Blockchain voting - the evolution of web voting or a new methodology?

Abstract

For the blockchain methodology, the use of distributed block relations, it's important to know how they affect the liberalization of relations in the country. The question is reasonable, and to investigate it, in many countries there are already prerequisites, projects.

The essence of the blockchain methodology reflects the principle of mathematical calculation of the value of a cryptographic hash function. When successfully solving this problem, a new block is added to the cryptosystem, with a small reward in cryptocurrency for the solved mathematical problem. Each token (block) in the system has its own transaction history, a chain of transactions.

In our work, we systematically analyze the problems of blockchain transaction management in the elective system and offer our solutions.

Literary and analytical review

The liberalization of blockchain and the democratization of the electoral system is a consequence of modern digital transformations in society, digital democracy [1].

By "electronic voting", we mean the voting procedure using scanning ballots and providing automatic counting of voter's votes, their transfer by telecommunications or mobile communications.

The selective practice state is based on various technical means of electronic voting [2]. Internet voting - on the website, on a special interface service [3].

Internet voting is implemented using:

1) technically equipped booth at the polling station (Fig.1);
2) Internet kiosks (as in the "electronic government" system) in public places;
3) remote web voting (voting point is selected by the voter) [4].

Work by @enbit88, forum name encipher

Figure 1. Voting at the Polling Station

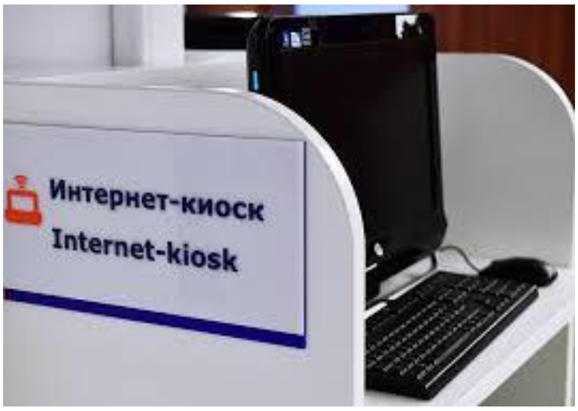


Figure 2. Internet Voting Kiosk

Figure 3. Remote Voting

The electoral blockchain system assumes that candidates (possible decisions made) are entered in "digital wallets" similar to cryptocurrency wallets [5]. The voter participates in the formation of the election outcome anonymously, i.e. participates in the formation of a "portion (token)" of state power, giving his vote to the blockchain system. All voters in the peer-to-peer network connect tokens using blockchain technology and the election result is formed.

Any registered voter shall exercise his/her right to vote "in this place, at this time, through this communication channel". The peer-to-peer model (P2P) of using blockchain voting practically (if there are no critical, force majeure failures) excludes falsification of the results [6] - [8].

But so far there are many uncertainties with transactions. This leads to conflicts with the law [9]. "The state should be a digital platform for both people [10] and cars".

For the first time, blockchain voting was tested in the Agora Voting project in the elections to the Spanish Cortes [11]. Now used in the USA, Switzerland, Great Britain, Japan, Sierra Leone and other countries. A number of countries (Ireland, Germany, France, etc.) tested the blockchain capabilities of their electoral systems. Then they suspended testing, including by decision of the Constitutional Court, as, for example, in Germany.

"From bad to worse?"

An article by a group of scientists from MIT [12] made a very critical analysis of the possibilities and need to use blockchain voting systems. We will make a critical analysis of the main conclusions, theses of this article.

1. "Blockchain technology does not solve the fundamental security problems that affect all electronic voting systems".

The blockchain methodology in voting systems will ensure the protection of the transfer of votes to the DB, access from the computer of each voter in the system. This is implemented programmatically, using the cryptographic code of a citizen.

Although blockchain, SMART contracts are legally rejected by many, but they allow voters to have parallel access to the updated digital "book of voits" [13], which is unchanged in the voting process. There may be a problem with the increase in transaction processing time [14].

2. "Electronic, online, and blockchain voting systems are more vulnerable to major disruptions than available paper-based alternatives".

As the experiment with online voting in the Moscow Duma shows, in three pilot constituencies, it turned out to be successful. Of the 11,228 people who registered to participate in the electronic elections, they appeared, that is, they voted using a smartphone, computer, tablet, almost 92%. 22% of voters came to the "classic, paper" polling stations.

In other European cities there is a comparable turnout [15]. There are also "technological advantages" - few "invalid bulletins" (technical failures), and the existing ones are quite fixable during further testing of the system. As for the transition to blockchain technology, it's systemically tested and largely verified.

International experts recognized that there is no such approach and results in Europe. Emmanuel Leroy, Secretary General of the international People's Sovereignty Movement, said: "Today I saw an example of excellent work and a truly transparent process. Unfortunately, this is not the case in France". But research in this direction in Europe is underway (for example, [16]).

