Blockchain Technology Application for Electronic Voting Systems

Valentin Sliusar
Institute of Systems and Software Engineering and Information Technology
National Research University of Electronic Technology "MIET"
Moscow, Russia
vslyusar@mail.ru

Aleksei Fyodorov
Institute of Systems and Software Engineering and Information Technology
National Research University of Electronic Technology "MIET"
Moscow, Russia

Aleksandr Volkov
Institute of Systems and Software Engineering and Information Technology
National Research University of Electronic Technology "MIET"
Moscow, Russia

Pyotr Fyodorov
Institute of Systems and Software Engineering and Information Technology
National Research University of Electronic Technology "MIET"
Moscow, Russia

Vladislav Pascari
Institute of Systems and Software Engineering and Information Technology
National Research University of Electronic Technology "MIET"
Moscow, Russia
vlad.id.04@gmail.com

2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus) | 978-1-6654-0476-1/20/$31.00 ©2021 IEEE | DOI: 10.1109/ElConRus51938.2021.9396400

***Abstract*—Remote electronic voting is the most promising way to increase voter turnout. The use of Blockchain technology will guarantee complete security and protection against hacking, ensure the secrecy of the vote and openness of the procedure for the society.**

The structure of the Blockchain voting is as follows. The user needs to have a mobile-specific address space. The mobile device identifier is recorded on the Blockchain as a wallet address that is associated with that user's token. The token will be limited in time in which it can be used for voting. Sending a marker (token) to a specific candidate address will constitute a vote. Received votes are securely stored in the Blockchain, and the correctness of addressing a vote to a specific candidate can always be checked in real time. All data that goes into the Blockchain vote is sent to it thanks to a smart contract.

The proposed method for constructing remote electronic voting will allow to reliably store obtained results in the Blockchain, increasing the cryptographic strength of the data and the transparency of the system, and, consequently, the confidence of users in it. Early receipt of the ballot will allow to participate in voting remotely, as a result, the turnout will increase.

The considered structure of Blockchain voting will have prospects of use not only in the electoral system, but at general meetings of shareholders, meetings of LLC participants, meetings of the board of directors (supervisory board), committees, forums, conferences and other events where voting is necessary.

Keywords—voter turnout; security; anonymity; transparency; remote electronic voting; mobile application; smart contract; Blockchain

I. INTRODUCTION

Low voter turnout remains one of the pressing problems in the voting system. The reason for the low voter turnout is the limited time and place of the event, as well as distrust in the way and method of voting.

The most promising way to eliminate these causes is remote electronic voting, which faced the impossibility of guaranteeing complete security and protection from hacking, ensuring the secrecy of voting and openness of the procedure for society, as well as guaranteeing the fault tolerance of the system as a whole.

However, new technological developments provide new opportunities and change this situation. The use of Blockchain technology will solve the problems of remote electronic voting.

As a result, the aim of the study is to develop a remote electronic voting system based on Blockchain technology, which will provide the users with the fulfillment of the following requirements:

- the ability to create lists of voting objects,
- the ability to register voting participants,
- the ability to vote anonymously,
- the ability to change your vote during the voting period,
- transparency of voting,
- guarantee of inadmissibility of deliberate change of voting results,
- fault tolerance guarantee.

Users of such a voting system should be able to create a voting procedure - create lists of candidates, restrict voting participants (allow citizens in a given jurisdiction to vote) and anonymously cast their vote or change their choice during the voting period.

978-1-6654-0476-1/21/$31.00 ©2021 IEEE

Every user of a remote voting system should be able to view voting results and transaction history in real time to ensure that voting is transparent.

The guarantee of the inadmissibility of deliberate changes in the voting results implies that intruders should not be able to change someone's vote, thereby influencing the course of voting and its results.

The guarantee of fault tolerance means that if a device with a voting database fails, the system must continue its work.

Blockchain technology is structured as a continuous chain of blocks. The block chain is built on the principle of decentralized information flow management and data storage [1]. Hence, Blockchain is a ledger of facts. Network users are anonymous individuals called nodes. All communications within the network use cryptography to reliably identify the sender and recipient. When a node wants to add a fact to the ledger, a consensus is formed on the network to determine where the fact should appear in the ledger. This consensus is called a block. The essence of the technology is that all data is stored on devices of Blockchain network users, in the form of blocks with information or copies of these blocks. The more users in the Blockchain network, the more reliable and high-quality the work of the system is [1]. Thus, Blockchain is a distributed ledger that is completely open to everyone. This registry has a unique property of immutability: if information was recorded in the Blockchain, then it is very difficult to replace or delete it, since all other records located in the block chain must also be changed, since each next block refers to the previous one [1]. Let's demonstrate this fact.

