Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 190 (2021) 582–589

Procedia Computer Science

www.elsevier.com/locate/procedia

2020 Annual International Conference on Brain-Inspired Cognitive Architectures for Artificial Intelligence: Eleventh Annual Meeting of the BICA Society

# Problems of Using Redactable Blockchain Technology

Yakob Mesengiser, Natalia Miloslavskaya

*The National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),*
*31 Kashirskoye shosse, Moscow, Russia*

## Abstract

Blockchain Technology (BT) involves maintaining a special log (or register of records), the amount of information in which increases with each new record. Maintaining such a registry in high-load systems, in which several thousand (or more) records can be added per second, creates a serious problem of storing such a volume of information. There are also cases, in which the blockchain security features, and in particular its immutable data storage, are a drawback. For instance, once stored in the blockchain, erroneous data cannot be removed. To solve this problem, it is possible to use the redactable BT (RBT). In this case, one can clear the registry of outdated (or unnecessary) information that is no longer suitable for solving the tasks assigned to the system. However, this issue has its own subtleties, features and rules for working with this technology. Therefore, the purpose of the paper is to identify the actual problems of the RBT usage.

© 2021 The Authors. Published by Elsevier B.V.
This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0)
Peer-review under responsibility of the scientific committee of the 2020 Annual International Conference on Brain-Inspired Cognitive Architectures for Artificial Intelligence: Eleventh Annual Meeting of the BICA Society

*Keywords:* Blockchain Technology; Redactable Blockchain Technology; Public Key Infrastructure; PKI, trust models, electronic signature

## 1. Introduction

The BT scope is wide, and it is actively growing. Here are some examples.

*Logistics and Transport*. The Lorus SCM has implemented BT to automate the acceptance of applications and the processing of transportation. This made it possible to guarantee the accuracy of data, digitalize up to 90% of communications between employees and eliminate delays during transportation. The system records any actions with the cargo that can be confirmed by each participant of the transport, for example, the start and end of the transport. The company will be able to control the entire transportation process and the actions of each participant. After the application is formed, performers and loading-and-unloading points are assigned. The date, time of loading and the characteristics of the shipment are entered in the database. Next, the contractor confirms the presence of the

1877-0509 © 2021 The Authors. Published by Elsevier B.V.
This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0)
Peer-review under responsibility of the scientific committee of the 2020 Annual International Conference on Brain-Inspired Cognitive Architectures for Artificial Intelligence: Eleventh Annual Meeting of the BICA Society
10.1016/j.procs.2021.06.068

cargo at each new point. The system automatically records the arrival of the order using GPS coordinates. When unloading the goods, the contractor also enters data on the date, time and condition of the cargo. All actions of the customer and the contractor, including payment for transportation, are controlled by a smart contract (an algorithm that gradually marks the achievement of each point).

*HR*. The RAMAX group of companies has developed the WORK'N'ROLL (W&R) blockchain platform, with which its employees can earn tokens for various achievements. The remuneration is paid in the form of virtual tokens or coins, which employees can exchange for various bonuses and privileges. In addition to issuing tokens, direct peer-to-peer transfers are possible on the platform. The blockchain platform, on which W&R is based, is open source. The front-end and back-end with business logic belong to the company. In this configuration, the solution has no direct analogues, and it is ready for use by HR services of various companies.

*Electronic Document Interchange (EDI)*. Specialists of the "Sibintek" digital cluster are testing BT in the EDI system between gas stations and suppliers of related products for mini-markets at gas stations. It is expected that this technology will expand the capabilities of EDI, which is widely used in retail. As a result, it was possible to automate the process of ordering and delivery. All parties involved in the process began to operate with the same information and synchronously track the delivery process. They also have the ability to sign reconciliation reports almost automatically. Due to the fact that it is impossible to delete or change records in such an EDI service without a trace, the parties can monitor the relevance of the data and conduct audits in real time [1].

However, the BT usage involves maintaining a special database (DB) – a log of all transactions that were carried out by users of the blockchain.

