Assessment of the Blockchain Technology

Viktoria Plemakova
Institute of Computer Science
University of Tartu
viktoria.plemakova@ut.ee

***Abstract*—The concept of the blockchain technology as a distributed database of digital events became popular due to the invention of Bitcoin. Although the blockchain technology supports a number of other cryptocurrencies it can be used in numerous other fields. This paper intends to give and overview of the technology and implementation possibilities.**

I. Introduction

A blockchain can be described as a distributed ledger or a database of digital events, such as transactions, that is shared among a number of participants in the network. It consists of blocks that are the records of past events, and chains are formed by connecting several blocks in chronological order. New blocks are added only if a consensus is reached by the majority of the blockchain network participants.

The blockchain technology first emerged with the invention of Bitcoin [1]. Bitcoin is a virtual currency as well as a peer-to-peer system that was first introduced in the whitepaper "Bitcoin: A Peer-to-Peer Electronic Cash System" in 2008. The paper introduced a peer-to-peer system to perform online payments without an intermediary, i.e. a bank. The name of the paper's author – Satoshi Nakamoto – is considered an alias and the real inventor or a group of inventors remains unknown.

The implementation of Bitcoin was released as an open-source project in the beginning of 2009. The beginning of the Bitcoin blockchain was a block of 50 coins which is also known as the genesis block. A few days later the first ever Bitcoin transaction took place between Satoshi Nakamoto and Hal Finney [2].

II. Technology

This section gives an overview of the technical part of the blockchain.

A. Data Distribution

A blockchain is distributed across multiple computers in the network. Communication between these computers is performed using the peer-to-peer model, meaning that there is no need for a central server [3]. Each node in the network contains a copy of the entire blockchain. This also means that whenever new transactions happen, every node in the network should be notified. After receiving unconfirmed transactions, any node can pack them into a single block and broadcasts the block to other nodes for verification.

B. Structure of a Block and its Identification

Each block in the blockchain consists of a header and the contents of the block. The content part of the block is made up of a list of transactions that happened at the same time whereas the header of the block contains at least:

- some technical information about the transactions
- a reference to the parent block
- timestamp of the block creation and proof-of-work.

Each block contains a hash of its predecessor in the header to reference the previous block. Thus referring to previous blocks by using hashes creates a chain of blocks as seen in Figure 1.

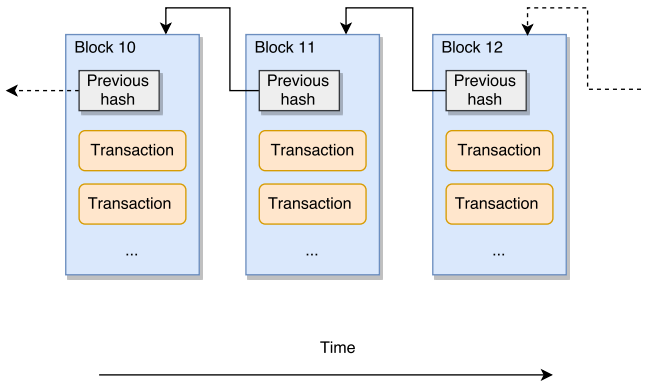

Fig. 1. Blocks are linked by the hash of the previous block

Each block in the blockchain can be identified by its block hash which is the hash of its header. For example, in Bitcoin the block hash is obtained by hashing the block header twice using the SHA256 algorithm. The block height is another way to identify a block. It refers to the block's position in the blockchain. The height of the genesis block is always 0 and every new block is placed one position higher than the previous one. The downside of the block height is that it is not a unique identifier since several blocks might want to claim the same position. [4]

C. Verification Process

Before the blockchain is updated, every new transaction needs to be verified. Unverified transactions are sent in a single block to all nodes. Since there is no trusted intermediary party, then the verification is performed by a consensus of the majority of the participating nodes. The consensus is reached only if all the transactions in the block and the block itself are

found valid. Therefore, if somebody would try to submit an invalid transaction, then the consensus would not be reached. Accepted block is added to the end of the blockchain where it cannot be removed or changed.

Since every node can suggest to add its block to the existing chain, then there is a need for a method which helps to decide which one to add. The decision cannot be made by merely relying on the order of the blocks' arrival because blocks can reach nodes at different times. Thus one of the solutions is to require that valid blocks contain the proof-of-work which is also a method used by Bitcoin.

Proof-of work is an answer to some time consuming mathematical problem. The answer to the problem is usually difficult to produce but simple enough to be quickly verified by other participants. It should also meet certain requirements to be considered valid. The proof-of-work makes it less likely for multiple blocks to be generated and broadcast to all of the nodes at the same time.

D. Resolving Conflicts

However, it might occur that two or more blocks are created at the same time on different nodes [5]. In this situation there are multiple possible continuations of the blockchain. However, only one of those paths can continue the chain.

