need for a key management infrastructure where digital certificate management is particularly cumbersome and expensive.

## The transaction phase

A Blockchain is a set of individual transactions that are grouped into blocks, each block containing the transactions issued since the last block (approximately every 10 minutes for Bitcoin). Each transaction is issued by a node that distributes it to all members of the Blockchain. The nodes that store the Blockchain verify the authenticity and legitimacy of each transaction by referring to the history of transactions recorded since origin in the Blockchain, then it is the miners who aggregate the valid transactions into a block and attempt to validate the block by solving a complex mathematical problem called Proof of Work (PoW). This problem-solving work is called "mining". The miner who completed the mining first releases his solution to all nodes that check the associated PoW proof. In case of proven validity, each node adds the block to the Blockchain and miners start to mine the next block. Massively placing a block in the Blockchain means that a consensus has been reached among the nodes. In the case where two miners simultaneously solve the PoW, the other nodes then receive two different valid blocks, corresponding to the same link in the chain. The two blocks are added to the chain at the same level, creating a fork effect starting two separate chains. This problem of duplication of the blockchains' self-regulates, simply by the fact that the longer Blockchain is considered valid. For Bitcoin, it is accepted that after 100 blocks have been added to the Blockchain, the duplication problem is solved. Of course, this assumes that all invalidated Blockchain transactions are incorporated into the valid Blockchain. As a result, a Bitcoin-type transaction is considered to have passed on the condition that it is "buried" in 6 blocks, which requires waiting 1 hour before the beneficiary can dispose of his Bitcoins and carry out a transaction himself. This condition is a very strong barrier to the use of Blockchains in a dynamic environment, which leads researchers to focus on alternatives such as the Proof of Stake.

## What is a transaction?

A transaction is always issued at the request of a node with the objective of being added to the Blockchain. Each Blockchain imposes a strict framework on the one hand and on the other hand, gives a certain latitude to the sending node to specify the conditions to be met for the transaction to be effective. For the Bitcoin project to spend Bitcoins, the implicit rule is to verify that a node has enough Bitcoins to issue the transaction, and the sending node may impose, in the form of a script written program, its own conditions such as the condition that the beneficiary proves its identity by issuing a valid signature or that several signatories are required to issue a new transaction. For Ethereum, it is up to the developers of Smart contracts to set all the rules. An example of a transaction or smart contract for Ethereum would be to initiate a transfer (in crypto-currencies) upon receipt of a package, or the opening of a door (vehicle, house rental...) after prepayment of the service... A transaction must necessarily contain:

* a transaction ID, which later allows you to point to this transaction;
* any useful information to validate the legitimacy of the transaction or, more broadly, to situate the context of the transaction. The Bitcoin project refers to inputs that allow the Bertrand issuer to identify several previous transactions to justify a sufficient balance, and to prove that it meets Anne and Alice's conditions to be a beneficiary (public key and signature);
* any useful information to formalize the outcome of the transaction. The Bitcoin project defines outputs that specify the beneficiaries of the transfer, the associated amount, and the conditions that the beneficiaries must meet to claim the amount back. Like a ledger, the balance can be achieved between inputs and outputs, but if the amount in output is lower than in input, it means that the miner can benefit from the difference for his mining work. It should be noted that transaction fees are sometimes mandatory and that the amount allocated encourages miners to integrate the transaction into their mining operation.

|  |  |
| --- | --- |
| **Protocol version number** | |
| **Number of inputs : 2** | |
| **Input 1** | Transaction ID of the transaction passed by user 1 |
|  | Index output of the transaction |
|  | Public key issued by user 2 |
|  | Proof issued by user 2 to satisfy user 1’s conditions |
| **Input 2** | Hash of the transaction passed by user 3 |
|  | User transaction output index 3 |
|  | Public key of user 2 |
|  | Proof issued by user 2 to satisfy user 3’s conditions |
| **Number of outputs : 2** | |
| **Output 1** | Amount transferred : 0.4 BTC |
|  | Transfer conditions (pubkey script) |
|  | Bitcoin account of user 4 |
| **Output 2** | Amount transferred : 0.3 BTC |
|  | Transfer conditions (pubkey script) |
|  | Bitcoin account of user 5 |

Previous transaction of user 1

Output : Amount transferred of 0.5 BTC

Hash

Previous transaction of user 1

Output : Amount transferred of 0.5 BTC

Hash

Figure 2: Simplified format of a Bitcoin transaction

## What is a block?

A block groups together a set of transactions and aims to crystallize the content of the transactions and the block, and the position of the block in the Blockchain in such a way as to make it impossible to accidentally or maliciously modify the content of the Blockchain. This crystallization is based on two essential complementary processes. First, the hashing functions used intensively and sometimes organized to produce a Merkle tree make it possible to stiffen the structure of transactions and blocks by welding all these elements together. The hash functions prevent a block in the chain from being partially modified but do not eliminate the possibility of overwriting the last blocks. It is the mining mechanisms coupled with the decentralized storage and computation architecture that guarantee a certain level of confidence.

