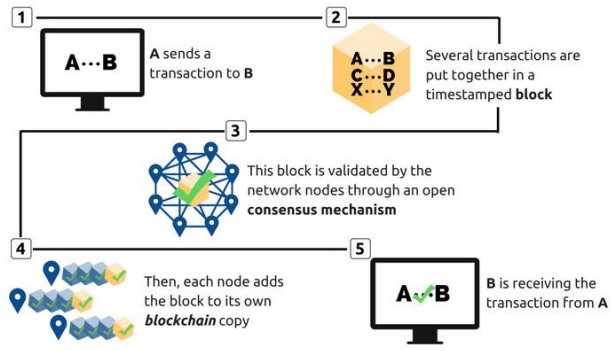
SCIENCE AND TECHNOLOGY BRIEFINGS
PARLIAMENTARY OFFICE FOR SCIENTIFIC AND TECHNOLOGICAL ASSESSMENT

Briefing 4 — Understanding Blockchains — April 2018

How A Blockchain Works



Source : OPECST from Blockchain France

Summary

The protocol that powers Bitcoin appeared 10 years ago as a combination of existing technologies. The blockchain enables decentralized and secure transactions without the need for a trusted third party.

The potential applications are much broader than just cryptocurrencies and while they are extremely promising, today the technology is generally not yet mature enough for large scale solutions.

Further research and innovation are needed to solve blockchain's scalability limitations as well as its high energy consumption.

Mrs Valéria Faure-Muntian and Mr Claude de Ganay, Members of the National Assembly, Mr Ronan Le Gleut, Senator

Context

This memo answers a request from the common fact-finding mission on "Use cases of the blockchain and other data certification technologies" created by the National Assembly. It will be followed by a more advanced memo. What we refer to as the blockchain are the **technologies for storing and transmitting data allowing the creation of distributed, duplicated ledgers, without a centralized authority, secured through cryptography, and organized into linked blocks of information at regular intervals of time**.

In order to understand how these digital ledgers work, utilising distributed peer-to-peer networks and forming the technological basis powering "cryptocurrency", a specific type of digital currencies[1], it is necessary to understand its origins[2].

Blockchain's Origins

The emergence of cryptocurrencies is partially linked to the **open source software movement**, created in the 1980's by Richard Stallman, as well as the "cypherpunk" movement[3], with the goal of leveraging encryption technology to create a digital currency and guarantee anonymous transactions. The first attempts – David Chaum in 1983 with e-cash then in 1990 with digicash, Wei Dai in 1998 with b-money and, especially, Nick Szabo with bitgold – all failed.

The invention of hashcash by Adam Back in 1997 was a significant achievement in the idea of validating transactions using cryptographic hashes, called "proof of work"[4]. The goal of these technologies is to remove the need for "trusted third parties", by relying instead on a distributed network of trust based on an immutable "digital ledger".

The obstacle to overcome lies in the problem of double spending (the risk that the same asset could be spent twice) and, more generally, around network fault tolerance, whether accidental or intentional[5].

The answer to these difficulties arrived in 2008 in an article by **Satoshi Nakamoto**[6]. The article explained an unhackable protocol running on a peer-to-peer network, the blockchain, as the technological stack behind a new digital currency, Bitcoin.

How the blockchain works

Bitcoin runs on a technology protocol that we now call blockchain. This refers to a chain of blocks as the transactions occurring between users of a network are grouped in "**time-stamped blocks**"[7].

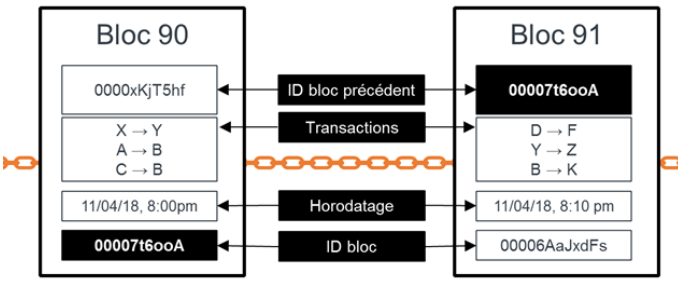
Once a block has been validated, currently every 10 minutes, the transaction becomes visible by everyone who has downloaded a copy of the ledger, potentially all of the network's users, who will update their copy of the blockchain with the new block.