Another BT's feature is that all records are organized into blocks – containers with transactions that are cryptographically linked to each other [2]. At the same time, the distributed DB is constantly expanding. Changing (or deleting) one of the blocks in the DB will cause the entire chain to fail (break) [3, 4].

It should also be noted that the BT usage in high-load systems, in which several thousand (or more) transactions are made per second, constantly requires more and more resources and creates a serious problem of storing and processing such a volume of information. To solve this problem, it is possible to use Redactable BT (RBT). Its use will allow to remove outdated (unnecessary or superfluous) data from the DB that is no longer suitable for solving the tasks assigned to the system. Also, the use of this technology will allow to control the DB volume, and to prevent a constant and uncontrolled increase in its volume.

However, blocks in BT are obviously immutable structures. Editing any block in the blockchain will lead to a violation of the hash code chain, which will eventually lead to a break in the entire chain. For RBT, it is important to understand how:

- The data that has already been entered in the blockchain is being edited;
- The problem of achieving consensus is being solved;
- The problem of ensuring consistency of the state of copies of the shared DB (DB replicas) and the transaction history with it on all network nodes is solved.

The purpose of this paper is to identify the actual problems of the RBT usage. To achieve this goal, the paper is organized as follows. The second section provides a brief description of the Distributed Ledger Technology (DLT) and BT. Section 3 describes the role of an Electronic Signature (ES) in BT. Section 4 presents the main approaches to editing the blockchain. Section 5 highlights the problems of using RBT.

## 2. Brief BT description

Before proceeding to the BT description, it is necessary to give a brief description of the DLT, since BT is the DLT embodiment. The DLT is a technology that describes a secure data structure (most often a DB) that supports an ever-expanding list of records, as well as rules and requirements for records [2]. It does not require a DB administrator and a centralized storage space. Adding new records to this DB is only possible when a consensus is reached. It should be noted that:

- DLT assumes a fully decentralized system. There is no such node that can be disabled to destroy or block the entire system, and there are no major and minor nodes – they are all equivalent;
- DLT assumes that it contains some DB for storing the ledger. Each node of the network maintains a synchronous (or almost synchronous) copy of the shared DB and its transaction history with the other nodes. Here one of the main problems arises – ensuring consistency of the state of copies of the shared DB and the transaction history with it on all nodes of the network;
- Any new entries in the ledger can only be made when a consensus is reached. This raises the problem of reaching consensus [3].

There are three types of blockchain:

- open type (permissionless) or public, allows to become a miner or node to an unlimited number of people, no registration or revocation of authority is required;
- closed type (permssioned) or private or corporate, restricts the circle of miners and nodes outside the community, registration is required for participation, when leaving the community, the access right is revoked;
- mixed-type or hybrid – an open–type blockchain that uses closed-type platform building technologies to achieve consensus [3].

A key feature of open-type platforms is a specific way to achieve consensus when writing new blocks to the ledger. Since the exact number of participants in an open platform is unknown at any given time, it is impossible to calculate how many nodes in the network should vote to reach a consensus. In this regard, the criterion for achieving consensus should be used not just a sufficient number of network participants, but some other value. As a solution to this problem, it is proposed to use a sufficient share of the network's computing resources – 50%.

In Proof-of-Work, each of the miners is involved in solving a computationally complex problem. In the Bitcoin system, for example, the task of selecting such a random "supplement" to the generated new block of the ledger is used, so that the hash code of the next new block written to the ledger satisfies a special condition, for example, that the first 20 bits of the hash code are zero. Since the hash function has mixing properties, it is impossible to guess in advance the value of a random additive that will result in the desired hash code. The only way is to iterate through all possible values sequentially. Sooner or later, one of the miners will find such an addition and send it and the hash code calculated by it to all the other nodes for verification. As soon as they are sure that the calculation is correct, the new block will be written to each of the nodes in its own copy of the ledger. Such computationally complex work by miners is not free: the one who first solves this problem will receive a reward in cryptocurrency. The very process of solving a computationally complex problem, which ends in a successful reward, is called cryptocurrency mining. To break the security of the blockchain, which uses Proof-of-Work to record transactions, an attacker needs to concentrate more than 50% of the network's computing power, which is much more difficult than simply creating a large number of fictitious participants, which will exceed 50% of the system's participants and who do not need to do anything but vote.

When proving the ownership of a stake (Proof-of-Stake), each of the participants of the blockchain network gets the right to certify the newly created block with its ES. This right is randomly transferred from one participant to another with a probability proportional to what share of the total volume of the cryptocurrency issued into circulation it has. This method encourages network participants not to transfer funds to other cryptocurrencies or fiat currencies, but to store them inside the network. A reward in the form of a cryptocurrency issue for creating a new block is not provided here, so the only type of reward is the commission for the completed transaction, charged to the sender of the funds. For most blockchain platforms with Proof-of-Stake, it is typical that the entire volume of cryptocurrency is issued immediately, when the platform is launched, although there are options with additional issuance. The Proof-of-Stake algorithm itself is arranged as follows: the entire time of the system operation is divided into time slots of equal length, in each of which one new block must be generated, added to the ledger. For each time slot, a leader is randomly selected among the platform participants. As noted above, the probability of the leader choosing a particular participant is proportional to the share of cryptocurrency available to him. The leader forms a block according to the rules established by the blockchain network protocol, after which he signs the block with his ES and sends it to all other participants for verification. After more than half of the total number of platform participants check the block created by the leader, including checking its ES under this block, and exchange messages about the positive result of the check, the block joins the ledger. Next, a new leader is selected for a new time slot, etc. To break the security of the DLT system, which uses Proof-of-Stake to record transactions, an attacker needs to concentrate more than 50% of the network's financial resources, which is also difficult to do, and by improving the algorithm, this threshold can be raised to 90%.

Protocols that allow consensus to be reached by voting are much less time-consuming than any of the methods used for open-type platforms (by several orders of magnitude).

No cryptocurrency is required for the operation of a closed-type blockchain platform. As in the case of open-type platforms, its key feature is the consensus mechanism implemented in them. Since for closed platforms, the number of miners and nodes is known exactly at any given time, the voting principle can be applied to achieve consensus. Strictly speaking, the DLT system requires the implementation of not just a consensus protocol, but the so-called atomic broadcast protocol, since replicas need not only to agree on the addition of single records to the ledger, but also to strictly preserve the order of transactions, and therefore the sequence of changes in the ledger states [3, 4].

The BT advantages and disadvantages are presented in Table 1.

Table 1. The BT advantages and disadvantages.

| Advantages | Disadvantages |
|---|---|
| All blocks in the blockchain are cryptographically linked to each other. | Redundancy of information. |
| Decentralization – there is no such node that can be disabled to destroy or block the entire system. | The amount of information in the ledger increases with each new entry. The use of BT in high-load systems creates serious problems for storing such a large amount of information. |
| The presence of a single ledger for all network participants. You can track the history of all transactions. | Performance – the speed of writing new transactions to the blockchain is significantly lower than in traditional systems, and compared to such highly loaded systems as international bank card payment systems, it is several orders of magnitude lower |
| Consensus – any new entries in the ledger can only be made with the consent of a majority of participants. | Reducing the speed of the network's response to external changes. |

## 3. The ES role in BT

All ES types can be divided into 2 classes: simple ES and advanced ES with two subclasses [5]. In the blockchain, all transactions are signed with an advanced ES to ensure the non-repudiation and authenticity of transactions.

But it should be understood that the advanced ES itself is a certain way formed "label", which is directly related to the signed data, and allows you to uniquely identify this data. The main feature of the tool for creating such "labels" is the use of the public key and the private key. But the following problem arises: any user in the public key cryptosystem environment risks sooner or later mistaking a fake public key for a real one. The confidence consists in the fact that a particular public key belongs to a particular owner. Authenticity is one of the most important criteria in the public key system environment, where the authenticity of each specific public key of an item instance must be determined. Accordingly, the following questions arise: how can we determine whether this ES was created by our correspondent, and whether the public key that is available to us really belongs to our counterparty; can this ES be trusted? To solve this problem, one need a mechanism by which it is possible to uniquely bind the public key and the private key to a specific person, as well as to verify that the public key belongs to this person. The Public Key Infrastructure (PKI) and various trust relationship models were developed.

The PKI has a DB for storing certificates (for example, certificates in the X. 509 format). At the same time, it provides services and protocols for managing public keys. These include the ability to issue (issue), revoke (revoke), and trust certificates. The main PKI’s feature is the presence of components known as the Certification Authority (CA) and the Registration Authority (RA). The CA issues certificates and signs them with its private key. The CA combines people, tools, and processes, which serves the purpose of enrolling new users in the PKI structure and further administering the system's regular users.

There are two trust models that dictate to users their actions to determine the authenticity of certificates. Direct trust is the simplest of the trust relationship models. In this scheme, the user is convinced that the certificate is authentic, because he knows exactly who he received this certificate from. The direct trust model can be used in an open-type blockchain. In the hierarchical trust model, there are a number of root CA that the trust extends from. These CAs can either certify end-entity certificates themselves, or they can authorize other certificates that will certify end-entity certificates along some chain. The hierarchical trust model can be used in a closed-type or hybrid blockchain. A local CA and RA can be deployed within the organization, and each miner and (if necessary) node will be issued a certificate. External blockchain users who are not part of the organization can trust the organization's CA.

## 4. Redactable BT

Since there is currently no generally accepted definition of the RBT term, in this paper, it is a secure distributed data structure (DB) that supports an ever-expanding list of blocks/records with timestamps that are linked to each other and form a chain of blocks, and sets rules for transactions associated with these blocks [2, 3]. No centralized storage space is required. Various consensus-building mechanisms can be used to add new blocks/records to this DB.

Important differences between the definitions of the RBT and BT terms:

- The definition of the BT term specifies that blocks are non-editable structural units. There is no such requirement in the RBT term;
- It is allowed to have a DB administrator.

Today, there are two main approaches to editing the blockchain.

1. *Using an additional blockchain*. Changes to the main chain will be made to it. Imagine that you need to make changes to the Bi block of the main chain. In this case, the necessary information about the changes, as well as information about the block *Bi*, *B(i-1)* and *B(i+1)*, is entered in the block with corrections *B'k*. It should be noted that both the main block chain and the patch block chain have the same root (the initial block). This method is shown in Fig. 1 [7]. It should also be noted that the nodes of the blockchain, which are stored by both blockchains, must set certain rules and conditions in advance, under which blocks from the main chain will be "replaced" with blocks from the chain containing edited information, since there is no explicit replacement. Otherwise (if the developers do not take this feature into account), the second chain with fixes will not be involved in any way.

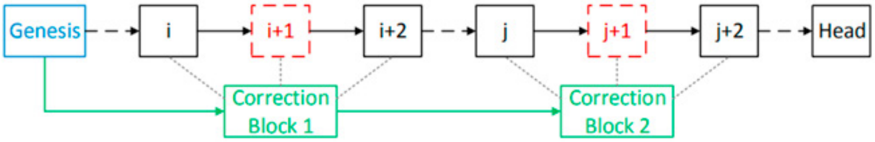

Fig. 1. Using an additional blockchain to store changes to the main blockchain.

2. *Using chameleon hash functions*. Chameleon hash function is a hash function that allows you to efficiently generate collisions for when you know the special key information *Skey*. Without knowing the key *Skey* information, finding collisions is much more difficult. Thus, by replacing the standard hash function in the blockchain (for example, SHA-256) with a chameleon hash function, or by feeding the hash function SHA-256 with the hash code of the chameleon hash function, it is possible to change the contents of the block (provided you know the key information *Skey*), without changing the hash code of the block itself. The method of editing blocks in the blockchain database using the chameleon hash function is shown in Fig. 2. A miner or a group of

miners can change the data in an existing chain without destroying the chain of hash codes linking the blocks [8, 9]. When using this approach to editing the blockchain, the existing block chain is explicitly changed.

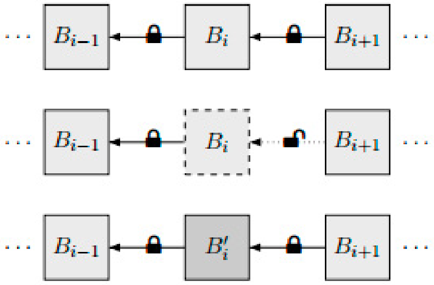

Fig. 2. Editing blocks in the blockchain chain when using the chameleon hash function.

It should be noted that in order to use such a function in the blockchain, it is necessary to revise and/or expand the set of fields that make up the block in advance, since a verification string $\xi$ is required for the chameleon hash function to work correctly [8].

A distinctive feature of the chameleon hash function approach compared to the additional block chain approach is that it is possible to delete any blocks in the chain. Let us consider the following example. Fig. 3 shows the BC1 blockchain containing blocks from Fig. 3.

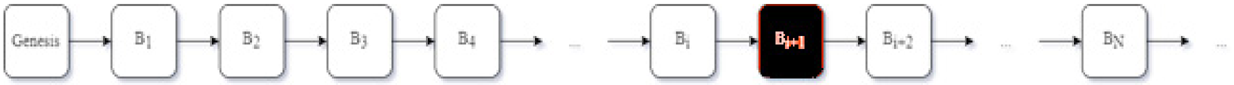

Fig. 3. BC1 blockchain.

The block to be deleted is highlighted in black. To do this, follow these steps: delete a block $B_{i+1}$; replace the hash code of the previous block in the block $B_{i+1}$ with the hash code of the block $B_{i+1}$ with the hash code of the block $B_i$; find a new validation line $\xi'$; and include a new validation line in the block $B_{i+2}$.

## 5. Problems of achieving consensus and ensuring consistency of the state of the shared DB copies and the history of its transactions on all network nodes

Let us consider the problems of achieving consensus and ensuring consistency of the state of copies of a shared DB (DB replicas) and the history of transactions with it on all network nodes. It should be noted in this research the issues of using RBT in a closed-type blockchain, for which the number of miners and nodes is known in advance, is considered.

*The problem of reaching consensus*. It is important to keep in mind that when using the chameleon hash function for editing, secret key information *Skey* is also present. Only when using it, it is possible to edit blocks in the blockchain database. There are several possible solutions to the problem of achieving consensus when using the chameleon hash function:

1. Entrust *Skey* to a pre-determined (for example, by holding a general vote) responsible party, such as an administrator. Let us call this side the coordinator. In this case, consensus, as such, cannot be reached, since the coordinator has unlimited access and can edit blocks in the blockchain DB without the consent of the other network participants. This editing method is only suitable for a closed-type blockchain [9];
2. Applying a secret sharing scheme (SSS) or a threshold secret sharing scheme (TSSS). Key information *Skey* is shared between the *K* participants. Consensus will be reached if *P* participants participate in the block editing process:

   a) For the SSS, it is necessary to use all parts of the original key information *Skey*, i.e., $P = K$. To combine the key, it is necessary to use a consensus protocol in distributed systems, which assumes the response of each of the network participants;
   b) For the TSSS, it is necessary $2 \leq P < K$ to share the original key information *Skey*. To combine the key, it is necessary to use an algorithm for achieving consensus in distributed systems, which assumes the response of each of the network participants. Parts of the key are passed as input to the algorithm or coordinator, who, in the case of receiving *P* shares of the initial key *Skey*, receives the initial key *Skey* itself and edits a predefined block.

   After editing a block, the key *Skey* is destroyed on the side where the block editing algorithm is executed [9];

3. Achieving consensus using threshold signature scheme (TSS). If all the options described above for achieving consensus are not applicable, the following method may be used:
   a) Within the organization, one should deploy a PKI, create local CA and RA;
   b) A private key *PK* and a public key *PbK* are generated. The *PK* is divided into shares $PK_1', PK_2', PK_3', PK_4', \ldots, PK_P'$ and shares are distributed to miners eligible to vote on blockchain changes in such a way that each share is sent to only one miner;
   c) Make the key *Skey* available to the coordinator in advance;
   d) Miners, after checking all transactions in the block, and, in case of successful verification, calculate their part of the ES $Sign_1', Sign_2', Sign_3', Sign_4', \ldots, Sign_P'$ using their share of the key for the added block and send it to the coordinator;
   e) The coordinator, using the TSS, "combines" the various shares $Sign_1', Sign_2', Sign_3', Sign_4', \ldots, Sign_P'$t into a common one $Sign$. If it is possible to check $Sign$ with the key $PbK$, then a consensus is reached, and the party responsible for editing the blockchain changes the block, including all the shares $Sign_1', Sign_2', Sign_3', Sign_4', \ldots, Sign_P'$ there [8, 10, 11]. Since the block contains all the shares $Sign_1', Sign_2', Sign_3', Sign_4', \ldots, Sign_P'$t, and they are unique for each data set, the coordinator cannot independently change the contents of the block, since the ES will not be checked. If the coordinator decides to add such a block to the blockchain, then there will be no trust to this block, and it won`t be accepted.

It is important to note that in the case of using an additional chain and a chameleon hash function, using Proof-Of-Work as the only mechanism for achieving consensus is not enough, as, for example, since most miners must not only verify the correctness of transactions, but also accept the changes that will be made to the blockchain. It is possible to use a slightly modified Proof-Of-Stake mechanism to achieve consensus (the weight of each vote will be determined in advance) [11].

To apply both approaches to editing the blockchain, it is necessary to review and/or expand the set of fields that make up the block.

*The problem of ensuring consistency of the state of copies of a shared DB (DB replicas) and the history of transactions with it on all network nodes*. To solve this problem, it is possible to use a standard mechanism for distributing blocks between blockchain nodes. However, it is important to note that, in the case of chameleon hash functions, the block is already in the network participants, and they, after receiving the edited block, must replace the old block with a new one.

The mechanism presented in the Accenture patent for distributing blocks after editing them is as follows [9]:

- The following parameters are input to the algorithm:
   a) The entire chain *C*, the blocks in which are subject to editing;
   b) A set of indexes $N_1, N_2 N_3, \ldots, N_k$that represent the positions of blocks in the chain *C*;
   c) New values $data_{N_1}, data_{N_2}, \ldots, data_{N_k}$ containing a set of actions or data for blocks with indexes $N_1, N_2 N_3, \ldots, N_k$.
- After the blocks in the chain have been edited and/or deleted, an updated chain $C'$ is created, which the coordinator broadcasts to all nodes as "special". Nodes, having received such a chain, accept it even in favor of longer ones and, in the future, start working with it.

However, it should be understood that this approach has one significant drawback: if the coordinator is compromised (hacked), then the lack of verification at the nodes of the correctness of the changes applied to the chain can lead to overwriting the entire blockchain chain, which can lead to irreversible consequences.

It should be understood that information cannot be immediately and permanently removed from the blockchain. A mechanism is needed to temporarily exclude information that, in the opinion of the coordinator or most miners, is outdated (unnecessary or superfluous), unsuitable for solving the tasks set for the system, and, if necessary, restore the excluded information. Of course, after a certain period of time, the information excluded can be permanently deleted. However, there is no such mechanism.