As shown in Table 1 for the Bitcoin project, a block is composed of a header that includes signage useful for the operation of the Blockchain and content in which transactions are grouped. The header includes a nuncio, i.e., a random number useful for the mining operation and other elements explained below.

For each transaction is calculated an identifier (TxID) which is the hashed content of the transaction. The Merkle tree then makes it possible to solidify all the transactions by calculating successive hashes, until the root of the tree is found. The result is then entered in the block header, which has the advantage of strongly linking the header content to the block content and subsequently proving the integrity of the block content. Then it remains to ensure the integrity of the block's place in the Blockchain. This property is essentially ensured by a chain of blocks between them, and this from the first block of the chain called "Genesis Block". In Figure 3, Block 2 is well located between Blocks 1 and 3, which can be verified by ensuring that the hash of Block 1 is correctly filled in in the header of Block 2 and similarly for the hash of Block 2 in the header of Block 3.

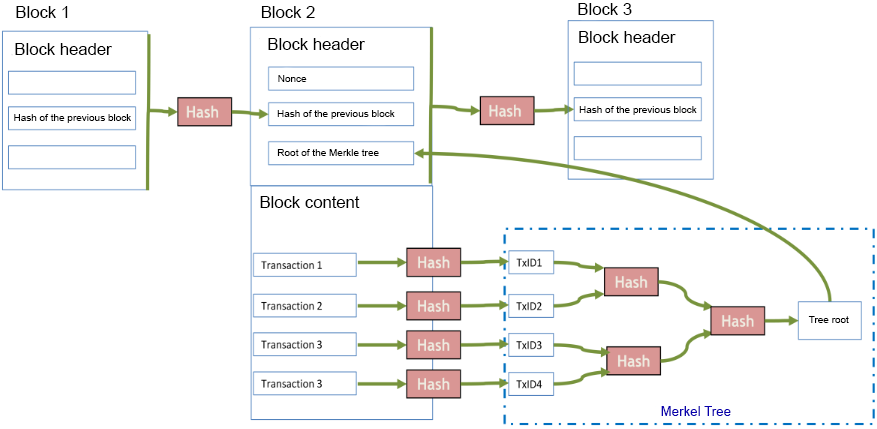


Figure 3: Simplified format of a Bitcoin block

## The mining operation to obtain PoW (Proof of Work) proof

Mining is the operation that allows the miner to find a valid block by solving a complex mathematical problem and giving himself a win. More precisely, before starting to solve the problem, the minor adds an additional transaction to the block to be processed. This transaction called "coinbase" transaction does not meet the rules of standard transactions (output amount less than input amount), because the minor can create currency within the limit set by the Blockchain policy. This "coinbase" transaction specifies the beneficiary who is the minor and the amount of the win. In this way, after the problem has been resolved, if the block is accepted by the miners in the Blockchain, the winnings will be acquired by the miner, as well as all transaction costs. It should be noted that the reward of the block decreases over time and that miners will increasingly rely on transaction fees for their remuneration. The problem to solve, also called PoW for Proof of Work, to validate a block requires a lot of calculations on the part of the minor and consists in finding the value of the 32-bit Nonce field to be filled in in the block header so that the hashing of the block header results in a result below a certain value. The smaller this value, the more difficult it is to solve the problem. To maintain the same computational complexity over time, it is interesting that the Blockchain adjusts the level of difficulty. This is the case for the Bitcoin project, which is based on a 10-minute block average mining time. Thus, every 2016 blocks that correspond to a theoretical period of two weeks, an average is calculated; if the average time is too short, the difficulty is then revised upwards; if it is too long, the difficulty is revised downwards.