Each transaction uses asymmetrical cryptography, originally appearing in the Diffie-Hellman protocol in 1976, relying on a pair of keys, one private and the other public, linked together by an elliptical curve algorithm (ECDSA). The public key can be shared and allows you to receive transactions, the private key must be kept secret. Protecting these private keys is the singular way to securely keep control of your bitcoins. Although it is possible to trace all of the transactions linked to a public key, it is still an anonymous system as the owner of that public key is not necessarily known. The time and date information encoded in a block is referred to as its "**timestamp**".

Each block, besides the transaction and timestamp, has a unique identifier (Block 90 with a black background in the graphic below) composed of a "**hash**" connecting blocks to each other[8]. Technically, "hashing" converts a specific group of data into a hash, meaning a short digital signature unique to itself. The encryption algorithm used is called a "cryptographic hash function". The hash of a set of data can be considered a digital fingerprint, smaller and less complex than the original data, but identifying it uniquely and precisely.

Hashing is considered to be "one-way": it is designed so that once a hash is created, meaning a fixed-length digital fingerprint created from an input of variable length data, it is impossible to reverse engineer the original data[9]. The hashing algorithm used by bitcoin is one of the most common: the Secure Hash Algorithm-256 (SHA-256), so-named because it produces 256 bit hashes.

Blockchain Structure



Source : Blockchain France

■ Network nodes, « miners » and consensus

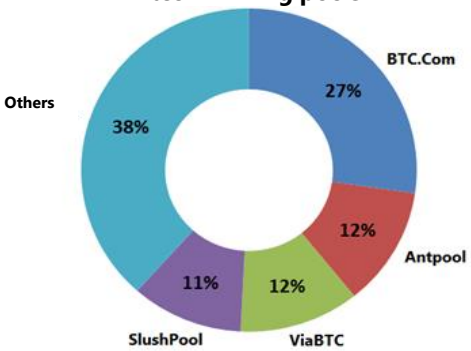
Each block is validated by users known as "miners" (a reference to gold miners), and is then communicated to network nodes, users that possess copies of the entire ledger, who continuously update it. This validation of blocks prevents the risk of malicious attacks[10]. There is no centralized authority of trust as users observe and manage one other. This security, a source of trust, is one of the cornerstone ideas of the blockchain[11]. That fact that hundreds of copies of the ledger are simultaneously and regularly updated through a cryptographic competition, renders blockchains practically indestructible. A "**consensus mechanism**" decides who validates the next block to be added to the chain. In the case of Bitcoin, this is called "**proof of work**" because it is linked to a complex cryptographic problem successfully resolved through "mining", which is repeated on average every 10 minutes[12].

Mining starts by obtaining a hash, beginning with a certain number of zeros, of the block that the miner wishes to solve. This operation, extremely resource intensive in terms of computer processing power, is motivated by the reward in Bitcoins for the winning miner. The validated block is then transmitted from peer-to-peer to each node which adds it to its copy of the blockchain.

If two blocks are validated at the exact same moment, miners use either one and **two parallel chains** are created. The protocol expects that rapidly **only the longest chain will survive**, practically meaning the blockchain that the majority of nodes have adopted. **Mining revenue** is complemented by **fees** taken for each transaction that they add to the blockchain. The amount is theoretically determined freely by the users, but miners prioritize the highest fees, which vary as a function of the number of transactions in the queue.

