Science, Engineering & Education, 4, (1), 2019, 3-8

Application of Blockchain Technology

Krasimir Krumov, Atanas Atanassov*

University of Chemical Technology and Metallurgy, Sofia, Bulgaria

Received 23 July 2019, Accepted 14 October 2019

ABSTRACT

This paper aims to provide the basics of decentralized databases in the newest Blockchain structure. The principles of construction and the way of working are introduced. The known strengths and weaknesses are considered. A short comparative analysis between Blockchain and the old database structures was made. We have also paid attention to future opportunities for exploitation, as well as the assessment of the development over time.

Keywords: Blockchain, Decentralization, Future DB, dAPP in Blockchain, Proof of Work Algorithm, Proof of Stake algorithm.

INTRODUCTION

This report provides a brief overview of the Blockchain technology [1, 3] of its principles, features and applications. The meaning of the term Blockchain is a chain of blocks. This is a linked block structure that represents a distributed and decentralized database. The blocks are connected together in a constantly growing chain. Blocks contain transaction records encrypted cryptographically. In addition to transactions, each block contains information about the previous block (Fig. 1) and is verified with a timestamp. This provides chronological integrity of the information in the chain and enables traceability back to the first block.

Thus, technology provides security through design itself. Typically, the block chain is stored in the network in distributed form - with copies of the structure in the computer of each participant in the network. There is not exactly one master copy specified. This storage equality uses a peer-to-peer relationship [11] and adheres to a validation protocol for the new blocks. Once a block has been validated and recorded, it cannot be changed without the approval of the rest participants of Blockcahain. Blockchain has been developing over the past few years, as it is at the heart of crypto money and transactions with them.

Initial cryptographic block chain protection studies are related to developments by S. Haber and W. Stornetta from 1991/92 [4, 5, 8]. Their development is related to a system that ensures that the timestamp of a document cannot be changed. In 2008, for the first time, the term block is being used, and this is associated with Satoshi Nakamoto, who is developing a new concept for

* *Correspondence to: Atanas Atanassov, University of Chemical Technology and Metallurgy, 8 Kliment Ohridski, 1756 Sofia, Bulgaria, E-mail: naso@uctm.edu*

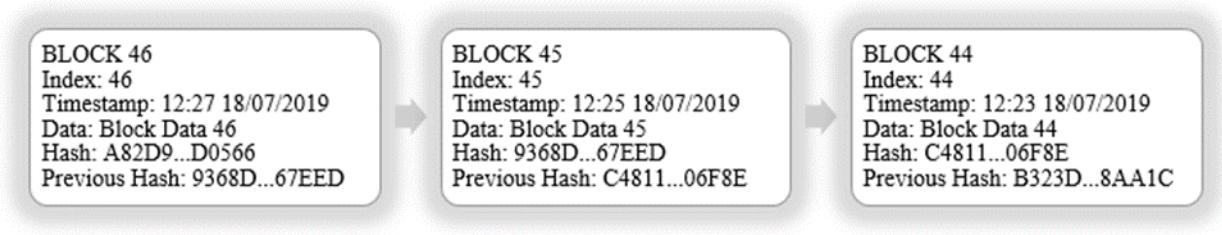

Fig. 1. Bockchain structure.

adding new blocks in the chain, and adding a new Hashcash method for encrypting information. From 2016 many organizations and corporations, including IBM, World Economic Forum and others open computer centres with the main goal - development and application of the Blockchain technology.

CHARACTERISTICS OF THE BLOCKCHAIN

Some of the key features of the Blockchain structure are:

• Decentralization - there is no need to maintain a server because every computer that plays a role in the cluster plays the role of a client and a server;

• Security (a copy of the information is available to each participant);

• Accessibility - Peer to peer connection is used through the Internet protocol;

• Resilience or inability to change (associated with protocol).

All of the above advantages are at the heart of the idea and development of this innovative method of disseminating information. There are also negative sides such as:

• Inability to store large volumes of data. This is related to the limited amount of information that can be published in each block. Otherwise, there will be swelling, unlimited chain growth and hence inability to store.

• Encryption, data shuffling - a principle that determines storage reliability, but at the same time requires power for decryption when accessing and data usage is needed.

CHARACTERISTICS OF THE BLOCK

The block (Fig. 2) consists of a header and a body. The body includes transactions. For example, in Bitcoin network, the average block size is about 1MB, and it may contain more than 500 transactions.

