Advances in Economics, Business and Management Research, volume 81
1st International Scientific Conference "Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth" (MTDE 2019)

System for automated accounting, control and payment of services based on the technology of the blockchain, the hash chain and methods of cryptography

Makarov A.M.
Department of information and communication technologies, mathematics and information security
Pyatigorsk state University
G. Pyatigorsk
mellin_22@mail.ru

Postovalov S.S.
Department of information and communication technologies, mathematics and information security
Pyatigorsk state University
G. Pyatigorsk
poroh20100@yandex.ru

Pisarenko E. A.
Department of information and communication technologies, mathematics and information security
Pyatigorsk state University
G. Pyatigorsk
gmu41@yandex.ru

Abstract — One of the important possible directions of blockchain technology implementation is the sphere of housing and communal services. The use of blockchain in accounting for the received utilities and payment for them can make these processes absolutely transparent, understandable and verifiable, which is not always done with the current system of payment for housing and communal services. The paper describes the algorithms of interaction between suppliers and consumers of housing and communal services on the basis of blockchain technology, hashchain and cryptography methods. Blockchain procedures for concluding a contract for the supply of utilities, accounting for consumption, billing, payment for services and resolving problems have been developed. The proposed methods allow both providers and consumers of ESIA to guarantee the accuracy and reliability of the data, as well as their protection and indestructibility.

Keywords — blockchain, cryptography, management.

I. INTRODUCTION

The transition of the world economy and its management systems to digital technologies allows to stimulate their development in the direction of the gradient of movement from regional structures to global socio-economic systems. In this case, there are problems that need to be solved both in the technical and humanitarian spheres. It is worth highlighting the digital blockchain technology, which literally broke into the digital management technology, taking to its credit the methods of cryptography, which gave it such qualities as the elimination of unnecessary intermediaries, the integrity and reliability of data, a high degree of data protection from falsification, their openness with the simultaneous ability to save personal data. The fee for these advantages is to attract quite complex and expensive crypto-resistant technologies, which, in turn, require information literacy of the population of the country [4]. As noted in [11]: "the Layman, being in a condition of hybrid reality, regards his existence as a" situation on the alert", constantly feeling vulnerable under the onslaught of large-scale digitalization, extending up to the usual space of life itself. In other words, the digital world, penetrating all existing, has created a digital environment". Solving many problems-automation of accounting of consumed services, their payment, maintenance of personal accounts of users of services, information technologies have generated also the corresponding problems [2]. These include the leakage of personal data, the possibility of unauthorized access and data corruption by attackers, data substitution during transmission, etc.the Solution to such problems can be the use of blockchain and hashchain technologies, which this work is devoted to.

The aim of the work is to develop the application of digital technologies blockchain and hashchain, in relation to socio-economic systems. In particular, the possibility of using blockchain technology for registration and accounting of the provision and payment of services in the system of housing and communal services in Russia is considered. These structures are the basis of the actually developed system.

II. RESEARCH METHODOLOGY

Today, the interaction between citizens and suppliers of household goods takes place through management companies, which creates inconvenience for each of the parties. In the system of housing and communal services, the activities of intermediaries are hidden from everyone, and with any inconsistencies in the accounting of supplies and payment for services, it is very difficult to find the cause of the discrepancy.

In addition, intermediaries carry out various types of fraud that harm both suppliers and recipients of services. This contradiction can be resolved by using blockchain distributed registry technology, which is transparent and immutable at the same time [5,6,10]. Thus, it is possible to change the interaction of exchange participants in the direction of increasing the transparency of the system and automation of accounting in it [1, 7, 8, 12].

Figure (Fig. 1) shows an automated system of accounting, control and payment for services based on blockchain and hash-technology and cryptography. It contains:

– i-x subscribers - consumers of services 1,2,..., k-ordinary citizens who got used to see in the house electricity and hot water;

– blockchain network 5, or the blockchain of contracts, which contains the data exchange between the subscribers and the management company, contracts, customers, and readings from the counters when paying on the contract;

– subscribers providing services: 15,16, M-companies ready to provide ordinary citizens with the above facilities for payment;

– blockchain network 7, which contains data on invoices for payment from subscribers providing services and the fact of payment of these invoices by subscribers-recipients;

– blockchain-network 8, which duplicates the readings of subscribers ' counters in a format suitable for reading by the management company, the service of state services and subscribers providing services;

– MC (management company), performing a role in this scheme, similar to the role of the miner. The difference is that the criminal code within the network is in a single copy and has no competitors. In the future it will be called the MC or just the miner.

Blockchain network is a set of distributed registers of different systems interacting with each other[12].

At the same time, distributed registers of subscribers consuming services 21, management company 22, ESIA(Unified identification and authentication system.) 23 and subscribers providing services 24 are created.

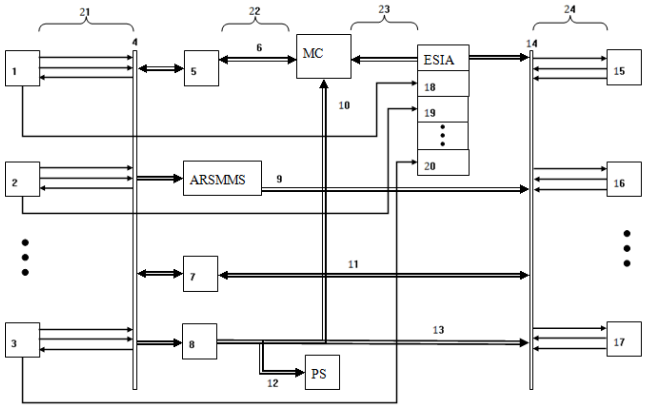

Figure 1. A system for automated accounting, control and payment of services based on blockchain technology and hiscan and cryptography

Within the framework of this scheme, the following interactions are carried out:

1. Connection of a new subscriber to the network, conclusion of a service contract

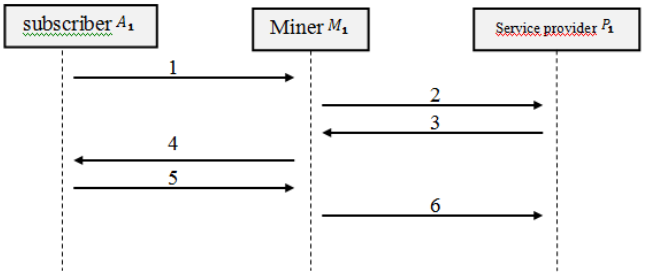

Figure 2. Algorithm of conclusion of the subscriber's and service provider's contract

1. The subscriber A_1 fills in the data D_{A1} of the service provider's P_1 contract form, encrypts it with the help of (provider's public key) KO_{P1}, creates $ЭЦП_{A1}$:

$$T_{A1} = f(KO_{P1}, D_{A1}, ЭЦП_{A1}) \quad (1)$$

Having formed its internal block T_{A1}, it sends it to the network blockchain 5, where the block enters the queue of all those not yet included in the external sides of the chain.

It is assumed that the subscribers are not specialists, and all operations related to the formation of internal blocks, encryption, transfer-receipt of keys, etc.occur automatically.

2.Miner prepares external unit B_n based on the previous hash of the outdoor unit circuit blockchain B_{n-1} and data all the internal data queue:

$$B_n = f(N, hB_{n-1}, r, t, T_1, T_2, \dots T_n) \quad (2)$$

after successful establishment, sends the outdoor unit on the roster, where he becomes part of the blockchain contracts.

3.The service provider finds the internal block T_{A1} addressed to it from the subscriber A_1 in the data of external blocks of the blockchain network . He opens it with his secret encryption key KC_{P1}, complements his part in the contract data D_{P1}, draws up his internal block

$$T_{P1} = f(KO_{A1}, D_{P1}, ЭЦП_{P1}) \quad (3)$$

and sends it to the network of blockchain, where the block falls into the queue of all not yet issued in the outer side of the chain.

4.Miner prepares external unit B_n based on the previous hash of the outdoor unit circuit B_{n-1} and data all the internal data queue:

$$B_n = f(N, hB_{n-1}, r, t, T_1, T_2, \dots T_n) \quad (4)$$

after successful establishment, sends the outdoor unit on the roster, where he becomes part of the blockchain contracts.

5.The subscriber A_1 finds the internal block T_{P1} addressed to him from the service provider P_1 in the data of external blocks of the network . Opens his secret key KC_{A1}, signs the contract data D_{A1}, draws up a new internal block

$$T'_{A1} = f(KO_{P1}, D'_{A1}, ЭЦП_{A1}), \quad (5)$$

after directs the blockchain to the network, where the block enters the queue of all not yet decorated in the outer side of the chain.

6.The miner prepares the external block B_n taking into account the previous hash of the external block of the chain B_{n-1} and the data of all internal ones in the queue

$$B_n = f(N, hB_{n-1}, r, t, T_1, T_2, \dots T_n): \quad (6)$$

after successful formation , sends the external block to the registry, where it becomes part of the blockchain contracts.

As a result, the service provider finds the internal block T'_{A1} addressed to it from the subscriber A_1 in the data of the external blocks of the network . Reveals its secret encryption key is already generated and signed the contract.

.

2. Payment for services

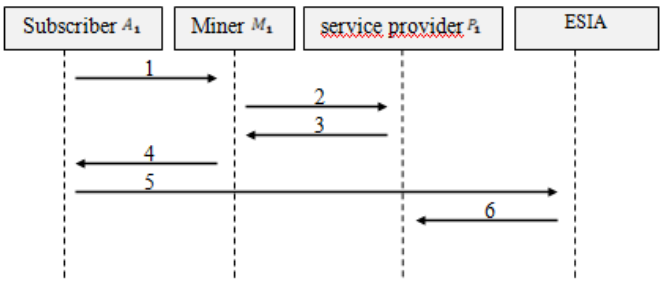

Figure 2. Algorithm of the bill payment service provider

1.The subscriber A_1 records the counter data D_{A1} or a counter that supports automatic transmission of readings over the network is read BY. Encrypts D_{A1} with and KO_{P1} signs $ЭЦП_{A1}$:

$$T_{A1} = f(KO_{P1}, D_{A1}, ЭЦП_{A1}) \quad (7)$$

After forming its internal block T_{A1}, it sends it to the blockchain network, where the block enters the queue of all not yet included in the external blocks of the chain.

2.The miner prepares the external block taking into account the previous hash of the external block of the chain B_n and the data of all internal ones in the queue: $B_n = f(N, hB_{n-1}, r, t, T_1, T_2, \dots T_n)$, (8)

after successful formation , sends the external block to the registry, where it becomes part of the blockchain contracts.

3.The service provider P_1 finds the internal block T_{A1} addressed to it from the subscriber A_1 in the data of the external blocks of the blockchain network . Opens it with his secret encryption key KC_{P1}. Based on the data D_{A1}, P_1 generates an invoice for services D_{P1} for A_1, encrypts them with a public key KO_{A1} and signs $ЭЦП_{P1}$

$$T_{P1} = f(KO_{A1}, D_{P1}, ЭЦП_{P1}) \quad (9)$$

Having formed its internal block T_{P1}, it sends it to the blockchain network, where the block enters the queue of all those not yet included in the external sides of the chain.

4.The miner prepares the external block B_n taking into account the previous hash of the external block of the chain B_{n-1} and the data of all internal queued:

$$B_n = f(N, hB_{n-1}, r, t, T_1, T_2, \dots T_n), \quad (10)$$

after successful formation, sends the external block to the registry, where it becomes part of the blockchain contracts.

5.The subscriber A_1 finds the internal block T_{P1} addressed to him from the service provider P_1 in the data of the external blocks of the blockchain network . Opens the account from the service provider D_{P1} with the secret key KC_{A1} and carries out payment through ESIA by means of the personal office.

6.ESIA transfer money to the service provider P_1.

III. AUTOMATION OF ACCOUNTING

The algorithms and schemes above represent a data exchange system that stores the entire history of transactions securely and transparently, and the data of all participants are protected by encryption. In addition, it allows ordinary citizens to establish contact with service providers in a single interface and without hassle, because all the processes of confirmation and transmission are automatic, and all subscribers are protected from fraud, see and can check on what conditions contracts are concluded, what amounts are charged by suppliers, how much money they received from subscribers, etc. [3].At the same time, the role of management companies is changing, which from intermediaries become participants in the exchange process between different links and can not imperceptibly affect the reporting due to the characteristics of the blockchain [9].

Due to the possibility of building such a system, the following description of the entities of this system and their interaction is proposed:

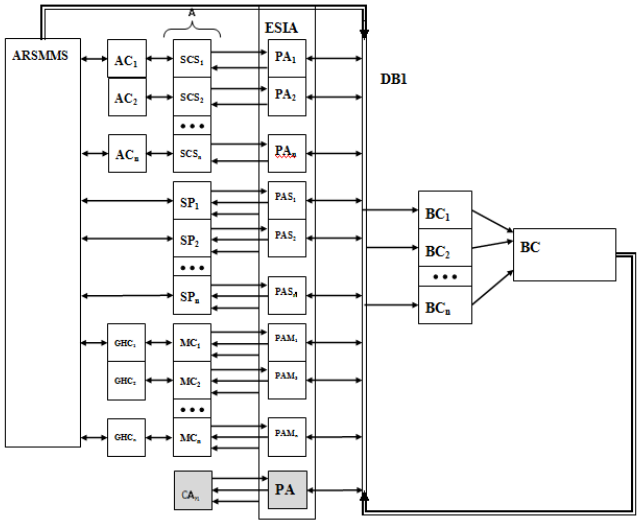

Figure 3. Scheme with the Union of accounts for the consumer and payment through the AW of the consumer

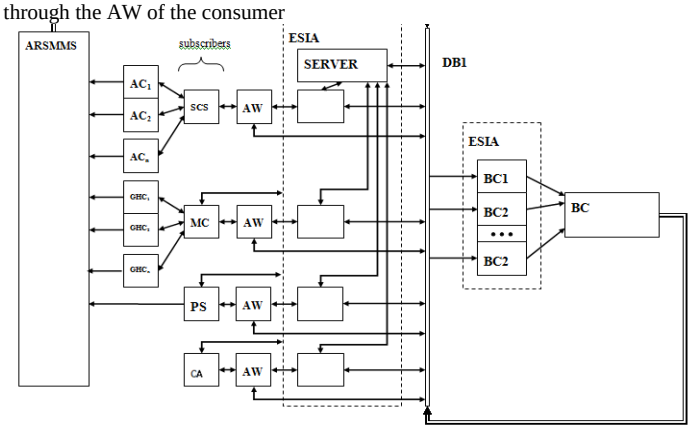

Figure 4. Accounting Structure with the division of accounts by meters and payment through the account of ESIA

18,19,20 (PA_n) — Personal accounts on the servers of ESIA
ESIA - Unified identification and authentication system.
15,16,17 (SP_n) — service provider
(AC_n)- apartment counters
(GHC_n) - General house counters
AW – automated workplace.
(DB) — data bus
BC - Blockchain networks 5,7 and 8, whose description corresponds to the above given in the article. At the same time, blockchain network 5 is BC1, blockchain network 7 is BC2, blockchain network 8 is BC3
21 (DR1)— distributed register of subscribers-consumers of services
22 (DR2) — distributed register of management companies
23 (DR3)— distributed register of private offices on the portal of ESIA
24 (DR4) — distributed register of service providers
ARSMMS — the automated recording system for monitoring and measuring sensors, communication with them via radio to servers of the agencies providing services
m — number of subscribers of service consumers
n — number of services providing

