Available online at www.sciencedirect.com

ScienceDirect

IFAC PapersOnline CONFERENCE PAPER ARCHIVE

IFAC PapersOnLine 51-30 (2018) 693–696

# Implementation of directed acyclic graph in blockchain network to improve security and speed of transactions

**I.D. Kotilevets*, I.A. Ivanova**, I.O. Romanov***, S.G. Magomedov***, V.V. Nikonov***, S.A. Pavelev*****

**MIREA - Russian Technological University,*
*Moscow, Russian Federation (email: ikotilevets@gmail.com)*
***MIREA - Russian Technological University,*
*Moscow, Russian Federation (email: mgupirabota@bk.ru)*
****MIREA - Russian Technological University, Moscow, Russian Federation*

**Abstract:** The article describes the advantages provided by the implementation of a directed acyclic graph in the blockchain network. The advantages and known limitations of common blockchain networks are described. It is shown how directed acyclic graph allows increasing the speed of transactions between the network nodes and scaling the channel width due to the formation of parallel chains instead of the single true chain in common blockchain networks. Consequently, it is shown how blockchain network with directed acyclic graph also eliminates the concept of mining, allowing for transactions without the corresponding fees.



*Keywords:* blockchain; network; security; transactions; capacity; directed acyclic graph.

## 1. INTRODUCTION

One of the biggest problems today in the information technology is the problem of security. The number of cybercrime is growing, including those related to identification data theft. According to the analytical agency Cybersecurity Ventures, Morgan S. (2016), the annual damage from cybercrime will reach 6 trillion dollars by 2021.

To solve this problem, many companies began to use the blockchain, because this technology is able to protect data and make their audit more transparent.

Blockchain literally means "block chain". In other words, the blockchain is a log with data records. Under the data any kind of information can be implied. All information is combined into blocks, and then cryptographic blocks are linked into a chain using a set of mathematical algorithms, as described by Morozov D.M. (2016).

This technology can be used in absolutely different areas. From the distribution of multimedia (Paperchain - a decentralized tool for standardized collection, storage of metadata and exchange of this information between the various participants of the music industry), real estate (UBITQUITY - SaaS blockchain-platform for records of property and related property rights) to operations with goods and raw materials (Uphold - platform for moving, converting, making transactions and storing any form of money, goods or raw materials), data management (in company Factom identification blockchains are used to implement a database management system and data analysis in a variety of areas) and the organization of private and public administration (Advocate, a platform for improving the interaction of citizens with government representatives, aimed at helping both ordinary members of society and applicants for positions of managers in local government).

Blockchain-based systems prevent a range of different attacks.

### *1.1 Man-in-the-middle attacks*

Man-in-the-middle attacks correspond to a type of cryptographic attack in which an attacker can intercept messages and secretly replace them with different ones. This is quite real in modern data networks, where information from one user is transmitted to another through many intermediate nodes that are not controlled by these users. This type of attack and organization of secured data transfer to prevent it were discussed by Magomedov Sh. (2017).

In a blockchain-based system, this type of attack is almost impossible to implement. When a user publishes data to the blockchain, all nodes in the network also receive this information. Information is written to the block, and blockchain cryptography protects the integrity of the registry. Therefore, publishing fake data from the attackers will not work because the fake is immediately recognized.

### *1.2 The manipulation of data*

Not so long ago, hackers were able to compromise the site of the Linux Mint operating system and downloaded an infected version of the system with a built-in backdoor. Typically, developers provide hash amounts to allow users to verify a copy of the software, but in this case, hackers were able to publish the hash amounts of their version, so no one suspected of forgery. The problem of data manipulation was


10.1016/j.ifacol.2018.11.213

researched by Voit A. et al. (2017), Popov G. and Magomedov Sh. (2017).

However, user of a blockchain network can publish a hash associated with a single file, operating system image and other data that requires protection. In this case, if hackers get to the information and change it, they will not be able to correct the hash amount recorded in the blockchain.

