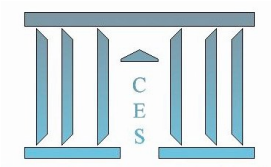
# Public Blockchain versus Private blockhain

Dominique Guegan

UNIVERSITÉ PARIS 1
PANTHÉON SORBONNE

Documents de Travail du
Centre d'Economie de la Sorbonne

CES Working Papers




# Public Blockchain versus Private blockhain

Dominique GUEGAN

**2017.20**


Maison des Sciences Économiques, 106-112 boulevard de L'Hôpital, 75647 Paris Cedex 13
http://centredeconomiesorbonne.univ-paris1.fr/
ISSN : 1955-611X

# Public Blockchain versus Private blockchain

**Dominique Guégan**

University Paris 1 Panthéon-Sorbonne, and labEx ReFi ,

106 bd de l'Hôpital, 75013 Paris, France

Email: dguegan@univ-paris1.fr

(this work was achieved through the Laboratory of Excellence on Financial Regulation supported by PRES HeSam under the reference ANR-10-LABEX-0095}

In this document we introduce some thoughts relative to the concept of blockchain, how it works and what are the issues for the banking industry. Therefore, we first recall what cryptography is, then we introduce the concept of blockchain as a protocol for transmitting information in a secure way, distinguishing two possible approaches: the decentralized public approach and the centralized private approach. The notion of cryptocurrency is introduced and two examples of applications of the public blockchains that are the bitcoin and the etherium are provided.

There are many questions and issues. Obviously there are numerous discussions around the bitcoin and beyond the technical problems, we can list some open questions relative to the blockchain as the understanding of the attacks to 51% and the way to circumvent them, the double spending, the principle of decentralized clock, the crashes scenarii, the transfers of assets, the smart contracts, the regulation, ... We want to focus on the difference between the use of the public blockchain (without a third party) and what can be called the private or semi-private blockchain.

There is lot of controversies from both users and developers of the public blockchain versus the private blockchain. It seems necessary to clarify these two uses and the good way will be to use different terminologies. For the moment, we keep both terminologies. On the other hand it seems necessary to discuss all the possible approaches of the private blockchain, which range from the "press-button" and the associated risks, to a technical and secure development, which is still in its infancy. At least the need to identify the risks associated with these approaches, identify them and propose strategies need to be developed. Of course a piece of regulation is possible but it has to be done.

## Introduction

We specify the different notions useful to understand the concept of cryptocurrency and blockchain.

- Cryptography

Cryptography is a discipline dedicated to protecting messages (ensuring confidentiality, authenticity and integrity) using keys. This technique is ancient and dates from antiquity. For a long time it was considered as an art, and only became a science in the 20th century. It was the massive use of computers that democratized its use. There are several types of cryptography's algorithms: the

classical cryptography (easily decipherable), Symmetric cryptography algorithm (with a secret key), asymmetric cryptography algorithms (with public or private keys). In the latter case, the public key allows the encryption and the private key the decryption. There are several asymmetric cryptographic algorithms including RSA (encryption and signature), or DSA (signature). Asymmetric cryptography is used to ensure the authenticity of a message. The signature of the message is encrypted using private key attached to the message. The recipients then decrypt the cryptogram using the public key and normally retrieve the signature. This ensures that the sender is the author of the message.

- The Hash function

The signature of a message generally does not exceed 256 bits and to transform a large set of information into a small set of information, a hash function is used (which does not make it possible to return to the original set). For example, the SHA-256 function will be used to obtain a 256-bit message.

- The transfert of a message

When a message is encrypted, it is then transferred through secured protocols. With the Internet (TCP-IP) there are already computer protocols that allow the creation of an infrastructure that transfers data packets from point A to point B.

- Blockchain

Alternatively, blockchain is a secure, transparent technology for storage and transmission which operates without a central control device that can be used to transfer data from point A to point B. It is a distributed database that manages a list of records mechanically protected against tampering or modification by storage in nodes through its decentralized timeline. A blockchain, as a database, contains the history of all the exchanges between its users since its creation. It is shared by its various users, without intermediaries, which allows each one to check the validity of the channel. The fact to share is based on a consensus, and historically to arrive at this type of consensus we used "proof of work". This method uses energy as a means of verification that the "miner" has done a good job. The blockchain protocol therefore uses a cryptographic system based on a decentralized system of proofs: the resolution of the proof requires a high computing power, provided by the miners. In order not to be falsifiable, a blockchain requires that no hostile operator at any time have more than half the computing power of the chain.

