The Digitalization of the Russian Financial Market: The Use of Technologies of the Distributed Ledger by the Institutions of Custodian Infrastructure

K.R. Adamova* and I.E. Pokamestov

Department of Financial Markets and Banks, Financial University under the Government of the Russian Federation, Moscow, Russia

Abstract: Over the past 30 years financial markets have moved from a highly centralized to a globalized system that includes all the world's stock exchanges and other financial institutions. The global stock architecture has united the world market.

Traditionally, trading in financial instruments took place between stock brokers and traders who made personal transactions on trading platforms. At that time, stock brokers were monopolists of the market, only their information, their recommendations were the only source of information for investors. This was before the dotcom revolution, when communication became simple and accessible to everyone. Trade has been transformed from physical to electronic form, today you can buy securities, currencies and any derivatives in any quantity, at any time and from anywhere in the world. Development of blockchain technologies is integrated into financial transactions. Financial intermediaries are forced to follow the market and actively introduce new technologies in their processes.

This article will consider the possibility of using the technology of the distributed ledger by institutions of custodian infrastructure. Today, a number of Russian financial institutions are developing their own projects using blockchain.

Keywords: Blockchain, financial market, custodian infrastructure, securities, distributed ledger.

1. INTRODUCTION

One of the main elements of the securities market infrastructure is the Depository system. This is an integral part of the Record-keeping system for rights to securities. Over time, new technologies have emerged that have had a positive impact on various areas of activity. Considering the most popular technological innovation-the system of distributed ledger, the possibility of their implementation in the activity of securities record-keeping was evaluated. This system has its advantages, which can have a positive impact on the Record-keeping system as a whole. But at the same time, innovations should not have a detrimental effect on efficiency compared to the current Depository system.

The subject of the study is one of the technologies of modern times – blockchain as an instrument of custodian activity.

The main purpose of the work is to analyze the existing blockchain technology and the possibility of its application by custodian institutions at the present stage of development of the financial market of the Russian Federation.

To achieve this goal in the course of the work the following tasks are solved:

- study of the nature and processes of blockchain technology at the current stage;
- analysis of existing blockchain projects in the Russian financial market;
- assessment of the possibility of mass introduction of blockchain into the domestic Depository industry at the present stage.

The scientific novelty of the work is to consider the blockchain technology as a tool for accounting operations in the field of custodian activities from a practical point of view.

2. LITERATURE REVIEW

During the preparation of the study and its implementation were studied next the legislative acts regulating the custodian activities:

1. Federal law “On the securities market” dated 22.04.1996 No. 39-FZ (as amended);
2. Federal law “On joint-stock companies” dated 26.12.1995 No. 208-FZ (as amended);
3. The Federal law “On the Central Depository” dated 07.12.2011 No. 414-FZ (in the current edition);

*Address correspondence to this author at the Department of Financial Markets and Banks, Financial University under the Government of the Russian Federation, 127276, Bolshaya Marfinskaya Str., No.4, Bld.3, App. 94, Moscow, Russia; Tel: +79037668661; E-mail: kadamova@fa.ru

E-ISSN: 1929-7092/18

4. Federal law “On amendments to certain legislative acts of the Russian Federation in connection with the adoption of the Federal law “On the Central Depository”” dated 07.12.2011 No. 415-FZ (as amended);

as well as the works of Russian and foreign scientists, the main of which: K. R. Adamova (2013), B. I. Alekhin (2018), A. G. Guznov (2018), Melanie Swan (2017), etc., including articles in periodicals and electronic publications.

The main monographs touch upon the theoretical foundations of depository activities, while some articles in periodicals (Adamova, 2013) address the main problems of the functioning of institutions of depository infrastructure, including the multi-level institutional structure and problems of the implementation of shareholders' rights in this regard.

3. THE MAIN PROBLEMS OF MODERN DEPOSITORY AND SETTLEMENT INFRASTRUCTURE OF THE RUSSIAN FINANCIAL MARKET

Depository and settlement infrastructure of the Russian financial market is a set of financial institutions that ensure the functioning of the securities market as a single system, namely: depositaries, registrars and clearing organizations. This part of the financial market has developed in Russia at a significant pace; the main evolutionary changes have been carried out in the period from 2011 to the present time, since the adoption of the two fundamental documents:

1. The Federal law “On the Central Depository” dated 07.12.2011 No. 414-FZ;

2. Federal law “On amendments to certain legislative acts of the Russian Federation in connection with the adoption of the Federal law “On the Central Depository”” dated 07.12.2011 No. 415-FZ;

With the adoption of the Federal law No. 414-FZ “On the Central Depository” dated December 7, 2011, the Russian Depository system became a two-tier system and the priority of these registers of the Central Securities Depository over the data of the register of registered securities holders was established. At the same time, amendments were made to the Federal law “On joint-stock companies” dated 26.12.1995 No. 208-FZ, allowing to start the process of digitalization of corporate actions, the transfer of interaction between securities owners and registrars to electronic document management not only in the implementation of operations in the register, but also in the implementation by the owners of securities of the rights secured by these securities. This was the impetus at the beginning of the reform of corporate actions.

The problem of investors-holders of securities, which had existed for many years and which was unsolvable due to the impossibility, at times, to exercise their rights, in particular votes, became solvable. At the moment, this problem is partially solved by the wider introduction of electronic document management (EDM), but in addition to EDM technologies, new financial technologies appear and we will consider them and assess the prospects for implementation in the financial market of Russia.

4. THE TECHNOLOGY OF DISTRIBUTED LEDGER

The modern world is a huge number of elements, interconnected and united by a global network. Economic relationships and transactions are carried out through commercial information networks that allow to overcome national, regional and legal boundaries, linking its participants on different trading platforms that allow to manage assets and realize the rights arising from these assets. Most of these networks are based on the principle of the register.

Distributed ledger technology is a blockchain-based approach to information exchange and storage[1].

Blockchain, in turn, is a multifunctional and multilevel information technology designed for reliable record-keeping of various assets. Potentially, this technology covers all areas of economic activity without exception and has many applications. It creates new opportunities for the search, organization, evaluation and transfer of any discrete units.

