UDC 004.738.5:332.1:681.5

3. BLOCKCHAIN IN IT

Holub D.S. Master's degree student, group 376501

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Liakh Y.V. – Senior Lecturer

Annotation. Recently, blockchain has been used in various fields, such as cryptocurrencies, digital asset management, cybersecurity improvement and smart contracts. Due to its principles of operation, including decentralisation, reliability and transparency, blockchain is becoming increasingly popular and various organisations are studying this technology and applying it in their activities. The article analyses the disadvantages and prospects of introducing blockchain into modern IT systems, and how the blockchain has evolved in recent years.

Keywords. Blockchain, technology, cryptocurrencies, generation, decentralisation.

There is no person who has never heard of blockchain technology. In recent years, blockchain has attracted the attention of thousands of users and it has been applied in various industries. It all started with the creation of an alternative to fiat funds – cryptocurrency, which was based on blockchain, and then it gained popularity and began to develop. Currently, blockchain is used not only to create cryptocurrencies, but also in other areas for data storage, data protection, data transfer, sharing transmission and much more.

What is blockchain technology? Blockchain is a decentralised and distributed ledger that records transactions on multiple computers. When compared with traditional data storage methods, which are usually stored on a central server, the blockchain stores data in a decentralised manner. Decentralisation means that there is no single point of failure and the data is immutable, and the blockchain has the best cryptographic protection, which makes blockchain-based applications very resistant to forgery or hacking.

How does the blockchain work? The scheme of work of the blockchain is illustrated in Figure 1.

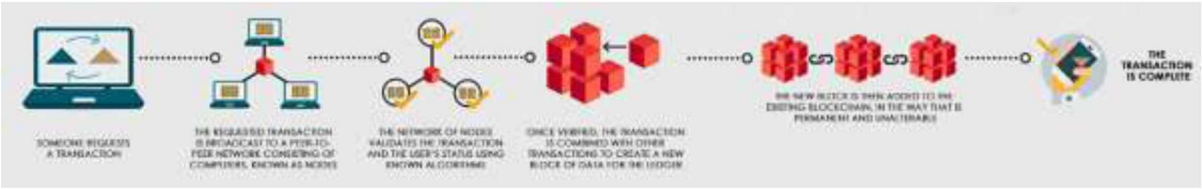

Figure 1 – Work of the blockchain technology

Blockchain technology is entering the forefront of the IT industry, because it allows you to create and use decentralised applications (DApps) and decentralised finance (DeFi). These applications work in a peer-to-peer network, which allows people and organisations to use applications without mediators and centralised servers. DApps and DeFi are decentralised applications based on blockchain technology that provide enhanced privacy, security, and scalability. DeFi takes the provision of financial services that banks traditionally offer to a new level, such as lending, borrowing and trading. An important feature of using DeFi, rather than banks, is the basis of the blockchain, which does not need intermediaries, which significantly reduces fees and ensures wider availability of financial services.

Blockchain technology increases user trust due to its one more feature – transparency. The blockchain registers all completed transactions and this information is available to all network participants. Therefore, it is difficult to manipulate or falsify data. This feature of blockchain technology allows effective collaboration between users through increased accountability and security.

One of the important advantages of using blockchain technology in IT is to increase efficiency, reduce costs and the likelihood of errors. Blockchain technology is a peer-to-peer network, so it does not need intermediaries, such as banks, financial institutions and other institutions or people. Thanks to this, the blockchain simplifies and speeds up various processes. For example, in logistics, it is necessary to track goods in real time and at the same time verify the authenticity and origin of these goods. Blockchain will reduce time and resources by using smart contracts.

So, another advantage has been revealed – smart contracts, which allow you to optimise business processes using automation. Smart contracts are self-executing contracts, the code of which specifies the specific terms of the agreement, and the smart contract is considered fulfilled if all the conditions are met.

Despite all its advantages, blockchain technology also has its drawbacks. The most key disadvantage is scalability. With a large number of transactions, blockchain technology can become slow and inefficient. And the most important problem in mining is the impact of energy consumption on the environment.

Only recently blockchain technology has begun to develop and popularise, so the issue of regulation related to blockchain technology is still developing and time is needed to take into account all the nuances and create a comprehensive regulatory framework that will be valid for the whole world.

Due to the advantages discussed above, the popularity of using blockchain technology has been growing in recent years. Because of the high interest, many organisations began to study the blockchain technology and how to use it for their own purposes. From its humble beginnings to its widespread applications, blockchain has come a long way in a relatively short period of time. At this stage, the blockchain has undergone five important changes in its structure, functionality and usability. All these changes can be classified as first-, second-, third-, fourth- and fifth-generation blockchains.

