Blockchain in the Field of Voting

Olga A. Safaryan[a], Kirill S. Lemesko[b] and Elena V. Pinevich[c]
Don State Technical University, Rostov-on-Don, Russia

Keywords: Blockchain, Innovative Technologies, Electronic Voting, Distributed Ledger.

Abstract: Using a distributed ledger allows you to create a simple and at the same time reliable system for storing and processing any digital data. So, on the basis of a distributed ledger, the Blockchain technology was developed, which is a sequential combination of blocks (a specific set of data) into a chain. This chain is protected by methods of hashing and cryptography, which makes it very difficult for an unauthorized user to access the data. Blockchain found active use of in the financial sector, where most modern cryptocurrencies are built on its basis. Over time, it became clear that Blockchain technology can be used in many areas of activity, for example, in the field of electronic voting. Research on the development and implementation of a Blockchain-based electronic voting system is underway in many developed countries and universities. In this article, we consider and analyze the prospects for the transition from the traditional voting system to voting based on Blockchain technology, as well as the possible risks of using the technology. Also, within the framework of the article, an example of software implemented on the principles of Blockchain technology is presented, illustrating the main functions of working with data.

1 INTRODUCTION

The effective life of any human society is inextricably linked with the voting process. With the help of this process, important economic, social, industrial and political issues are resolved, on which the future well-being of countries and states depends. That is why the voting process must be convenient, efficient, and most importantly, safe.

For a long time, public issues were resolved by a narrow circle of people by raising a hand or throwing a set object into an urn (Khmurovich, 2018). With the development of society and the increase in the number of citizens living in the states, the voting methods have also changed. They became more open and accessible, polling stations, ballot boxes and ballots appeared (Safaryan, 2020). These changes made it possible to register and take into account the opinion of millions of people throughout the state. However, such a system has significant drawbacks: the possibility of forging ballots, forgery of voting results; social pressure on voters; high cost of conducting electoral activities (presidential elections in the Russian Federation in 2018 - about $ 250 million).

Today, it is relevant to conduct digital electronic voting (Russia, USA, India, Canada, Estonia) jointly or instead of traditional voting using paper ballots. The transition to the electronic form made it possible to minimize the costs of organizing and conducting voting, however, the issue of the safety of this process remains open. Hacking or falsification of votes is the most frequent and main problem faced by participants in the electronic voting process in today's elections (Golubitchenko, 2019). This is due to such factors as: low security of the hardware of the electronic system, errors in the compilation of software, errors and vulnerabilities of the server component of the system. Due to these vulnerabilities, an attacker can gain unauthorized access to stored confidential information, modify or download it. That is why the issue of security of electronic voting systems is relevant at the moment (Izotov, 2018).

Creation of technologies and tools based on a distributed ledger can improve the level of security, quality and performance of a variety of digital systems, as well as solve the problems inherent in

[a] https://orcid.org/0000-0002-7508-913X
[b] https://orcid.org/0000-0001-9114-9721
[c] https://orcid.org/0000-0001-6008-7222

Safaryan, O., Lemesko, K. and Pinevich, E.
Blockchain in the Field of Voting.
DOI: 10.5220/0010617200003170
In *Proceedings of the International Scientific and Practical Conference on Computer and Information Security (INFSEC 2021)*, pages 48-53
ISBN: 978-989-758-531-9; ISSN: 2184-9862

these systems (Melanie, 2017). So, on the basis of Blockchain technology, it is possible to build an electronic voting system, with a minimum potential probability of hacking this system. Therefore, the use of secure distributed registers in electronic voting systems on the Internet is relevant and legitimate. Such decisions and agreements tend to increase the number of voters, simplify the voting process and reduce costs by eliminating paperwork and requiring fewer human resources.

The security challenges faced by electronic voting systems today can be overcome by applying the replication, cryptography and verification mechanisms that Blockchain technology uses in their development (Chernikova, 2017). This technology will provide an ubiquitous, scalable solution to current and legacy voting methods, providing safe and secure digital voting, which will have a positive impact on the security and transparency of such systems, and therefore on user confidence in them.

2 RESEARCH METHODOLOGY

This article presents the results of work on an analytical study of the possibility of using distributed ledger technology - Blockchain, in electronic voting systems. Also, the results of work on the empirical development of a program for introducing Blockchain into an electronic voting system are presented in the form of software implemented on the principles of Blockchain technology, which illustrates the main functions of working with data.