### *1.3 DDoS-attack*

The primary purpose of DDoS is to limit the capacity of a network resource, such as a server or infrastructure that supports a particular company's site. Servers have certain limits of requests that are processed at the same time. If the number of calls to the server exceeds the capabilities of any infrastructure component, service level issues occur. And the scale of these problems depends on the purpose of DDoS-attacks.

Not so long ago, information security specialists from the company Recorded Future, Moriuchi P. and Chohan S. (2018), found that several organizations of the financial sector were exposed to one of the largest DDoS attacks of recent time.

Usage of blockchain technology abandons centralized DNS servers and implements a system in which name and IP-address pairs are registered in the blockchain network and distributed across all nodes. This will ensure transparency and security at the same time. As shown by Dickson B. (2017), hackers will not be able to target the whole infrastructure by attacking a single cluster.

### *1.4 Hacking Internet of Things devices*

According to a study by F5 Networks, Boddy S. and Shattuck J. (2017), the number of attacks on Internet of Things devices and infrastructure has increased by 280% since the beginning of 2017. For the most part, this is due to the spread of malware called Mirai. Hackers break into Internet of Things devices and use them to carry out DDoS attacks and host Trojan infrastructure. At the same time, researchers from the company Recorded Future, who discovered the largest DDoS-attack, claim that the botnet is formed from 13,000 devices of the Internet of Things. Meanwhile the criminals have changed the tactics of formation of botnets and are specifically looking for devices with known vulnerabilities.

The blockchain can help protect the Internet of Things for the same reasons it can help deal with Man-in-the-Middle attacks, data compromise and DDoS attacks - the legitimacy of information and a clear process of approving it.

However, blockchain is still not widely used, and there are certain reasons for this.

## 2. LIMITATIONS OF BLOCKCHAIN

Blockchain technology is not without its drawbacks, among which we will consider the following in more detail:

- Scalability limits;
- Low transaction speed
- Unreliable consensus mechanisms.

### *2.1 Scalability limits*

In many blockchain networks specific algorithms of consensus are used. These algorithms have the same problem: each full network node must process each transaction. This is due to the decentralized structure of the blockchain. Instead of a single center that is responsible for security and functionality, each node in the blockchain network contributes to the overall security by confirming each transaction and storing a complete copy of the network state.

This method provides resistance to censorship, independence from regulators and provides certain security guarantees. But on the other hand, the number of transactions that a blockchain network is capable of processing is equivalent to the capacity of one network node.

This leads to two practical conclusions:

1. Low- capacity. The blockchain can only process a limited number of transactions.

2. Low speed of transaction execution. The processing of the transaction block takes a significant amount of time.

In other words, as the size of the blockchain grows, so do the demands on the storage, capacity and processing power of each network node. There may come a time when block processing will require so many resources that there will be too little nodes capable of handling this load.

### *2.2 Unreliable consensus-building mechanisms*

Users who make transactions on the blockchain do not need to trust a third side. This achieves anonymity, the ability to resist restrictions without anyone's approval.

A mechanism that has been used for a long time in a non-trusted blockchain and is able to effectively counter attacks is called a consensus algorithm. The consensus mechanism allowed the bitcoin blockchain to become the first widespread global decentralized transaction registry.

Proof-of-Work (PoW) is a scheme based on solving problems that are difficult to solve but easy to verify. Users of the blockchain network perform complex resource-intensive calculations using their computing power, and the system, for example - bitcoin, rewards them with new bitcoins and transaction fees. The more the miner's computing power, the more "weight" it has in the adoption of decisions by consensus. The structure of the bitcoin blockchain is shown in figure 1.

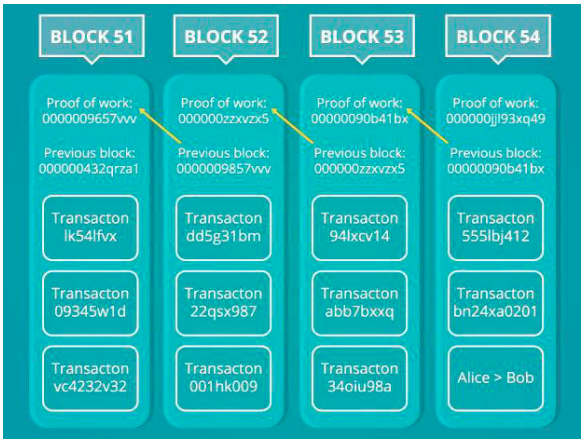


Fig 1. Structure of the bitcoin blockchain

PoW solved the so-called double spending problem without the involvement of a trusted third side. However, the PoW protocol is imperfect, and serious work by researchers and developers is still required to create a more viable consensus mechanism. The main problems of PoW include:

1. The need for special equipment. The disadvantages of the Proof-of-Work consensus include the need to use special hardware. In 2013 application-specific integrated circuit (ASIC) chips were developed. They were developed exclusively for mining, increasing its efficiency by 10 to 50 times. But they cannot be used anywhere else but mining.

Since then, mining with a conventional processor has become completely unprofitable: you can mine only through an ASIC device made independently or purchased from the manufacturer. This contradicts the decentralized nature of the blockchain, where everyone has the opportunity to contribute to the security of the network.

2. Power inputs. Miners employ computers of enormous power, carrying out calculations in the limits of the Proof-of-Work algorithm, but all this computational work does not benefit the society otherwise.

As public blockchains such as bitcoin using the Proof-of-Work consensus will be growing in scale, energy consumption will only increase. If the purpose of the public blockchain is to scale to millions of users and transactions, then wasted energy will not contribute to this goal. These fundamental problems of open blockchains were discussed in the work of Belov A. (2018).

## 3. IMPLEMENTATION OF DIRECTED ACYCLIC GRAPH

With the solution of these problems can help directed acyclic graph - the case of a directed graph, in which there are no paths starting and ending at the same node. Such a graph can also use topological sorting. Its growth can go only in one direction - from the early blocks to the later.

Blocks in this structure are not arranged sequentially one after another, and can go from earlier to later, but at the same time confirm not one, but several transactions. Thanks to this we get the following:

1. The system determines the parent transactions;

2. Then the system signs their hashes and includes the following translations;

3. A tree structure of transactions is formed, where each transaction will be considered confirmed and unchanged.

In the blockchain blocks cannot be created in parallel. Associated storage structure only allows for a single chain in the whole network. Data about transactions that occurred at about the same time are written to the block. Then miners compete with each other, trying to check the block as quickly as possible and get rewarded. However, if you change or even remove the concept of mining from such a network, its capacity can be increased by X times, simultaneously generating X blocks.

Apart from blockchain, directed acyclic graphs are used in compilers, artificial intelligence, statistics and machine learning. In other words, directed acyclic graphs are used in those areas where the speed of transactions is extremely important. Some implementations of the platforms based on directed acyclic graphs were described by Aryanova T. (2018).

Combining blockchain and directed acyclic graphs is based on the idea of parallel chains, while the blocks themselves retain their importance. Different types of transactions are executed simultaneously on different chains. A comparison of the blockchain structure and the directed acyclic graph is shown in figure 2.

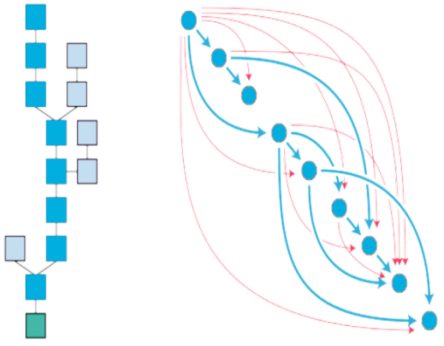

Fig 2. Structure of the blockchain (on the left) and blockchain-based directed acyclic graph (on the right)

However, it can happen that at the same time hashes of multiple users of the network will be received, and they will be eligible for confirmation of a block. This can lead to time branches. The truth of a particular transaction is determined by the number of transactions behind it. The speed of the transaction returning to the network is the lower the more transactions are behind it, which makes the transaction more secure. After the transaction is verified, it must be associated

with an existing relatively new operation in the blockchain network with directed acyclic graph. However, if you associate transactions only with earlier transactions, the network becomes too wide to check for new transactions. Ideally, blockchain network with directed acyclic graph selects the existing most recent transaction to which the new transaction relates. The point is to keep the network capacity within certain limits, providing a quick check.

Due to the blockless structure, transactions are processed directly on directed acyclic graph networks. This process is much faster and demands much less resources than in the case of blockchains based on Proof-of-Work and analogues. Current implementations of blockchain networks with directed acyclic graph are able to process up to 10000 transactions per second.

The blockchain network with directed acyclic graph also eliminates the concept of mining. Confirmation takes place directly in the transactions themselves. For users this means that transactions are almost instantaneous and do not require significant corresponding fees.

## 4. CONCLUSIONS

By combining the blockchain and directed acyclic graph, it is possible to create a network in which the main disadvantages of blockchain technology - low transaction speed and scaling problems - are eliminated. Through the use of multiple parallel chains, the speed of transactions can increase greatly. This is also achieved because all data does not need to be written to the block. The resulting network can, for example, be used on low-power devices such as the Internet of Things devices.

## REFERENCES

Aryanova T. (2018) DAG How platforms based on directed acyclic graph work URL: https://chaining.ru/2018/01/30/dag-kak-rabotayut-platformy-na-osnove-napravlennogo-atsiklicheskogo-grafa/ (obtained 02.04.2018)

Belov A. (2018) Fundamental problems of open blockchains URL: https://cryptocurrency.tech/fundamentalnye-problemy-otkrytyh-blokchejnov-chast-3/ (obtained 02.04.2018)

Boddy S. and Shattuck J. (2017) The Hunt for IoT: The Rise of Thingbots URL: https://f5.com/labs/articles/threat-intelligence/ddos/the-hunt-for-iot-the-rise-of-thingbots (obtained 02.04.2018)

Dickson B. (2017) How blockchain can improve cybersecurity URL: https://bdtechtalks.com/2017/01/11/how-blockchain-can-improve-cybersecurity/ (obtained 02.04.2018)

Magomedov Sh. (2017) Organization of secured data transfer in computers using sign-value notation *ITM Web of Conferences* (DOI: 10.1051/itmconf/20171004004) Vol. 10

Morgan S. (2016) Cybersecurity and cybercrime statistics URL: https://cybersecurityventures.com/cybersecurity-and-cybercrime-statistics/ (obtained 02.04.2018)

Moriuchi P. and Chohan S. (2018) Mirai-Variant IoT Botnet Used to Target Financial Sector in January 2018 URL: https://www.recordedfuture.com/mirai-botnet-iot/ (obtained 02.04.2018)

Morozov D.M. (2016) Links of one chain: pros and cons of blockchain URL: http://lib.custis.ru/Звенья_одной_цепи:_плюсы_и_минусы_блокчейна (obtained 02.04.2018)

Popov G. and Magomedov Sh. (2017) Comparative analysis of various methods treatment expert assessments *International Journal of Advanced Computer Science and Applications* (DOI: 10.14569/IJACSA.2017.080505) Vol. 8 # 5 p. 35-39.

Voit A., Stankus A., Magomedov S., Ivanova I. (2017) Big Data Processing for Full-Text Search and Visualization with Elasticsearch *International Journal of Advanced Computer Science and Applications* (DOI: 10.14569/IJACSA.2017.081211) # 8/12 p. 76-83