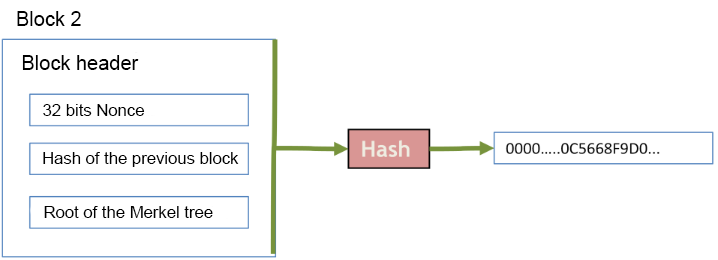


Figure 4: PoW type mining work on the header of the Bitcoin block

## The simple validation operation by PoS (Proof of Stake)

The objective of PoS validation is to reduce the PoW mining procedure. The stakes are both ecological with lower energy costs compared to PoW and economical with a better reactivity of the Blockchain, which can register transactions more quickly, and larger volumes of transactions processed. The Ethereum project is working on the PoS algorithm called Casper, to which it plans to migrate within one to two years. Casper should achieve block validation performance of a few seconds or even less than 1 second, and should thus allow the processing of 20,000 transactions per second. From a functional point of view, PoS validation is even more decentralized than PoW validation. Indeed, with PoW, the nodes perform exactly the same mining operations from the validation of transactions to the resolution of the problem, which has the disadvantage that it is finally China with large resources involved that is now centralizing Bitcoin mining. With the PoS Casper approach, nodes are organized into several subgroups so that the volume of transactions to be validated is distributed over several of these subgroups, resulting in better performance. The system favors the nodes with the highest commitment, i.e. those with the largest portfolio and therefore the most to lose in the event of malicious intent because a system of fines is in place to deter bad behavior. If the PoS principle is promising, at first sight, caution should be exercised because, for the time being, even if it is being tested on Ethereum, it has not really proven its worth, unlike the PoW process already tested in the large-scale Bitcoin and Ethereum projects.

## Proof of Formulation (PoF) – the future consensus model

FLETA has developed a PoF (Proof-of-Formulator) to quickly generate and distribute blocks using the Formulator reward sequence to designate the mining target and reduce the diffusion rang (Fleta business whitepaper, 2019)e. In addition, the existence of the observer node allows for immediate authentication and prevents the range of blocks. Anyone can make the formulator, so the door is open to everyone. It is possible to obtain a reduced calculation time because the extraction sequence of the formulator is fixed, which considerably reduces the diffusion range of the new blocks.

This technology has several advantages (Fleta business whitepaper, 2019):

The PoF consensus is much safer and faster than the PoS consensus.

Unlike the PoW consensus, PoF does not require excessive IT resources and does not depend on how much is at stake for someone. For this reason, it reduces competition to know who operates and creates blocks each round. PoF also has built-in mechanisms to prevent the possibility of any type of fork.

Incentive mechanisms to mine

Without the mining carried out by the miners, the Blockchain would not be able to function. It is therefore essential to identify a gain (or crypto-fuel) attractive enough to encourage a sufficient number of miners to mine and store the Blockchain. It should be noted that the minor must have significant computational powers, even very important for the PoW mechanism. The gain must, therefore, offset the purchase of the equipment, but also the effort to maintain the equipment in use and the electricity bill. The winnings are paid to the miner for each successful mining operation accepted by his peers, in the form of a transaction that he adds to the block. Designers are free to define the nature of crypto-fuel for minors. Crypto-fuel is generally linked to the activity carried by the Blockchain. It can be about winning cryptocurrency, as is the case for the Bitcoin project, or in the same way as traditional loyalty techniques: storage space, computing resources, a few hours of car rental, a stay in a hotel, a trip, or a greater ability to vote in a voting process... In any case, this incentive process requires the definition of a virtual unit that allows you to accumulate earnings according to the efforts made, in the same way as a loyalty card. This unit, which is also a cryptocurrency, is called ether in the Ethereum project. Thus, each node has a volume of ethers earned and associated with its account and its owner decides when to consume its ethers.

# The different types of blockchains

## Public blockchains

Public blockchains are almost all developed and maintained by communities of independent developers (in Open Source) and target complete disintermediation against historical trusted third parties.

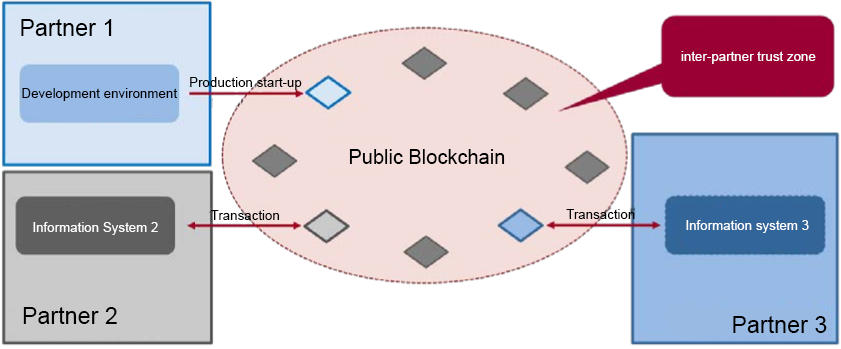


Figure 5: Public Blockchain

They promise to be able to support micro-services in the form of "smart contracts" that would make it possible to amplify the fragmentation of value chains, as the appearance of Apps on smartphones has been.

