ISSN 2278-3091
Volume 9 No.2, March - April 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse166922020.pdf
https://doi.org/10.30534/ijatcse/2020/166922020

The Mechanics of the Blockchain Technology

Nakonechnyi V.S.[1], SteshenkoG.M.[2], BuchykS.S.[3], KresinaI.O.[4], RusnakA.V.[5]
[1]Taras Shevchenko National University of Kyiv, 01033, Ukraine.
[2]Taras Shevchenko National University of Kyiv, 01033, Ukraine.
[3]Taras Shevchenko National University of Kyiv, 01033, Ukraine.
[4] National Academy of Legal Science of Ukraine, 01015, Ukraine
[5] National Academy of The Security Service of Ukraine, 01022, Ukraine

ABSTRACT

Recently, blockchain technology has been actively discussed all over the world. The world's largest organizations have declared 2017 the year of blockchain. Our country is no exception. Therefore, this technology has attracted the attention of Russian specialists (not only programmers, representatives of technical professions, but also government officials, notaries, and large firms that are ready to keep up with the times). In particular, on June 16, 2017, a Memorandum of cooperation in the implementation of the latest information technologies, in particular the blockchain system, was signed in Seoul, Korea.

Key words : Mechanism, Blockchain, technology, Bitcoin.

1. INTRODUCTION

For the first time, the blockchain system was used as the basis for the functioning of the digital currency Bitcoin (Bitcoin).

The blockchain is a structured database, a "chain of blocks", where each block is linked to the previous one. The block contains a set of records (information). Each new block with information is added to the end of the chain. Thus, a kind of "register" of data is created, in which data is entered in a strict sequence.[2] the number of blocks is unlimited. The content block can contain any information: about actions, people, objects, transactions, serial numbers, issued loans, and the like.

In other words, the blockchain is a distributed public registry based on modern cryptographic algorithms that contains a database of all previously performed operations, which is decentralized in nature, and what is contained in the public sources of the Network. This is a structured system with specific rules for building transaction chains and accessing information.

According to the developers, this system excludes theft, fraud, and violation of property rights. Facts stored in the blockchain cannot be lost. They stay there forever. In addition, the blockchain stores not only the final state, but also all previous States. Therefore, everyone can check the correctness of the final state by listing the facts from the beginning.

2. MATERIALS AND METHODS

The blockchain works with a complex encryption system (keys). Each block has its own unique key. The inability to "break the chain", that is, to make edits to a block or add a block between others, is ensured by the fact that the codes (hashes) of the previous and subsequent blocks are linked together and making changes to one block immediately makes it and all other blocks that follow it invalid, which is automatically displayed on the screen.

A hash is a unique code that changes when even one character in the text changes, is calculated using a complex mathematical formula, and will always be the same for the same information. Therefore, there can't be two different hashes for exactly the same information. This system is used, in particular, to protect your information, money, because you can see what is happening to them. The principle works here: you can't spend more than you have, which also makes it possible to control absolutely all operations that occur, where, when, and how much money is spent. In particular, there are proposals to use decontamination to ensure the safe operation of, for example, pacemakers, robots, aircraft, Autonomous cars, which implies that they can not be hacked. After all, as supporters of the introduction of this system note: it is easier to hack the Central server and get access to all the information together, change or delete it, than to break the decentralized system.

You can name both the advantages of the blockchain and the problems that arise in connection with its use. The advantages of using the blockchain system include:

1) decentralization, that is, the entire network is used, not a single computer (organization, person, etc.). In this case, even if one or more computers (a person) cannot perform any functions (liquidated, arrested, etc.), others store this information, which makes it difficult for hackers to attack and fake information (although no one is immune from this);

2) proof of each transaction: there is cryptographic confirmation of each transaction, record, and so on. In particular, the keys are private (belonging to a particular person) and public (which can be used by all users of this network), that is, if there is one person or one computer;

3) transparency (shared access): be someone who can always see exactly what operations were performed;

4) security: information is stored with the use of cryptography;

5) inability to make changes to "signed" block: information that was in the blockchain is checked and if the verification is a kind of "seal," and this data is synchronized between all participants, from this moment information cannot be changed;

6) computational logic: the digital nature of the registry works in such a way that transactions in the blockchain can be linked to computational logic and can actually be programmed, which allows users to configure algorithms and rules for automatic execution of transactions between nodes;

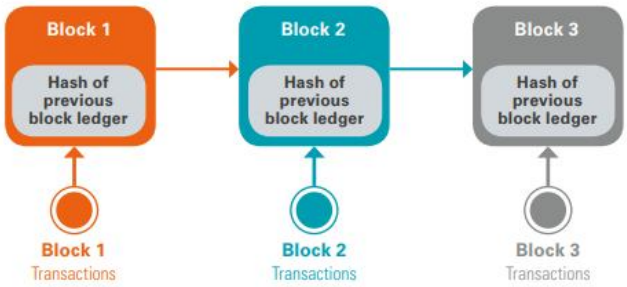

Figure 1: Individual Blocks Referencing Transactions in a Chain [1]