The organisation of miners into "**pools**"[13] creates a risk that an organised majority controls the validation of new blocks. User trust in the system is a shared goal among miners, intending to guarantee respect of the rules, along with the idea of an invisible hand protecting private interests. It is important to highlight however that four pools, 3 of which are Chinese, rely on massive mining farms control more than 60 % of the necessary processing power required for Bitcoin's blockchain and can use this dominant position against the interests of other users.

Bitcoin mining pools



Source : Blockchain.info (5-9 april 2018)

Consensus methods other than "proof of work" exist and are often more centralised[14] : the main alternative, which presents a greater risk of malicious use[15], is "**proof of stake**", based on ownership of the specific cryptocurrencies, which is divided into several methods such as "**proof of hold**", based on the time you've held the token, "**proof of use**" based on the quantity of

transactions, and "**proof of importance**" based on reputation.

Two other methods, that are less used but should be mentioned, are: "**proof of space**" based on the amount of storage space available and "**proof of burn**", regarding the destruction of cryptoassets, in order to obtain the trust of the network.

Reforming the *blockchain* : *hard* and *soft forks*

It is possible to modify the rules governing a blockchain, which we refer to as a *fork*. This means that a modification of the programming code must be updated by the entire network. Any individual can propose modifications but they generally originate from few developers (a group of around 40 in the case of Bitcoin). There are two types of evolutions: "soft forks", when blocks produced by the new version can be added to nodes functioning under the old version, and "hard forks", where no backwards compatibility is possible. When they are not unanimously adopted, hard forks can result in alternative versions of the original blockchain. In 2017, Bitcoin Cash and Bitcoin Gold were born from hard forks of Bitcoin. A hard fork also allow you to rollback transactions to a previous state of the specific blockchain allowing you to cancel specific transactions.

The challenge of scalability

The **ability to handle growth in the amount of transactions** is one of the key challenges for blockchain, starting with Bitcoin. Up until 2017, Bitcoin was only capable of on average 4 transactions per second (20 in 2018). This challenge of scalability is still a problem. It contributed to the rise of other cryptocurrencies, more than 1500 as of this report, often referred to as "*altcoins*". It also encouraged further innovation, still fairly young technologically, such as parallel blockchains with different but complementary functions ("sidechains" for Bitcoin, "sharding" or "plasma chains" for Ethereum), leveraging databases linked to the blockchain ("side databases") or the creation of a new protocol layer, lighter and faster, on top of the blockchain but benefitting from its security ("lightning networks" for Bitcoin, "state channels" for Ethereum).

Other applications for the blockchain ?

The role of the blockchain as the **underlying technology of multiple cryptocurrencies** is a predominant use case. However, these protocols **can be applied to numerous sectors** creating diverse new applications, outside of the specific context of finance: for example, civil licensing and certification, land/title registry, notarization as well as protection of intellectual property. Few applications, however, have managed to marry strong use cases with a mature technological solution. Ethereum provides an infrastructure adapted to these tools in the form of smart contracts written into the blockchain that execute autonomously, decentralized applications called "dapps"[16] as well as Decentralized Autonomous Organizations or "DAO"[17].

Programming the *blockchain* : *smart contracts*

Smart Contracts are programs written into the blockchain. In reality, it is possible to add programming code in the same way as transaction data. These are not contracts in the legal sense, but programming code that verify or execute a contract during its negotiation or application. Compared to typical programs, smart contracts have the advantages specific to the blockchain. Also, their execution is irreparable and their code is freely verifiable by the different network nodes. Notably, this allows the verifiability of escrow funds. Implementation requires certain preliminary steps, notably more profound verification processes, given the immutable or unchangeable nature of the ledger, as well as the development of a programming language adapted to the limitations of size/quantity of data unique to a distributed network. Also, the execution of most proposed use cases, is conditional on the import and export of information. Whether it is to measure temperature, deliver a package, verify that work has been realized, or provide the arrival time of an airplane, a third party source, called an oracle in the Ethereum ecosystem, must create the link between the blockchain and the rest of the world, which returns us to an idea of "trusted third party".