At the present time, two types of blockchain are considered:

- A blockchain is called public if each participants can read it and use it to carry out transactions but also if everyone can participate in the process of creating the consensus. There is therefore no central register, nor a trusted third party. The governance of public channels, resulting from the open source movement and cypherpunk, is simple: "Code is Law". In this system, the nodes of the network validate the choices discussed and initiated by the developers by deciding whether to integrate the proposed modifications. This operation is based on "cryptoeconomics", the combination of economic incentives and verification mechanisms using cryptography. Based on a community, or alternative, approach to the

economy, this system has demonstrated its strength and resilience. Any public blockchain necessarily works with a coin or token.

- On the other hand, a blockchain is called private} (or semi-private) if the consensus process can only be achieved by a limited and predefined number of participants. Write access is given by an organization and read permissions can be public or restricted. The "blockchain of place" evoked in several articles are examples of private channels. In this case, the consensus process is controlled by a preselected set of nodes. The private blockchain does not use necessarily mechanisms based on cryptography.
- **In the case of the private blockchain, there is no mining, no proof of work, no remuneration. This is what entirely differentiates the two types of storages and transmission technologies.**

A crypto-currency or cryptographic currency is an electronic money on a peer-to-peer or decentralized computer network based on the principles of cryptography in order to validate the transactions and also the issue of the currency itself. Today, all crypto-currencies are alternative currencies, as they have no legal tender in any country. Crypto-currencies use a working proof system to protect them from electronic counterfeiting. Many crypto-currencies have been developed but most are similar and derive from the first complete implementation: the Bitcoin.

We give two examples of cryptocurrencies using public blochain:

- The Bitcoin is a cryptographic currency and a peer-to-peer payment system invented by Satoshi Nakamoto, which announces the invention in 2008 and publishes the open-source software in 2009. Its unit of account is the bitcoin, limited to 21 million units and divisible up to eight decimal places. Bitcoin is the largest decentralized cryptographic currency with a capitalization close to 14 billion euros in 2016. It is a programmable currency.

The bitcoin protocol is a decentralized trust mechanism to avoid the use of a trusted third party. It is therefore the first decentralized currency that depends on a protocol based system. The principle of decentralization is that everyone can participate in the drafting of the code (nevertheless someone can limit the right of entry). The blockchain of the bitcoin is the set of files of all transactions, whether it is valid or not. The use of cryptography allows the security of transactions, as well as their shipment all over the world. At the moment the most successful example of public channel is the protocol Bitcoin.

Bitcoins are created according to the source code of the software, in return for transaction processing. Some users use the processing power to verify, save and secure transactions in the chain of blocks. This activity, called mining, allows participants to be remunerated, for each new validated block, by newly created bitcoins and by the costs of the transactions processed. Bitcoins can then be exchanged for other currencies, goods or services. The price of crypto-currency is fixed mainly on specialized market places and fluctuates according to the law of supply and demand.

Transactions between network users are grouped in blocks. Each block is validated by the nodes of the network called "miners", according to techniques that depend on the blockchain type. In the blockchain of the bitcoin this technique is called the "Proof-of-Work", and consists in solving algorithmic problems. Once the block is validated, it is time-stamped and added to the string of

blocks. The transaction is then visible to the receiver as well as to the entire network. This process takes some time with respect to the blockchain we are talking about (approximately ten minutes).

- Ethereum is the second largest decentralized cryptographic currency with a capitalization of more than 1 billion euros. Ethereum is therefore a decentralized exchange protocol allowing the creation by users of intelligent contracts thanks to a Turing-complete language. These intelligent contracts are based on a computer protocol that verifies or enforces a mutual contract, they are deployed and publicly viewable in the blockchain. The transaction is then visible to the receiver as well as to the entire network. The transaction process with Ethereum takes approximately 15 seconds.

## Questions concerning the private blockchain protocols

In what follows, we list and discuss some of the questions regarding the development of private blockchains.