“The Byzantine army is besieging the city. The generals need to develop a single strategy of action that will lead to victory, even if among them are traitors, deliberately distorting the information about the number of their troops and the time of the offensive" - so formulated "the task of the Byzantine generals” — one of the classic in cryptology[2]. It is about how to

[1]Official website of the Bank of Russia [Electronic resource] / / Development of technologies of distributed ledgers/ URL: http://www.cbr.ru/Content/Document/File/36007/reestr_survey.pdf (date: 07.04.2018)

[2]Wikipedia – The Free Encyclopedia [Electronic Resource] // Byzantine fault tolerance [web-site]. URL: https://en.wikipedia.org/wiki/Byzantine_fault_tolerance (Date: 03.04.2018).

harmonize the actions of the participants in the system, united by one goal, but deprived of trust in each other.

If you do not use the tools of mathematics, the obvious solution seems to be the creation of a single supervisory and inspection body that will guarantee the participants of the system the accuracy of the information received. For hundreds of years mankind has been on this path. Banks and payment systems serve as guarantors of money transfers.

Blockchain technologies are changing the usual logic, and the necessity for intermediaries is eliminated. This is achieved through a special form of storing transaction information on all computers of the system — in distributed ledgers or databases.

In 2008, Satoshi Nakamoto[3] invented a new way to achieve social consensus[4], which allow to confirm the truth of all transactions without the participation of a third party. This name was first discovered in the blocks of the decentralized bitcoin network. It is the first name of the owner entered there.

The easiest way to demonstrate this is to briefly explain the essence of the work of blockchain technologies on the example of transfers in bitcoins.

Each transaction takes place online and is only a message that a certain user transfers to another user a certain amount of bitcoins. Once the transaction is completed, it becomes visible to miners.

None of the transactions will be considered completed until it is included in the so — called block-this is what miners are doing. Each block contains information about thousands of processed transactions. For it to be considered formed, the miner must calculate the hash function-a number-letter string, which is converted into an incoming array of data.

The hash function contains information about the previous block, which means — about all transactions made since the emergence of bitcoin as a currency. If you change at least a bit of information in the previous chain, the hash function will change beyond recognition. It turns out that the distributed database in the blockchain is a chain of blocks, each of which refers to the previous one.

Keeping a history of bitcoin transactions ensures that the user does not transfer to someone an amount that he or she does not have. Blockchain technology allows you to avoid double spending-a situation where a person twice tries to spend the same amount. The key to this is a large number of users and economic motivation of miners.

The motivation of miners who spend time and money to calculate the hash function is quite simple. As soon as the block takes its place in the chain, the miner that formed it receives a certain amount of bitcoins — so their emission occurs. Miners also collect Commission from each transaction. According to the rules established by Nakamoto, the amount of remuneration is reduced by half every 210 thousand blocks.

One of the obstacles to the direct adaptation of the public blockchain, which is bitcoin, was its openness. In such a network, any participant is able to read data from the blockchain and write them, creating new transaction blocks. In other words, public blockchains are resistant to censorship. However, this feature ceases to be an advantage in the context of internal work processes of a large company — in this case, access control comes to the fore.

Here, the so-called exclusive “authorized” blockchains came to the aid of companies. Exclusive blockchain is the blockchain where the transaction processing is carried out with a certain list of subjects with established personalities. Read access to data is also usually limited, although certain rights may extend beyond the scope of blockchain operators.

For example, in a financial blockchain supported by several banks, the data will be available to the regulator and law enforcement agencies, as well as customers of banks will be able to view their data. In addition, this scheme can be used by developers of third-party financial applications built on the basis of the blockchain with limited access to a certain set of information.

And world organizations are already studying the possibility of building their own exclusive blockchain. Three large Dutch banks ABN Amro, ING and

[3]Satoshi Nakamoto is the pseudonym of the person or group of people who developed the bitcoin cryptocurrency Protocol and created the first version of the software in which this Protocol was implemented. Several attempts have been made to reveal the real person or group behind this name, but none of them have been successful.

[4]Consensus is the collaborative process that the members of a blockchain business network use to agree that a transaction is valid and to keep the ledger consistently synchronized. Consensus mechanisms lower the risk of fraudulent transactions, because tampering with transactions added to the ledger would have to occur across many places at the same time. (URL: https://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-glossary-bluemix-trs/index.html).

Rabobank are investigating the use of blockchain for payment systems. And, for example, Citigroup has built three blockchain and internal currency on their basis in order to minimize the risks when interacting with other banks.

Exclusive blockchains provide greater control over the system by the company. The bottom line is that such networks allow, for example, to quickly updating functionality. Therefore, their use is most justified in institutions working with registers and accounting systems — exclusive blockchains form a more controlled environment, compared to public blockchains.

Another exclusive feature of the block chain is a transparent management structure. They also offer greater flexibility and adaptability compared to the open blockchain infrastructure. This allows exclusive blockchains to find application in solving very specific business problems-property rights management, journalism and electoral system.

Many experts believe that they will solve many problems of financial organizations that are not able to solve, say, bitcoin. For example, the compliance of the law “On the portability and accountability of life insurance” (URL: http://www.hipaa.com/) or policies to combat money laundering (AML) (URL: https://www.anti-moneylaundering.org/).

Closed blockchains provide an interesting opportunity for companies to use distrust and transparency in internal and inter-corporate scenarios.

Creating blocks in an exclusive blockchain does not require proof of work (proof-of-work). Instead, for a consensus in an exclusive block chain can be used well-studied consensus algorithms with authenticated parties, as, for example, the above-mentioned problem of the Byzantine generals. Another example is the block creation Protocol used in BitShares[5]. In such algorithms, each transaction processor has a private and public key pair. The creators of blocks are known and determined by the block's digital signature.

No financial institution can consider the absence of “itself”. Permissionless-systems that are open to any participant, have significant performance limitations — bitcoin blockchain gives about two transactions per second. Unfortunately, this speed is not suitable for most business tasks.

There should be a legal entity within the system that gives participants the right to" login", ensures that the system works and minimizes legal risks. If we put information in an open network, no one can guarantee its security.

For example, the bitcoin blockchain can be suspended but cannot be destroyed. At the moment, the cost of such a "stop" is estimated at hundreds of millions of dollars, and this is the real danger that the participants of this network are discussing. If someone has such means, he in theory can stop the network for some time by sending a large number of transactions to the system. It is clear that sooner or later the network will work again, but in the case of bitcoin there is no administrator who would guarantee the restoration of its operation and closed access to the network for attackers.

Summarizing the above, to explain the work of the blockchain, a scheme is composed, which contains 6 stages (see Figure **1**).

Stage “A” is that one of the participants wants to make a transaction. To do this, they enter a certain set of data to be debited from their accounts cryptocurrency, money, securities or something else, depending on the specification of the blockchain network. If all data is correct, the transaction enters a new forming block (stage “B”).

New blocks in stage “C” are sent to all network participants (in the case of cryptocurrency – miners) for data verification. Checked the data, on account of necessary quantity of means, etc.

When the newly formed blocks are checked, each member of the network writes this block to its own database instance (stage “D”), which contributes to the immutability of data, since it is possible to change one database, but at the same time several tens, or even thousands, is problematic. As soon as the transaction data are in the formed block, then immediately there is a write-off/transfer of funds.

With the onset of the “E” stage, the new block enters the block chain, which contains data on absolutely all transactions since the beginning of the blockchain network operation. At stage “F” the transaction is considered to be completed.

[5]BitShares — open-source, public, blockchain-based, financial platform, real-time. It provides a decentralized asset exchange, like the NYSE, but for cryptocurrencies, without the necessity to trust a centralized Fund. BitShares is provided by “BTS” cryptocurrency that is used for payment of network activities or collateral.URL: https://bitshares.org/.

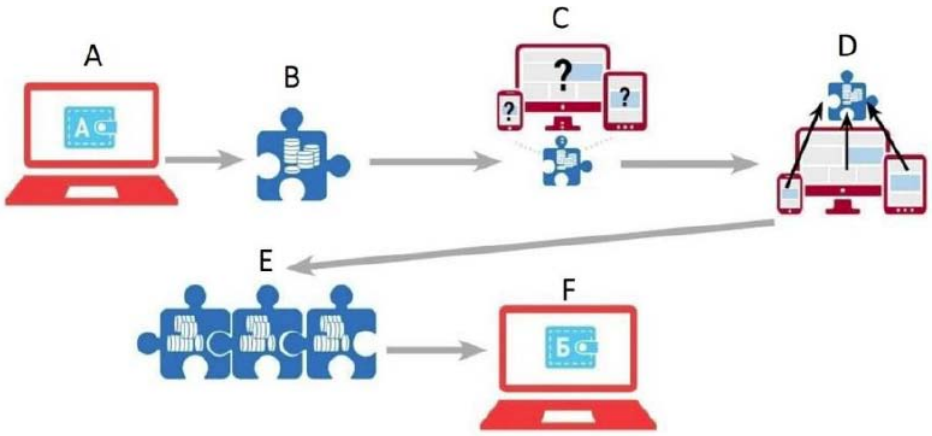

Figure 1: Blockchain network operation scheme

5. THE USE OF BLOCKCHAIN BY INSTITUTIONS OF CUSTODIAN INFRASTRUCTURE AT THE PRESENT STAGE

The article proposes to consider the working draft of the NCO JSC "National Settlement Depository" (NSD JSC) associated with the voting system of shareholders. Active development began in 2014 together with Hyperledger and continues to this day.

This system is based on the "authorized" blockchain, which should ensure the reliability, immutability and transparency of the data, and most importantly – the absence of intermediaries. This project was started because the voting process involves a fairly large number of participants distributed geographically. This procedure is quite simple and is carried out in an isolated space of participants.

The main advantage is the fact that it is not required to transfer all the securities accounting to the blockchain. But with a full transition in the future of Depository accounting in the blockchain, there will be no problems associated with the combination of data.

Let's consider the classical scheme for the registration of securities presented in Figure **2** and on the basis of which will be discussed further in the blockchain-the mechanism.

In Figures **2-5**, use the following designations: issuer is the Issuer of the securities, registrar (reg) is the Registrar, CSD is the Central securities Depository, ICSD – global custodian, nominee – a nominee holder, the custody is the custodian or the Depository.

The Issuer issues one thousand shares, which are all accounted for by the Registrar on its balance sheet. Further, there is a division by owners: 150 belong to an individual – the holder of shares, 50 – to a legal entity, and the remaining 800 are located on the CSD account (in our case – NSD JSC).

The next level consists of those securities that are recorded in the accounts of the Central Bank, of them: 450 securities - in the accounts of nominal holders, 280-in the accounts of global depositories and 70 securities owned by the client of the Central Bank, which has its own account in this structure.

The securities in the accounts of the global custodian belong to its clients. As for the nominal holders-depositaries, the situation is similar. Part of the securities in the accounts of clients and the other part of the lower – custodian structures-custodians.

This information is necessary for further consideration of the voting system, which is based on a relatively new technology of distributed data storage.

Each nominal and real holder of the share has its own "wallet" (see Figure **3**). Nominal holders of transit purses, through which are passed the "coin" (the right to vote securities), to the owners who cast their votes according to their preferences.

The Registrar has a special status and is the beginning of the vote distribution chain for "wallets". Holders of shares he transfers voices into their accounts, and nominal holders get them for further distribution at their level (see Figure **4**).

After the distribution of votes in the wallets has taken place, the holders cast their votes according to their preferences on the issues raised in the voting (see Figure **5**). If the question involves a cumulative vote, the number of votes of each holder is increased by N times depending on n options.

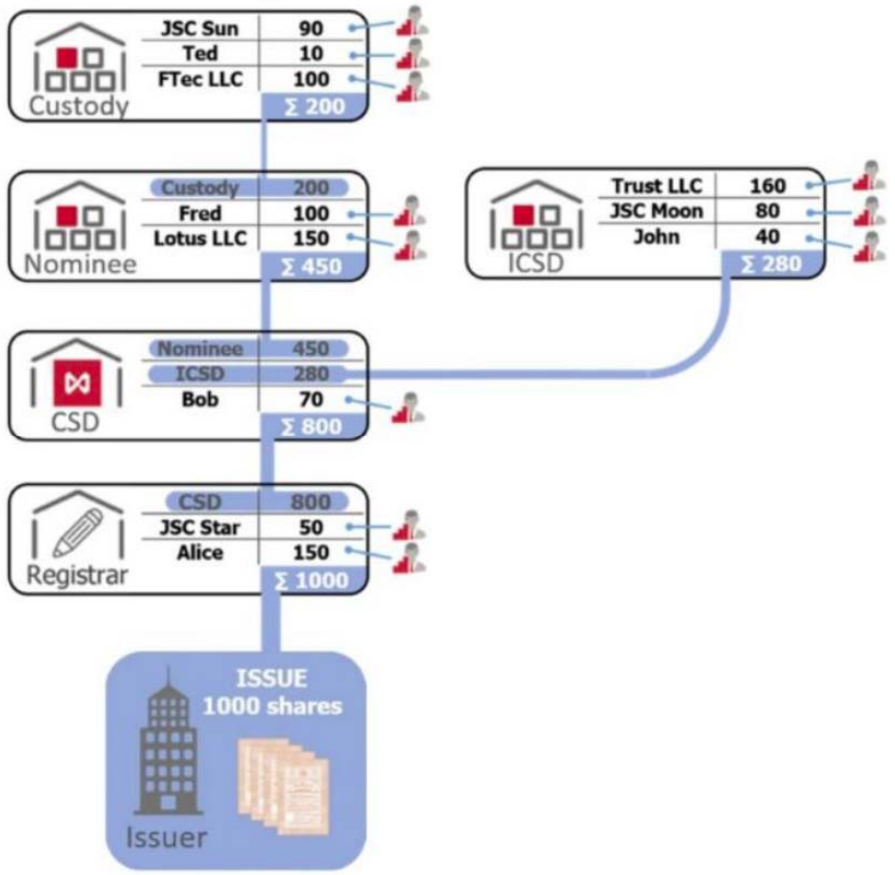

Figure 2: The classical scheme of registration of securities.

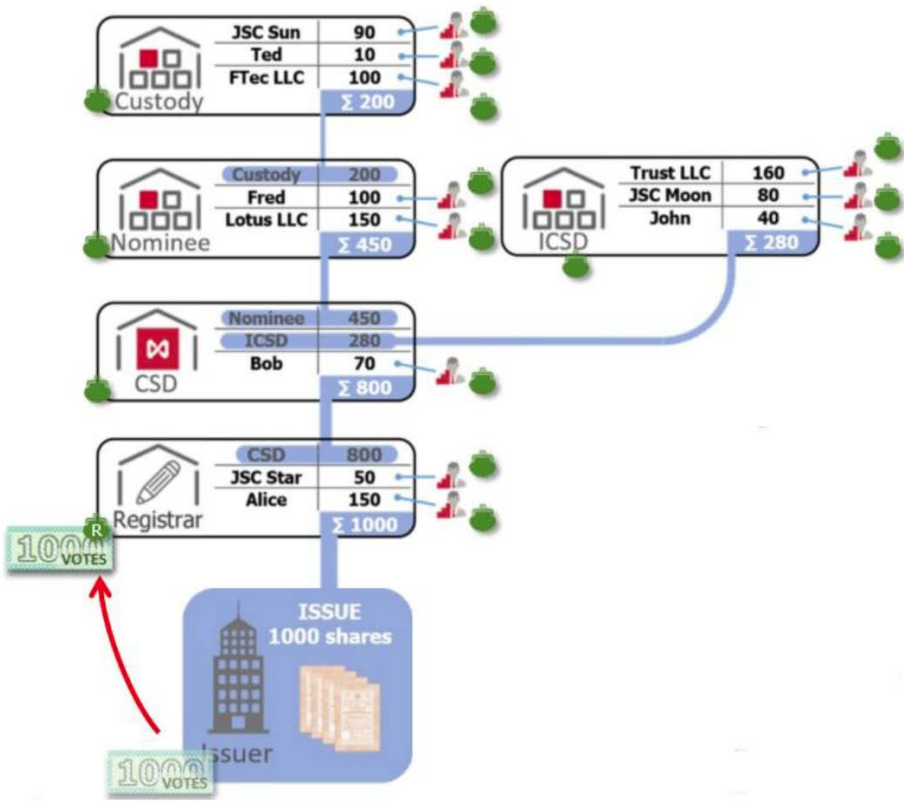

Figure 3: "Wallets" of the holders and the first stage of voting.

