UDC 004.75 **DOI:10.30837/rt.2020.1.200.10**

P. STETSENKO, G. KHALIMOV, Prof., Dr. of Science, Y. KOTUKH, Phd.

ANALYSIS OF ATTACK SURFACES ON BLOCKCHAIN SYSTEMS

This paper presents a study of attack surfaces and possible ways of conducting various attacks on decentralized systems based on Blockchain technology. To accomplish the task, the effectiveness of the attack is studied relative to the plane of its application, namely, relatively:

- cryptographic designs of Blockchain technology;
- distributed architecture of systems based on Blockchain technology;
- Blockchain application context.

Several attacks have been identified for each of these planes, including malicious mining strategies, coordinated peer behavior, 51 % attacks, domain name attacks (DNS), distributed denial of service attacks, delayed consensus achieving, Blockchain branching, orphaned and obsolete blocks, digital wallet thefts and privacy attacks. It then investigates the causal relationship between these attacks and analyzes how one fraudulent action can lead to the possibility of other attacks. A minor contribution of this work is to highlight effective countermeasures adopted by Blockchain technology or proposed by researchers to mitigate the effects of these attacks and fix vulnerabilities in Blockchain-based decentralized systems.

Despite the functionality that Blockchain technology brings to applications, recent reports highlight the security risks associated with the given technology. For example, in June 2016, an unknown attacker managed to withdraw US $ 50 million from the DAO, a decentralized autonomous organization that operates according to the rules of smart contracts based on Blockchain technology [1]. In August 2016, adversaries have stolen Bitcoin cryptocurrency worth $ 72 million from the Bitfinex exchange in Hong Kong [2]. In June 2017, Bitfinex also experienced a distributed denial of service (DDoS) attack, which led to a temporary suspension of its work. Several Bitcoin and Ethereum exchanges (a decentralized Blockchain platform) have also suffered from DDoS attacks, which often impede service availability for users. These attacks have application-specific consequences. For example, for Blockchain cryptocurrencies, the process of constant investment in their work is important, therefore DDoS attacks can cause cryptocurrency devaluation.

Blockchain security is paramount for potential users to participate. For example, investors primarily take into account the security of cryptocurrencies when studying the risks associated with investing in them. Understanding the threats associated with Blockchain systems in general is the first step towards building a secure architecture for decentralized Blockchain-applications. The aim of this work is an in-depth study of attack surfaces for Blockchain technology.

Blockchain technology will be used in many applications in a wide variety of digital fields, so analyzing attacks that could jeopardize existing applications is an urgent task. The paper presents a classification of attacks in three classes:

- attacks related to cryptographic constructions and algorithms used by Blockchain technology (for example, branching of a Blockchain ledger, obsolete and orphaned blocks);
- attacks related to the architecture of a peer-to-peer network, on which Blockchain systems are mainly built (for example, malicious mining, 51 % attack, delay in achieving consensus, DDoS attack and DNS attack)
- attacks related to the context of applications that use Blockchain technology (for example, Blockchain absorption, double-spend attacks and wallet application theft).

The aim of this work is to single out the nature of attacks aimed at decentralized Blockchain-based systems, peer-to-peer architecture and applications. The paper analyzes the causal relationship between conducting an attack and the emergence of opportunities for other attacks because of this and presents the sequence of possible attacks. The work considers the consequences of attacks for Blockchain systems using the example of Bitcoin cryptocurrency. The result of the work can be

applied to development of an integrated approach to building secure Blockchain-based decentralized systems.

1. Attacks on Blockchain technology

1.1. Branching attacks

Branching is a state in which the nodes in the network have a different view of the state of the Blockchain ledger, persisting for long periods of time or indefinitely. Such branches can be created unintentionally due to failures in the mechanism for achieving consensus or incompatibility when updating client software. Branching can also be caused by malicious actions that use conflicting validation rules, or by "malicious mining" (section 2.1). In addition, malicious branching can be either soft or hard, the latter occurring when new blocks accepted by the network are invalid for nodes that have a knowledge of the Blockchain ledger before the branching begins. On the other hand, soft branching occurs when some blocks are invalid for nodes that have a case idea after the branching occurs. Thus, the branching of the Blockchain transaction ledger is a contradictory state that can be used by attackers to cause confusion, conduct fraudulent transactions and spread mistrust in the network [3]. An example of hard branching, which results from peers following conflicting Blockchain ledger status rules is shown on fig. 1.

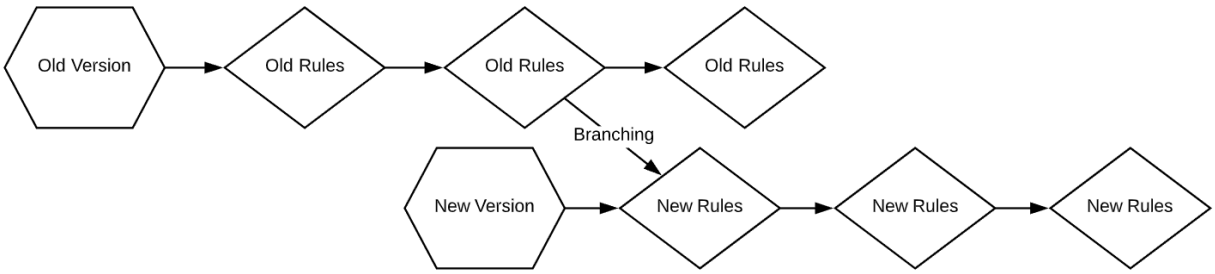

Fig. 1. An example of a hard branching of the Blockchain ledger

An example of the use of Blockchain ledger hard branching is the rollback of transactions on the Ethereum platform to return digital assets after a successful attack on a decentralized autonomous organization (DAO) and theft of a third of the cryptocurrency [1]. However, this required the agreement of most network nodes. In such a scenario, if the delay in achieving consensus is due to a majority attack (or 51 %-attack) or DDoS-attacks, fraudulent actions become difficult and long delays can ultimately lead to the depreciation of the cryptocurrency.

1.2. Obsolete and orphaned blocks

In the process of achieving consensus between participants in the system, two forms of inconsistencies may arise that may leave valid blocks not added to the Blockchain transaction ledger.

1. An "obsolete block" is a block that has been successfully calculated but not accepted in the current main version of the ledger (that is, the version that is most difficult to recreate). Section 2.1 presents that the Blockchain attack vector, known as "malicious mining," can lead to the creation of obsolete blocks in the network, which deprives an honest miner of his reward.
2. An "orphaned block" is a block whose previous (parent) hash field indicates an unauthentic block that is not included in the Blockchain transaction ledger, and therefore cannot be checked and validated.

These discrepancies can be introduced by an attacker or caused by competition conditions in the mining process. Obsolete blocks can initially be accepted by most networks, but they can be rejected later when confirmation is received for a longer chain of blocks (i.e., the new current major version of the transaction ledger state) that does not include this particular block. Fig. 2 shows an example of a Blockchain ledger with obsolete and orphaned blocks.

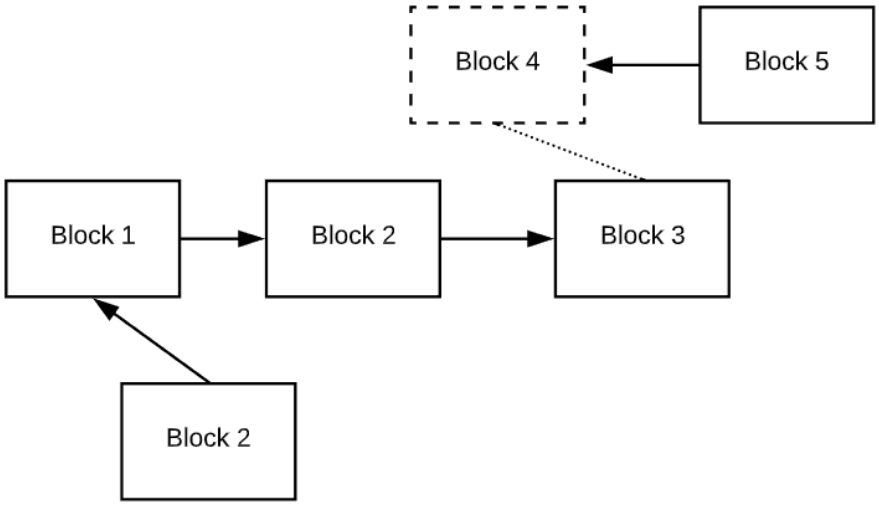

Fig. 2. Example of Blockchain ledger with obsolete and orphaned blocks

It should be noted that the obsolete block (lower block 2 and block 4) are valid, but they are not part of the Blockchain ledger. The orphaned block (block 5) does not have a block preceding it belonging to the current main version of the Blockchain ledger.

In Bitcoin cryptocurrency, the first orphaned block was found on March 18, 2015, this was the beginning of the period of the largest number of orphaned blocks, which lasted until June 14, 2017. Since then, not a single discarded block has been calculated [4].

1.3. Blockchain attacks counteraction

Elimination of the consequences of soft branching of the Blockchain transaction ledger is a relatively simple process, for this it is necessary to achieve a unified opinion on the state of the ledger by all nodes of the network and to resume the decentralized system from this point on. Enabling hard ledger branching can be a difficult task because conflicting versions can be time-consuming and with a large number of transactions over the period of branching. Although the rollback to the ledger version preceding hard branching is a fairly global operation within the framework of a Blockchain-based decentralized system, the decision to carry it out can be achieved by the same principle of consensus building that was presented earlier.

The number of orphaned blocks in Bitcoin cryptocurrency has been decreased due to the transition to highly centralized mining-pool networks, which reduced the likelihood of orphaned blocks, which is high enough for a decentralized mining process.

2. Attacks on Blockchain peer-to-peer network architecture

The peer-to-peer network architecture that underlies Blockchain technology serves as the basis for providing certain guarantees, including security. However, at the same time, this architecture actually contributes to several attack surfaces described in this section.

2.1. The malicious mining

An attack called "malicious mining" is a strategy that some miners choose to try to increase their rewards by intentionally keeping their blocks closed. Instead of revealing the calculation of each block to all participants, such miners continue to calculate new blocks covertly to get a longer version of the Blockchain ledger than the current main system version. As soon as the general main version of the ledger begins to approach the length of the hidden version of the ledger of the malicious miner, they publish the calculated blocks for a reward [5]. The scheme for carrying out an attack of malicious mining is presented in fig. 3.

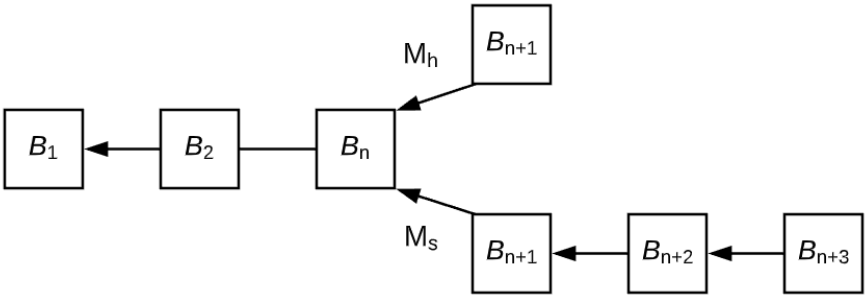

Fig. 3. The scheme for carrying out an attack of malicious mining

Consider the Blockchain ledger with blocks B_1, B_2,…, B_n. Suppose an honest miner M_h has successfully calculated the next block B_{n+1}, and on the same network, the malicious miner M_s has also calculated the next block B_{n+1}. The attacker does not disclose the fact that he successfully calculated a new block and successfully extracts two more blocks – B_{n+2} and B_{n+3}. At the moment, most of the network has a general view on the current main version of the Blockchain transaction ledger, however, despite this, an attack of malicious mining can be carried out.

Let the honest miner M_h has the hash value of block B_{n+1} below both the target threshold set for the current period by the system and the hash value of the attacker block M_s B_{n+1}. If you publish the calculation of only these two blocks, then the new current main version of the ledger with the M_h block would be accepted because of its greater computational complexity compared to the M_s block. Then, after some time, the attacker M_s reveals the calculation of all of his blocks – B_{n+1}, B_{n+2} и B_{n+3}. The mechanism for achieving consensus of Blockchain technology is designed so that the version with a large number of successfully calculated blocks will invariably be selected as the new main version of the ledger. Thus the network switches to the ledger version with M_s blocks, and the B_{n+1} block of the honest miner M_h, for the successful calculation of which computational resources have already been spent, will be considered obsolete. The incentive for an attacker to apply such a mining strategy is to maximize block rewards by covertly calculating and then publishing a longer version of the Blockchain transaction ledger.

The successful conduct of this attack entails the negative consequences of the Blockchain system, since it invalidates the blocks calculated by honest miners who put their computational resources into the operability of a decentralized system. When conducting this attack simultaneously, several attackers open it for other attacks, the relationship between them is shown in fig. 4.

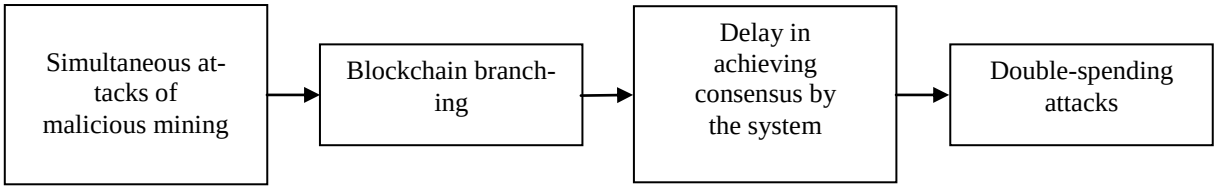

Fig. 4 Consequences of the simultaneous conduct of malicious mining

In the case when two attackers simultaneously carry out this attack, that is, they compete for adding their version of the transaction ledger to the system, the likelihood of branching of the Blockchain ledger increases (section 1). Branching, in turn, can delay in achieving consensus on the network, and this, in turn, can lead to other potential attacks, such as double waste attacks (section 3.2).

2.2. 51 % Attack

A 51 % attack or a majority attack occurs when a single attacker, a group of nodes, or a mining pool (a combination of miners) in a network reaches most of the total computational power of min-

ing in the system and gets the ability to manipulate the functionality of the Blockchain system. Having 51 % of the processing power allows an attacker (s) to:

- prevent verification of transactions or blocks, that is, make them invalid;
- cancel transactions in some time after their confirmation, thereby realizing a double-spending attack;
- not allow other miners in the system to calculate any blocks for a short period of time [6].

In this attack, the attacker's blocks will be added to the Blockchain ledger with a higher probability, since the available computational power allows the attacker to calculate new blocks faster than other participants in the system. An attacker can include fraudulent transactions in their blocks or use them to implement double-spending attacks. Transactions in Blockchain systems are irreversible, and only one transaction of two identical ones can be considered valid.

The 51 % attack is not only theoretical, in July 2014 the association of miners "GHash.IO" owned more than 51 % of the computational power in the Bitcoin network [7]. This has raised concerns about the reliability of cryptocurrency and its vulnerabilities. Later, "GHash.IO" was decreased in size and closed in October 2016. It should be noted that for fraudulent activities it is not always necessary to have more than half of the processing power of the network. A wide range of attacks can be carried out with a sufficient degree of probability in the presence of even 25 % of the computational power of the network.

2.3. DNS-attacks

When you initialize a new node in the network of the Blockchain system, i.e., when you first connect a new member to the network, he will not know about active peer nodes. For example, in the Bitcoin network, to detect them, a bootstrap phase is required, which uses DNS. DNS seeds are requested by the nodes upon joining the network to obtain additional information about other active peers [8]. However, DNS opens up a wide plane for attacks on the Bitcoin network, such as a man in the middle, cache poisoning, etc. As a result, using the plane of DNS attacks, an attacker can potentially isolate the peer nodes of the Blockchain system (by providing them incorrect list of active peers at the boot stage), distribute fake blocks with fraudulent transactions among new nodes, invalidate transactions, etc. [9].

2.4. DDoS-attacks

DDoS-attack is one of the most common attacks on online services. Blockchain technology, despite being a peer-to-peer system, remains susceptible to DDoS-attacks. This is confirmed by successful DDoS-attacks on Blockchain applications such as Bitcoin and Ethereum [10,11]. Manifestations of DDoS-attacks can vary, depending on the nature of the functionality of the Blockchain application, the features of its network architecture and the behavior of peer nodes. For example, on a Bitcoin network, a 51 % attack could lead to a denial of service. In particular, if a group of miners gains significant hash power, they will be able to prevent other participants from adding their calculated blocks to the Blockchain transaction ledger, invalidating current confirmed transactions, thereby causing a malfunction of the system. Intentional branching of the Blockchain ledger can take on the nature of a hard branching, which, in turn, also leads to similar consequences of denial of service.

Another possibility for conducting a denial of service attack is a limited number of transactions in each block of the Blockchain ledger, which can be processed by the network in a separate period of time. For example, on average, Bitcoin cryptocurrency networks require 10 minutes to add a new block, the maximum amount of which is 1 MB. The average transaction volume is approximately 500 bytes, which allows you to place about 2000 transactions in a block, and the maximum number of transactions added to a block in Bitcoin cryptocurrency is 2210 [4]. Based on this, the average transaction processing speed cannot exceed 200 transactions per minute. Taking into account the fact that each transaction requires at least two peers that must participate in the transaction, the total number of active peers served by the network per minute (i.e. when the block containing the transaction is added to the ledger) will be not less than 200.

An attacker can use the operational feature of a decentralized system described above by introducing entities controlled by him into the system, for example, controlling several wallets. In addition, using these entities, an attacker can perform several transactions with a minimum amount of funds between different entities controlled by him. By creating a sufficiently large number of such transactions in a short period of time, the attacker creates a high computational load on the network, necessary to calculate and add his transactions to the ledger. This causes a denial of service for honest users or significantly increases the time for confirming user transactions, which undoubtedly also negatively affects the functionality of the entire system. Moreover, using large delays in confirming transactions of honest users, an attacker can initiate other attacks, for example, a double spending of funds that are not confirmed due to delays.

The Bitcoin cryptocurrency protocol provides that miners do not influence which transactions should be included in the block they compute [8]. Currently, blocks can contain transactions with values up to 0.0001 BTC, which makes it possible to populate the network with low-cost transactions.

2.5. Consensus Delay

Another attack related to the peer-to-peer nature of the Blockchain network is the delay in achieving consensus. This attack was partially presented in the previous section and consists in filling the network with false transactions in order to delay or prevent other participants from reaching consensus on the main version of the transaction ledger. Such delays can be caused either by forcing the network to extract blocks with minimal transactions, or by forcing time to reach consensus on damaged blocks. In particular, since accepting or rejecting false blocks can take a lot of time, this process negatively affects the system's performance and further exacerbates the negative consequences for Blockchain applications, where transactions must be guaranteed to be confirmed with a minimum delay.

2.6. Countermeasures against Peer-to-Peer Architecture Attacks

In a number of researches on malicious mining strategies, countermeasures were proposed that reduce the likelihood of success of this class of attacks and mitigate possible negative consequences [5, 12, 13]. One of the proposed solutions for preventing malicious blocks from being hidden is the "lifetime" of the block, after which the block is automatically rejected by the network and cannot be added to the Blockchain ledger without re-calculation [14]. Another measure to counter malicious mining is a scheme that reduces rewards for an attacker. The essence of this scheme is to add a time stamp to the block, which cannot be falsified, to display the time of calculating the block, then when adding new blocks to the Blockchain ledger, preference is given to more blocks with a newer (fresh) timestamp [13]. This method makes it unprofitable to hide a large number of calculated blocks; thereby conducting such an attack loses all meaning for an attacker, since he will not receive any benefit.

With regard to counteracting the attacks of the majority (51 % attacks), the concept of an improved mechanism for achieving consensus was proposed – a two-phase proof of the work done [7]. The new mechanism for achieving consensus is based on the continuous Markov chain, which includes two computationally complex tasks instead of one. The states of the continuous Markov chain prevent the increase of any particular association of miners above the boundary norm, lowering rewards for miners.

To prevent denial of service attacks aimed at combining miners, a model based on game theory was proposed [15]. Other countermeasures include limiting the minimum amount of funds to create a transaction and increasing the block size to accommodate more transactions, which would increase the system throughput. Another way to increase the system throughput is to reduce the complexity of computing new blocks, which would reduce the time to calculate one block and thereby increase the speed of transaction confirmation in the Blockchain system. It should be noted that each of the proposed methods has its drawbacks. A fairly large number of researches were devoted to the problem of countering DNS attacks, however, the studies were mainly carried out on classical

(on premise) architectures [16]. The attacks discussed in this section are relevant not only for the Bitcoin cryptocurrency, but also for Blockchain-based decentralized systems in general, as they help to identify potential attack planes and the relationships between various attack classes. However, the study of attack surfaces for Blockchain-based systems built in the cloud remains relevant.

3. Attacks on Blockchain Applications

Blockchain technology and its underlying peer-to-peer architecture are separate from application services that use them. Depending on the nature of the applications, they will have their own vulnerabilities. This section presents attacks aimed at Blockchain applications.

3.1. Blockchain Ledger Data Processing

In systems with an open Blockchain ledger, each user has access to transaction data added to the ledger. However, analyzing an open transaction ledger can provide useful information to an attacker. This process is known for processing the data of the Blockchain ledger or Blockchain ingestion, and this process can have negative consequences for the Blockchain system or its users. For example, a credit card company in the open market may use the analysis of data from the open transaction ledger of the Blockchain system to examine and optimize its own transaction processing schemes in order to compete with digital currency. A demonstration of the potential use of publicly available Blockchain ledger data for creating relationships with transaction data and user identification based on graph analysis is presented in [17].

3.2. Double-spending attacks

To demonstrate a double-spending attack, consider the following scenario. In cryptocurrencies, the goal of creating a transaction is to transfer ownership of a digital asset from the sender's address to the recipient's public address, and the value of the transaction is signed using the private key. Once the transaction is signed, it is transmitted to the network in which the recipient verifies the transaction. Verification by the recipient occurs when the recipient looks at the sender’s unspent transaction output, verifies the sender’s signature and waits for the transaction to be calculated by the miners and added to the Blockchain transaction ledger with the new block. This process can take several minutes, and in the Bitcoin cryptocurrency its average time is 10 minutes.

On systems with fast transaction confirmation, or if the recipient trusts the system, he can send the product to the sender of the transaction before it is accepted by the network. This gives the sender the opportunity to sign the same transaction and send it to another recipient. Signing the same transaction with a private key and sending it to two different recipients is called a double-spending attack. During this attack, there are two transactions obtained from the same unspent output of the sender, and only one of them is ultimately added to the Blockchain transaction ledger, and the attacker receives two products by paying only one of them. A delay in consensus on the network (section 2.5) or an attack of 51 % (section 2.2) may increase the attacker's chances of successfully conducting double-spend attacks.

3.3. Digital Wallet Theft

The theft of a digital wallet has negative consequences for the Blockchain system, since the keys associated with peer nodes are stored in the user's digital wallet. For example, in Bitcoin cryptocurrency, by default, the wallet is stored in unencrypted form, which allows an attacker to know the user's credentials and the nature of the transactions conducted by him. There are many services that offer secure storage of digital wallets of users, however, these services can also be compromised, and data can be taken by attackers [1].

3.4. Countermeasures against attacks on Blockchain applications

Many different countermeasures have been proposed with respect to attacks on Blockchain applications. For example, to protect blocks, it is recommended that you keep wallet backups and pro-

tect the keys used to sign transactions. Passwords are easy to crack, so a separate password strength policy is required in the system.

New decentralized cryptocurrency platforms, such as Zcash, hide transactions and maintain the anonymity of users in the Blockchain ledger, thereby preventing the possibility of processing data that is publicly available in the transaction ledger. A double-spend attack is practically unrealizable in systems with fast transaction confirmation, but in systems with a low rate of adding new blocks to the transaction ledger, such an attack has a high chance of success. One of the possible approaches to solving the problem is the use of one-time (or multiple) signatures, such as the extended Merkle signature scheme (XMSS) [18,19].

Conclusion

In this paper, we investigated the attack surfaces for Blockchain technology. Attacks on cryptographic designs of Blockchain technology, peer-to-peer network architecture and applications are considered. The study identified the main threats to Blockchain-based decentralized systems and analyzed the latest security researches of decentralized systems based on Blockchain technology. Some attacks can be carried out with a fairly high probability even despite the existing countermeasures, the work also demonstrated the relationship between the various sequences of attacks.

References:

1. Siegel D. Understanding the DAO attack. [Online]. 2016. Available: https://www.coindesk.com/understanding-dao-hack-journalists .

2. Baldwin C. Bitcoin worth 72 million stolen from Bitfinex exchange in Hong Kong [Online]. Reuters, 2016. Available: http://reut.rs/2gc7iQ9.

3. Kwon Y., Kim D., Son Y., Vasserman E., Kim Y. Be selfish and avoid dilemmas: Fork after withholding (FAW) attacks on Bitcoin, in CCS '17: Proceeding of the 2017 ACM SIGSAC Conference on Computer and Communications Security. 2017. P. 195-209.

4. Eyal I., Sirer E. G. How to disincentivize large Bitcoin mining pools. Bitcoin Block Explorer. 2014. [Online]. Available: https://www.blockchain.com/charts.

5. Eyal I., Sirer E.G. Majority is not enough: Bitcoin mining is vulnerable // Proceedings of the Eighteenth International Conference on Financial Cryptography and Data Security. 2014. P. 436-54.

6. Bitcoin Community. “51 % Attack”. 2017. [Online]. Available: https://learncryptography.com/cryptocurrencyl5l-attack.

7. Bastian M. Preventing the 51 %-attack: A stochastic analysis of two phase proof of work in Bitcoin. [Online]. 2015. Available: https://goo.gl/nJsMzV.

8. Bitcoin developer guide. [Online]. 2017. Available: https://bitcoinorg/en/developer-guide.

9. Kang A.R., Spaulding J., Mohaisen A. Domain name system security and privacy: Old problems and new challenges. [Online]. CoRR. 2016. Available: http://arxiv.org/abs/1606.07080.

10. Muncaster P. World's largest Bitcoin exchange Bitfinex crippled by DDoS. [Online]. 2017. Available: http://bit.ly/2kqo6HU.

11. Cimpanu C. Bitcoin trader hit by 'severe DDoS attack' as Bitcoin price nears all-time high. [Online]. 2017. Available: http://bit.ly/21A5iT6.

12. Sapirshtein A., Sompolinsky Y., Zohar A. Optimal selfish mining strategies in Bitcoin // Financial Cryptography and Data Security. Springer. 2016. P. 515-532.

13. Heilman E. One weird trick to stop selfish miners: fresh Bitcoins, a solution for the honest miner // Financial Cryptography and Data Security. Springer. 2014. P. 161-169.

14. Solat S., Potop-Butucaru M. ZeroBlock: Preventing selfish mining in Bitcoin // arXiv Preprint. ArXiv: v:1605.02435. 2016.

15. Johnson B., Laszka A., Grossklags J., Vasek M., Moore T. Game-theoretic analysis of DDoS attacks against Bitcoin mining pools // Financial Cryptography and Data Security. Springer. 2014. P. 72-86.

16. Silva P. DNSSEC: The antidote to DNS cache poisoning and other DNS attacks // An F5 Networks, Inc Technical Brief. 2009.

17. Fleder M., Kester M.S., Pillai S. Bitcoin transaction graph analysis // arXiv Preprint Xiv:1502.01657. 2015.

18. Huilsing A., Butin D., Gazdag S., Mohaisen A. XMSS: Extended hash-based signatures. [Online]. 2015. Available: https://www.ietf.org/id/draftirtf-cfrg:xmss-hash-based-signatures-10.txt.

19. Saad M., Mohaisen A., Kamhoua C., Kwiat K., Njilla L. Countering double spending in next-generation Blockchains // 2018 IEEE International Conference on Communications. Kansas City. 2018.

Kharkiv National University
of Radio Electronics

Received 25.01.2020