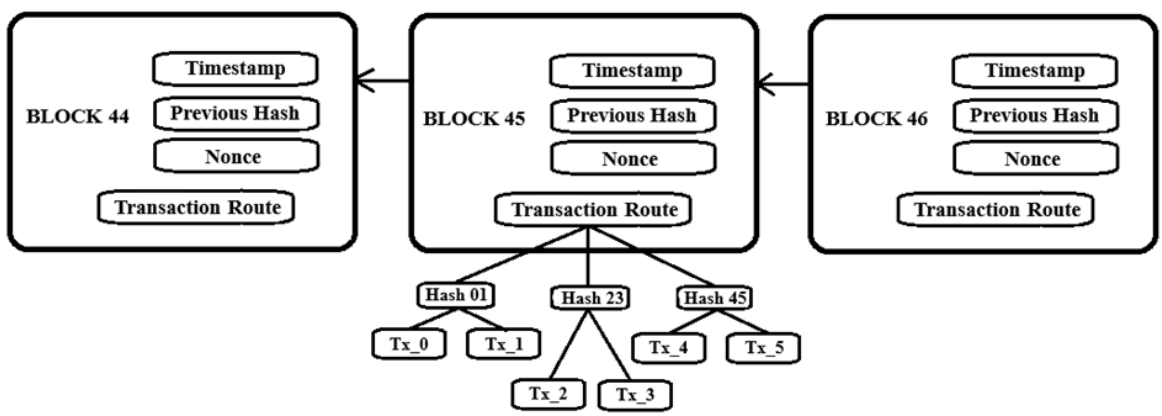

Fig. 2. Structure of the block in a Blockchain.

The header of the block contains:

• the hash value of the header of the previous block (the parent);

• the hash root of the Markle tree, which is built through a recursive hash of pairs of transactions, and thus covers the hash value of the transactions in the block.

Each block uses [2, 6] the hash of the previous block to form its own hash, and this becomes its unique identifier in the chain. This means that when replacing or adding a single transaction to a block, it must change its hash value and reconstruct the entire chain after it. Given that a copy of a block is stored on many computers on the network and a consensus is needed for each change, if this is not the case, this task becomes impossible.

A key role in building and maintaining the Blockchain is hashing. By cryptographic hash function based on a mathematical algorithm, the input data is converted into a fixed length source string, called hash, hash value, or digital signature. The cryptographic hash function has the following characteristics:

- hash value is easily generated;

- the decryption (i.e. the restoration of the original hexadecimal entry data) is impossible;

- it is not possible for different input data to obtain the same hash value - i.e. there is no collision.

There are different cryptographic hash functions. For example, in a BitKey block, SHA-256 (Secure Hash Algorithm 256-bit) is used that generates a 256-bit (32 bytes) hash value. Typically, it is represented as a hexadecimal number consisting of 64 digits.

CHANGE OF THE DATA OR ADDING A NEW BLOCK

In the procedure for modifying or adding data to an existing block in an a Blockchain or adding a new block, different approval methods are used. The pattern of approval is called consensus among network participants. This is a process of approval, confirmation of data by all or the majority of participants. This reconciliation process is done automatically through the consensus protocol. For example, the Bitcoin Network uses the Proof of Work (PoW) protocol.

Network participants (Nodes) communicate with each other to accept (decide) which new block to be included in the structure (Fig. 3). When consensus is reached, the whole structure is refreshed. In the process of implementing the consensus

Fig. 3. Reaching consensus to modify data in the block.

algorithm - each participant (Node) performs the calculation work - mathematical operations for finding the hash of the new block. Therefore, this process is connected with the necessary critical computing power. The devices used are powerful computers with many virtual processor cores available. The process is subdivided into subtasks, resulting in faster calculations. A major minus in the described consensus algorithm PoW remains energy intensity. For each participant in the network, computational power, connectivity (guaranteed internet connection), energy capacity (a major energy option) are needed. All of these features are graded as negative, and so other blocks of consensus algorithm are being developed in block technology. They aim to eliminate the negatives and achieve a higher speed of work. One new algorithm is PoS (Proof of Steak) [10]. This algorithm does not require the use of powerful machines and hence the reduction in power consumption. This algorithm is still in the process of development and development is due to be introduced into the Ethereum cryptographic network.

APPLICATION OF BLOCKCHAIN TECHNOLOGY

The main application in the past and the foundation of Blockchain‘s technology is the creation of virtual crypto currency. Many of the most famous and exploited are: Bitcoin, Etereum, Ripple, LiteCoin and others. Each currency has its peculiarities and ideas at its creation, and the most serious benchmark in the exchange system remains the founder of Bitcoin.

Some history [13] is provided in Table 1.

Using virtual currencies in the near future can push the exploitation of real money into the normal world. Currently, these currencies are too unreliable (with a view to a stable exchange rate), are not well received among traders and suppliers. And although it all makes virtual currencies imperfect and with a relatively unclear future,

Table 1. History of Bitcoin network**.**

Year	Event
2007	Satoshi Nakamoto begins working on the Blockchain concept
2008	Bitcoin.org was registered and first white papers published
2009	First bitcoin transactions took place
2010	First real world bitcoin transactions for 10000 bitcoins took place Mt. Gox is established as an bitcoin exchange in Japan
2011	Bitcoin reaches parity with US dollar
2012	Blockchain block #1819191 is largest with 1322 transactions Coinbase coin wallet is founded in San Francisco First hackers attacks on Mt. Gox
2013	First bitcoin ATM in San Diego Coinbase to raises 5000 000 ventures NY State Dept. of Financial Services subpoenas 22 bitcoin companies
2014	PayPal announces Bitcoin integration New York regulator announces lighter rules for Bitcoin companies
2015	Bloomberg Markets magazine –Suddenly Blockchain is hot

the convincing benefits of these are also evident. And they are: almost no fees and commissions in the payment and conversion; avoiding unnecessary intermediary institutions such as banks and other credit institutions. From this point of view, the economic benefit of virtual money is highly determined. Naturally, there are also negatives, because certain virtual currencies are created with the idea to be unchecked. This helps exploit them for negative purposes. This raises the question of the meaning of creating new currencies and technologies and the ethical nature of progressive new technologies. Notwithstanding the above, the absolute fact is that many banks and financial institutions have been making investments in block technology and networks since 2017. These are related to lending, share transactions, security of transactions.

