SECTION 9. INFORMATICS AND CYBERNETICS

DOI: 10.46299/ISG.2024.MONO.TECH.1.9.1

9.1 Aspects of blockchain technology as a component of information security

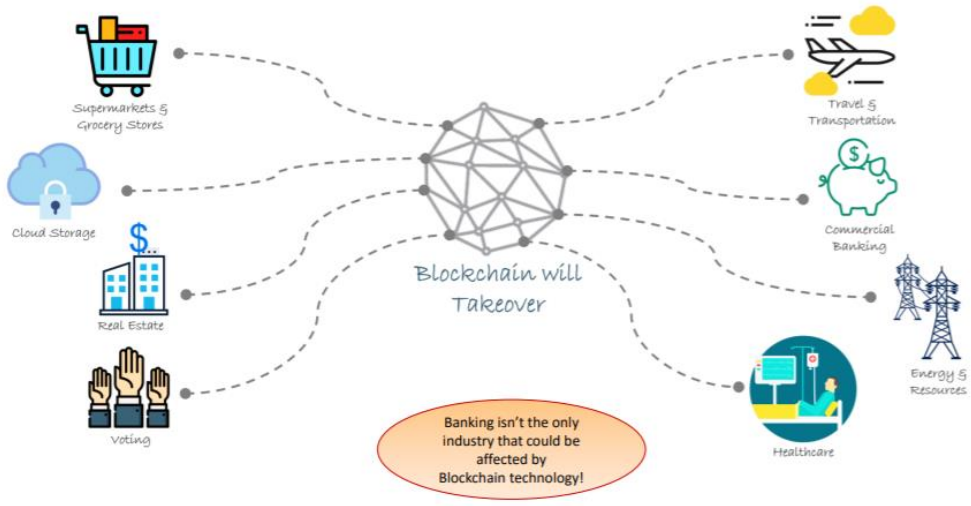
With the development of means of information communications and the possibility of harming the information that is stored and transmitted with their help, information security arose. Ensuring information security helps to protect information and information infrastructure from negative influences. Such influences may be accidental or intentional, internal or external, and the result of their interventions may be the loss of important information, its unauthorized change or use by third parties. It is possible to ensure complete and reliable information security only if a comprehensive and systematic approach is used. The information security system must be built taking into account all current threats and vulnerabilities, as well as taking into account those threats that may arise in the future, so it is important to ensure the support of continuous and reliable control.

Blockchain technology began its development as the basis of the Bitcoin cryptocurrency, but later became a promising technology for information security. Blockchain offers ample opportunities to maintain a high level of data security through robust encryption mechanisms, data integrity, network resilience, and scalability. As a result, the transition from a traditional information security system to a blockchain-based system can be beneficial for organizations in almost any industry [331].

Taking into account all the advantages of Blockchain technology and the existing threats of modern information systems, the development of new methods of ensuring information security based on Blockchain is an urgent and important task, both from a scientific and a practical point of view.

Today, there is a rapid development of information and telecommunication systems and technologies and, as a result, their wide application in various spheres of society. A significant number of modern public and private institutions use information and telecommunication systems to manage production processes, support decision-making, save and process information, search for necessary data, etc. Almost all of

these systems work on the principle that process management is centralized and full control over the system can be gained by gaining access to the main central server. As a result, the risk of compromising the entire system, the number of ITS vulnerabilities and threats increases (Pic. 1).



Pic. 1 – Fundamentals of Blockchain Technology

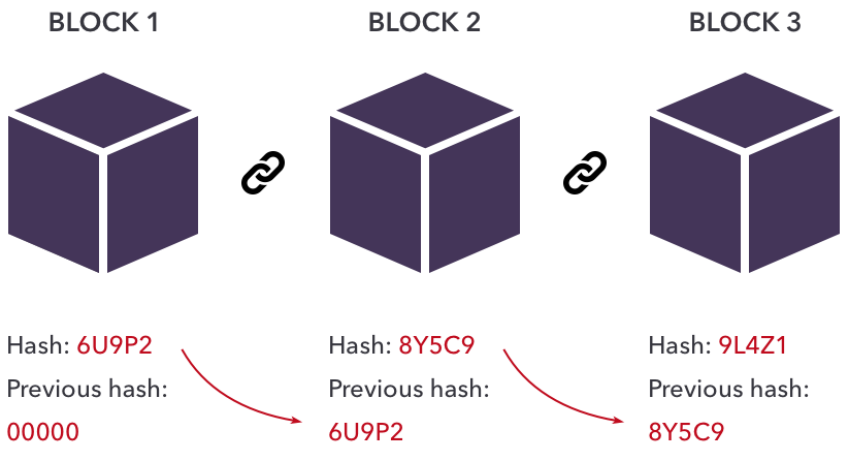
In connection with the public interest in blockchain technology and its active application in various fields, such as finance or accounting, it is appropriate to conduct an analysis of the effectiveness of blockchain application in the field of information security. The first work on a block chain protected by cryptographic functions was described in 1991 by Stuart Haber and W. Scott Stornetta. They wanted to implement a system where the timestamps of documents could not be tampered with or damaged. In 1992, Bayer, Haber, and Stornetta used a Merkle tree in the project, which improved efficiency by allowing multiple documents to be included in one block.

The first version of the blockchain was developed by a person (or group of people) known as Satoshi Nakamoto in 2008. This approach to organizing the work of the distributed ledger was embodied by Nakamoto in 2009, when he developed the main component of the Bitcoin cryptocurrency, where it acts as an open ledger for all network transactions [332].

The term Blockchain, with its name, partly characterizes the principle of operation of the technology itself. "Block" is a block, "chain" is a chain. From which it follows

that Blockchain is a chain of blocks. But not just a chain. It maintains a strict sequence determined by complex cryptographic functions. Blocks are data about transactions, agreements and contracts within the system presented in cryptographic form. All blocks are built in a chain, that is, they are connected in series. To add (write) a new block, you need to check the sequence of previous blocks. Let's consider the work of Blockchain in more detail. Each block or entry in the Blockchain registry contains basic information, its own calculated hash, and the hash of the previous block. The set of data stored inside the block depends on the intended purpose of Blockchain. For example, the Bitcoin Blockchain contains information about the sender, the recipient and the number of coins transferred. Each block's hash will be unique, as will the data stored within the block. Its uniqueness can be compared to a human fingerprint. Making any changes to a block will immediately cause the block hash to change. The third element of the block is the hash of the previous block. In this way, a sequence of blocks is formed. This model makes Blockchain secure. Let's consider an example. Figure 1 shows a sequence of three blocks [333].

Each block has its own hash and the 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 because it does not exist, this block is called the genesis block. Let's try to break the integrity and make unauthorized changes to block 2. Changing even one character in block 2's data will change its hash, which will automatically change all subsequent blocks and render them invalid. But using hashing alone is not enough to prevent the creation of fake blocks. Today's computers are very powerful and can calculate thousands of hashes per second (Pic. 2).



Pic. 2 – Sequence of blocks

Therefore, there is a high probability of forging a block and recalculating all subsequent blocks to make the blockchain valid again. To prevent such cases, the blockchain has a Proof of Work algorithm. Its essence is to find a hash function, the result of which starts with a certain number of zeros. This mechanism slows down 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 network's overall block sequence. Proof of Work makes it much more difficult to forge blocks, because after forging one block, all subsequent blocks must also be listed through Proof of Work. The sharing of this mechanism along with block hashes forms the basis of Blockchain security. There is another way Blockchain protects itself and that is decentralization. Instead of using a centralized entity 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, obtain a full copy of the registry, and participate in the validation of the block sequence. After creating a new block, it is sent to all nodes connected to the network to verify the hash (authenticity of the block). If the verification is passed, each node adds a new block to its copy of the Blockchain. All nodes reach a consensus, agreeing on which blocks are valid and which are not. Forged blocks will be rejected by other nodes in the network. Therefore, in order to successfully falsify a block in the blockchain, it is necessary to calculate its hash and the hash of all subsequent blocks through the Proof of Work algorithm, as

well as have access to more than 50% of the network nodes, which is practically impossible [334].

According to the principle of its work, Blockchain has such advantages as:

- decentralization (the main data storage server is missing. All records are stored by each network participant);

- transparency of work (any of the participants can check all transactions taking place in the system);

- security (all operations are reliably protected by cryptographic functions);

- reliability (any attempt to make unauthorized changes will be rejected by other members of the network).

The blockchain network does a good job of maintaining data integrity. Due to the existence of many copies of the database and making changes to it only after confirming the correctness of the information by other network participants, the information remains protected from intentional, unauthorized or accidental changes, as well as any changes in the process of storage, processing or transmission. Information becomes impossible to change due to technical failures in the operation of the network node or due to the human factor, because operations are confirmed thanks to complex mathematical functions. As a result, the information remains unchanged and correct. Ensuring this category of information security enables stable operations, making the right decisions and the ability to save data in the form in which it was created. According to the principle of availability, information should be available to authorized persons at the right time. In the blockchain network, each participant is considered authorized and at any time can read or write data and participate in the verification of data added by other participants. Confidentiality of information is achieved by providing access to it with the least privileges, that is, an authorized person should have access only to those data that are defined for her by access rights. Each member of the network can get a full copy of the database on his device and read all the data in it, which fundamentally contradicts the principle of data privacy. Storing data in the blockchain in an encrypted form will not fundamentally solve the problem of privacy, because in most cases, confidential data does not lose its relevance over time, like, for

example, personal data. And decoding the received data becomes a matter of time and depends on the computing power of the attacker who is trying to access the information.

Blockchain technology has a number of advantages, in particular, it is possible to single out several key characteristics that influenced its development [335].

Decentralization. If we consider conventional centralized systems (governing bodies), then each transaction must be confirmed by a central trusted link, for example, how such a link can act as a central bank. In turn, this leads to unavoidable costs for IS provision. In other words, a transaction in the blockchain network can be conducted between any two equal users without authentication by a central server. Thus, the application of blockchain technology can significantly reduce the costs of maintaining the functioning of servers (including development costs and operational costs) and solve certain tasks of security and ensuring the necessary performance.

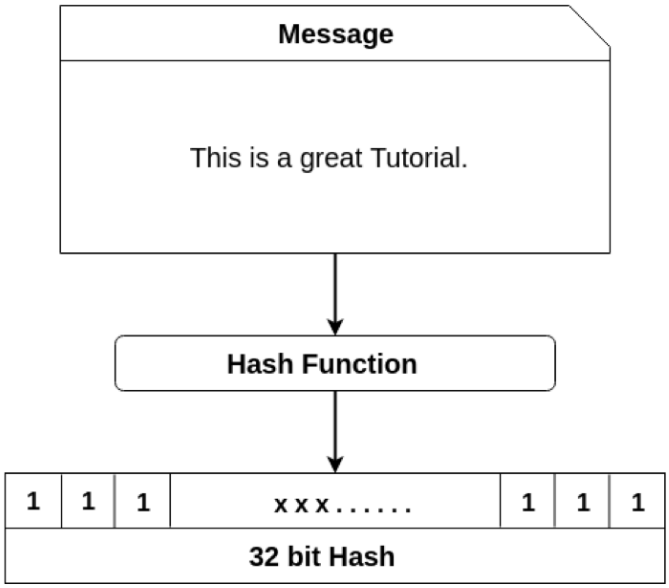
Immutability. Any transaction in the blockchain network is confirmed by other participants of this network and recorded in the corresponding block. Each network node has at its disposal the data of all transactions that have taken place in the network. It is impossible to make changes to transactions because blocks and transactions are verified by other nodes. If the majority of nodes (users) believe that the transaction is valid, it is recorded in the registry. This helps ensure transparency and integrity of information. Thus, without the agreement of the majority of nodes, no one will be able to add transaction blocks to the distributed ledger.

Anonymity. Each user can interact with the blockchain network using generated addresses. In addition, the user can generate multiple addresses to avoid unique identification. There is no central server that stores user identification data. This fact ensures a certain degree of privacy regarding the transactions included in the blockchain. Anonymity is achieved only in public blockchain networks, described in more detail in the next section.