By structure, each block contains a set of transactions in the form of some data, hash of the block and hash of the previous block. The data stored inside a block depends on the purpose of the Blockchain. A hash in a block can be compared to a fingerprint. It identifies the block and all of its contents, it is always unique. When a block is created, then the hash is calculated. Changing anything inside the block will cause the hash to change. In other words, hashes are very useful when you need to detect changes in blocks. If the hash of a block changes, the block is no longer the same block. The third element inside each block is the hash of the previous block. Since each block contains the hash of the previous block, it effectively links the blocks into a chain and makes the Blockchain technology secure (see Figure 1).

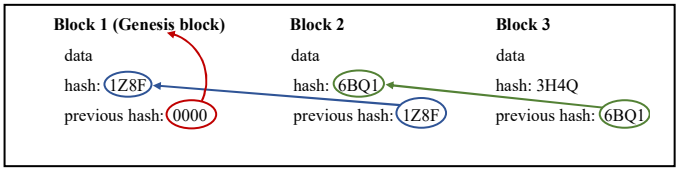

Fig. 1. Chain of three blocks.

Each block has its own hash and knows the hash of the previous block. Therefore Block 3 points to Block 2 and Block 2 points to Block 1 (see Figure 1). The first block (Genesis block) is special, it cannot point to the previous block, because it is the first one. It is called a generating block.

If we assume that someone changes (falsifies) Block 2 (see Figure 2), then this will lead to a change in the hash of this block. In turn, this will invalidate Block 3 and the following blocks as they no longer hold a valid hash of the previous block. Thus, changing one block will invalidate all blocks following it. But the use of hashes is not enough to prevent tampering.

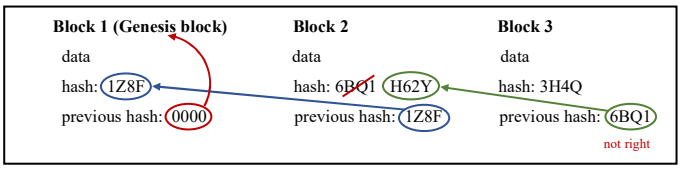

Fig. 2. Changing the hash of a block.

Computers nowadays are very fast and can significantly change the block and recalculate all the hashes of other blocks to make the Blockchain valid (valid) again. Therefore, to avoid this, Blockchain uses a mechanism called "proof of work" [1]. This mechanism slows down the creation of new blocks and makes it much more difficult to falsify (change) blocks, because if the first block changes, you need to recalculate the "proof of work" for all subsequent blocks. Thus, blockchain security is based on the sharing of hashing and proof of work. But there is another way that Blockchain protects itself, and that is by decentralization. Instead of using a central entity to manage the chain, Blockchain uses a peer-to-peer network (P2P network) that is available to everyone to connect. When connected to this network, the user receives a complete copy of the Blockchain to ensure that the chain is valid.

If someone creates a new block, then this new block is sent to all nodes connected to the network. Each node checks a new block to make sure the block is valid (hash check). If everything is in order, each node adds a new block to its copy of the Blockchain. All nodes in the network reach consensus. They agree on which blocks are valid and which are not. Fake blocks will be rejected by the rest of the nodes of the Blockchain network. Thus, in order to successfully falsify a chain, it is necessary for all changed blocks and those following them in the chain to repeat the "proof of work" and take control of more than 50% of the peer-to-peer network in order to establish a consensus. Only then will the falsified block become credible to everyone else. It's almost impossible.

Summarizing the above, it can be noted that the Blockchain technology, due to its decentralization, database replication between network participants, data immutability and the preservation of all transactions in the form of a block chain, allows using these positive qualities in order to eliminate the shortcomings of electronic voting systems.

Blockchain technology is constantly evolving. One of the latest developments has been the creation of smart contracts. The idea of integrating Blockchain with the real world using pre-programmed conditions and transferring them to all nodes is called a smart contract [1]. Thanks to the smart contract, there is no need for a notary or any other authorized person recognized by both parties.

To date, in many developed countries of the world, the electronic voting system based on Blockchain technology has

successfully passed the test and even in some states has been adopted not only at the municipal or regional level, but also at the federal level. For example, in Estonia, a Blockchain-based voting system for company shareholders was successfully tested, and the idea of creating a blockchain-based voting platform at the state level was put forward [2]. The United States of America in West Virginia has launched a Blockchain voting pilot project in 24 counties. It is intended for absentee voting and differs from its counterparts in efficiency and preservation of anonymity [3].