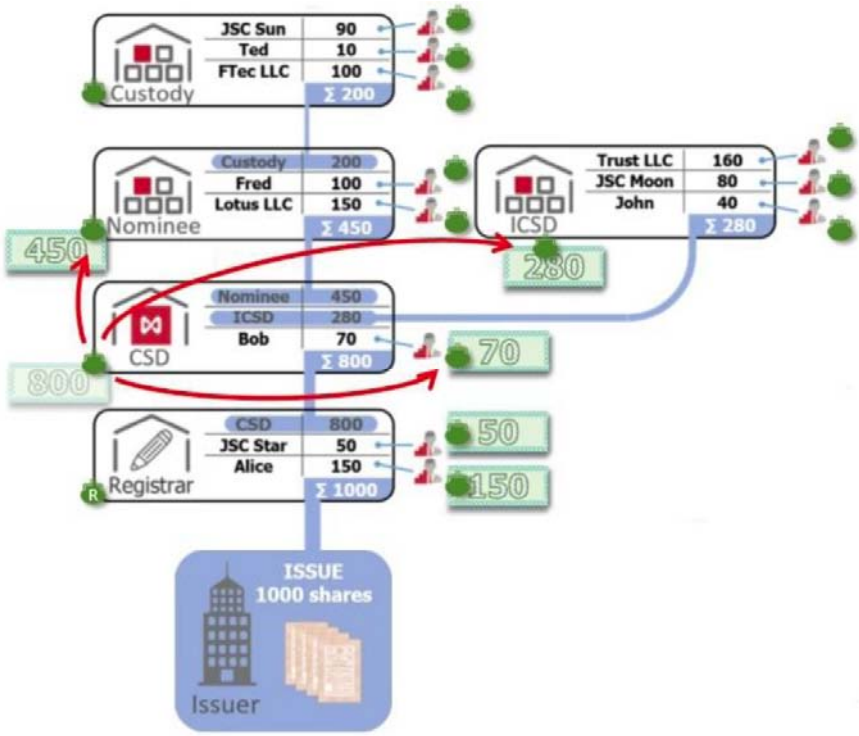

Figure 4: The mechanism of distribution of "coins" at the stage of the CD.

The given register of votes shows how the votes are taken into account in the distributed database. This scheme is quite simplified, as only 11 shareholders are listed here. In the real market of these shareholders can be several hundred thousand, as well as a more extensive list of nominee holders.

Each question that may have additional conditions has its own sub-levels:

- register positive responses, the case of negative responses;
- register of abstentions;
- register of those who did not vote for one reason or another.

Each register is also divided into sub-levels, which are built according to the distribution of securities in the Depository system. As an example, the scheme shown in Figures **2-5** was transferred to an acceptable form for the voting system. The "+" sign in the cells indicates that the list has lower sublevels.

This database of votes has its own characteristics. Only votes that are on the "wallets" of the end owners are taken into account. The number indicated at the upper levels is the maximum possible sum of the votes of the lower levels. This technical feature was registered to check the number of counted votes and does not affect the voting process itself.

The construction of a question for voting may be different, if a choice is given between several options (in the scheme-candidates), the vote is held in cumulative form, which implies a multiplication of the available votes by a coefficient equal to the number of options.

Also this takes into account such facts as the impossibility of taking part in voting on certain issues. This is mainly due to any legal restrictions. In this case, the share holder will have 0 "coins" on his wallet.

If the shareholder does not wish to vote on some issue, after the end of the voting period, his vote will go to "not vote". This is necessary to ensure that the votes are properly taken into account and that the "free" votes are not misused.

The main advantage is the anonymity of each "wallet". In other words, each voting participant can see how his votes were taken into account after the results, but in addition to his votes he is not able to see the state of the other voting participants ("confidentiality"). Even when using the Zero-knowledge to proof the algorithm. The cryptographic algorithm in this case consists in the proof of impossibility of calculation of votes of other participants, proceeding from final results.

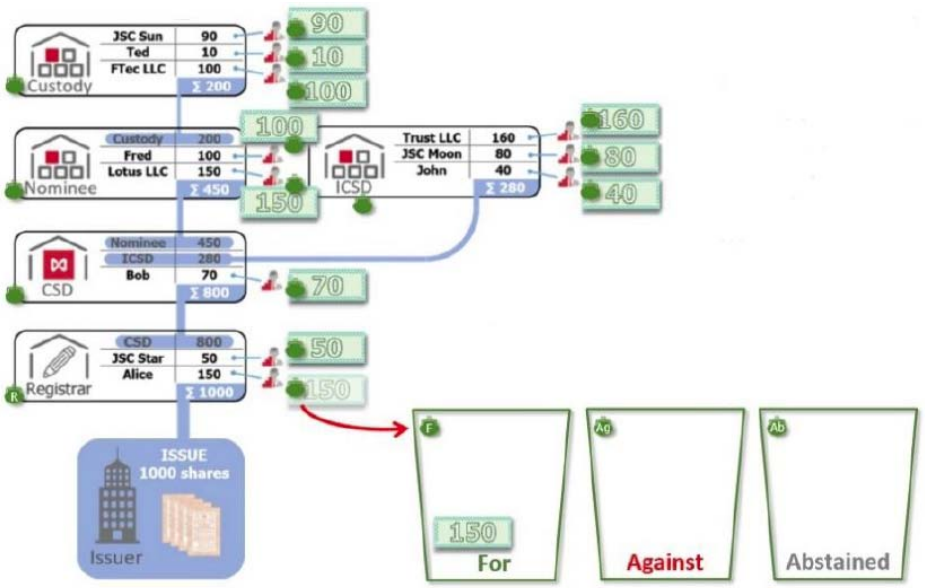

Figure 5: Order of distribution of votes.

Another advantage is the reliability, which is to record all events distributed network with multiple nodes. This eliminates the risk of retroactive changes and distortion of data that is already included in the database. The network itself calculates the results, which prevents falsification of data. Also, the distributed network does not allow double voting.

Network transparency plays an important role. Any member of the network can check the accuracy of the data. The owner of the "votes" fully controls the passage of their instructions and their account in the results. Specialized or public authorities may conduct online audits after certain rights have been granted. Due to transparency, less conflict conditions are created, and all possible conflicts are easy to resolve.

6. IMPLEMENTATION OF THE DISTRIBUTED LEDGER IN CUSTODIAN ACTIVITIES

In September 2017 NCO JSC "NSD" together with OJSC "MegaFon" and JSC "Raiffeisenbank" held the first Russian transaction on placement of securities on a blockchain-based platform. Corporate bonds were chosen as a pilot project.

Corporate bonds are a tool for issuers who want to raise funds without entering the open securities market. The main features are[6]:

1. The issue is carried out without registration of the securities prospectus and without state registration of the report on the results of the issue;
2. The issue of bonds only in documentary form with mandatory centralized storage;
3. The amount to be repaid and interest paid exclusively in cash;
4. Placement occurs only on a closed subscription;
5. The issue identification number is assigned to the CSD.

The issue of corporate bonds takes place in 4 stages.

The first stage consists in the adoption and approval by the Executive body of the Issuer of the decision on placement of securities, as well as in parallel with this, the terms of the issue of commercial bonds.

The second stage is the conclusion of the necessary contracts with NSD JSC (emission account agreement, Treasury account agreement, EDO agreement, agreement on the provision of services for the assignment of identification number to the issue of commercial bonds) and the provision of the necessary set of documents[7].

[6]Legal reference system "Consultant plus" [Electronic resource] // the Federal law dated 22.04.1996 No. 39-FZ (as amended on 31.12.2017) "On the securities market" URL: http://www.consultant.ru/document/cons_doc_LAW_10148/ (Date: 11.04.2018)

[7]Official website of NCO JSC "NSD" [Electronic resource] // the List of documents to be submitted by legal entities residents of the Russian Federation in NCO JSC NSD. URL: https://www.nsd.ru/common/img/uploaded/files/Documents/raskas/form/docs_otkrytie.pdf (date accessed: 17.04.2018)

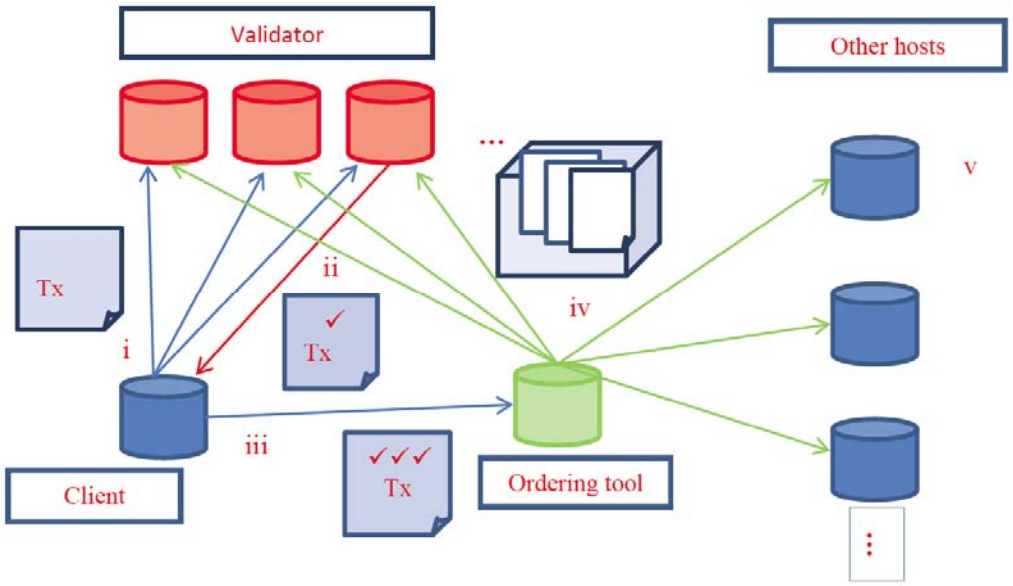

Figure 6: Working Scheme of Hyperledger Platform.

Official website of the Japanese stock exchange [Electronic resource] / / Japan. exchange Fund group: trends studies the use of distributed Ledger technology in the capital market. URL: http://www.jpx.co.jp/english/corporate/research-study/working-paper/b5b4pj000000i468-att/E_JPX_working_paper_Vol20.pdf (date accessed: 20.04.2018).

The third stage is performed by the CSD and is to assign an identification number to the issue of commercial bonds. To do this, the Issuer must provide a list of additional documents[8].

The fourth stage - after assigning the number, the date of the placement start is agreed, and then the placement itself takes place. At the very end, a notification on the results of securities placement is drawn up, which is sent to the NSD JSC (CSD).

But this tool was chosen for testing in the blockchain for a reason. Commercial bonds have a number of advantages over, for example, exchange-traded bonds: there is no need for the state registration of the issue, prospectus and report, placement on a closed subscription, a simplified set of documents, no special requirements for the financial position and terms of existence of issuers, and the Issuer can be any business company that has fully paid its authorized capital. Below there is a scheme of working process (Figure **6**).

To conduct a pilot transaction, a blockchain platform based on Hyperledger (URL: https://www.hyperledger.org/). Hyperledger project created under the auspices of the Linux Foundation (URL: https://www.linuxfoundation.org/) is an initiative to create various blockchain platforms and supporting open source tools. The project involves a whole range of companies from around the world: technology giants, consulting companies, representatives of various industries and start-up teams. The project was launched in December 2015, and now five blockchain platforms and four tools for working with blockchain platforms are actively developing. Hyperledger is open to all its members are equal and adhere to the principles of “clean” open source code.

Because Hyperledger is not as widely known as Bitcoin (URL: https://bitcoin.org/ru/) or Ethereum (URL: https://www.ethereum.org/), to make it easier to understand the topology of this blockchain network and the processes taking place in it, let us briefly consider its features of architecture.

Consider the implementation of the transaction on the blockchain the platform Hyperledger. Unlike public platforms like Bitcoin or Ethereum, Hyperledger has two special roles:

- Validator (endorser) — a node that checks and executes a transaction, and then returns it back to the client with the results and its signature.
- Paradisiacal (orderer) is the node that establishes the sequence of transactions and routes them to other nodes of the DLT network.

[8]Official website of NCO JSC “NSD” [Electronic resource] / / Documents regulating interaction with issuers on the circulation of commercial bonds. URL:https://www.nsd.EN/EN/documents/misc/index.php?36 id=924&i 36=3#p1_pravil (date accessed: 17.04.2018)

To reach consensus on transaction validation, validation policies[9] (endorsement policy) are used – a set of rules that determine which node can be a validator, and how many validator signatures are sufficient to make the transaction valid. In this case, the validation policy is set separately for each smart contract[10] created in the blockchain network. For example, in a policy, you can specify that a transaction will be valid if two of the three specified nodes confirm it.

How a transaction is created and executed:

1. The client sends the transaction to the validators (endorsers).

2. The validators execute the transaction and return it to the client with the execution results and their signature.

3. The client collects the required number of signatures of validators and sends the transaction from the set of answers of the validator to the "Orderer".

4. "Order" combines transactions into a sequence of blocks and sends them out.