There are public blockchains, open to all, and private blockchains, whose access and use are limited to a number of actors.

The opponents to the Bitcoin say that it is as a system impossible to regulate, opaque, slow and less technically efficient than some new protocols. There are many arguments against these positions. At present, the debate is far from being decided between public and private channels, with the underlying debate between centralized and decentralized systems. The debate on the bitcoin is not considered here.

Banks are interested in similar protocols to make their transfers even more secured. In this case, they must create their own blockchain, which then becomes a private blockchain (as opposed to the public blockchain terminology used for the bitcoin protocol). So to enter the era of blockchain technology banks need a fully distributed registry. Several initiatives have emerged to set up private or hybrid blockchains: these are regulated blockchains, which would only allow a limited number of players to register transactions and have the registry. An example is R3 CEV, a FinTech blockchain around which gravitate 25 international banks.

Remember that a blockchain is a technology of digital storage and transmission at minimal cost, decentralized, and totally secure. Concretely, it is a ledger containing a list of all exchanges carried out between the users of this blockchain since its creation. This register is decentralized, stored on user servers, works without an intermediary, thus eliminating infrastructure costs. It is an unfalsifiable history of exchanges, being kept and updated in real time independently by all users. To manipulate this registry, you have to access and modify at the same time tens of thousands of independent databases, which seems a technically impossible feat (up to now). Users validate each transaction through a transparent process that prevents manipulation. They check, for example, through the register, that the sender is the owner of what is sent, and that the data receiver is the appropriate correspondent. Groups of validated transactions are finally entered in the register, in the form of a string of unalterable blocks: the blockchain. This is the process that is used for the bitcoin,

for example, **but it does not reflect what is done when working with a centralized system which is the characteristic of the private blockchain**.

What are the criteria used for banks: reliability, security and reduced costs?

- reduction of "infrastructure costs related to international payments, trading and compliance". In other words, thanks to the blockchain, the banks will be able to reduce their operating costs and increase their profitability.
- Implementation of new services based on blockchain and simplification of a lot of processes : micro-payments, low-cost transactions, micro-credits for consumption ...

Since the public blockchain can be assimilated to a public, anonymous and unfalsifiable public accounting book, what blockchain potentials (and how) can be used for the creation of private blockchain?

At present, the use of the private blockchain can be categorized into three categories: (i) Applications for the transfer of assets (monetary use, but not only: securities, votes, Industrial patents, connected objects, security of diplomas, stocks, bonds, etc.); (Ii) Applications of the blockchain as a register: this ensures better traceability of products and assets; (Iii) Smart contracts: These are stand-alone programs that automatically execute the terms and conditions of a contract without requiring human intervention once started.

What risks and limitations are associated with these applications? In the "private" case, the blockchains replace the centralized "trusted third parties" (bank trades, notaries, cadastres, etc.) by distributed computer systems. It is necessary to analyse and to control the risks, the security, the cost. What are the economic, legal, governance or ecological boundaries, and also all the questions around taxation, territoriality, and property need to be identified and argued. Besides, as any secured systems, once compromised, we might need to have a backup solution, which might not be easy to get here.

Other elements that can be considered for private blockchain:

- Individual data are currently concentrated in the hands of US companies such as Google and Microsoft, servers by nature vulnerable to computer attacks and US government requirements. The blockchain might impact sovereignty.
- The norms of the blockchains are not yet written: new rights and duties have to be defined.
- Choice of company: to what extent will we accept to replace the historical trusted authorities (banks, governments, etc.) with computer programs?
- How to manage cultural and social diversity through mathematical laws? The answers to these questions will lay the foundations for the future use of the blockchain.
- It is easy to draw a parallel between the current situation of the blockchain and that of the Internet in the 1990s: we are at the beginnings of a revolution whose scope is still difficult to measure but which is link to infinite applications. To achieve this objective, more technical knowledge is necessary.

**In Conclusion:**

If the public blockchain is based on the emergence of a new form of digital trust, the philosophy of the private blockchain is quite different. The actors of the private blockchain do not want to participate in the public blockchain. Their approach rests on a centralized control, absent in the public blockchain. Are private blockchain more fragile than public blockchains? The debate is opened.