Among private projects, the Voatz pilot project should be noted. This project is a mobile electoral platform for electronic voting that allows you to vote from a mobile device using the security built in the latest versions of smartphone technology and the immutability of the Blockchain. To date, Voatz has conducted more than 30 successful live elections, including voting at congresses of state parties, at city meetings, and at student government elections [4]. The Follow My Vote project also gained popularity. This project is at the demo stage, but has already received a lot of publicity and fame. The developers strive to create a platform for voting, which will allow to achieve transparency of elections without compromising the privacy of voters, and to obtain an accurate voting result [5]. Among Russian developers, Kaspersky Lab distinguished itself by creating the Polys electronic voting platform, protected by Blockchain and encryption [6]. Pay attention to the project “Active Citizen” - a platform for holding open referendums in electronic form, created at the initiative of the Moscow City Government in 2014 [7]. The Moscow voting service switched to Blockchain in November 2017. The counting and saving of votes are carried out by creating smart contracts. The voting results are implemented in different forms: from the adoption of laws of the city of Moscow (for example, on the ban on the sale of alcoholic energy drinks) and resolutions of the Moscow Government (for example, on increasing the eco-class of buses in Moscow) to departmental decisions (for example, approval of park improvement projects).

Despite numerous developments, to date, no country has yet used Blockchain technology in elections.

II. The Proposed Model of Construction of a Remote Electronic Voting System Based on Blockchain Technology

The remote electronic voting system uses mobile communication. To participate in voting through a mobile application, you must install it on your mobile device.

The proposed model of the remote electronic voting process based on Blockchain technology contains the following stages:

A. ID confirmation

To conduct mobile voting, a citizen must first confirm his citizenship in this jurisdiction. To do this, he must appear at the identity verification point, present an identity document to the Operator (an independent third party authorized to verify the identity and voting rights of the user of the mobile application). As a result, only those Voters who have the right to vote will have access to voting. This procedure is required for Voters to access electronic voting.

To confirm the identity of the Voter, the CEC will set a specific time before the start of the elections (for example, during the election campaign period). This procedure will completely fall on the election organizers (Operators), which is why the system cannot be called fully automated. On the other hand, the Voter's appearance at the checkpoint corresponds to the transparency of the identity card.

B. Registration

The user will have to use the Blockchain technology, so he needs to have an address space in it. It can be obtained by identifying your mobile device with the Operator using an optical QR code reader (the QR code is in the mobile application). Thus, the Operator registers the Voter in the Blockchain network. The QR code of the mobile device is recorded on the Blockchain as a wallet address, and the system automatically generates a voting token (ballot) that is associated with that user's wallet.

Voting procedure

Voting occurs when a Voter sends a token to the chosen candidate's wallet, similar to sending a regular crypto token, where the cast vote is recorded as a transaction on the Blockchain. In the process of sending a crypto-token from your wallet to another wallet, anonymity is maintained. Likewise, the token sent by the Voter is not traceable to the Voter's identity, since cryptography is used and the registration process takes place using the identifier (QR code) of the Voter's mobile device.

The token will be limited in time, which is set by the Election Administrator, and then it will burn itself using a smart contract or become invalid. Setting the voting period automatically affects the activity of the “Cast your vote” and “Change your vote” buttons in the user's mobile application. If the user logged into the mobile application before the start of the voting period, then the “Cast your vote” button is inactive. During the voting period, the “Cast your vote” and “Change your vote” buttons become active. At the end of the voting period, the “Change your vote” button becomes inactive. If the user of the mobile application did not have time to vote during the voting period, then the “Cast your vote” button becomes inactive.

This approach to issuing a ballot allows you to participate in elections on the date of their holding, and receive a token before they start. The given vote also binds to a specific address space in the Blockchain network, which is indicated when issuing a token.

C. Viewing voting results and transactions

The received votes are securely stored in the Blockchain, and the Voter can always check the correctness of addressing the vote to a specific candidate in real time by clicking on the link “My transaction” in the mobile application. After this check, the indecisive Voter can anonymously change his vote at any time before the close of the voting period by clicking on the desired candidate and confirming his choice, after which the token will be sent to the appropriate candidate wallet.