The difference between open or public blockchains and closed or private blockchains

The difference between **public** and **private** blockchains is not based on blockchains for public entities (like government administrations) and blockchains for private entities (like companies or NGOs) but rather on the open or closed character of the blockchain. The blockchain protocols can be described as either open to writing and reading information without restriction or that either one of those activities requires third party authorisation. We refer to **open blockchains** as **permissionless** and **closed blockchains** as **permissioned** or again as public or private blockchains.

Blockchains with unrestricted access are the more well-known, supporting Bitcoin and Ethereum, for example. As previously seen, anyone can become a node and these networks require consensus.

There are a large number of protocols with **limited access**, several fairly advanced and already operational. Among those, "*consortium*" blockchains regroup multiple independent organisations, even competitors,

using the blockchain to archive secure transactions into a decentralised ledger or share certified documents, without needing a trusted intermediary. Other protocols can be used in the same organisation to simplify or automate sharing certified documents and communication. In a private blockchain, a regulatory authority authorises new members and manages read/write access. This authority may act on its own or be governed by the various participants. Compared to a public blockchain, private blockchains can operate by simple majority. It only takes 3 participants to operate a private blockchain whereas it can take thousands for a public blockchain.

A debate exists whether private blockchains are "*real*" or "*false*", given that usage of the term "blockchain" has become a **marketing gimmick**. Applying blockchain technology to many applications is not always justified, given that many database solutions with shared, secure functionality could suffice, and also given that alternative technologies to distributed ledgers are under development: *hashgraph*, *tangle* or *directed acyclic graph* (DAG).

The success of certain fundraisings specific to the cryptocurrency ecosystem (Initial Coin Offering or ICO) are also questionable. These creations of digital assets (called tokens), exchangeable for cryptocurrencies represented more than $3 billion in 2017, which may appear rather irrational given that they offer no guarantee to investors.

A more comprehensive and detached approach seems necessary given the passing fad specific to entrepreneurial ecosystems. This kind of popularity or "**bandwagon**" approach can be seen in other disruptive technologies, such as artificial intelligence, big data, cloud, IoT, as well as the blockchain, and are often more about clever marketing strategy than actually the significant innovation and disruption that they promote.

Energy and environmental considerations

Besides the questions of scalability, security, financial regulation and legal framework, blockchains also represent significant energy and environmental impact. The electrical needs that proof of work creates for the blockchain are considerable.

Their estimation is subject to debate but energy consumption just for Bitcoin is at least **24 TWh/year**[18].This energy expenditure being directly linked to the financial interest for miners, it has scaled exponentially[19]. Given this rapid growth, the reduction every four years by half for mining fees (called halving)[20] seems insufficient in assuring fair competition. Increased processing power or the use of surplus energy production do not decrease energy consumption. In reality, mining profit/interest is a function of hedging these costs.

The impact in terms of greenhouse gas emissions is even more significant given that the majority of mining pools are in China, the country with the highest carbon emissions level in the world[21]. Research needs to solve **blockchain's energy consumption challenge**, for example the French program BART[22] (« Blockchain Advanced Research & Technologies »), which should allow the blockchain to use less energy, applying strong consensus methods leveraging advanced cryptography, while at the same time developing new frameworks providing increased reliability and scalability.

OPECST Office websites:

http://www.assemblee-nationale.fr/commissions/opecst-index.asp

http://www.senat.fr/opecst

Endnotes

[1] Cryptocurrencies are not legal tender, are not regulated by a central bank and are not created by historical financial establishments. The European Central Bank defines three types: video game tokens (limited to gaming for internal trading), those using a unidirectional flow (purchased using real currency but cannot be converted back to the original currency), and those with bidirectional flow such as cryptocurrencies like Bitcoin (able to be converted with real currency in both directions).