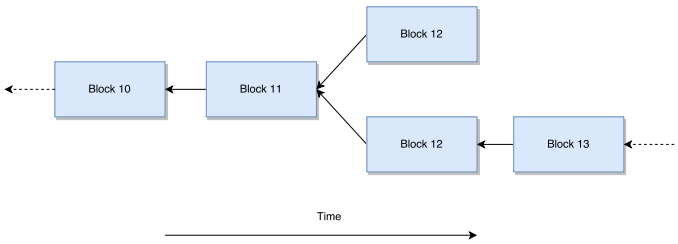

Fig. 2. Blockchain accepts the longest path [5]

Bitcoin solves this problem by using the longest chain rule [5]. Each node continues building the chain using the first block it receives which results in different branches in the blockchain. Whenever one of the possible paths becomes the longest, it is considered the valid one as seen in Figure 2. Non-active branches are dropped and every node switches to the longest one.

E. Security

The blockchain technology does not involve any trusted third party who would process every transaction. Therefore, there is a need to make sure that the transactions are secure when they are shared over the Internet. For protection the transactions have to be signed with a digital signature using the public key cryptography. The public key is used to check the signature of the transaction and the private key to sign it initially.

Blockchain is also considered immutable, meaning that once a block is added to the chain it cannot be removed or changed in any way [6]. One of the reasons that adds the security to the blockchain is the fact that it uses hashing. It is not that easy to derive the original data from the hash and even a little modification in the data would also change the hash. Thus changing the data of a block would also change its hash. This instantly makes all of the following blocks invalid. Since the blocks are linked by the hash of the previous block, the new hash of the block would not match the one that the next block had stored as its parent's hash.

If some node wanted to change a block in the past then it would also have to rebuild every following block, so that the hashes and linking would be right. Furthermore, producing proof-of-work for every following block would be extremely time consuming, especially if the tampered block is not one of the most recent ones. In case of multiple available paths in the blockchain if somebody would want to have their path accepted to the main chain they would have to first make a change in the block as well as make their path the longest due to the longest chain rule. However, this again means that the dishonest node should be able to compute the proof-of-work faster than the rest of the network.

III. Implementation

The main concern would be defining the properties of a block in the implementation. Blockchain as a technology became more known due to the popularity of Bitcoin which resulted in emergence of several other cryptocurrencies. However, blockchain can in fact be used for keeping other types of data instead of financial transactions. It can be applied in notarization processes, cloud storage services and even music industry to name a few [2].

Therefore, the content of the block depends on the needs of the developer or organization. Even though the content could be different for each implementation, the header of the block should definitely contain the previous block's hash. The header can include additional information depending on, for example, the choice of the proof-of-work function. In case of Bitcoin, the header contains a field called nonce which is important in solving the proof-of-work task.

In addition, adding new blocks to the chain is dependent on the consensus mechanism. The most popular method is the already mentioned proof-of-work. One of the alternatives is the proof-of-stake [7] which was first implemented by PeerCoin. While in case of proof-of-work a node has to spend a certain computational power to solve a problem, in case of proof-of-stake the node has to prove that it owns a certain amount of money (its stake). Node-to-Node, Practical Byzantine fault tolerance and a variety of other consensus algorithms are available and the choice depends on expectations towards security, performance etc. [8]

Blockchains can be both private (permissioned) and public (permissionless). In case of public blockchains such as Bitcoin everyone can join and make contributions to the chain as well as participate in the consensus process. Public blockchains are considered fully decentralized. Private blockchains might grant the read and write rights only to a few participants and might be used only internally by some organizations.

IV. Conclusion

This paper covered the technology behind the blockchain and what aspects need to be considered when implementing it. Blockchain is distributed across severals computer nodes who share transactions and blocks using the peer-to-peer model. A new block of data is added after the blockchain network reaches the consensus that the block is valid by checking the proof-of-work. Security is provided by using digital signatures and cryptographic hashes. The core of the blockchain implementation is deciding the block structure and the consensus mechanism since the blockchain can be used in different scenarios.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[2] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Applied Innovation*, p. 6, 2016.

[3] A. Lewis, *A Gentle Introduction To Blockchain Technology*. BraveNewCoin, 2015. [Online]. Available: http://bravenewcoin.com/assets/Reference-Papers/A-Gentle-Introduction/A-Gentle-Introduction-To-Blockchain-Technology-WEB.pdf

[4] A. Andreas, *Mastering Bitcoin*. O'Reilly, Media, 2014.

[5] Y. Brikman, "Bitcoin by analogy," 2014. [Online]. Available: http://www.ybrikman.com/writing/2014/04/24/bitcoin-by-analogy/

[6] A. Lewis, "A gentle introduction to immutability of blockchains," 2016. [Online]. Available: https://bitsonblocks.net/2016/02/29/a-gentle-introduction-to-immutability-of-blockchains/

[7] "Proof of stake." [Online]. Available: https://en.bitcoin.it/wiki/Proof_of_Stake

[8] S. Seibold and G. Samman, *Consensus Immutable agreement for the Internet of Value*, 1st ed., 2016. [Online]. Available: https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf