A.E. Khrushkov, A.A. Ptuknin, E.M. Bozhko
Ural Federal University named after the first President of Russia B.N. Yeltsin
Yekaterinburg, Russia

BLOCKCHAIN TECHNOLOGY

Absract: The article is devoted to the modern technology “Blockchain", designed to store data on transactions, transactions, everything that needs to be recorded and checked. At the moment, the use of this technology is limited to only a few areas, but this is only the beginning of its path. The main advantages of Blockchain technology are its openness and decentralization.

Key words: blockchain, technology, transactions, hashing.

Blockchain is a continuous sequential chain of blocks (a linked list) containing information and built according to certain rules. Most often, copies of the block chains are stored and are independently (in an extremely parallel way) processed on a variety of different computers [4]. The blockchain can store such information as data on property rights, or on the issued loans. The main advantage of the system is that the registry is stored on thousands of computers, and if desired, any user of this network can get access to the current version, and that makes this technology absolutely transparent and promising.

The operation of blockchain can be compared with a puzzle. A block is an array of data, into which one enters the information about the transactions, which arrived into the network after creating the previous block, and then each new block is attached to the previous one using mathematical algorithms. To create a new block, you need to compute a cryptographic fingerprint – a hash that results from hashing. Hashing is the transformation of an array of input data of arbitrary length into a bit string of fixed length, performed by a certain algorithm [3].

This technology is implemented with the help of a large number of computers working in the same network, which solve complex crypto tasks, that is, they pick up a special code that will allow to obtain the hash.

The process of block searching is called mining. After solving the problem, a new unchangeable block is formed.

The entire reliability and security of the block chain is founded on cryptographic hashes. The hash is issued by the system as an enormous number. For a given data set, the hash function produces one hash that has two extremely important properties:

- The first is that, even if you have a key, you cannot learn the original data set.
- The second property is that it is almost impossible to find another data set resulting in the same hash.

When you change the data, the resulting hash changes completely. All data blocks are always open to everyone, thus, they can easily track any change of information. This is the main feature and advantage of this technology, as the authentication of the information is simple and accessible.

Blockchain technology is completely decentralized, no one has power over it, and there is no authority that could prohibit transactions or block access to the blockchain; a third party is not required to confirm the transfer of information.

Implementation Algorithm

In 2002, the US National Security Agency announced the creation of a SHA-2 hash function, which 6 years later evolved into the SHA-256 algorithm and formed the basis of the world's first crypto currency, and to this day has remained the basis of the technology.

Technically, the SHA-256 algorithm works as follows: the original message is divided into blocks, then each block is divided into 16 words. The algorithm passes each message block through a loop with 64 or 80 rounds. The results of processing each block are added together, the resulting value being the value of hash function. The hash function is a function that implements an algorithm and performs the transformation of an array of input data [1].

Applications

Blockchain is a distributed public data base, in which there is no centralized supervision of the process. With the help of blockchain you can keep records, store data, make transactions. These operations can be performed in such spheres of life as:

- Financial operations
- Real estate transactions

- Insurance
- Logistics
- Traffic violation
- Marriage registration

The first practical application of blockchain technology took place in 2009, when bitcoin crypto currency was created on its basis.

Nowadays, different states are actively considering ways to introduce this technology into the voting system in the elections. China wants to transfer the operation of the National Social Insurance Fund on the use of the blockchain technology. Startups in medicine and copyright also use blockchain technology. Identification systems, web browsers and social networks are also being developed on this basis.

The so-called smart contracts, greatly simplifying the procedure for signing contracts, sound more and more familiar. The program code automatically monitors the conditions and confirms their fulfillment. All participants in the process can at any time audit the transaction.

Advantages and disadvantages of technology

The main advantages of blockchain technology are its openness, safety, and security. The technology also allows to cut transaction costs. It reduces the time of transactions from several days, or even weeks, to several hours enabling companies and institutions to get rid of unnecessary expenses.

The disadvantage of this technology is scalability. At the moment, the blockchain technology cannot provide for a huge number of transactions within a short time. For example, the MasterCard or Visa payment system handles about 45,000 transactions per second, while the Bitcoin crypto currency using blockchain technology handles only 7. The load on the electrical networks also increases, because all complex calculations make computers consume a huge amount of power.

The probability of "51 percent attack" should not also be overlooked. In other words, if a group of network members appears that will be able to concentrate 51 percent of the processing power in their hands, they will be able to act in its own interests, confirming only the transactions profitable for them. But this is unlikely to happen, since it requires very powerful resources, which are virtually impossible to implement in practice [2].

The development of blockchain technology has changed the approach to the arrangement of business operations. It marked a new era of reliable and intelligent applications for the registration and exchange of

physical, virtual, tangible and intangible assets. Thanks to cryptographic security, decentralized consensus and a common open registry, blockchain technologies may fundamentally change the organization of our economic, social, political and scientific activities.

А.Е. Хрушков, А.А. Птухин, Е.М. Божко
Уральский федеральный университет имени первого Президента России Б.Н. Ельцина
Екатеринбург, Россия

ТЕХНОЛОГИЯ BLOCKCHAIN

Аннотация: статья посвящена современной технологии “Blockchain”, предназначенной для хранения данных о сделках, транзакциях, обо всем том, что нужно записать и проверить. На данный момент использование этой технологии ограничено лишь несколькими сферами, но это лишь начало её пути. Главными достоинствами технологии “Blockchain” являются ее открытость и децентрализованность.

Ключевые слова: блокчейн, технология, транзакции, хеш-функция.

СПИСОК ЛИТЕРАТУРЫ:

1. Кнут Д. Искусство программирования. Том 3. Сортировка и поиск. – В 4-х томах. Пер. с англ. – 2-е изд. – М.: Вильямс, 2007.
2. Статья, на которую можно ссылаться: что такое блокчейн // Хабрахабр URL: https://habrahabr.ru/company/emercoin/blog/329276/ (дата обращения: 28.01.20018).
3. Hellerman, Herbert. Digital Computer System Principles. – N.Y.: McGraw-Hill, 1967.
4. Nakamoto, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. – 2008.