For subscribers consumer services fixed apartment counter services (AC_n).For subscribers managing companies fixed general house counters (GHC_n). The meters can be connected to a common automated monitoring system (ARSMMS). In this case, the information is collected automatically and sent by the system to the common data bus (BD_1). In situations where the meters are not connected to a common automated monitoring system, it is possible to implement manual removal of information — subscribers send meter data manually or through the automated workplace (AW). It is also provided for connection to the system of subscribers who do not have their own counters of services, but whose connection is necessary within the framework of housing and communal relations.

Each subscriber works with the system through an automated workstation (AW). AW automatically communicates with the BC network for data exchange. The functionality of AW includes: algorithms for storing personal data, cryptographic transformation, hashing, the ability to download, update and store the current version of the blockchain network (BC) database to participate in the formation of a distributed registry. If the subscriber is not interested in maintaining the integrity and decentralization of the network, AW has the functionality of data exchange on the state of BC from an authorized server of the state. services (PS) through the personal account in the system of ESIA.

As part of the information exchange, subscribers form internal data blocks. The internal data block is formed by means of AW and contains the addresses of the recipient and the sender, the digital signature of the sender, the timestamp and the minimum comprehensive information about the subject and parameters of the transaction, then the data (information about the counter data, service bills, checks, receipts). Data can be encrypted by means of AW to maintain the privacy.

After forming, the internal blocks are sent to the common data bus(read access to which all subscribers have), and to the queue of other external data blocks that are waiting to be included in the next external BC block.

The external block BC contains a limited-size data-fit array of internal blocks of subscribers, their hash amounts, the hash amount of the previous external block of the chain and its own hard-to-generate hash amount.

When an external block is formed and its hash sum fits the current complexity of the system, it arrives at the common data bus where it is read by the PS server and the aw subscribers involved in the decentralization of the network. Transactions of the external block can be viewed by any subscriber and confirm their existence, in situations where it is necessary to maintain confidentiality, the internal block will be encrypted with an asymmetric encryption algorithm and the subject and parameters of such a transaction will remain secret (addresses, signature, and hash amount will remain public, providing transparency).

Personal account or AW directly accepts the necessary transactions and processes the algorithms corresponding to their subject area.

Public services are a trusted state body whose responsibilities, according to the logic of the General algorithm include: the content and security control of personal user accounts and access channels, providing subscribers with servers that store the current chain of BC blocks and access to these servers, maintaining the health of objects forming external blocks.

With the help of such a system, it is possible to implement such types of transactions: billing for the use of the service from SP to SCS or from SP to SCS, payment of the bill for the use of the service through the ESIA site with duplication of the receipt to the BC network, recording a copy of the contract between SP and SCS.

The algorithm of formation of the invoice for the use of the service and its payment

1. To start the formation of the account for the service, the network Participant who has the right to do so (SP, MC, SCS), hereinafter "the requesting party", must receive data from AC/GHC (if any) SCS, hereinafter "the receiving party", this occurs either through an appeal to the ARSMMS or the formation of a request through the ESIA network.

1.1. In the first (Fig. 3) in the case of the requesting party sends AC/GHC data to the ARSMMS , that reads the data required AC/GHC, forms them into the internal unit, after, is sent by DB1 to the BC network, is included in the last in the chain of the external unit. As soon as the outdoor unit includes the message data AC/GHC passes the test, the requesting party, automatically reads them from DB1 through the PA or directly with AW.