## 6. Conclusion

The BT and RBT analysis allows us conclude that these technologies have a great potential for development. The use of these technologies helps to solve one of the main problems in DLT systems: the problem of ensuring trust between the participants of interaction. However, RBT has a number of disadvantages. The paper described various problems with the RBT usage, but some of them remained unresolved or not fully resolved. Further research will address the following issues: creation of a trusted loop, within which it will be possible to use BT and RBT; development of a mechanism for nodes to verify the chain received from the coordinator, containing edited blocks; development of a mechanism to temporarily exclude from the data processing loop information that, in the opinion of the coordinator or the majority of nodes, is outdated, unsuitable for solving the tasks assigned to the system, and, if necessary, to restore the excluded information.

## Acknowledgement

This work was supported by the MEPhI Academic Excellence Project (agreement with the Ministry of Education and Science of the Russian Federation of August 27, 2013, project no. 02.a03.21.0005).

## References

[1] Blockchain. Knowledge Base. URL: https://ict.moscow/projects/blockchain/ (access date: 04.03.2021). In Russian.

[2] Miloslavskaya N. Designing Blockchain-based SIEM 3.0 System. Information and Computer Security (UK). Emerald Publishing. 2018, 26(4): 491-512. DOI: 10.1108/ICS-10-2017-0075.

[3] Miloslavskaya N., Tolstoy A., Budzko V. and Das M. Blockchain Application for IoT Security Management. Chapter 7. In: Essentials of Blockchain Technology. CRC Press, Taylor & Francis Group, USA. October 31, 2019. Pp. 141-168. DOI: 10.1201/9780429674457-7.

[4] Zapechnikov S.V. Distributed ledger systems as a tool for ensuring trust between business process participants. Information Technology Security. 2019, 26 (4): 37-53. In Russian (access date: 04.03.2021).

[5] Mesengiser Y.Y, Dubov S.S. About electronic signature and its prospects in the digital economy. Rossiyskiy tekhnologicheskiy zhurnal (Russian Technological Journal). 2018; 6(5): 5-14. URL: https://rtj.mirea.ru/upload/medialibrary/1fc/RTZH_5_2018_5_14.pdf (access date: 04.03.2021). In Russian.

[6] Zimmermann F. Introduction to PGP cryptography. PGP Corporation. 2004. URL: https://royallib.com/book/tsimmermann_filipp/vvedenie_v_kriptografiyu.html (access date: 04.03.2021). In Russian.

[7] Marsalek A., Zefferer T. A Correctable Public Blockchain. 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering. URL: https://ieeexplore.ieee.org/document/8887342 (access date: 04.03.2021).

[8] Kondapally A., Sindhu M, Lakshmy K.V. Redactable Blockchain using Enhanced Chameleon Hash Function». 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)/ URL: https://ieeexplore.ieee.org/document/8728524 (access date: 04.03.2021).

[9] International Publication Number WO 2017/202759 Al. CRYPTOLOGIC REWRITABLE BLOCKCHAIN. Accenture Global Solutions Limited, GSC Secrypt, LLC. November 2017. URL: https://patents.google.com/patent/WO2017202759A1/en (access date: 04.03.2021).

[10] Selenya O.A., Salomatin S.B. Threshold scheme of digital signature on elliptic curves with a split secret. Technical information protection tools: Abstracts of the XIV Belarusian-Russian Scientific and Technical Conference. Minsk. 2016. P. 42. URl: https://libeldoc.bsuir.by/handle/123456789/9941 (access date: 04.03.2021). In Russian.

[11] Ke Huang, Xiaosong Zhang, Yi Mu, Xiaofen Wang, Guomin Yang, Xiaojiang Du, Fatemeh Rezaeibagha, Qi Xia, Mohsen Guizani. Building Redactable Consortium Blockchain for Industrial Internet-of-Things. IACR Cryptol. ePrint Arch. 2019: 1110 (2019). URL: https://allquantor.at/blockchainbib/pdf/xu2019redactable.pdf (access date: 04.03.2021).