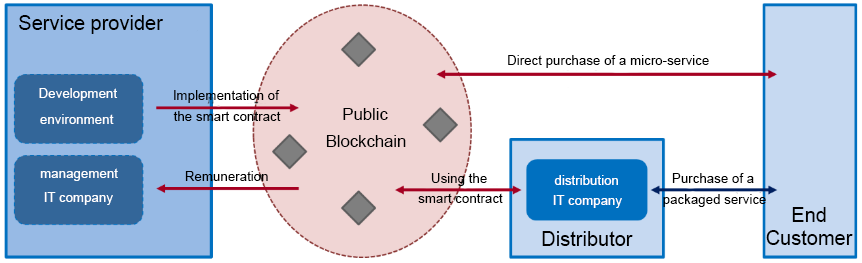


Figure 6: The promise of smart public contracts

The particularity of public blockchains is that they are entirely based on the trust that can be placed in the computer code underlying the exchanges; as such, it is important to highlight the strong resilience to date of the Bitcoin blockchain that has already existed for 9 years (Agrawal, 2019). Legally, the reflection is beginning to take shape around the blockchain:

* For example, through the "eIDAS" Regulation25 of 23 July 2014, which establishes a common basis for secure electronic interactions between citizens, businesses and public authorities DAS;
* but also the decree of 28 September 2017 on the presumption of reliability of the signature process, since the blockchain uses cryptographic processes similar to those of the electronic signature;
* or even on the elements of compatibility/convergence with the GDPR (General Data Protection Regulations).

Nevertheless, the transnational nature of transactions, particularly in the case of public blockchains, can lead to legal uncertainty. Indeed, whether in Common Law or in continental law, the legal environment and its interpretation are not uniform. Beyond legal uncertainty, and despite ongoing debates and reflections, it is above all the "new" character of the blockchain concept that makes the adoption of public blockchains by companies still weak and makes them turn more towards consortium or private blockchains. Nevertheless, it should be noted that companies that have acquired a certain maturity in this field tend to multiply their links with public blockchains because of their transverse and universal nature.

## Consortium blockchains

Consortium blockchains rely on software developed by public blockchains, but instantiate them in universes that could be described as "privatized". Indeed, unlike a public blockchain, for which anyone can download the blockchain program, mine transactions and carry out direct exchanges, the nodes of a consortium blockchain are a priori located inside the datacenters of the consortium members and updates of the source software can be a priori controlled by the consortium (Agrawal, 2019).

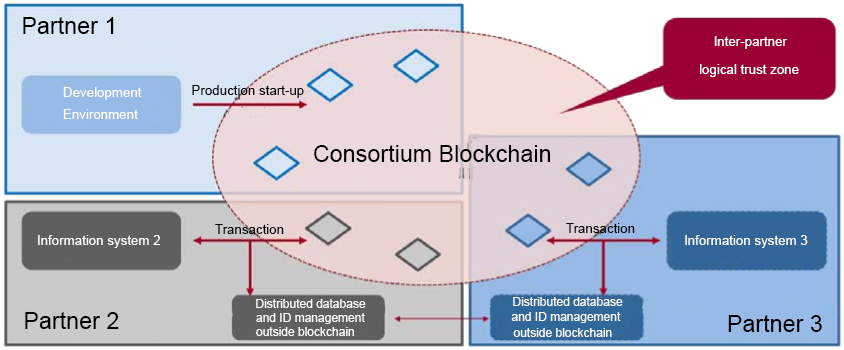


Figure 7: Consortium Blockchain

The main advantage of this consortium logic is revealed in the B2B world where this type of blockchain simplifies marketplace systems and potentially reduces transaction costs. From a legal point of view, consortium blockchains offer an acceptable security potential, which must nevertheless be formalized in the framework of a consortium agreement covering all legal risks, starting with those carried by former trusted third parties (Agrawal, 2019). On the technical level, the implementation of a hybrid architecture, combining blockchain architecture and traditional architecture, has created a space of technical trust at a lower cost by capitalizing on the potential of the blockchain in a secure universe in a traditional way (particularly for identity management, databases, and inter-partner flow exchanges...).