2.1 Main Part

The center of the e-voting system proposed for implementation is the distributed register technology. A distributed registry is a database stored on multiple devices, which in turn have a complete copy of all information contained in the database (Krivoshapkin, 2018). The work of distributed ledger technology is to integrate all these devices into one network.

The first practical application of distributed ledger networks was Blockchain, which is a network consisting of a chain of blocks organized in a linear order. Each of the blocks contains information about the changes taking place, and also contains a unique identifier or hash code of the previous block, including the very first block written to the network (Kuteinikov, 2019). As soon as the block size reaches its maximum size, it is joined to the previous block in strict chronological order. On the basis of the Blockchain, the world's first cryptocurrency Bitcoin was built, which revolutionized the world financial market.

To ensure the reliability of the information entered into the distributed network, the principle of consensus is used (Kuzmin, 2017). The essence of the method is that all information potentially entered into the registry is checked by every device on the network. Information is entered into the register only when a consensus (agreement) is reached between all network users. This allows you to protect the network from entering inaccurate information, and also prevents attempts to change already recorded information.

Achieving consensus in distributed networks can be implemented by the "proof of work" method, the "proof of stake" method, or the PoW + PoS method, which is a mixture of the first two methods. These are the most applicable methods at the moment, however, work is constantly underway to improve these methods or create new ones.

The proof-by-work method is characterized by the solution of a complex cryptographic problem by each device. In Blockchain, the essence of the problem is to find the case of addition to the block hash code, so that a condition of a special kind is satisfied, for example, so that the first twenty bits of the hash code are equal to zero. If the calculation is successful, the participant receives a reward in the form of cryptocurrency, this process is called mining. When proving shares, each network node gets the right to assign the block created by the network to itself, having assured it with its electronic signature. This right is randomly transferred from one node to another with a probability proportional to what share of the cryptocurrency of the total volume of the cryptocurrency issued in the blockchain network it possesses.

The security of the distributed ledger network is organized by the method of secure information hiding - cryptography. In the Blockchain, in order to disclose information inside a block, a network participant needs to know how the information was encrypted, that is, to know a unique cryptographic key assigned to each block.

At the moment, cryptocurrencies are not the only application of distributed ledger technology. A smart contract is an agreement that enforces the rights and obligations of the contracting parties by performing digital transactions in a distributed ledger in a strictly defined sequence and upon the occurrence of certain circumstances (Tenetilova, 2018). Such a "smart" contract allows you to exclude a third party in the process of concluding and executing an agreement, which allows you to reduce the cost of the transaction and increase its reliability. It is the smart contract that is the main tool for creating a secure electronic voting system on the Blockchain.

Distributed ledger technology, although quite progressive, still remains a technology at an early stage of development, which has its own problems and limitations. The advantages of distributed ledger networks are: openness and transparency; decentralized organization of the system; immutability of the information entered; equal rights of all users of the system; high resilience due to the distribution of a large number of copies of data; uninterrupted operation of networks; simplified nature of transactions (Safaryan, 2020).

The main disadvantages of a distributed ledger are:

- low speed of networks, depending on the capacity of hardware equipment. For example, the processing speed of one transaction in Bitcoin is 10 minutes, while the centralized operator of VISA payment cards routinely processes 2000 transactions per second;
- there is a possibility of a cryptographic algorithm vulnerability, the so-called "attack 51" when an attacker, having at his disposal enormous computing power, takes control of transaction confirmation and block generation;
- distributed ledger technology is a threat to the existing financial system, as a result of which many states are in no hurry to introduce technology inside the country, which significantly hinders the development of technology.

Despite a number of limitations, e-voting systems are being actively developed all over the world. For example, in 2020, a nationwide vote was held in the Russian Federation on amendments to the Constitution of the Russian Federation. Most regions used well-established voting methods, however, in the Moscow and Nizhny Novgorod regions of the Russian Federation, it was possible to vote through an electronic voting system based on the Blockchain. Also, in 2019, a vote was held in the State Duma of the Russian Federation based on Blockchain. Despite the fact that such a system cannot be called completely decentralized (voting took place through state servers), experts note that these are confident steps of Blockchain technology in the field of selective activity (Korneev, 2020).

In world practice, cases of using Blockchain voting are also not uncommon, however, most of such systems are developed mainly by startups of enthusiasts (followmyvote.com, agora.vote) and only a small part - by state companies. And yet, experiments on public voting using Blockchain are carried out annually in many developed countries.