1.2. In the second case (Fig. 4) the requesting party makes a request in the ESIA system, the request is displayed in the PA or on the AW of the receiving party. The last should read the AC/GHC manually and place them in the internal block data with AW, which will send an internal block DB1 in the network of BC, where he will join last in the queue of the circuit the outdoor unit. As soon as the outdoor unit includes the message data AC/GHC validated, the requester, reads data AC/GHC from DB1 through the PA or directly with AW, automatically.

2. Once the requesting party has received the AC/GHC data (if any), the formation of an account to the receiving party begins. Account data (which is comprehensive information required for payment) are generated in the internal block and sent to DB1, where BC will be included in the last in the chain of the external block. Once it is validated, the receiving party automatically reads the data from DB1 via PA or directly from A, and becomes familiar with the composition of the account.

3. The receiving party shall pay for the account via ESIA, upon successful completion, these receipts of payment sent to the requestor, cekret network warhead way similar to claim 2 of the present algorithm. Receipt of funds by the requesting party occurs normally in accordance with the provisions of the law.

Algorithm of duplication of this agreement for the provision of services

Comprehensive information necessary for the unambiguous identification of the contract of its parties and the subject matter is recorded in the internal unit by both parties and sent to DB1 via WS or PA. In DB1, internal blocks are included in the last open external block. After checking the external unit, contract data is included in the BC network.

A contract is considered to be signed if there are two copies of it in the BC network, each of which is signed by digital signatures of the parties and the hash amounts from the subject of the contract coincide. To cancel the contract, the documents responsible for this operation must also be duplicated in the BC network.

The system operates in four modes:

Mode of automated reading of counters of subscribers-consumers of services (SCS).

The SCS apartments are equipped with chips that read data from the meter adapters and convert them into a digital addressable code. Bus DB1 it goes to the automated recording system data of the measuring sensor, which is formed by a radio signal, transmitting the meter readings on the SCS server of the service providing bi-directional data bus DB3 on the data bus DB2. In the structure of service delivery is formed by inner block that contains information about the invoice for payment of the i-th SCS. Then, with the help of the system of forming the outer hash function the BC blockchain network, blocks are inserted in the shared circuit BC. The block data comes to the outputs of all SCS, i.e. a distributed registry is implemented. Only SCS can open the block and get the account data to which the information is sent, but others can confirm the fact of the transaction, the hash of the transaction and its parties. After receiving the invoice, the subscriber must make a payment through the personal account of the state services, the latter pay the amount directly to the SP. Upon receipt of payment, SP issues a receipt for the subscriber's funds, which is sent by DB2 to BC2. The new block is embedded in the BC block chain and sent to all SCS subscribers as a distributed d registry.

The mode of formation accounts for payment for the services of MC and receipt accounts to receive the criminal charge for her services.

In the MC form an electronic invoice for payment of the SCS service MC for keeping houses places in inner block DB5 unit arrives at BC1 where is the external side and the data is embedded in the circuit. So the data comes to the inputs of all subscribers via DB1 in the distributed register DR3, but the unit can only open the subscriber to whom it is addressed. SCS pays the amount indicated in the invoice in the personal office of the state service in the address of the management company. MC generates a receipt for payment from SCS and sends in the form of distributed registry DR2

Mode of questions, complaints, suggestions SCS, etc.

In this mode, the SCS form on an electronic form their question on an electronic template, include the template in their internal data block, and send it on the data bus where the block is included in the external circuit of the blocks of the BC3 network, then on the DB6 to the management company. at DB7 in urban structure and DB8 in SP with a distributed registry DR4. The answer forms the MC, the ESIA and SP through the blockchain network BC3 in the form of a distributed registry.

Mode of conclusion of the contract by services with subscribers-consumers of services.