5. Each of the nodes checks whether the transaction complies with the validation policy, and "loses" it in its registry instance.

Because the deal was "pilot", it was only 3 subjects: NCO JSC "NSD" acted as the operator of the transaction and network administrator, and OJSC "MegaFon" and JSC "Raiffeisenbank" as participants in the transaction. Only securities, not cash, were involved in the accounting operations.

Each participant has deployed its own network node, as well as additional components provided by the Hyperledger architecture: NSD JSC has deployed the Orderer, which provides the formation of an ordered flow of transactions, and installed the client part with the UI, which provides the functionality of the transaction operator. OJSC "MegaFon" and JSC "Raiffeisenbank" set the client side UI that provides the functionality of a party to the transaction.

Registries were created in the network, access to which was limited by the internal mechanism of network channels. The register of securities, which is available to all participants, has the only smart contract "SecurityMaster", which kept a list of securities. Free registry of account balances, participants with smart contract "Book" that reflects the account balances of participants, only available NCO JSC "NSD". The register of account balances, JSC "Raiffeisenbank" and the registry of accounts of OJSC "MegaFon" is available only for NCO JSC "NSD" and above. The register of transactions between the participants is available only to NSD JSC and those participants who conduct the transaction (in this case, it is the Bank and the communication operator). Smart contract "Instruction" registered and processed all transactions of this pair of participants. Working scheme of NCO JSC "NSD" project interface based on Hyperledger presented below on Figure **7**.

Also, in the balance sheet registers of JSC "Raiffeisenbank" and OJSC "MegaFon", one smart contract "Position" was created, in the context of which the balances of the participant's accounts were reflected. If the transaction was carried out and legalized only through the blockchain, the process would look like this:

1. In the transaction Register, both parties create purchase and sale instruction transactions that are stored in the context of the "Instruction" smart contract»;

2. When you receive the second statement of a pair of "buying and selling", they are matched with each other in smart contract "Instruction" and get the status "matched";

3. When a client of NCO JSC "NSD" receives a notification about the mapping, then the Unified registry checks balances on accounts of participants of the transaction;

4. If the balance check is successful, the client of NSD JSC creates transactions in the smart contract "Instruction", which change the status of the relevant instructions to "execute", and then creates transactions to change the balance of accounts for the smart contract "Position".

There is an approved procedure for regulating securities trading, in which the transaction is considered legally significant if it is carried out through the regular system of securities accounting of NSD

[9]Validation policy-configuration to determine which node is a validator or how many nodes are required to confirm a transaction.
[10]Smart contract is a computer algorithm designed to conclude and maintain commercial contracts in blockchain technology

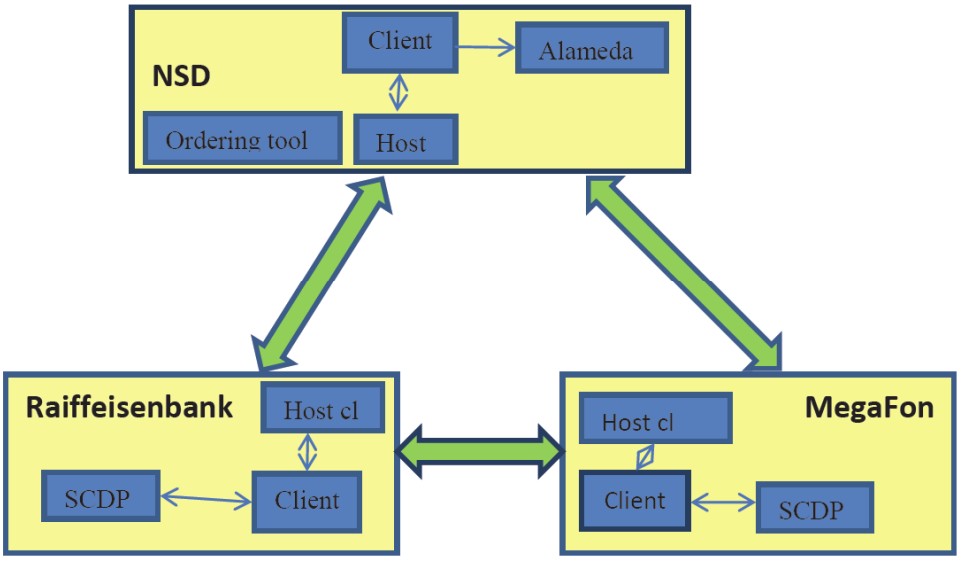

Figure 7: Working scheme of NCO JSC "NSD" project interface based on Hyperledger.

Alameda JSC. To meet this condition, the process of the transaction added special stages of formation, signing and processing of orders of the current format, using "combat" electronic digital signatures of the transaction participants. In addition, in order for the transfer of orders through the blockchain to be considered legitimate, NSD JSC signed a license agreement and an additional agreement to the Agreement on electronic document circulation with the parties to the transaction.

As a result, the process of the transaction began to look like this:

1. OJSC "MegaFon" and "Raiffeisenbank" JSC, each at its own site, create counter instructions for sale and purchase, respectively, and transfer them to the smart contract "Instruction".

2. In the "Instruction" smart contract, statements are mapped to each other.

3. If the mapping is successful, then:

- NCO JSC "NSD" on your node creates and "attaches" to the instructions of each participant to the corresponding file in order to load into the "lameda".

- In inventory balances of participants in the transaction (smart-contract "Position") is sent to the transaction on change of accounting of securities in the accounts.

4. Transaction participant:

- Removed from the blockchain files instructions to "Alameda".

- Sign of their "combat" electronic digital signatures to the respective work areas.

- Placed back into the blockchain.

5. NCO JSC "NSD" retrieves the subscribed file of the instructions and downloads in the "Alameda".

6. "Alameda" processes a transaction and creates a file of statements, which then sends the transaction participants.

All project participants were primarily interested in the study of legal issues associated with conducting transactions through the blockchain, and the identification of technical and organizational difficulties that may arise when deploying a blockchain network in real conditions. Moreover, organizations are different, each with its own infrastructure and network policy, rules of interaction between external and internal networks, and so on and so forth.