It took Blockchain a decade to finalize its efficiency and reliability in the financial sector (cryptocurrencies, smart contracts). The technological community is daily working on modifying ready-made solutions and creating new ones, thanks to which, today we can confidently say that Blockain technology will soon be generally recognized as a new field of activity - the field of electronic voting.

2.2 Research Results

The distribution, safety and immutability of data in the form of a block chain allow the use of Blockchain technology in an electronic voting system in order to eliminate shortcomings and improve the security of electronic voting.

The Blockchain voting system has the following qualities and capabilities:

- the ability to create polls and lists of objects to vote for them;
- registration of participants for each created poll;
- decentralization of data;
- availability;
- transparency;
- inability to make unauthorized changes affecting the voting results.

In this system, each user will be given the opportunity to create polls or polls, after which the user will be assigned the status of an administrator, which will allow him to change the lists of participants. In addition, in order to ensure the transparency of voting, each user is given access to the results of a vote or poll, as well as access to viewing the blockchain.

The operation of this system should be independent of the operation of the central server, and should continue to function in the event of a server failure. The distributed registry allows you to ensure the smooth operation of the system due to the fact that a complete copy of the data is stored on each device connected to the system, shifting part of the server's work to the devices.

In order to exclude the possibility of influencing the course of voting and its further results, methods of cryptography and hashing are used, which protect the electronic voting system from unauthorized access by an attacker.

To implement the software product, the Python programming language is used, since it has all the tools you need to create software.

The software implementation is presented in the following steps:

- we create the first genesis block, from which the entire subsequent chain of blocks will begin.
- create a block.py file and include libraries: json, os, hashlib;

```
{
   "vote": "Lemeshko Kirill
Sergeevich",
   "passport": 1111 111111,
   "candidate": "1",
   "hash" = " "
}
```

Listing 1: The first block.

- we write the path in the directory: this line saves new blocks:

```
blockchain_dir = os.curdir +
'/blockchain/'
```

Listing 1: Directory path.

- block hashing: the function performs block hashing when using the md5 method:

```
def get_hash(filename):
file = open(blockchain_dir +
filename, 'rb'). read() #sending the
hash of the pre-existing block
return hashlib.md5(file).hexdigest()
```

Listing 2: Hashing process.

- moving files: the received files from the directory are forwarded in blocks to the folder:

```
def get_files():
files = os.listdir(blockchain_dir)
return sorted([int(i) for i in
files])
```

Listing: 3: Moving files.

- data integrity check: this function calculates the hash value of the created block and the hash value of the previous block, and then compares the obtained values. If the hash values match, then the previous block has not been changed, and the check function returns the hash value of the newly created block.
- storage of new blocks: this function is responsible for the creation and storage of new blocks and their values based on the entered data.

This code was created for the purpose of decentralized voting (Kobylinsky, 2017). Using separate blocks, the program encrypts confidential information about the voter. The application itself has a simple and user-friendly interface.

```
def check_intergrity():
#1.read the hash of an existing
block
#2.calculate the hash of an existing
block
#3.compare the received data
files = get_files()
result = []
for file in files[1:]: #[2,3,4,5]
f = open(blockchain_dir + str(file))
# '2'
h = json.load(f)['hash']
prev_file = str (file - 1)
actual_hash = get_hash(prev_file)
if h == actual_hash:
res = 'Ok'
else:
res = 'Corrupted'
#print('Block {} is: {}'
.format(prev_file, res))
results.append({'Block' : prev_file,
'results' : res})
return results
```

Listing 4: Integrity check.

```
def write_block(vote, passport,
candidate, prev_hash= ' '):
files = get_files()
prev_file = files[-1]
filename = str(prev_file + 1)
prev_hash = get_hash(str(prev_file))
data = {'vote' : vote,
'passport' : passport,
'candidate' : candidate,
'hash' : prev_hash}
with open(blockchain_dir + filename,
'w') as file:
json.dump(data, file, indent = 4,
ensure_ascii = False)
```

Listing 5: Storing new blocks.

2.3 The Discussion of the Results

In this article, we pointed out how the Blockchain distributed ledger technology can be used in electronic voting systems, how much progress has been made in this area, and the possible benefits of introducing technology into the field of public voting.

The solutions proposed by the scientific community fail to ensure the security and privacy of traditional choices, or have serious usability and scalability problems. Therefore, Blockchain is increasingly attracting the attention of the scientific and political community.

Blockchain shows good results in electronic voting systems, however, experts note a number of problems that need to be solved for the subsequent successful use of the technology. First, most of the electronic voting systems allowed for use in real selective activities are under the full control of the state, for example, as noted earlier, the use of state servers, which is why such systems cease to be decentralized. Secondly, there is a controversial issue regarding the identification of voting users; it is not beneficial for the state to vote anonymously. Thirdly, it is necessary to resolve the issues of choosing software for use in the electronic voting system. This is due to the fact that blockchain technology has many types of implementations, with their own advantages and disadvantages (Hy-perledger, Iota, Ethereum, and others). For the effective functioning of the system, it is necessary to find the most suitable blockchain implementation model and optimize it for the given goals. Additionally, it is necessary to think over a solution to the main problem of Blockchain technology - scalability. Since all the recorded information is recorded on each device operating in the system, it is necessary that these devices have a huge amount of storage memory, calculated in tens and hundreds of gigabytes.

It can be concluded that today, electronic voting is still a controversial topic in both political and scientific public circles. Despite the great potential of distributed ledger technology and several world examples of the application of this technology in voting, it can be noted that for the confident widespread implementation of technological solutions based on Blockchain, further research, testing and refinement of such systems is required.

3 CONCLUSIONS

Blockchain distributed ledger technology offers democratic countries a new opportunity to move from traditional elections using ballots and polling stations to the most economical, efficient, and most importantly, difficult to hack electronic voting system.

In the course of the implementation of the work, a software product of an electronic voting system based on Blockchain technology was developed. This software allows you to conduct secure polls of users of the system, while saving the results obtained in the form of a chain of blocks. User registration in the system is organized by creating an account in the network, in which a smart contract is deployed with the addition of a user to the white list of a particular survey created. The use of the developed software will allow organizing an effective and reliable electronic voting system in any area of public activity.

REFERENCES

Chernikova, E. (2017). *Analysis of information security in blockchain technology.* Association of Scientific Researchers "Siberian Academic Book", pages 260-264.

Golubitchenko, M. (2019). *The relevance of the blockchain system application in the Russian federation*. Publishing house: Science and Education, pages 122-124.

Izotov, M., Meskhi, B., Knyazeva, Y. and Simonyan, T. (2018). Problems and perspectives of creation and management of the process of preparation of innovational technological projects Founders: Asociacion de Profesionales y Tecnicos del CONICIT: 39 (1), 4p

Khmurovich, I. and Skudnyakov, Y. (2018). *Information protection using blockchain technology.* Publishing house: Belarusian State University of Informatics and Radio Electronics, pages 95-96.

Kobylinsky, D. (2017). *How to create an electronic voting system on the blockchain?* URL: https://habr.com/ru/post/340342/, date of request: 01.03.2021.

Korneev, A. (2020). *Voting on amendments to the Constitution of the Russian Federation. Why was it necessary to implement the blockchain.* URL: https://www.rbc.ru/crypto/news/5efc2b519a79477d32ad3fb1, date of request: 26.02.2021.

Krivoshapkin, K. (2018). Prospects for the implementation of Internet voting on blockchain technology in elections and referendums in Russia. Publishing house: Problems of science, 6-14.

Kuteinikov, D. (2019). Features of the use of technologies of distributed ledgers and block-check chains (blockchain) in popular votes. *Actual problems of Russian law*, 9(106): 41-52.

Kuzmin, M. (2017). Development of a software system for voting based on blockchain technology. *Science of the present and the future*, 1:73-75.

Melanie, S. (2017). *Blockchain: Blueprint for a New Economy.* Publishing house: Olympus – Business.

Safaryan, O., Aldyrev, M. and Cherkesova, L. (2020). Analysis of the application of blockchain technology in public administration. In the book: *Actual problems of science and technology. Materials of the national scientific-practical conference*, pages 922-925.

Safaryan, O., Lemeshko, K. and Aldyrev, M. (2020). Analysis of the practical implementation of distributed ledger technology. In: *Progressive Technologies and Processes. Collection of scientific articles of the 7th*

All-Russian Scientific and Technical Conference with international participation, pages 87-92.

Tenetilova, K. (2018). Research of blockchain technology for the implementation of secure electronic voting: *Scientific journal of young scientists*, 2(11): 48-50.