If we talk about the classic type of contract, there is always a chance that one of the parties will violate it. Currently, the state uses legal mechanisms and the judicial system to "motivate" the parties to the agreement to behave honestly, which takes a lot of time and money, and decisions are not always fair(fig. 1). Using the blockchain will speed up, simplify and reduce the cost of the procedure, because the conclusion of the contract requires the participation of both parties, and neither one nor the other can deceive the system (blockchain) with the already set parameters for the execution of the contract. This implies the following "positives" of implementing and using blockchain:

7) save time (the system works 24 hours a day, 7 days a week);

8) saving resources (in particular, public funds).

According to J. Zittrain [3], blockchain is a capacious term that includes, first of all, history, philosophy, Finance, law, regulation, and only then – cryptography and technology.

Summarizing the above, we can state that blockchain is a truly revolutionary technology, it allows us to reach a kind of "consensus" in the distributed world, to do without intermediaries, which can be used in all spheres of public life (health care, Finance, media, etc.), and therefore: new business models are "born"; the level of fraud is reduced; processes (work) between business agents are simplified.

However, we are still at the very beginning of the modernization process that is being proposed. Many issues are unresolved, the specific process of implementing such technologies, the consequences of possible errors, liability and compensation for harm is not clear. After all, we are not talking about "buying coffee or a bottle of water in the machine", when the transaction is actually performed automatically: for a specific amount deposited, the machine provides the selected "product". Even in this case, in the event of a malfunction of the machine, it is possible to call the operator and the person will be refunded the money paid, because the goods were not received, which in fact is a recognition that the contract "did not take place". But how such situations will be solved "behind the blockchain" is still unknown, and a completely acceptable solution for all potential participants has not yet been proposed.

Obstacles to the introduction of blockchain technology in our lives are also associated with high energy costs, problems with scalability, inertia of market players, the need in some issues to reach a consensus between a large number of participants, as well as the lack of a legal framework. The blockchain technology was conceived as free from the government and middlemen and formed a large community cryptoanalyst.

As noted, for the first time, the blockchain system was used as the basis for the functioning of the bitcoin cryptocurrency. In particular, the introduction and use of bitcoins (as a cryptocurrency) was aimed at avoiding the use of such types of currency as the dollar, Euro, etc. (which are centralized) and providing the ability to pay in a decentralized currency Network. Bitcoin is not the only cryptocurrency. But it has become very popular. The popularity of bitcoin is explained by the fact that it is reliable (safe to use): after all, the information is carefully checked. This is a mathematically protected "currency" that supports a grid of equal users; digital signatures authorize each transaction, ownership is passed along the transaction chains, and the order of transactions is controlled by the blockchain (fig. 2). For each block, it is necessary to solve a complex mathematical problem, that is, attackers must compete with all users of the bitcoin system at the same time. The advantages of using bitcoin in the it Sphere are anonymity, non-interference of the authorities, and low transaction fees. However, its disadvantages are: difficulties in exchanging bitcoins for other currencies; ideal suitability for illegal transactions and tax evasion (for which it can be banned by the government); high energy costs for calculations with the purpose of protection using the blockchain.

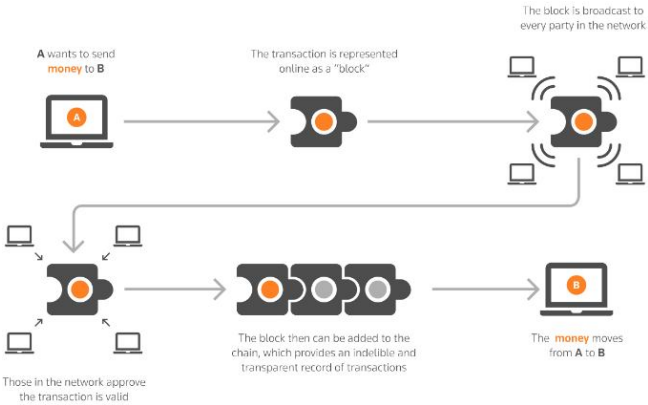

Figure 2: How blockchain works

In General, the use of cryptocurrencies implies the need to use the appropriate "platform" for the same application

and each time using a "new" Protocol, and the main goal is to work on the basis of one common universal Protocol, that is, using programming, a person writes a rule, and the program itself executes this rule [4].

