UDC 004.75 + 004.77

A.V. Kulikovskyi PhD student
(National Aviation University, Ukraine)

Distributed Ledger Blockchain and its application

Distributed Ledger and Blockchain Technology are described. The successful application of this technology in Ukraine government is considered and a new approach to construction of different systems based on Blockchain technology is proposed.

In recent years there has been rapid development of information technology areas and there are more and more of its components. One such technology is a distributed ledger Blockchain, allowing for greater storage reliability, integrity, availability and reliability.

Distributed Ledger is a database distributed between multiple network nodes or computing devices. For the first time, the technology was described in 1991 by a group of scientists and was designed to preserve digital documents without the possibility of forgery, change or creation of another date. Each node receives data from other nodes and stores a complete copy of the ledger. Node updates are independent of each other. The main feature of the distributed ledger is the lack of a single management center. Each node independently compiles and writes updates to the ledger independently of others. Then the nodes vote for the update to make sure that most nodes agree with the end-version. Voting and agreement about the authenticity of one of the copies of the ledger is called consensus. This process occurs automatically using the consensus algorithm. The agreement has just been reached - the distributed ledger is updated and the last agreed version is stored on each node.

Blockchains are one form of distributed ledger technology. It represents a sequence of blocks that are interconnected, and the connection itself between blocks is protected by cryptographic functions, so once recorded information in the registry is stored there permanently and cannot be modified or deleted. This approach to organizing the work of a distributed registry was described in 2009 by the developer under the pseudonym Satoshi Nakamoto for the creation of cryptography.

Let's consider the work of Blockchain more expanded. Each block or record in the Blockchain ledger contains basic information, its own hash and hash of the previous block. The set of data stored inside the block depends on the purpose of the Blockchain. For example, bitcoin Blockchain contains information about the sender, the recipient and number of coins. The hash of each block will be unique, as well as the data stored inside the block. Its uniqueness can be compared with a fingerprint of a person. Making any changes to the block at once will change the hash of the block. The third element of the block is the hash of the previous block. Thus the sequence of blocks is formed. This model makes Blockchain safe.

Consider an example. Figure 1 shows a sequence of three blocks. Each block has its hash and hash of the previous block. Block 3 points to block 2, block 2 to block 1. The first block is special, it cannot point to the previous block, since it does not exist, this block is called the genesis block.

Let's try to break the integrity and unauthorized changes to block 2. Changing even one single symbol in data block 2 will change its hash, which automatically will change all subsequent blocks and make them invalid. But using only hashing to prevent the creation of counterfeit blocks is not enough. Computers today have great power and can calculate thousands of hashes per second. Therefore, there is a high probability to block the block and list all the subsequent blocks to make Blockchain valid again.

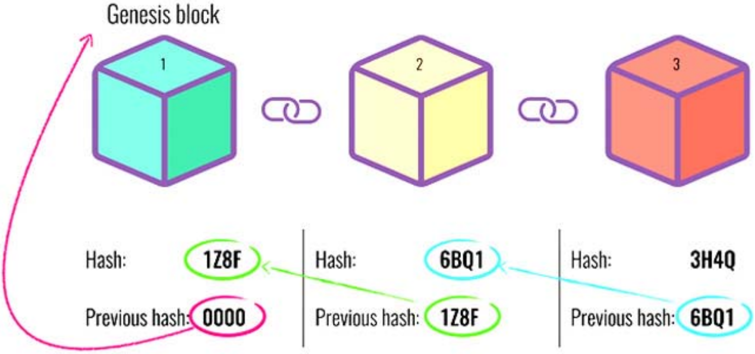

Fig. 1. Sequence of blocks

To prevent such cases, Blockchain has a Proof of Work algorithm. His essence is to look for a hash of functions, whose result starts with a certain number of zeros. This mechanism slows the creation of new blocks and protects against DDoS attacks. In the case of Bitcoin, it takes about 10 minutes to calculate a new block and add it to the overall sequence of ledger blocks.

Proof of Work greatly complicates the possibility of counterfeiting of blocks, since by falsifying one block, all subsequent blocks also need to be counted through the Proof of Work. Sharing this mechanism together with block hashes is the basis for Blockchain's security.

There is another way Blockchain protects itself and this decentralization. Instead of using a centralized object to manage the entire sequence, each node has its own copy of the registry and uses a peer-to-peer network to communicate with other nodes. Anyone can join the network, get a full copy of the registry, and participate in checking the validity of the block sequence. After creating a new block, it is sent to all networked nodes to verify the hash (authenticity of the block). If the check is completed, each node adds a new block to its copy of Blockchain. All nodes reach consensus, agreeing with what blocks are valid and which are not. Fake blocks will be rejected by other nodes in the network. Therefore, in order to successfully counterfeit a block, it is necessary to transfer its hash and hash of all subsequent blocks through the Proof of Work algorithm, and also have access to more than 50% of nodes of the network, which is practically impossible.

Despite the fact that the interest in Blockchain is increasingly related to the field of finance, the possibilities of its application are not limited to this area. But it should be noted that the use of Blockchain is appropriate only where it is necessary to handle a unique digital asset.

Ministry of Justice of Ukraine in partnership with the State Agency for E-Governance, the East Europe Foundation, and the BitFury Group, have launched a state-owned electronic trading platform for trademarks CETAM, the world's first auction on the basis of Blockchain technology. Today, the platform CETAM operates under the name of OpenMarket. Launching an updated trading platform enabled the system to operate without intermediaries, which allowed increasing transaction speeds, significantly reducing costs and preventing corruption. It has become impossible to delete or falsify data, each user can independently verify their validity and verify the accuracy of the data.

The second draft of the state level in Ukraine was the transition of the StateGeoCadastre of Ukraine to Blockchain technology. It was implemented by the Ministry of Agrarian Policy and Food of Ukraine together with the State Agency for Electronic Governance and Transparency International Ukraine. Due to the transition of the StateGeoCadastre to Blockchain it becomes impossible to modify or delete data as a result of unauthorized interference.

Blockchain finds practical application to confirm the authenticity of authorship and property rights. For digital identity and validation. In this case, Blockchain can be used to store any type of data and execute various transactions in a secure and open manner. In addition, the creation of identity in Blockchain can provide more control over access to personal data and the degree of their openness to others. Blockchain also finds application in such areas as e-voting and public administration.

References

1. Mills D., Wang K., Malone B., Ravi A., Marquardt J., Chen C., Badev A., Brezinski T., Fahy L., Liao K., Kargenian V., Ellithorpe M., Ng W., Baird M. Distributed ledger technology in payments, clearing, and settlement. Washington, D.C., 2016.
2. Hancock M., Vaizey E. Distributed Ledger Technology: beyond block chain. London, 2016.
3. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008.
4. The Difference Between Blockchains & Distributed Ledger Technology URL:https://towardsdatascience.com/the-difference-between-blockchains-distributed-ledger-technology-42715a0fa92 (accessed: 10.09.2018)