The first-generation blockchain certainly includes Bitcoin, which appeared in 2009. The main purpose of its creation was reliable money transmission without intermediaries and solving problems of fiat – inflation and high commission. Over time, the deflationary properties of Bitcoin have been confirmed by an increase in its value, but at the same time, commissions on the Bitcoin network are not as low as before, so they are unlikely to be suitable for transactions for small amounts. Now Bitcoin is more suitable as a means of saving, rather than a method of payment. The main disadvantage at the moment is the limited functionality and energy-consuming Proof-of-Work consensus algorithm.

From altcoins to the first-generation blockchain, Litecoin can be attributed. The task of this altcoin is to improve bitcoin. Due to the commission and slow bandwidth, Bitcoin is not the preferred choice for calculating and paying for products and services, so the developers decided to create a convenient and fast payment system – Litecoin, which should remove these disadvantages. To this goal, the developers have reduced the block formation time to 2.5 minutes, which is 4 times faster than Bitcoin, and increased the throughput to 56 transactions per second, which is 8 times more than Bitcoin [1].

Bitcoin, the world's first cryptocurrency, introduced the concept of a decentralised, peer-to-peer digital currency that operates on a secure and transparent public ledger known as the blockchain. This stage laid the foundation for the future of blockchain technology and set the stage for its rapid growth.

The stage of development of the second-generation blockchain is attributed to the launch of the Ethereum network in 2015. Second-generation blockchains have expanded the capabilities of the traditional blockchain technology and achieved full computing power, that is, not only decentralised databases, but also fully functioning computing environments. These environments are controlled by smart contracts, algorithms that can automatically perform complex operations or their chains when the user performs certain actions. These smart contracts are executed by the blockchain technology and can also work to ensure communication between blockchains. This property made it possible to make Ethereum the first blockchain technology for decentralised applications that perform on-chain operations. Also, thanks to smart contracts, most of the other areas that were popular until then, for example, DeFi and non-fungible token (NFT), appeared.

Despite the popularity of the Ethereum blockchain platform, the expansion of its use is hampered by low performance and high transaction fees, especially those related to smart contracts. However, in 2022, that is, after 7 years of launching the mainnet, Ethereum managed to change the Proof-of-Work (PoW) algorithm to a more modern Proof-of-Stake (PoS). But this did not solve the scalability problem. And although its developers plan to implement sharding, it is not known exactly how long it will take and whether it will be implemented in principle [2]. Since Ethereum, the function of smart contracts has been built into all universal blockchains in one way or another.

The second-generation blockchain also includes the TRON and EOS projects. TRON is a decentralised digital platform based on blockchain technology and smart contract functionality. TRON is a global entertainment system for the free exchange of digital content between users. They can upload, store and transfer content, rent it out, deploy a decentralised application, issue their tokens – and this is just a short list of possibilities. The main idea of creating this system is to expand the capabilities of the traditional media industry using blockchain technology. Another project, EOS, is also based on blockchain technology. It works on a Delegated Proof-of-Stake (DPoS) consensus mechanism, which is designed to increase scalability and efficiency. One of the main goals of EOS is to solve the blockchain trilemma by providing scalability without compromising security or decentralisation. EOS strives to combine the best features of various smart contract technologies to create a reliable platform for large-scale applications, so this platform is more designed for high-load commercial purposes, for example, a large commodity business.

After the advent of the Ethereum blockchain network, there was a lot of competition in the field of blockchain platforms – each of the competitors sought to offer their own solution to the problems of past generations. At this stage, the problem of scalability is being solved by adding a bridge between blockchain ecosystems through which coins can be transferred. Also, important attention was paid to energy efficiency, which made it possible to create the PoS algorithm mentioned above. This algorithm does not require the use of expensive and energy-consuming equipment.

One of the first competitors of Ethereum among the third-generation blockchains can be called Cardano, a platform for creating DApps. In addition to using the PoS algorithm, it also implements a more advanced smart contract mechanism, which includes the possibility of their formal verification.

Another example is Solana, which is an alternative to Ethereum 2.0. This project is based not only on the PoS protocol, but also on the Proof of History (PoH) protocol. The PoH protocol allows you to record a transaction even before the information is added to the blockchain, thereby increasing throughput. The PoS protocol allows users to earn coins for betting. In order to ensure high-speed operation, high hardware requirements are imposed on the validators of this network. However, over time, it became clear that the Solana protocol is not reliable: due to local problems with nodes, this network often stops working, which is unacceptable for the blockchain [3].

