УДК 004.77
Vadym Mykhailov[1], Nataliia Zhukova[2]
[1]student of group CST-130, National University «Zaporizhzhia Polytechnic»
[2]PhD (Philology), assistant prof. National University «Zaporizhzhia Polytechnic»

BLOCKCHAIN AND HOW IT WILL CHANGE THE WORLD

There has been a lot of hype going around recently about bitcoin and other cryptocurrencies. It all started in 2008 when an anonymous developer or group of developers named Satoshi Nakamoto invented new electronic peer-to-peer cash system that had ability of conducting transactions without any government or banking system involvement which means that this system is decentralized. It has its own currency - digital token, Bitcoin.

Blockchain takes that model of ownership and decentralizes it. It gives the ownership, the power, and the voting rights to everyone, based on a distributed consensus model. No single authority can ever lock your funds, repossess what you own, or prevent you from transferring that property to somebody else. You are the only owner of your bitcoin wallet. With great power comes great responsibility: because of its decentralization no one is going to protect you if you lose access to your wallet or if your digital possessions get stolen by hackers.

Bitcoin is based on the system called "blockchain" which consists of blocks of data about transactions. Each block needs a special algorithm to be solved in order to be created. Users who solve these algorithms get bitcoin tokens in reward, this process is called "mining" and computers that are involved in mining are called "nodes". Each block also contains data about the previous block, hence cannot be altered in the future. This system controls itself and it is surprisingly secure, because in order to alter information about transactions hackers need to get access to 51% of nodes, there are thousands of them around the world, so it is practically impossible. Even creators will not be able to make major changes to the system after it has been opened to public.

The blockchain is a decentralized database where all the transactions are stored and validated that has value. The value can represent anything at all, e.g. money, lands, jewels, etc. With blockchain technology, you can transact directly to its receiver, which indulges any third party. The impact of blockchain here is establishing peer-to-peer transactions rather than a client-server model.

Blockchain will change the world by getting rid of centralized control. Although the public blockchain system is autonomous, a private blockchain system does need authentication to function. But it can still reduce the level of centralized control.

Using the hash function and cryptography method, all the transactions are encrypted, and none can keep track of your transactions. One of the best things about blockchain is that it promotes transparency.

Blockchain will change the world by getting rid of corruption. As we are still operating on legacy network systems and paper-based documents, it is easy for fraudulent parties to alter them. But blockchains are completely immutable by nature. It is impossible to alter contents inside a block. If someone tries to tamper with it, all the nodes in the system will reject it instantly.

However, there is a number of challenges associated with blockchain.

51% attacks are among the most discussed ones. Such an attack may happen if one entity manages to control more than 50% of the network hashing power, which would eventually allow them to disrupt the network by intentionally excluding or modifying the ordering of transactions.

Despite being theoretically possible, there was never a successful 51% attack on the Bitcoin blockchain. As the network grows larger the security increases and it is quite unlikely that miners will invest large amounts of money and resources to attack Bitcoin as they are better rewarded for acting honestly. Other than that, a successful 51% attack would only be able to modify the most recent transactions for a short period of time because blocks are linked through cryptographic proofs (changing older blocks would require intangible levels of computing power). Also, the Bitcoin blockchain is very resilient and would quickly adapt as a response to an attack.

Another downside of blockchain systems is that once data has been added to the blockchain it is very difficult to modify it.

Blockchain uses public-key (or asymmetric) cryptography to give users ownership over their cryptocurrency units (or any other blockchain data). Each blockchain address has a corresponding private key. While the address can be shared, the private key should be kept secret. If a user loses their private key, the money is effectively lost.

Blockchains are highly inefficient. Since mining is highly competitive and there is just one winner every ten minutes, the work of every other miner is wasted. As miners are continually trying to increase their computational power, they have a greater chance of finding a valid block hash, the resources used by the Bitcoin network have increased significantly, and it currently consumes more energy than many countries, such as Denmark, Ireland, and Nigeria.

Blockchain ledgers can grow very large over time. The Bitcoin blockchain currently requires around 200 GB of storage. The current growth in blockchain size appears to be outstripping the growth in hard drives and the network risks losing nodes if the ledger becomes too large for individuals to download and store.