After a Voter has voted, he can view the interim online voting results, and check the public transaction register to

ensure that his vote was counted in the vote count. To do this, he needs to follow the link "All transactions" in the mobile application. The voter can find out the final voting results in the mobile application online after the deadline for the voting.

The user interface of the mobile application automates and hides the process of sending a token to a specific address. Instead, voters see a simple online interface for selecting a candidate (a list of candidates with a checkbox opposite each for placing a marker of their choice) and a "Cast Your Vote" button.

The remote electronic voting system is designed in such a way that all data that enters it is sent directly to the Blockchain network thanks to a smart contract.

A smart contract is a program code [1], the structure of which allows organizing data storage in the form of a list of structures. One such structure is the voting structure. All basic information is recorded in it: the list of Voters admitted to voting; date, time of the beginning and end of voting; list of all votes; list of voters; list of the number of votes for the candidate; names of candidates.

The development of a smart contract algorithm for the proposed model of remote electronic voting is shown in Figure 3.

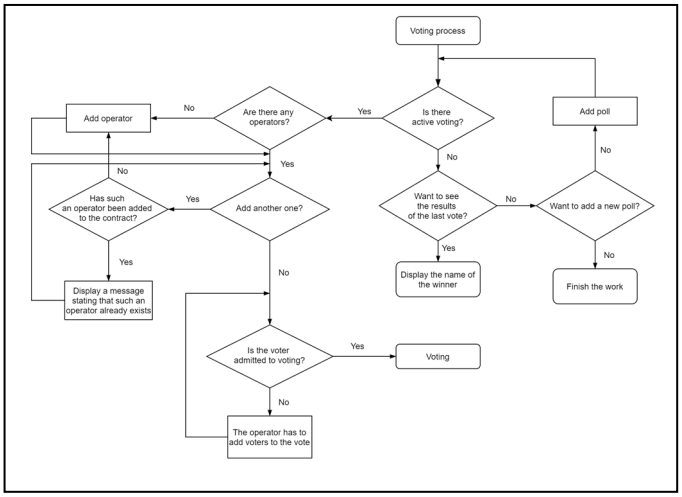

Fig. 3. Smart contract algorithm for remote voting.

Interaction of a smart contract with users (Administrator, Operator, Voter) occurs through transactions in the Blockchain network. The user sends tokens to the address of the contract, and the contract responds by sending other tokens in accordance with the code of his program (see Figure 4).

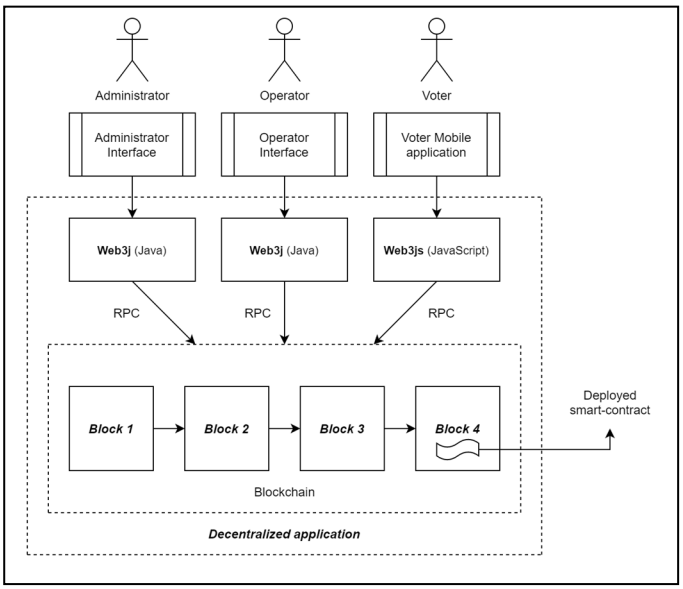

Fig. 4. Diagram of the interaction of a smart contract with users.

III. Results of the Proposed Model

The proposed model for building a remote electronic voting system based on Blockchain technology has great potential:

1. Increased transparency of the voting process. There will be no need to trust the central electoral authorities, who count the votes and often have their own interests. The system makes it possible to control the voting process in real time, therefore, increases user confidence in it.

2. Guarantee of anonymity for the voter. No one, except the voter, will know that a particular wallet belongs to him. As a result, no one will be able to find out how each voter voted, unless the voter himself announces that this wallet belongs to him.

3. Improving the reliability and security of the system. The system will allow reliable storage of voting results in the Blockchain network, increasing the cryptographic strength of the data. The security of the system lies in the fact that it is impossible to hack one block in the system without affecting others, since the continuity of the chain will be disrupted. Any falsification of data will require access to all blocks with information in the devices of users of the Blockchain network. Hence, hacker attacks and manipulations such as in the case of electronic voting can be avoided.

