Fabien Le Bronnec is a software developer currently graduating with a Master's degree. He works for ComptaCom, an accounting company sets in Laval. His memoir, entitled "The blockchain beyond crypto-currencies", was produced for the "Institut d'Informatique Appliquée" of Laval in June 2018.

Blockchains, beyond Crypto-currencies

Since the creation of Bitcoin by a mysterious Satoshi Nakamoto in 2008, the blockchain technology has been much talked about. To many, blockchain is little more than a "buzz word" tied to the financial frenzy surrounding crypto-currencies. But as a matter of fact, crypto-currencies are more of a side effect of the blockchain technology than a finality. Furthermore, everyone talks about blockchain, but not many understand really what it is and what it can do.

The study was meant to explore these two problematics. In its first part, it did aim to provide a technical explanation and description on how a blockchain works. This technical description was run through the study of technical articles on the Internet, generally aimed at developers and engineers. Blockchain being a quite complex aggregation of technologies, it was broken down in smaller, simpler concepts in order to ease the reader comprehension.

The second part was about what can be achieved through blockchain technology. It was conducted by exploring news articles and specialized blogs. The different identified uses of the blockchain were then ordered in a classification. Each use case was then illustrated by real life examples.

A blockchain is first and foremost a distributed database which provides mechanisms to ensure it cannot be forged. It gets its name from the fact that it is at its core a chain of linked blocks of data. The main interest of the blockchain is that it offers an innovative solution to the age-long problem of the "byzantine generals", in which the different nodes of a network cannot trust each other. The idea is to use a *consensus method* shared by all the network nodes, so that each one of them can, at any time, verify the coherency and validity of all the data in the base. This verification is actually very fast and easy, that is because the complexity lies in adding data - a new block - to the chain.

A node of the network which adds data to it is called a *miner.* In order to add a new block to the chain, a miner has to resolve a complex computing problem called the *proof of work.* All miners are in competition with each other, as each time a miner adds a block to the chain, every other one must start the problem over. This fact added to the high energy consumption required for the problem resolution resulted in the creation of another consensus method, the *proof of participation* or *proof of stake*. In short, it is a way to ensure that miners have too much to loose to try to sabotage the chain. The logic behind it is much more complex than the logic behind the proof of work, but also much simpler to compute, and thus way more efficient.

The main use case is obviously crypto-currencies, as both came to existence together with Bitcoin and as such it has to be discussed. The crypto-currency has to be though before all as an

incentive for the miner to participate in the chain. When a node successfully adds a node to the chain, it is rewarded by an amount of money. This money can freely be given by a user to another. In its simpler form, the database part of such a blockchain essentially acts as an unforgeable registry of the transactions. Bitcoin always aimed to be nothing but a proof of concept of the blockchain, and the speculative madness surrounding it is nothing but a side effect.

But going further, there are many possible use cases. Each and every one of them rely on the three main concepts offered by the blockchain : tamper-proof, distributivity and automation.

A blockchain being a program, it is well possible to feed it with scripts which it is able to execute. In its simpler form, such a script has one or more conditions which trigger its execution. The benefit of the blockchain is that said conditions being part of itself cannot be faked, no more than the result of the execution. This concept is called *smart-contracts* and it could be used to automatize as diverse things as triggering assurance policies execution or resolve bets without the need of a third party – in our cases an expert or a bookmaker.

Another major use case is to help prevent fraud and improve traceability, for example by saving every step of the life of a product in a blockchain. Producers, distributors and even customers could verify at any time that said good is genuine. For governments, it would offer a way to simply assert that the product complies with legal requirements. Such projects are already in use to fight fraud in food or financial industries.

Despite existing for 10 years, blockchain remains quite a recent concept. Many observers herald that it will revolutionize the information technologies, and even our day-by-day life, but this revolution obviously has yet to come and crypto-currencies are nothing but the tip of the iceberg. As a matter of fact, world governments do not seem to be eager to lose their control on currencies and financial transaction and it seems hard to know if we will get to pay our rent or taxes in crypto-currency in a near future.

But I think we are going to see emerging many projects in the years to come that use blockchain as a mean rather than an end. The worldwide renewed exigence for decentralization, transparency and security offers many opportunities in which blockchain could reveal a precious tool. Most of these projects are going to be made at two extremities of companies spectrum. Either by small startups, which are going to “bet” on the concept, or by big players - like banks or governments – who have the meanings and the capacity to build the new standards of tomorrow.