The first difficulties appeared before the platform was launched: JSC "Raiffeisenbank" and OJSC "MegaFon" were not ready to give direct access to their existing electronic digital signature keys to foreign and strange software. In this regard, a special utility for uploading/downloading of order files has been developed so that they can be signed outside the platform SOFTWARE.

Further difficulties were related to the fact that the platform was developed and debugged in Amazon Web

Services, and at the time of its launch, it had to work in a harsh heterogeneous world instead of a sterile-homogeneous cloud environment.

Fortunately, the implementation of the platform involved the use of Docker containers, so the differences related to the use of participants of different operating systems RHEL (URL: https://www.redhat.com) and Ubuntu (URL: https://www.ubuntu.com/) did not affect the operation of network nodes.

The main problems were related to the internal features of Hyperledger and the fact that the network infrastructure was built differently in both companies. For example, the node of the Bank did not see itself at its external address, or there were mysterious "sticking" of the service responsible for uploading/downloading files, which could be removed only by restarting the service.

7. CONCLUSIONS

To sum up, the distributed registry systems are already operating in different countries. In Russia, this technology has also found its application, but there are legislative restrictions that do not allow the full implementation of blockchain in the sphere of capital markets. The main limitation, which affects the activity of securities accounting, is primarily related to the execution of orders of the depot of the blockchain network participants. They are not officially recognized as a legal justification for the transfer of ownership of securities.

The characteristics of the platforms of the distributed registry (DLT) is necessary to allocate the confidentiality of the data among all members of the network. It is quite important in the financial industry, because information plays an important role in this area. Initially, a distributed registry was created to share a database that stores all the data of all nodes. Some platforms have started to use encryption to restrict access to third parties. Throughout the existence of the blockchain, network participants always think about eliminating vulnerabilities of existing cryptographic methods, since the frequent use of decryption keys can increase the risk of data loss. The main trends are in favor of changing the structure of distributed databases: from the old type of networks, in which each user (node) stores the entire database (but the entire database can take up significant amounts of memory, which causes additional load on the server nodes), to networks in which each node stores only a certain amount of data, which reduces the amount of memory occupied and partly warns against "leaking" information to undesirable users, and transaction data fall only to those nodes, which are directly related to them.

Given the fact that transactions do not have to be split across all nodes, the new networks increase the speed of entry into the distributed database. The drive to maximize privacy and productivity has led to the separation of functions and roles on the latest versions of distributed Ledger platforms for capital markets.

The considered project of NSD JSC has a number of positive factors that favorably affect the optimization of processes:

- A single point of entry;
- Direct digital exposure between participants and NCO JSC "NSD" under the product;
- Reduction in the time between conclusion of the Contract of purchase and sale and securities settlement and funds through digital registration of contracts using smart contracts and automate the execution of these contracts;
- Calculation speed (t0);
- Cryptographic protection in the transactions;
- Data confidentiality;
- Data immutability;
- Ensuring system reliability through distributed data storage.

Thus, the blockchain technology has significant advantages that allow solving a significant number of problems in the activities of accounting institutions, which are reflected on investors now.

In case of giving up the chance to blockchain technology we need to promote serious changes in Russian stock market legislation. The first changes needed in Federal law "On the securities market" dated 22.04.1996 No. 39-FZ. In this law we need new point which will allow the investors to prove their rights with through blockchain transactions and not only with the receipt from depo account. And second changes needed in Federal law "On the Central Depository" dated 7.12.2011 No. 414-FZ.

At the moment, it is difficult to assess the further fate of the blockchain in the financial markets, but today many financial institutions are actively developing their own settlement and accounting systems. The future securities accounting system should be beneficial for all market participants using a distributed register.

REFERENCES

Alien, B. I. Securities Market: textbook and practice for academic highlighting / B. I. Alien. - 2nd ed.. and extra — M. : Publishing house “Yurite”, 2018. - 497 p. - (series: Bachelor. Academic Course).

Anti-money laundering (AML) policy [Electronic resource] / - access Mode: https://www.anti-moneylaundering.org/

Blockchain: back-office block-Buster // Autonomous research [electronic resource] / access Mode: http://www.autonomous.com/fintech/d9335db1-bf1a-4ab2-8d1d-a36cb747a6ae (proven 24.04.2017)

Federal law “On amendments to certain legal acts of the Russian Federation in connection with the Federal law “On the Central Depository”” dated 7.12.2011 No. 415-FZ// http://www.consultant.ru/document/cons_doc_LAW_122866/.

Federal law “On the Central Depository” dated 7.12.2011 No. 414-FZ//: http://www.consultant.ru/document/cons_doc_LAW_122865/.

Federal law “On the securities market” dated 22.04.1996 No. 39-FZ // URL: http://www.consultant.ru/document/cons_doc_LAW_10148/.

Guznov, A. G., Rozhdestvensky T. E. Public-prove regulation of the financial market in the Russian Federation: monograph. — M. : Publishing House “Yurrite”, 2018. - 438 p. - (Series : Actual monographs).

Japan Exchange Group: a trend in studying the use of distributed Ledger technology in the capital market. URL: http://www.jpx.co.jp/english/corporate/research-study/working-paper/b5b4pj000000i468-att/E_JPX_working_paper_Vol20.pdf

Prateek Rani, Aditya Srinivasan, digitalization of financial markets: impact and future/ / international journal of research in Finance and marketing, 2015 -.29-33

Swan, Melanie. Blockchain: new economy Scheme : [translation from English]. - Moscow: Olimp–Business Publishing House, 2017. - 240 p., Il.

The Federal law “About societies actions” dated 26.12.1995 No. 208-FZ // URL: http://www.consultant.ru/document/cons_doc_LAW_8743/.

The law “On mobility and accountability of life insurance” [Electronic resource] / - access Regime: http://www.hipaa.com/

Received on 04-06-2018 Accepted on 01-10-2018 Published on 12-11-2018

DOI: https://doi.org/10.6000/1929-7092.2018.07.46