4. System fault tolerance guarantee. Blockchain technology is built on the principle of decentralization, forming a network of user devices, each of which stores a copy of the voting data. If one or more devices with voting data fails, the system will continue to work, since the data will be replicated to the devices of all network participants in which the decentralized application is running.

5. Increased civic engagement. Early receipt of the ballot will allow you to participate in voting remotely. The system makes it possible to participate in voting regardless of the location of the voter, which became a significant guarantee of the observance of the active electoral right of those voters who

cannot appear at the polling station on election day and vote with an absentee certificate. As a result, voter turnout will increase.

6. Increased efficiency. The voting process is associated with significant costs, organizational difficulties and time losses both for voting and data processing. The proposed method of remote voting will not take as much time and money for organizing elections (printing ballots, salaries for members of election commissions, renting premises, etc.) as at present. The opportunity for a voter to cast his vote without leaving home will save time on the trip to the polling station.

7. Increased processing speed. The decentralization of the Blockchain network will allow real-time viewing of voting results throughout the country as a whole, although each region/city/district can operate its own node of the system to distribute the load.

However, the proposed remote voting system is not fully automated, since today there are no services that could guarantee identity verification on the Internet.

There is also no way to verify that the person who submitted the citizenship documents is the same person who is actively behind the device during the voting, so the citizens themselves will be responsible for actions using the application. The project prohibits the transfer of an individual mobile device with an installed mobile application for use by another person.

IV. Prospects for use

The sales market for the developed system of remote electronic voting will have prospects not only in the electoral system, but also in various organizations that need remote voting, which allows ensuring the greatest security and, at the same time, the transparency of the system and confidentiality in relation to users, in comparison with services based on traditional databases.

Among the main sales segments of the remote voting system based on Blockchain technology, it is worth highlighting the following:

- government organizations conducting voting for citizens;
- organizations that conduct anonymous voting to make important decisions;
- other categories.

The main consumers of the product from the first segment can be state organizations representing the regional/city/district authorities, which conduct votes concerning the life of the region/city/district.

The second segment represents organizations that elect candidates for high-ranking positions by means of remote voting (for example, at general meetings of shareholders, meetings of LLC participants, meetings of the board of directors (supervisory board), management board, committees) or making decisions within the company through anonymous voting, in which all employees are involved.

The third segment consists of legal entities or individuals conducting remote surveys on specific topics at forums, conferences or other events held remotely.

V. Conclusion

In order for the proposed model of a remote electronic voting system based on Blockchain technology to be fully automated, it is necessary to implement identity verification on the Internet. Then there will be no doubt that the person who submitted the citizenship documents is the same person who uses the device during voting.

The most important priorities for the further development of the remote electronic voting system and its introduction into the legal system are the modernization of the electoral process, technical equipment of the population and the state, as well as education of the population in the field of modern technologies.

References

[1] Zaninotto F. (April 28, 2016). "The Blockchain Explained to Web Developers, Part 1: The Theory". Available at: https://marmelab.com/blog/2016/04/28/blockchain-for-web-developers-the-theory.html (Accessed April 09, 2019).

[2] Solodkiy S. (August 13, 2017). "Overview of the application of blockchain technology in public administration". Available at: https://medium.com/ @ slavasolodkiy / overview-applications-of-blockchain-technology-in-government-ac53602cec7f (Accessed April 09, 2019). (in Russian).

[3] Galaburdina A. (March 29, 2018). "USA Introduces Blockchain For Election Voting". Available at: https://jourtify.com/ssha-vnedrjaet-blokchejn-dlja-golosovanija-na-vyborah/ (Accessed April 09, 2019). (in Russian).

[4] Voting Redefined. Available at: https://voatz.com (Accessed April 09, 2019).

[5] Why Online Voting. Available at: https://followmyvote.com (Accessed April 09, 2019).

[6] Shmyrova V. (November 27, 2017). "«Kaspersky» has created a blockchain-based voting platform". Available at: http://www.cnews.ru/news/top/2017-11-27_kasperskij_vynes_na_narodnyj_sud_izbiratelnuyu (Accessed April 09, 2019). (in Russian).

[7] «Active Citizen» on the Blockchain. (November, 2017). Available at: https://ag.mos.ru/blockchain (Accessed April 09, 2019). (in Russian).