A blockchain is a distributed ledger technology

This article is complementary to the research "**Blockchain technology and the Canadian media industry**", a project undertaken by Telefilm Canada, the Canada Media Fund, and Badel Media, in collaboration with the Pôle médias HEC Montréal.

Published on May 2, 2019
10 minutes of reading

Defining the blockchain

Defining the blockchain in a simple way is never easy and each subject specialist will approach it in a different way and in a different context. But to sum it up, some fundamentals have to be presented. It is often they that allow the reader to visualize the applications and the scope of this technology.

Let's say right now that the blockchain consists of computer protocols, mostly open source, and is part of the Distributed Ledger Technologies (DLT) family. Ledgers have historically been records of information about transactions, usually the transfer of an asset, its use or its ownership from one person or organization to another. Their computer version, a DLT, is not a new concept and several approaches and technologies emerge, complementary or competing with each other.

What particularly distinguishes the blockchain from the other DLTs is the notion of **consensus**. In other words, the establishment of a mechanism from a set of rules accepted by network participants, and necessary for its proper functioning. Let's stress again that **distribution is at the heart of the blockchain**: distribution of information, processes, roles and responsibilities, in a common vision, a common goal. Consensus is the essential element at the base of the governance of a decentralized system that wants to no longer be based on a central supervisory authority.

Key features

If we decide to limit the description to its simplest, we can define the blockchain as a database. A database that has the particularity of being distributed, that is to say, in a way, replicated and synchronized on the different computer nodes of a network.

This distribution has the following benefits:

- Greater **transparency** of data, through the multiplication of access points; which facilitates their authentication but especially their follow-up, ie their **traceability**;
- **Immutability** of these data: already secured by the cryptography techniques used on a blockchain, the data entered into a distributed ledger will be all the more immutable as each "copy" of this register must be consistent with the others.

Basic uses of the blockchain

All applications of the blockchain relate to at least one of these four uses:

- The **cadastre**, or the chronological register of transactions between authenticated entities;
- The **transfer of value** that induces disintermediation as a potential impact;
- **Automation**, via smart contracts, or coded contracts, which have the benefit of greater efficiency of administrative and business processes;
- **Digitization of assets** with the promise of creating new forms of values and business models.

As part of this introduction to the basic operation of technology, we focus on the first two points: **cadastre** and **value transfer**.

Basic elements of operation

It should also be noted that the operation described primarily concerns public blockchains of the bitcoin blockchain type. Private and hybrid or consortium blockchains (eg linked to an organization or business sector) will have types of consensus that are not generally based on the same principles. They will therefore be much less "decentralized" in the true sense of the term because these blockchains are more about distributing roles and processes, increasing traceability and efficiency, establishing new types of relationships between stakeholders, with a common goal of responding to a sectoral issue.

Let's summarize here the basic elements of public blockchains:

- Data is encrypted and "sealed" in blocks, once a validation and authentication process is completed via the consensus mechanism accepted by network members. This mechanism is also based on cryptography principles. For the bitcoin blockchain (started in January 2009 and the first business application of blockchain technology), this consensus is called Proof-of-Work.

- The blocks are connected to each other by a unique identifier. In the end, these interconnected blocks constitute a chain. The longer a chain is, the more it becomes secure and resistant to modification. Attempting to modify the data in a block would amount to compromising the integrity of the chain itself. Any modification is traceable and the possibility doubtful, given the lack of equivalency between data in the affected block and that of the other blocks in the chain.

- A Blockchain is theoretically unalterable because taking control of one involves taking control of 51% of a network’s nodes. Once again using Bitcoin as an example, this type of action would require extremely powerful computing resources, therefore making it difficult to hack such a system. Despite the environmental impacts (electricity consumption, etc.), it is this requirement for computing resources that ensures the system’s reliability.

Consensus, governance, and trust

Distributed ledger technology introduces a type of collective accounting, which is theoretically verifiable by anyone in real-time. Given the absence of a central control authority, the system itself, with its decentralization and its consensus mechanism, becomes the **trust** protocol between participants, which is certainly its greatest innovation from a technological and **governance** perspective.

Mining is the centerpiece of the system's confidence. This mining operation, characterized by computer resources that are made available to a network through incentives and compensation, allows the verification of new transactions and records them in the register following approval by the consensus protocol in place in the network. For example, the Bitcoin blockchain confirms transactions following a competitive resolution mechanism involving mathematical calculations therefore known as Proof-of-work.

Mining based on Proof-of-work

Every computer connected to a blockchain can, in theory, become a "miner". This is because, in principle, mining (in its current form as proof of work) requires ever greater computer resources. Generally speaking, these resources are of the ASIC type (Application-Specific Integrated Circuit), in other words, systems developed for a specific application.

In this function, the miners choose a group of transactions from a pool of all the transactions awaiting verification by the network. The rewards granted to miners in exchange for processing play an important role in determining the choice and therefore the priority of the transactions to process. This is because the economy of mining is based logically on creating a net profit in each operation (compensation for transaction processing versus the cost of computing resources).

Bitcoin's miners are compensated through a combination of newly issued virtual currencies and transaction fees or commissions. As an illustration of this idea, at the moment, the first miner to solve the mathematical problem related to the verification of a block of transactions that are ready to be approved is rewarded, with 12.5 new bitcoins.

This can extend to the number of bitcoins that are or will be injected into the network, up to a maximum of 21 million (at the end of August 2018, a little more than 17 million were in circulation and the last bitcoin should be issued around the year 2141, or 132 years after its creation). This is based on a rate that decreases sufficiently over a long enough period of time to attain 21 million, where the "extraction process" also becomes the essential activity behind the issuing of new bitcoins.

Inside a block

The competitive process of the Bitcoin blockchain is configured in such a way that every 10 minutes a new block is formed. To respect this rate, the calculation to be performed is subject to an adaptable level of difficulty that depends on the calculating power of the entire network. Additionally, the rate can vary completely, depending on the consensus protocol used by a blockchain other than that used by Bitcoin.

But before another block can be created two steps must occur:

1) The miners must first **solve a specific mathematical problem**: a cryptographic hashing function that seeks to randomly identify a value (a nonce) whose juxtaposition with the data of a previous block produces a *hash*, which must be under a certain threshold (the mathematical problem to be solved). Put simply, this hash is also the unique digital signature of a block and is a unique string of characters (256 in the Bitcoin blockchain). When data in a block changes, a new hash is generated. Hence, a problem of correspondence that can be easily detected over a decentralized network whose nodes possess the same number of copies of the ledger. The hash is a sort of

fixed-size, standardized image that makes it practically impossible to find an output value based on an input value. Therefore, the original block of a chain cannot be modified. Unchanging, this initial block is known as the *genesis* block.

2) Once a miner has solved the problem, it must **broadcast the block to all of the other computers in the network who then verify it.** Only blocks containing unanimously approved transactions are added to the chain. Blocks (of a variable maximum size, but for example no larger than 1 MB in the Bitcoin blockchain) are integrated into a chain in chronological order. Every approved and broadcast block is characterized by its signature (*Hash*), its *Timestamp*, and a data field describing the transactions. The immutability of a blockchain is supported by the fact that it is copied in its entirety to the nodes on the network (the total size of the Bitcoin blockchain at the end of August 2018 was approximately 180 GB).