## Private blockchains

Technically, private blockchains are consortium blockchains but applied to the different entities of the same company or organization; the usefulness of deploying these systems today lies in simplifying and facilitating intra-company exchanges by replacing control nodes with distributed systems (Agrawal, 2019). The first applications observed in companies by the working group concern the synchronization of financial data and repositories.

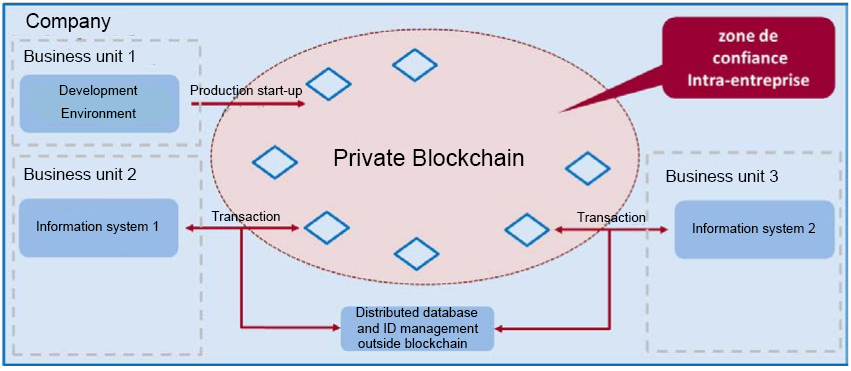


Figure 8: Private Blockchain

Comparison table

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Blockchain type | Name | Reading the register | Completion of a transaction | Validation | Example |
| Open | Public blockchain without permission | Open to all | Anyone can do it | Anyone, provided they make a significant investment in computing power (PoW) or in crypto money ownership (PoS) | Bitcoin, Ethereum |
| Public blockchain allowed | Open to all | Participants autorisés | All or some of the authorized participants | Sovrin |
| Closed | Consortium | Restricted to authorized participants | Authorized participants | All or some of the authorized participants | Banks operating a shared registry |
| Private licensed (company blockchain) | Totally private or limited to a set of authorized nodes | Limited to the network operator | Limited to the network operator | Internal bank register shared by subsidiaries |

Table 1 adapted from Berbain C. (2017), " La Blockchain : concept, technologies, acteurs et usages ", Annales des Mines - Réalités industrielles, August.

# What is the basis of trust?

A Blockchain has the following assets to build trust:

* Decentralized architecture based on a large number of nodes depending on various organizations. This means, unlike a centralized architecture where decisions can be made unilaterally, that consensus must be reached or more than 50% of the nodes (or computing power) must be controlled to have an effect on the system. The fact that the architecture is based on a multitude of nodes that ensure the validation and storage of the Blockchain also guarantees better service availability (Werbach, 2018).
* Attractive incentive mechanisms: Nodes must be sufficient in number and from different organizations to guarantee the independence and availability of the Blockchain.
* Traceability and auditability of the entire transaction chain: The publication in the public space of all transactions carried out since the origin of the Blockchain (Block 0 or "Genesis Block") allows everyone to verify the integrity of the chain, and to trace all movements associated with an account. Thus, there is no longer any possibility of cheating; everything is visible, everything is known, within the limits of the guarantees offered by pseudonymity (Werbach, 2018).
* Transparency of algorithms: The code used to mine, to interface with the Blockchain, or to implement a smart contract is readable by all. The advantage is that it allows experts from the user community to review the code and alert in case of suspicion. Trust is therefore based on alert launchers.
* Authenticity of transactions protected by pseudonym: Transactions must be approved by the account owner(s) using sufficient cryptographic security equipment to prevent orders from being placed without their knowledge. To adapt to technological advances, it is important to provide mechanisms with an adaptive level of security (Werbach, 2018).
* A rigidified blockchain with important safety guarantees: The blocks contained in the Blockchain and the sequence of these blocks must be rigidified to avoid any subsequent alteration of the Blockchain. To do this, it is necessary to rely on the distributed nature of the architecture, and on a strong consensus mechanism. To this, it is possible to add a mechanism to encourage good behavior, a mechanism to deter bad behavior, and cryptographic equipment to provide strong technical guarantees. PoW relies on consensus and computationally expensive cryptographic evidence, while PoS relies on consensus and incentive and deterrence mechanisms that have not yet been proven on a real system (Werbach, 2018).