[2] Further understanding of the history and functionality of these technologies can be learned from the following texts: : Don and Alex Tapscott « Blockchain Revolution » Penguin Random House ; « La Blockchain décryptée – les clefs d'une révolution » Blockchain France ; Jacques Favier and Adli Takkal-Bataille « Bitcoin » CNRS edition ; Laurent Leloup « Blockchain : La révolution de la confiance » Eyrolles ; Stéphane Loignon « Big Bang Blockchain » Tallandier ; « Bitcoin et Blockchain : vers un nouveau paradigme de la confiance numérique ? » Revue Banque edition ; IEEE Spectrum « Blockchain World », IEEE ; « Comprendre la blockchain » éditions Uchange ; National Institute of Standards and Technology « Blockchain Technology Overview » U.S Department of Commerce ; Andreas Antonopoulos « Mastering Bitcoin : programming the open blockchain » O'Reilly, available in French at this link. The following websites can also be referenced : www.bitcoin.org https://bitcoin.info www.coindesk.com https://cointelegraph.com https://blockchainfrance.net https://blockchainpartner.fr et https://journalducoin.com. TA-SWISS, the Swiss Centre for Technology Assessment, member of the EPTA network, will soon be publishing its blockchain study.

[3] The portmanteau "cypherpunk" invented by Jude Milhon, is the combination of the word cypher and "cyberpunk", it itself a combination of the words cybernetic and punk in reference to the technologies of dystopic science fiction novels. Tim May published the "Crypto Anarchist Manifesto" in 1992 and Eric Hughes followed in 1993 with his "A Cypherpunk's Manifesto".

[4] The first proofs of work appeared in 1992 through the work of Cynthia Work and Moni Naor.

[5] The technical solution to these network failures solves the Byzantine General's Problem, cf. Leslie Lamport, Robert Shostak et Marshall Pease « The Byzantine Generals Problem », ACM transactions on programming languages and systems, vol.4, n° 3, juillet 1982.

[6] Satoshi Nakamoto is the pseudonym of the founders of bitcoin and the first blockchain. He named Gabin Andresen, CTO of the Blockchain Foundation, as his successor. The functionality of this cryptocurrency and the blockchain were explained in the foundational article published on the Internet in 2008 « Bitcoin: A Peer-to-Peer Electronic Cash System » (traduction in french).

[7] In 1991, Stuart Haber and W. Scott Stornetta were the first to propose a time-stamped blockchain: article link.

[8] Hash trees were invented by Ralph Merkle by 1979, also called « Merkle Trees ». In the case of Bitcoin, they allow the creation of a hash for the entire group of transactions in a block, called a root or top hash (Merkle Root). The hash of this block is a combination of the hash of its transactions and the hash of the previous block.

[9] So while it is relatively simple to produce a hash for a selection of data, it is relatively impossible to reconstruct the original data from a hash given today's computational resources. This function is « one-way » because while the first calculation is easy, the reverse calculation is realistically impossible. In reality there are 2^{256} different possible hashes.

[10] A "Sybil" attack is based on multiple forged identities which can permit certain users to have disproportionate influence on a network. Preventing these attacks relies on verifying new user creation (validating an identity by email for example) or in the absence of a control authority, creating complex computational calculations in the case of Bitcoin.

[11] We are referring to a "trust machine" like the title article for the October 2015 The Economist. This special edition on the blockchain helped it to escape the world of specialists and gain credibility in front of a mass audience, particularly in front of economic actors. The subtitle of this cover story "The technology behind bitcoin could transform how the economy works" hinted at the disruptive potential of the blockchain.

[12] Proof of work is an iterative, random calculation, such that its solution can take more or less time, but its difficulty can be adjusted in a way that the average solution time conforms to a given duration. For Bitcoin, this is 10 minutes, its difficulty being adjusted every 2016 blocks, around every 14 days. The difficulty of the hashing algorithms should progress at the same rate as the evolution of computational power.

[13] Participation in a pool guarantees more consistent revenue for miners. There are three main mining pools maintained in France: Big Block Data, Wizard Mining and Just Mining.