It should be noted that the above-mentioned draft Law contains a number of definitions of concepts, such as: cryptocurrency, cryptocurrency subjects, cryptocurrency owner, cryptocurrency exchange, cryptocurrency basket, cryptocurrency transactions, miner, mining, remuneration of the blockchain system, and others. In particular, cryptocurrency named software code (a set of symbols, numbers and letters) that is subject to ownership rights, which can act as a means of exchange, details of which are entered and stored in the blockchain as the accounting units of the current blockchain data (program code).

3. CONCLUSION

Blockchain, as a tool for implementing various important projects not only in the business sphere, but also in state regulation (in particular, for fighting corruption in the public sector, banking, etc.), is at the beginning of its path.

Studies of foreign centers for studying the introduction of such new technologies show that blockchain can be used in such areas as Finance (33%), government (29%), healthcare (27%), and others [6].

Given the trends in this area and the possibilities for their implementation, we can assume that the blockchain will be fully applied in our lives in 10-15 years and only if national legislation is adapted to the new realities of using information technologies.

At the same time, forecasts in the rapidly developing it sphere are a thankless thing, and the process can significantly accelerate. The implementation of blockchain technology in our country is currently being tested in various industries, and the overall prospects depend on their success.

In order to ensure confidentiality, in particular, it is proposed to provide that only the hash is stored in the blockchain, and not all information about the completed operation. In addition, the security of using this technology can also partially guarantee the use of not only a public but also a private key.

REFERENCES

1. B. Lucey, S. Corbet. 2018. **Why bitcoin proves regulation is the biggest challenge facing cryptocurrency**. Available at: https://economia.icaew.com/opinion/august-2018/why-bitcoin-proves-regulation-is-the-biggest-issue-facing-cryptocurrency
2. D. Bianchi. 2019. **Five reasons bitcoin could enter a more extreme death spiral**. Available at: https://economia.icaew.com/opinion/january-2019/five-reasons-bitcoin-could-enter-a-more-extreme-death-spiral
3. J. Zittrain. 2008. **The Future of the Internet and How to Stop It**. New Haven: Yale University Press.
4. S. Nakamoto. **Bitcoin: A Peer-to-Peer Electronic Cash System**.2008. http://www.cryptovest.co.uk/resources/Bitcoin%20paper%20Original.pdf.
5. A. Azaria, A. Ekblaw, T. Vieira, A. Lippman. **MedRec: using blockchain for medical data access and permission management**.International Conference on Open and Big Data (OBD), August 22–24, 2016. Piscataway, NJ: IEEE. http://ieeexplore.ieee.org/abstract/document/7573685/.
6. D. Kraft, **Difficulty control for blockchain-based consensus systems**. Peer PeerNetw. Appl. 9(2), 397–413. 2016. https://doi.org/10.1007/s12083-015-0347-x
7. M. Peck, **A blockchain currency that beat s bitcoin on privacy.** IEEE Spectr. 53(12), 11–13. 2016. https://doi.org/10.1109/MSPEC.2016.7761864
8. M. Sharples, J. Domingue. **In The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward**. Adaptive and adaptable learning. 2016. pp. 490–496 https://doi.org/10.1007/978-3-319-45153-4_48
9. H. Wang, K. Chen, D. Xu. **A maturity model for blockchain adoption**. Financ. Innov. 2(1), 12. 2016. https://doi.org/10.1186/s40854-016-0031-z
10. S.V. Klyuev, S.N. Bratanovskiy, S.V. Trukhanov, H.A. Manukyan. **Strengthening of concrete structures with composite based on carbon fiber** // Journal of Computational and Theoretical Nanoscience. 2019. V.16. №7. P. 2810 – 2814.
11. A. Semenutina, A. Khuzhakhmetova, V. Semenutina, I. Svintsov. 2018. **A method of evaluating pigment complex wood plants as an indicator of adaptation to dry conditions**. World Ecology Journal, 8(1), 69-82. https://doi.org/https://doi.org/10.25726/NM.2018.1.1.006
12. A. Zelenyak& S. Kostyukov. 2018. **Features of the development of architectonics of crowns of bushes as a criterion of decorativeness in green building**. World Ecology Journal, 8(3), 1-22. https://doi.org/https://doi.org/10.25726/NM.2019.99.51.001
13. A.j., D., & R, G. (2019). **Early detection of alzheimer's disease using predictive k-nn instance based approach and t-test method**. International Journal of Advanced Trends in Computer Science and Engineering, 8(1.4 S1), 29–37. https://doi.org/10.30534/ijatcse/2019/0581.42019
14. Ab. Rahman, M., Yi, S. Z., Shah, N. S. M., & Irfan, M. A. (2020). **Fever monitoring and alert system for children using thermographic camera**. International Journal of Advanced Trends in Computer Science and Engineering, 9(1.1 Special Issue), 316–327. https://doi.org/10.30534/ijatcse/2020/5591.12020