Transparency. Since each transaction on the network is verified and recorded with a time stamp, users can easily verify and track past records. For example, in the cryptocurrency Bitcoin, each transaction can be iteratively traced back to previous transactions. This improves the traceability and transparency of data stored in the

blockchain. Hash functions are one of the most widely used cryptographic algorithms in blockchain technology. These are cryptographic (but not encryption) algorithms designed to protect data integrity. Any piece of data can be hashed, regardless of its size or type. In traditional hashing, regardless of the size, type, or length of the data, the hash generated by any data is always the same length. A hash is intended to be used as a one-way function [336].

A hash function takes an input string (numbers, alphabets, media files) of any length and converts it into a new string of fixed length. The fixed bit length can vary (eg 32-bit, 64-bit, 128-bit, or 256-bit) depending on the hash function used. A string of fixed length is called a hash. This hash is the result of the hash algorithm (Pic. 3).



Picture 3 – Sequence of blocks

Hash functions arose out of the need to make content uniform and to use unique identifiers. The hash function provides cryptocurrency with a high level of security, and although theoretically nothing is completely secure from hacking, this approach provides the highest level of complexity available today. When using the hash function, you can achieve a high level of system security. Including, with its help, it is possible to hash passwords and encrypt other data. To be secure and usable for cryptocurrencies, a hash function must be collision-resistant, which means that it is impossible to find two input strings that will give the same result [337].

For an ideal hash function, the following conditions are fulfilled [338]:

- the hash function is deterministic, that is, the same message leads to the same hash value;
- the value of the hash function is quickly calculated for any message;
- it is impossible to find a message that gives the specified hash value;
- it is impossible to find two different messages with the same hash meaning;
- a small change in the message changes the hash so much that the new and old values seem uncorrelated [339].

Hash functions in the blockchain guarantee the "irreversibility" of the entire chain of transactions. Each new block of transactions references the hash of the previous block in the ledger. The hash of the block itself depends on all the transactions in the block, but instead of passing the transactions sequentially to the hash function, they are compiled into a single hash value using a binary hash tree (Merkle tree). Thus, hashes are used as a replacement for pointers in conventional data structures: linked lists and binary trees. The slightest change in any part of the input results in a huge change in the output; this is the undeniable security of blockchain technology. Changing any record that has previously occurred in the blockchain will change all hashes, making them false and out of date. This becomes impossible given the decentralized structure of the blockchain. The first block of the blockchain, known as the genesis block, contains transactions that, when combined and verified, produce a unique hash. This hash and any new transactions that are processed are then used as input to create a brand new hash that is used in the next chain block. This means that each block references its previous block through its hash, forming a chain back to the genesis block. Thus, transactions can be safely added. A hashing algorithm is considered secure until it finds a collision. Once this happens, the algorithm is considered officially invalid, as happened with MD5 and SHA-1. The SHA-256 (Secure Hashing Algorithm) hashing algorithm is used to convert an array of information into a hash in cryptocurrencies (Pic. 4).

Input	Output
Hello	185F8DB32271FE25F561A6FC938B2E264306EC304EDA518007D1764826381969
hello	2CF24DBA5FB0A30E26E83B2AC5B9E29E1B161E5C1FA7425E73043362938B9824
BANKEX Proof-of-Asset protocol	6C3C86FD24B044BC19FD1764EEB5D04E7EC8833199A62C85150B92B39D2C8CF5

Picture 4 – Example of SHA-256 hashing

SHA-256 is a one-way function for generating fixed-length (256-bit, 32-byte) digital strings from input data up to 2.31 exabytes (264 bits) in size, and is a special case of the SHA-2 (Secure Hash 2) family of cryptographic algorithms published by US NSA in 2002. Hash functions of the SHA-2 family are built on the basis of the Merkle-Damgard structure [340].

The main characteristics of the algorithm:

- block size indicator: 64 bytes;
- the maximum permissible message length: 33 bytes;
- characteristics of message digest size: 32 bytes;
- internal position length parameter: 32 bytes;
- number of iterations in one cycle: 64;
- the speed achieved by the protocol: approximately 140 Mb/s.

As a result of the analysis, it can be concluded that, according to the principle of its operation, the blockchain can be used with high reliability to build information and telecommunication systems that are designed to process and save open data in order to ensure their integrity and availability. It is not advisable to use blockchain in general for storing and processing confidential data, since anyone can access confidential data stored in an open blockchain database.