computing continues to grow in popularity, it is important for organizations to prioritize security and take proactive steps to protect their sensitive data.

References

1. AWS Security Best Practices / Jeff Barr – Amazon Web Services, 2018 – 76 p.
2. Implementing Identity Management on AWS / Lehtinen J. – Packt Publishing, 2021 – 504 p.
3. Cloud Computing Security: Foundations and Challenges / John R. Vacca – CRC Press, 2020 – 522 p.

BLOCKCHAIN TECHNOLOGY. DLT.

Priadko V. S., student
Gerasymchuk T. V., Associate Professor
Kharkiv National University of Radio Electronics

Today, few people can say they have never encountered, or at least heard of, blockchain or cryptocurrencies; those who can, are usually envied. Years of blockchain technology development in one direction - cryptocurrencies - and the monopolization of the cryptographically-secure distributed networks market by blockchains have shaped a firm thesis in the average observer: blockchain equals cryptocurrencies. Of course, part of this is true, almost always cryptocurrencies are built within the framework of one or several blockchains, but not all blockchains are created to bring one more value bearer into the world.

Blockchain is one of the ways to implement distributed ledger technology. A distributed ledger is one of the types of P2P networks in the first financial-economic approximation. Blockchain is not a separate technology that was created to deceive people for the purpose of enrichment, but rather a logical product of progress and work of scientists and engineers.

After the collapse of several centralized crypto exchanges, recent breaches of popular protocols (products that are entirely or partially built on the basis of blockchain), and the bankruptcy of some American banks, Western society, which had previously been rather unsympathetic to the decentralization of the financial system,

stigmatized all manifestations and uses of this technology. Initially understandable discontent spread to exchanges and institutional beneficiaries of crypto companies, but eventually generalized to the blockchain as a whole.

Ukraine, as a digital country, refrained from criticism and did not even implement regulation of crypto assets. Moreover, before the war, the Ministry of Digital Transformation planned to base the digital currency of Ukraine's central bank on the Stellar blockchain. Despite the Ukrainian government's loyalty, the decentralized application development industry was severely affected indirectly - due to a lack of orders and bankruptcy of clients.

To stop fearing this powerful technology, one needs to discard populism and approach from a technical perspective.

Distributed ledger technologies are a group of approaches and methods that allow data to be stored simultaneously on many physical machines, with the guarantee that no one will be able to change it after it have been recorded into the system. These systems are usually transactional - that is, each data mutation is a separate operation with ACID properties (to be true, one can argue about the scalability trilemma, but for simplicity, let's believe they are ACID). Moreover, such systems are not multitasking - transactions in them cannot be performed in parallel, except for some specific compromise architectures.

Blockchain technology, in turn, is a type of DLT, the properties of which are achieved by a special structure for storing transactions - in the form of blocks containing several transactions, from which a hash is taken. This hash - the hash of the current block - is stored in part of the next block and is hashed together with the transactions of such a block. In this way, each block of transactions contains a piece of information about the previous block, and the previous one - about the one before it, and so on.

Thanks to the special properties of cryptographical hash functions, namely their irreversibility and uniform mixing of information, we can guarantee that any change in such a chain of blocks - a blockchain - can be quickly, unambiguously, and justifiably exposed. In addition, the transactions themselves are also stored in a special data

structure that uses hash properties (in most cases it's a Merkle tree), so it is easy to determine which transaction has been compromised.

The only thing that may remain unclear is the mechanism for coordinating versions of this sequence of transaction blocks between multiple physical machines - the so-called nodes. This is a well-known problem, the so-called Byzantine Generals Problem. It has many compromise solutions, which is why there are at least a couple of dozen consensus algorithms in the industry. These solutions are compromise because if a majority of equal nodes agree to include an incorrect transaction in a block, such a block and such a branch will be considered valid and viable by the system. However, such situations are extremely rare and lead to the reformation of the entire sector.

This is what a simple classic blockchain looks like - a set of nodes, a hashed structure, and a consensus mechanism. There are also more exotic types, such as those implemented on the basis of a Directed Acyclic Graph, or with consensus based on reputation. But all of them, since they are built as a distributed ledger, require some internal carrier of value, which would represent the reputation of a node, the right to vote in a quorum, payment for changing the state of the network, and so on. Such a currency exists in every blockchain - it is usually called a native coin.

The architecture of the blockchain and the consensus mechanism provide for a fee to be charged for each sent transaction - and the more complex the transaction, the more power will be required by the nodes for its processing, the more it will cost. These funds are usually partially burned to keep the currency deflationary, and partially passed on to validators - special nodes that maintain consensus in the network - as a reward.

With the aim of technical enlightenment of society about blockchains, another topic should be considered - second-level solutions. Since sending transactions can be quite costly, industry leaders have come up with a way to lower this price - or rather, to reduce the number of transactions. To do this, abstract blocks are formed over the first-level network - according to the same hashing scheme that is already familiar to us. Then they form proof of block’s (or chain of blocks) validity and send it in a single transaction to the "mother" blockchain. Due to the reduction in the number of

transactions in the basic blockchain, the price of each of the L2 transactions decreases proportionally. This solution is called a rollup, and they mainly differ from each other in the method of forming proof of validity and verification.

Leading today are rollups formed with the help of zero-knowledge proof. This is a field of mathematics, not a specific technology, so there could be countless implementations of it, but primarily it is zkSNARK and zkSTARK.

The main idea is that you can prove something to someone without revealing that "something", declaring only that "something" is true. For example, you can prove that there is a certain amount of money on your bank account without revealing your balance. Or you can prove that there is a penguin in the picture, without revealing where exactly it is.

Retrospectively, zkSNARK and zkSTARK did not aim for broad implementation of zk-proofs, zero disclosure was obtained by them unintentionally, as an addition to succinctness or transparency respectively. However, despite this, they gave an impuls to the development of a new, advanced branch of computer science.

For this reason, I urge not to be prejudiced against any technology, because progress and innovations can not be criminal, only people and their application of the products of progress can be.

References

1. Governing Carbon Markets with Distributed Ledger Technology – Michael Mehling
2. Proofs, Arguments, and Zero-Knowledge - J Thaler

ANTI-VIRUS TOOLS: DETECTING AND PREVENTING MALWARE

Miedviediev A. O., student,
Suknov M.P., PhD, Associate Professor,
Kharkiv National University of Radio Electronics

As cyber threats and malware continue to evolve, the need for effective anti-virus tools becomes crucial. This article provides an overview of various anti-virus tools and their underlying detection and prevention techniques. By understanding the