# Risks and limitations

Neutrality of governance (Bauerle, 2019): Before investing time and money in a Blockchain, it is necessary to ask yourself the following questions: Is the neutrality of governance guaranteed? Are the actors involved, i.e., the small group of people involved in developing the code and protocol, really independent in their decision-making and ability to resist political, industrial and other pressures? If this is not the case, the fundamental principle of "decentralized" is no longer respected. If, in addition, all these actors have control over more than half of the Blockchain's computing power (see the point below on infrastructure neutrality), then the principle of consensus is also not respected for the following reasons. When an update of the Blockchain code with new operating rules is released in the Blockchain, a minor's administrator has the choice of accepting or rejecting the update, which may be a minor and backward compatible transformation of the rules - referred to as a "soft fork" - or a major transformation without backward compatibility - referred to as a "hard fork". To become functional, a "soft fork" requires the support of a majority of miners, while a "hard fork" requires the support of a much broader consensus. In the case of non-consensus with two significant populations of miners who detach, the initial Blockchain splits in two, with two Blockchains following their own path. In conclusion, it is easy to understand that a group of actors who would hold the majority of the mining capacity can, through collusion, modify the rules of governance, create "forks" that bring confusion, double spending and risk of devaluation of the cryptocurrency.

The neutrality of the underlying IT infrastructure (McMullen, 2016): The distribution of IT resources useful for calculations and storage in a blockchain must be balanced between organizations. The trend in Bitcoin has been the creation of mining pools, which, on several occasions, has led the three largest farms to bring together more than 50% of the network's power. It must be understood that this 50% bar is critical because it allows an organization or group of organizations to carry out the 51% attack, this attack allowing them to censor transactions (before the mining process), to promote the mining work of its miners to pocket the earnings instead of faster miners, to succeed in case of duplication of the chain to impose a longer chain with a reasonable probability of success, and thus to master the history of the chain. However, it should be noted that the 51% attack does not allow gains to be stolen or fraudulent transactions to be issued.

Programming errors (Bauerle, 2019): For programmable (or not) Blockchains, there is a high risk of human programming errors, as was the case in 2016 for the attack on the embezzlement attack on Ethereum "The DAO" (DAO for Decentralized Autonomous Organization). In four weeks, "The DAO" raised a spectacular $120 million through crowdfunding, but then lost a third as a result of an attack that revealed a programming error. This error allowed the scammer to loop indefinitely on the function, causing a cash outflow. In 2017, another attack implicated an error in the Parity Wallet wallet software and led to the theft of $30 million in ethers. Be careful, let's be clear, it's not the Blockchain technology that is being questioned here, but programming errors.

Double expenditure (Frankenfield, 2019): Double expenditure consists of issuing two transactions relating to the same object and which should normally be mutually exclusive. It is a deliberate malicious act of a participant who is normally arbitrated during mining. However, it can happen that in a chain splitting process, each transaction is independently validated by each chain. At this point, the beneficiary knows whether or not he has the earnings until the shortest chain is abandoned. For Bitcoin, the reasonable time considered is about 1 hour, equivalent to 6 blocks.

Transaction retention: A minor may have an interest in not sharing a transaction with high transaction costs. By keeping this transaction to himself until the successful mining of a block, he ensures that it will be included in one of his blocks and that he will receive the reward. This transaction may, therefore, take a long time to be included in the Blockchain. This retention attack will become more and more credible in the future as the payment model becomes more transaction-based as block rewards decline. Similarly, a well-connected miner can retain a block before broadcasting it to benefit from additional time in the mining operation. It is only when he receives a competing block that he will be able to massively broadcast his own block. These attacks force us to think about improving incentive mechanisms.

Money laundering (Phillips, 2018): The problem of money laundering arises as soon as a new means of exchanging money is available. Contrary to what one might think, the transparency of transactions in the Blockchain does not prevent money laundering, it just makes it more complex. Indeed, techniques exist to cover up the tracks and traceability. The first very simple step is to hold a multitude of accounts (some of which can even be used only once) and to carry out transactions between several of these accounts. Another approach to scramble traceability, called Join Corner in Bitcoin, is to merge several transactions into one. The more transactions merged (inbound and outbound), the better the protection because it is more difficult to link a debtor to a creditor. It should be noted, however, that the Zerocash approach ensures that transactions are not traceable and therefore makes it impossible to detect money laundering solely on the basis of the elements provided in the Blockchain.