In this mode, the SCS make up the contract for the provision of SCS and include in its internal block, which is received by BC2, where the formation of the outdoor unit and its sub-

sequent sending to the registry DR1 all SCS. SCS sign it with your electronic signature and sent back BC2 SP in the register of re.As a result of the work done by the authors, the block-chain technology was integrated into the system of housing and communal services, which has a different quality of service to consumers. The system for the first time in the history of its existence is a new quality of service ,thanks to the methods of cryptography,has solved the problem of equitable provision of services to both consumers and service providers.

References

[1] Andryukhin A.A. Methods of Protecting Decentralized Autonomous Organizations From Crashes and Attacks. Proceedings of the Institute for System Programming of the Russian Academy of Sciences. (Trudy Instituta sistemnogo programmirovaniya RAN) 2018. V. 30. № 3. P. 149-164.

[2] Babkin A.V., Burkaltseva D.D., Betskov A.V., Kilyaskhanov H.Sh., Tyulin A.S., Kurianova I.V. Automation Digitalization Blockchain: Trends and Implementation Problems. International Journal of Engineering and Technology(UAE). 2018. V. 7. № 3.14. P. 254-260.

[3] Brogan J., Ramachandran N., Baskaran I. Authenticating Health Activity Data Using Distributed Ledger Technologies/ Computational and Structural Biotechnology Journal. 2018. V. 16. P. 257-266.

[4] Gromovs G., Lammi M. Blockchain and Internet of Things Require Innovative Approach to Logistics Education. Transport Problems. 2017. V. 12. № S. P. 23-34.

[5] Kim H.-W., Jeong Y.-S. Secure Authentication-Management Human-Centric Scheme for Trusting Personal Resource Information on Mobile Cloud Computing with Blockchain. Human-centric Computing and Information Sciences. 2018. V. 8. № 1. P. 11.

[6] Kryukov A.P., Demichev A.P. Security Infrastructure for Distributed Computing Systems on The Basis of Blockchain Technology. В сборнике: CEUR Workshop Proceedings 7. Ser. "GRID 2016 - Selected Papers of the 7th International Conference Distributed Computing and Gridtechnologies in Science and Education" 2016. P. 338-342.

[7] Lee J.-H. BIDAAS: Blockchain Based ID as a Service. IEEE Access. 2017. V. 6. P. 2274-2278.

[8] Makarov A.M., Golyakova A.O., Osinin I.D., Postovalov S.S. Fundamental Design of Blockchain – Hashchain Networks With a Decentralized Register Based on Cryptography Methods. Advances in Intelligent Systems and Computing. 2019. V. 726. P. 620-629.

[9] Makarov A.M., Kiselev V.V., Golyakova A.O., Osinin I.D., Postovalov S.S. The introduction of digital blockchain technology in housing and utilities systems as an opportunity to create "smart cities" of the North Caucasus. Bulletin of expert advice. Vnedreniye tsifrovykh tekhnologiy blokcheyn v sistemakh zhilishchno-kommunal'nogo khozyaystva kak vozmozhnost' sozdaniya «umnykh gorodov» Severnogo Kavkaza. Vestnik ekspertnogo soveta. 2018. № 3 (14). P. 39-47.

[10] Pilkington M., Grant L.G., Crudu R. Blockchain and Bitcoin as a Way to Lift a Country Out of Poverty - Tourism 2.0 and E-Governance in the Republic of Moldova. International Journal of Internet Technology and Secured Transactions. 2017. V. 7. № 2. P. 115-143.

[11] Scientists are exploring the impact of the digital world on the perception of modern life. Site «Southern Federal University» (Uchonyye issleduyut vliyaniye tsifrovogo mira na vospriyatiye zhizni sovremennogo cheloveka. Sayt «Yuzhnyy Federal'nyy universitet») URL: sfedu.ru/news/60349 2

[12] Vorobyev G.A., Ryndjuk V.A, Kozlov V.A., Makarov A.M. Probabilistic models of cryptographic systems and their applications / 3rd International Conference on digital information processing, data mining, and wireless communications, Dipdmwc 2016, pp 160-163