[14] The cryptocurrency peercoin mixes proof of work and proof of stake, meaning that it adapts the mining difficulty as a function of the amount of cryptocurrency that each miner possesses. The cryptocurrency nem uses a proof of importance and Ethereum would like to focus on proof of stake but the transition from proof of work has been difficult to achieve over the last two years: its blockchain is still based on proof of work. Tezos is another project that aims to use proof of stake.

[15] Stronger solutions are under development. Silvio Micali, winner of the 2012 Turing Prize, has proposed and mathematically validated Algorand which can function properly even with a third of its nodes being malicious.

[16] Decentralized applications, which are in reality distributed, function due to programs written into the blockchain. Their usage still requires, however, third party intervention.

[17] DAO are organisations where the governing rules and procedures are written on the blockchain.

[18] Among the proposed estimations in April 2018 for the mining of the sole Bitcoin, Bloomberg suggests 20 TWh/year, Digiconomist, 60 TWh/year and Morgan Stanley, 140 TWh/year. A base estimate can be obtained by analysing the highest performing mining machine, the Antminer S9 (13,5*1012 hashs/s for an energy consumption of 1 323 W) and the total number of hash colocations (28*1018 hashs/s) for Bitcoin on April 4 2018. This suggests 2 million machines, for a total energy consumption of 2,7 GW, which gives 24 TWh per year.

[19] The Bitcoin Energy Consumption Index gives a 30 % increase in energy consumption for the month of March 2018. Digiconomist's day by day estimation : link. Karl J. O'Dwyer and David Malone showed, in this 2014 study, that the energy consumption of the network for Bitcoin between 0,1 and 10 GW of electrical power and that it is probably similar to the energy consumption of a country like Ireland (around 3 GW).

[20] Nakamoto's protocol provides that the Bitcoin reward for each minor validating a block should be divided by 2 every 210 000 blocks, which is around 4 years. It represented 50 bitcoins in 2012, then 25 in 2016, now 12.5 and will become 6.25 in 2020. It is distributed 100 blocks after validation.

[21] According to GIEC, China represents the highest carbon output in the world, with 1 050 grams of CO_2 per kWh of electricity produced.

[22] This initiative combines INRIA, Télécom ParisSud, Télécom ParisTech and SystemX.

List of scientific experts consulted

Mr Gérard BERRY, professor at Collège de France, member of the OPECST's scientific board

Mrs Emmanuelle ANCEAUME, responsible for IT research at the Institut de recherche en informatique et systèmes aléatoires (Irisa/CNRS/INRIA/IMT Atlantique/ENS Rennes/INSA Rennes/CentraleSupelec/Université de Bretagne Sud/Université de Rennes 1)

Mr Daniel AUGOT, research director at INRIA

Mrs Claire BALVA, president of *Blockchain* France and *Blockchain* Partner

Mr Nicolas COURTOIS, IT professor at University College London (UCL)

Mr Jean-Paul DELAHAYE, IT professor emeritus at Université Lille I (Centre de recherche en informatique, signal et automatique de Lille/CRISTAL)

Mr Gilles FEDAK, researcher at INRIA and president of iExec

Mr Georg FUCHSBAUER, researcher at École normale supérieure de Paris and at INRIA

Mr Fabrice LE FESSANT, researcher at INRIA and founder of OCamlPro, Move&Play and CleverScale

Mr Renaud LIFCHITZ, consultant and researcher in IT security and cryptography

Mr Gérard MEMMI, IT department director at Télécom ParisTech

Mr Ricardo PEREZ-MARCO, Mathematics research director (CNRS/Université Paris Diderot)

Mr Simon POLROT, lawyer, founder of Ethereum France and of VariabL

Mr Pierre PORTHAUX, president of *Blockchain* Solutions and of EmergenceLab

Mr Manuel VALENTE, director of La Maison du Bitcoin