The fourth generation of blockchains has provided a new mechanism – segmentation. It allows you to divide the blockchain into smaller segments or parts. An example of a fourth-generation blockchain is Near. It is based on a delegated PoS blockchain with support for smart contracts with a segmentation mechanism called Nightshade. A special feature of Near is that the Near chains are created as a single blockchain. In other words, each block created in Near contains snapshots of transactions occurring in each segment of the other chain. Each segment is supported by its own dedicated network of validators, and all these segments work in parallel. This means that Near can process about 100,000 transactions per second. Although this figure reflects high throughput capable of supporting a wide range of use cases, it is unlikely to be sufficient to accommodate large client databases.

The architecture of some fourth-generation blockchains is based on the mechanism of Byzantine Fault Tolerance (BFT). In the Polkadot blockchain, this feature is called Practical Byzantine Fault Tolerance (PBFT). The essence of this mechanism is that all nodes of the network must communicate with each other to achieve consensus. The PBFT achieves relatively low latency and high speed to achieve a unified network state.

But the disadvantage is that such a mechanism interferes with decentralisation, that is, with an increase in the number of participants, the burden on each of them increases due to the need to verify each participant. The Polkadot blockchain can process 1,700 transactions per second, although the theoretical maximum throughput is 100,000 TPS [4]. Polkadot also has compatibility difficulties, which is why this blockchain did not have a cross-chain bridge with the largest ecosystem – Ethereum until recently. And in August 2022, hackers were able to find an exploit in the code of the DeFi protocol Acala based on Polkadot, which led to multimilliondollar losses for its users. This also raises questions about the security of the code.

In the last few years, the fifth generation of blockchains can be identified. They have key differences from their predecessors. This generation solves the trilemmas of the blockchain. The essence of the blockchain trilemma is that developers cannot ensure all three principles of the blockchain: security, decentralisation and performance. Developers are forced to sacrifice one of the principles in order to maintain the other two at the proper level. This problem is solved by using dynamic sharding. Sharding is the allocation of additional resources for processing large amounts of data, which allows blockchain networks to show high flexibility: if the load increases, then network commissions decrease.

One of the popular fifth generation projects is Everscale. Sharding was originally built into its architecture. This blockchain is divided into separate "subnets" (workchains), the number of which can be relatively easy increased and which work with their own set of validators, and can also use their own virtual machine. In turn, workchains are divided into shards, transactions in which are confirmed in parallel. The masterchain is responsible for the communication between the workchains and the unified state of the network. Everscale uses the Soft Majority Fault Tolerance (SMFT) protocol, which ensures that no workchain sends an incorrect block to the masterchain. A validator that tries to send the wrong block is "punished" by slashing, that is, removing part of his steak. This also happens if the validator does not send or accept proof of receipt of the correct block (for example, while offline). Thus, the main criterion for the work of Everscale validators is honesty and integrity [5].

The multi-level architecture of Everscale and the flexibility that depends on the current load make it possible to scale this blockchain without noticeable restrictions, up to millions of transactions per second. And it is precisely this blockchain architecture that can claim to be a worthy solution to the problem of scalability, while maintaining a high level of security and decentralisation.

Technological progress does not stand still. As we can see, 15 years have passed since the creation and first use of blockchain technology. For so long, blockchain has undergone many changes and users will not stop trying to improve it even more and expand its capabilities. New protocols are emerging, problems are being solved and algorithms are being improved. Only one fundamental decision, which is the basis of the blockchain, remains unchanged. At first, blockchain was used only as an alternative to money, but now the use of blockchain has gone beyond the financial sphere, now it is used everywhere - in games, logistics, application creation and much more. Blockchain solves the problems of business, the state and each user.

References:

1. Litecoin vs Bitcoin: What's The Difference? [Electronic resource]. – Mode of access: https://www.coingecko.com/learn/litecoin-vs-bitcoin. – Date of access: 10.03.2024.

2. What is Ethereum? [Electronic resource]. – Mode of access: https://ethereum.org/en/what-is-ethereum/. – Date of access: 10.03.2024.

3. Is Solana Safe? [Electronic resource]. – Mode of access: https://www.benzinga.com/money/is-solana-safe. – Date of access: 11.03.2024.

4. Polkadot (DOT) [Electronic resource]. – Mode of access: https://www.investopedia.com/polkadot-definition-6362436. – Date of access: 12.03.2024.

5. What is Everscale? The Complete Beginner's Guide to The 5th Generation Blockchain [Electronic resource]. – Mode of access: https://blog.everscale.network/blockchain/what-is-everscale. – Date of access: 12.03.2024.