INFO-F-514 - Conference Report #2
Blockchain

Université Libre de Bruxelles

Hakim Boulahya

June 10, 2018

Blockchain is a technology that allow to decentralize an system to avoid using a thrusted third-party, such as a bank. The blockchain technology was first introduced by Satoshi Nakamoto [**?**] within the framework of the Bitcoin blockchain, a decentralized network that allow to exchange coins in form of transactions.

The different techniques first presented in [**?**], are a combination of different cryptographic functions that allow this massive scale decentralization. The goal is to make sure that a transaction that is acknowledge by the network, can be thrusted where no users can be thrusted. The different cryptographic protocols used allow to insure the will of a user to send his coins, avoid double-spending and insure that nobody in the network can change any past transactions.

Let's summarize the Bitcoin protocol. A coin is represented by a sequence of transactions. When Alice wants to send Bob a coin, she musts signed a SHA-256 hash, using the ECSDA digital signature algorithm, composed of the last transaction of the coin and the one that she wants to create. This new transaction will be send to the decentralized network, usually a peer-to-peer network. Miners in the network will provide a computational work called proof-of-work. The goal of the proof-of-work is to mint a block, a file containing multiple transactions, using a cost-function of the hashcash [**?**] (the proof-of-work) algorithm. A cost-function should be easy to verify but hard to compute. This mechanism allow to create a Blockchain, that can be seen as a linked list of blocks, where the proof-of-work make it hard to edit the blockchain because each added block is linked to the previous on in the blockchain.

One problem that arise using this protocol is the scalability problem. Because the number of transactions per block is fixed (the block creation frequency is also fixed) and the proof-of-work takes time, the amount of transactions that the bitcoin decentralized network can process is limited.

The debit of transaction is a major concern of large scale entreprise. In order to be able to use blockchain technology for different applications, such as banking, real estate, energy and others industry, it is important to be able to process multiple transactions concurrently. What has been proposed during the conference is the Fast Access Blockchain. A *public blockchain which overcomes the scalability challenge*. The challenge is stated as following: keeping the characteristics of a blockchain that is, permissionless, decentralized and open, and allowing multiple transactions to be acknowledge at the same time.

FAB Overview

References