CEST
Centro de Estudos Sociedade e Tecnologia
USP
Universidade de São Paulo
Bulletin - Volume 2, Number 4, October/2017

Blockchain: trust through algorithms

Lucas Lago

Most people have probably heard or read about Bitcoin, the most famous cryptocurrency among others, like Ethereum, Litecoin and Nxt. However, fewer people have heard of blockchain, a technology proposed in 1991, which became more widely known together with Bitcoin in 2008, and was very important for its success; as the technology is not usually the focus of the unspecialized media, only the cryptocoins.

While the digital currency gained notoriety, especially because of the evolution of its value in relation to the US Dollar, several implementations were proposed using the blockchain, displaying the flexibility of this technology. The technology was developed from the need of keeping an integral registry of all transactions done in the Bitcoin market.

> Several problems both in the government and private sectors can be solved with implementations based on the blockchain protocol.

To achieve this, this Blockchain was developed as a ledger for the Bitcoin market, registering the most recently made transactions in a process that can be summarized in the following steps:

1. Every transaction in the last couple minutes are grouped in a set called a block;
2. This block is distributed through the blockchain network;
3. Some users on the network, use their computers to validate the block, and are rewarded for their success. These users are called miners;
4. The validated block receives a temporal tag and is added in the end of the chain.

Since all transactions are publicly available, any amount of money can have its origin traced up to the moment it was added in the ledger, guaranteeing transparency in the process. The open and decentralized nature of the blockchain is used to provide trust to the transactions, eliminating the need for intermediaries.

To guarantee the integrity of a single block the blockchain protocol uses a mathematical technique called cryptographic hash: a simple hash function transforms variable length data into fixed length data; the cryptographic hash function executes the same transformation in an unidirectional way. The processing power necessary to revert a hash function and find details of the original information is largely superior than the processing power necessary to execute the hash function.

A hash function can transform any information in a sequence of letters and numbers that looks random. Each new block in the blockchain uses the information from the block index, the hash of the previous block, the data of the block, the date and time, and one extra number called "nonce" as an input to the hash function.

In case the hash generated using this "nonce" obeys the rules of the blockchain, the block is accepted as valid and transmitted through the network; in case the hash does not obey the rules, the "nonce" is altered for a new number and a new hash is calculated. This process is repeated until the computer finds one "nonce" value capable of creating a hash that obeys the rules of the blockchain. This process is called mining.

To create the hash of a new block, we use the hash of the previous block so this process is not able to create blocks that are not part of the chain.

One of the fundamental characteristics of the cryptographic hash functions is that there are very few entries that would generate the exact same hash. With this, from the moment a block is validated and inserted in the blockchain, it is very costly to create a second block with small modifications that would be also a valid block. With this guarantee, the chain becomes practically immutable. And this immutability is the characteristic that allows developers to create new digital applications in areas where this was not recommended, due to the risk of manipulation of data in digital registries.

Several problems both in the government and private sectors can be solved with implementations based on the blockchain protocol, because this technology can change several aspects of society from contracts to how our health records is stored.

In the music industry, as an example, artists like Imogen Heap are creating their own environment based on blockchain: the Mycelia. The idea of the artist is to create an environment where musicians have more control of their music and also are capable of receiving their fees without the interference of intermediaries.

In the government sector, there are several examples of the use of blockchains in several solutions. Sweden and Estonia both have interesting cases using blockchain for distinctive ends.

Since July 2016, Sweden is developing a land registry based on a distributed database. The idea is that the blockchain will be maintained by the registry authority, the Lantmäteriet, and will be replicated in banks, real estate companies, buyers and vendors, in a way that all the necessary information is accessible and secure for everyone involved in a real estate transaction. The swede solution is still being tested. But, with the possibility of saving hundreds of millions of dollars this technology will probably be rolled out soon.

Estonia, that has the use of technology as a motto for the country, has a project that is using blockchain in its national health system. Health related data from every Estonian citizen are already stored online, but not on a distributed blockchain platform. If successful, this new implementation will give more autonomy to the citizen, since he owns his medical data and can rest assured that information will be treated securely and privately, and stored in a trustworthy way in the blockchain.

With the technology available in Brazil nowadays, there is a need to trust institutions to guarantee the validity of information: registry officers guarantee the fact that marriages were celebrated; land registry officers guarantee the ownership of land and homes. This registries are stored in books that “guarantee” the impossibility of being manipulated.

There has always been a fear that in an Orwellian future data could be altered, manipulated or deleted by those in power, and this was even before the advent of digital storage of data - that in a way facilitates altering and substituting information. With the migration of this information to blockchains it will become significantly harder for people, like Winston Smith, to manipulate important information, and will do that without losing the speed and efficiency brought by storing these data digitally.

Lucas Lago *is a PhD student in Computer Engineering at Escola Politécnica da Universidade de São Paulo, and researcher at CEST-USP.*

Coordinator: Edison Spina

This article is a result from the author’s ascertainment and analysis, without compulsorily reflecting CEST’s opinion.