One of the new block apps seems to be in the logistics of transportation of goods. At least three countries are involved in this process, such as suppliers/shippers, carriers and recipients. The processing of each shipment/delivery is related to a number of transactions and documents such as bills of lading, invoices, proof of delivery, etc. By building a block network, its members will be able to validate all documents and transactions related to the logistics and supply chain processes. Because Blockchain technology uses a so-called distributed book that is cryptographically secure, it can manage intelligent contracts. A smart contract is a computer protocol designed to facilitate, verify or impose the negotiation or performance of a contract and the settlement between the parties on the basis of a particular currency or the crypt. Intelligent contracts allow for reliable transactions without third parties. Moreover, these contracts allow the traceability of default clauses where the party concerned is notified of the penalties imposed. The parties involved in such a contract are unknown but all participants in the block receive information about the deal and can monitor its accuracy. The application of such contracts, for example, may be between an energy supplier and a physical customer or an user company. A similar Blockchain system has been implemented in Australia since 2017. In practice, the application of this type of contract in various fields and activities is unlimited and this determines the possibility of strong development and applicability of the Blockchain networks in some important state and private structures:

• Certification services and notarial records;

• Election voting [7] for voter registration, identity verification and electronic voter reporting;

• Education in the issuing of diplomas, certificates and academic references,

• Healthcare - a health record with traceability of insurances, examinations, clinical pathways and prescription medication,

• Industrial production with the need to record processes and time changes in articles, etc.

• Insurance - health, property, automobile, etc. insurances and control of their provisions.

CONCLUSIONS

The main features, the principle of Blockchain technology, their advantages and disadvantages and their future use are discussed. Blockchain technology is a relatively new tool, but it has potential applications in many areas and organizations that use secure transactions without intermediaries.

The future of Blockchain networks is still unclear and difficult to predict. They are expected to undergo a number of transformations and changes.

Numerous studies [9] to develop these technologies indicate that in the near future by 2030:

Many governments will introduce their own crypto-loop, which will lead to a new era of payments, as well as regulation of unapproved crypto currencies.

In developed countries, a Blockchain identity should be put in place to replace identity documents, such as identity cards and passports, as well as property documents such as notarial deeds, car vouchers, etc.

Blockchain networks will lead to changes in world trade where many regulations and ontracts for import/export between countries will be authorized through these networks.

Aacknowledgements

The research is funded by the Research Fund (FNI) of the Ministry of Education and Science, under the project "Synergy between procedural philosophy and elements of artificial intelligence in the theory of education" № DN 15/9 from 11.12.2017.

REFERENCES

1. B. Singhal, G. Dhameja, P. Panda, Beginning Blockchain A Beginner's Guide to Building Blockchain Solutions , 2018, Apress Publishing.
2. What Is Blockchain Technology? www.cbinsights.com/research/what-is-Blockchain-technology/
3. D. Yaga, P. Mell, N. Roby, K. Scarfone, Blockchain Technology Overview, National Institute of Standards and Technology, 2008, doi.org/10.6028/NIST.IR.8202.
4. Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven, Bitcoin and cryptocurrency technologies: a comprehensive introduction, Princeton University Press,2016.
5. Haber, Stuart; Stornetta, W. Scott, How to time-stamp a digital document, Journal of Cryptology, 1991 issue 3(2) pp. 99–111,doi:10.1007/bf00196791
6. Damien Cosset, Blockchain : what is in a block?, 2017, https://dev.to/damcosset/Blockchain -what-is-in-a-block-48jo
7. 19 Industries that Blockchain Technology will change, //knowhow.company/Blockchain / tehnologiata-Blockchain -promenia-19-industrii/
8. https://en.wikipedia.org/wiki/Blockchain
9. Kate Mitselmakher, The Future of Blockchain Technology: Top Five Predictions for 2030, 11, October, 2018, https://www.Blockchain-expo.com/2018/10/Blockchain /future-of-Blockchain –technology.
10. B. Tasev, PoW vs PoS, (r)evolution of Blockchain , 2018.
11. A. Kovachev, Blockchain : Build your own P2P network from scratch with Automaton, 2018
12. Tasev, B., PoW vs PoS, (r)evolution of Blockchain , 2018, https://dev.bg/събитие/pow-vs-pos-revolution-of-Blockchain
13. B. Leemoon, Boom or Bust, Bitcoin a valuation framework, MBA 592 Advanced Project in Business Fall 2017, Wilkes University, UK, 2017, pp. 5.