Risk of vulnerabilities (Gupta, 2019): Transaction or smart contract code is most often open-source, but if this code is poorly designed, it can allow hackers to exploit the vulnerabilities it contains to the detriment of other users. The best-known example of piracy is that of The DAO, which resulted in a loss of more than 150 million dollars (in ethers). Following this famous hack, the Ethereum community made the painful choice to rewrite a posteriori the transaction history recorded in the Ethereum blockchain in order to dispossess the hacker of his loot and return the stolen ethers to all the victims. This type of problem raises the question of the immutability of blockchains ("Code is Law") in the face of the need to reintroduce human intervention within the framework of a smart contract in order to restore morality and public order. A doctrine exists, arguing that it would be possible to add an additional form of governance to the blockchains orchestrated by a clever set of smart contracts to define possible cases of arbitration in case of emergency. On the other hand, the purists of Bitcoin and its developments are in favor of preserving these ecosystems as much as possible from any human and political intervention.

# The future of the blockchain

## Cryptocurrency

The first application of the block chain is to be a support for encrypted currencies. This secure technology, allows the transfer of currencies without an administrative intermediary. Cryptocurrencies are not about to disappear because their use is multiple: anonymous purchasing, creation of a new banking system, secure transfers...

There are currently nearly a thousand different encrypted currencies and most of them use block chain technology. Some countries are working to develop a national cryptocurrency. Other entities are in the process of setting up a whole parallel economy based on the exchange of cryptocurrencies. This proves that these digital currencies are not about to disappear.

## Data Security

The block string can be used in the transfer of administrative data. Its traceability makes it possible to trace the chronology of the changes that have been made to it and its encryption allows almost total inviolability of the data. Estonia is the first country to adopt this technology to secure its citizens' data (Martinson, 2019).

The block chain is a particularly efficient system for processing and compiling all forms of information, such as the registration of transfers of ownership or legal contracts (Nielson, 2019). Until now, this data has been managed by centralized systems, often hosted on a single computer or a set of computers in the same location. All it takes is an error, a hack or a flaw in the system for all files to be corrupted. The block chain can prevent this.

## Protecting the IoT

The Internet of Things (IoT), which is taking up a little more space in our daily lives, is the name given to the connected objects around us. These are, for example, smart fridges or connected watches. But they can be smart-cameras that recognize the visitor and can be viewed from miles away. A new generation of billboards reacts to the movements of individuals on the public road: they are also connected objects. Just like kettles that store temperature choices according to the user's tastes or smart-tv.

The problem with IoT is that they are often objects with an Internet connection but not protected by antivirus software and only have primary management software that is difficult for the novice to access. But above all, the main weakness of these connected objects is that they are all managed by a central unit. Once infected, the virus can spread without difficulty. The 2016 Mirai botnet denial of service attack is a good example of the danger it represents (Ashford, 2017).

The block chain should allow device networks to protect themselves in other ways, such as allowing devices to form a group consensus on what is normal in a given network and to quarantine all nodes that behave in unusual ways. But the block chain has a competitor in this field: the Tangle technology is lighter and allows the same uses.

## Bypassing censorship

In China, students have begun to insert messages into the Ethereum blockchain to escape censorship in the country (Kshetri, 2019). Students at Beijing University, who wanted to report a case of sexual abuse by a professor in the 1990s, seem to have been the first to use this subterfuge.

By inserting texts into transactions with zero Ethereum, students write messages in encrypted and tamper-proof blocks. The Chinese government practises strong censorship on the web and its citizens, deleting messages that it does not like. But when these messages are stored in a block chain, China can no longer delete them. This way of circumventing censorship began in China, but it could be emulated wherever censorship - be it economic, activist or government - is applied.

## A promising future

These few examples show that the block chain is not about to be forgotten. This technology has advantages for all segments of society. Activists, politicians, bankers, industrialists, producers, administrations... there is no group that cannot benefit from the blockchain. The biggest obstacle is money: you have to have the means to be able to use this technology.

# Conclusion

In this article, we have seen the many possibilities offered by the BlockChain technology. This technology is a real breakthrough in the world of information storage, transaction, and traceability. Whether you want to use a Public or Private BlockChain, a certain level of knowledge is required to master this complex technology.

In the future, this technology could become indispensable, whether in the certification of a document, the creation of a cadastre or transactions between individuals. On average, every 10 minutes, a new bitcoin block is added to the chain only by mining operations (How many bitcoins are there ?, 2019). This exponential growth of the Blockchain could pose storage and synchronization problems in the future.

Blockchain's revolutionary technology offers a high potential for applications in many different industries and sectors. Although some industries have already begun to adopt the blocking chain in their companies, many are still exploring the best ways to get started.

Blockchain is a new name in the world of technology, but it is certainly the one that will last. From the very beginning, the technology has gained tremendous popularity from their very first application of cryptocurrencies. Every day, new areas of application are discovered and tested. Once adopted and accepted globally, technology will transform our current way of life.

# References

Agrawal, H. (2019, September 6). *Different Types Of Blockchains In The Market and Why We Need Them*. Retrieved from coinsutra.com: https://coinsutra.com/different-types-blockchains/

Ashford, W. (2017, October 4). *Mirai IoT botnet code release raises fears of surge in DDoS attacks*. Retrieved from computerweekly.com: https://www.computerweekly.com/news/450400311/Mirai-IoT-botnet-code-release-raises-fears-of-surge-in-DDoS-attacks

Asolo, B. (2019, March 28). *Blockchain Public Key & Private Key: A Detailed Guide*. Retrieved from mycryptopedia.com: https://www.mycryptopedia.com/public-key-private-key-explained/

Bauerle, N. (2019). *What are Blockchain’s Issues and Limitations?* Retrieved from coindesk.com: https://www.coindesk.com/information/blockchains-issues-limitations

Berbain, C. (2017). La blockchain : concept, technologies, acteurs et usages. *Annales des Mines - Réalités industrielles*, 6-9.

*Block hashing algorithm*. (2019, May 13). Retrieved from Bitcoin wiki: https://en.bitcoin.it/wiki/Block\_hashing\_algorithm

Blockchain France. (2016). *Qu’est-ce que la blockchain ?* Retrieved from Blockchain France: https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/

*Blockchain Size*. (2019). Retrieved from blockchain.com: https://www.blockchain.com/fr/charts/blocks-size

Côme, B. (2017). La blockchain : concept, technologies, acteurs et usages. *Annales des Mines*, 6-9.

Evans, J. (2019). *Blockchain Nodes: An In-Depth Guide*. Retrieved from nodes.com: https://nodes.com/

*Fleta business whitepaper.* (2019). Retrieved from fleta.io: https://fleta.io/download/190426\_Buisness\_Whitepaper\_EN\_web.pdf

Frankenfield, J. (2019, August 17). *Double-Spending* . Retrieved from investopedia.com: https://www.investopedia.com/terms/d/doublespending.asp

Gupta, R. (2019). *Hacking into Blockchain: Is Blockchain Security a Concern?* Retrieved from plugandplaytechcenter.com: https://www.plugandplaytechcenter.com/resources/hacking-blockchain-blockchain-security-concern/

*How many bitcoins are there ?* (2019, September 21). Retrieved from buybitcoinworldwide.com: https://www.buybitcoinworldwide.com/how-many-bitcoins-are-there/

HydroMiner. (2019, May 20). *Proof-of-Work vs. Proof-of-Stake*. Retrieved from medium.com: https://medium.com/@hydrominer/proof-of-work-vs-proof-of-stake-7b3afe24f0cc

Kotow, E. (2019, February 26). *What is Blockchain Hashing?* Retrieved from hedgetrade.com: https://hedgetrade.com/what-is-blockchain-hashing/

Kshetri, N. (2019, February 26). *Chinese internet users turn to the blockchain to fight against government censorship*. Retrieved from theconversation.com: https://theconversation.com/chinese-internet-users-turn-to-the-blockchain-to-fight-against-government-censorship-111795

Martinson, P. (2019). *Estonia – the Digital Republic Secured by Blockchain.* Retrieved from pwc.com: https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf

McMullen, G. (2016, July 20). *Constitutional Code & Blockchain Neutrality: Lessons in governance from The DAO attack*. Retrieved from medium.com: https://medium.com/ipdb-blog/constitutional-code-blockchain-neutrality-26c8b359e542

Naziridis, N. (2018, June 8). *Comparing ECDSA vs RSA*. Retrieved from ssl.com: https://www.ssl.com/article/comparing-ecdsa-vs-rsa/

NCCIC. (2018, September 4). *Understanding Digital Signatures*. Retrieved from CISA cyber infrastructure: https://www.us-cert.gov/ncas/tips/ST04-018

Nielson, B. (2019). *Blockchain Solutions for Cyber & Data Security*. Retrieved from richtopia.com: https://richtopia.com/emerging-technologies/blockchain-solutions-for-cyber-data-security

Phillips, K. (2018, November 1). *Blockchain is not the answer to money laundering… yet*. Retrieved from fnlondon.com: https://www.fnlondon.com/articles/blockchain-is-not-the-answer-to-money-laundering-yet-20181101

Rosic, A. (2016). *What is Ethereum?* Retrieved from blockgeeks.com: https://blockgeeks.com/guides/ethereum/

Werbach, K. (2018). *The Blockchain and the New Architecture of Trust.* The MIT Press.