3. "Adding new technologies to elective systems can create new potential for attacks".

Obviously, security problems greatly affect the block-democratization of voting. Anonymity is the main thing in any voting system. It's often impossible to track. But not in blockchain-oriented systems, the reliability of which for short-term (operational) transactions is extremely high due to the algorithms used and their reliability, estimates of traditimic complexity. And the voting period - very short - no more than 14-20 hours.

Proposed solutions

We offer our solutions to improve the blockchain voting system.

Firstly, we believe that blockchain voting is a methodology for organizing public voting (not only elected). Therefore, it should be systematically investigated.

Secondly, the blockchain also changes the performance criteria of the election system and voting system, allows you to self-tune on the profile of the voter. This will make it possible to cope with the task of preserving the secrecy of voting and confidentiality at a sufficient level. But there is a problem of mass development of blockchain technology. In Russia, this is confirmed by a survey by the National Agency for Financial Research, for example, only 4% are well aware of the system, 16% have heard about it. Therefore, we also conducted a similar survey of students. He gave, in particular, variances and deviations for the two small groups surveyed (24 and 25 person), respectively, equal to D1 = 0,005, D2 = 0,025 and S1 = 0,029, S2 = 0,086.

Thirdly, to increase voter turnout, reduce fraud (see their legal classification and "portraits" in [17]) or combat disenfranchisement and coercion, fuzzy and neuro-systems should be used. These systems are taught ("training with a teacher" method) using examples of such violations.

The "binding" of the ballot to the one voting in the blockchain system is implemented, in our opinion, as in tested systems, according to the scheme: "token (voice) - transaction (submission) - confirmation (comparison with the profile of the voter) - placement in the chain (voice accounting)".

Structural diagram is given in Fig.4.

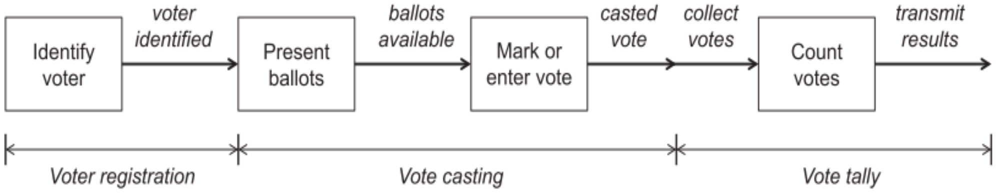


Figure 4. Remote Forms of Voting

A good solution is offered here - the use of risk management (audit, see, for example, [18]) to identify vulnerabilities. As proposed by the International Association of Trusted Blockchain Applications (INATBA) for the development of blockchains in the EU. A practical solution is based on consensus algorithms and DLT development practices.

In building the system, the DGO specification was used, which I prepared as part of the previous competition.
https://firebasestorage.googleapis.com/v0/b/ton-labs.appspot.com/o/documents%2Fapplication%2Fpdf%2Fk54gsp6kkhtmouln-GOV20.pdf?alt=media&token=728260b4-06ce-48fb-a72dae4e0

Also, to eliminate critical factors, I analyzed the work "Results of the technical audit of electronic voting on 09/08/2019 in Moscow"
https://drive.google.com/file/d/1CcUXwRFCoSQ1NxzQtdwpi1spUQxSrWLE/view

At all stages of interaction with a Free TON`s smart contract (a debot with a voting interface), the privacy of voting will be guaranteed by zero-knowledge protocols based on the complexity of discrete logarithms and homomorphic commitments. With this approach, the secrecy of the vote will not be violated even if it is possible to associate encrypted voter votes with specific people.

To prevent scalable and undetectable attacks, including system attacks, and device security breaches, you can use the duplication of the smart contract HASH data at each stage in a separate workchain or any other public decentralized blockchain. This ensures stability and subsequent testability. You can verify HASH through a smartphone, using the SURF browser.

To provide End-to-End Verifiable voting, you can use the work
https://link.springer.com/chapter/10.1007/978-3-662-46803-6_16
In which the process of building such a system is described in sufficient detail. Since ZK-snark is used, you can also check if your vote passed or not. But unlike other auditors, you know that your vote is your vote. Others can see confirmation only that the vote has been received from a verified voter. Also, the voter will not be able to receive a public HASH transaction and violate the "protection against Coercion" rule (If I have a receipt, I can prove how I voted, therefore confirm to the party attempting to buy my vote.)[20,21]

Voters should be able to enter their details and confirm their voting rights, but there should be no transparency of the votes cast until the end of the voting. ZK snark will allow you to operate only with a verifiable anonymized hash of your right to the ballot, which is quite enough for user verification.

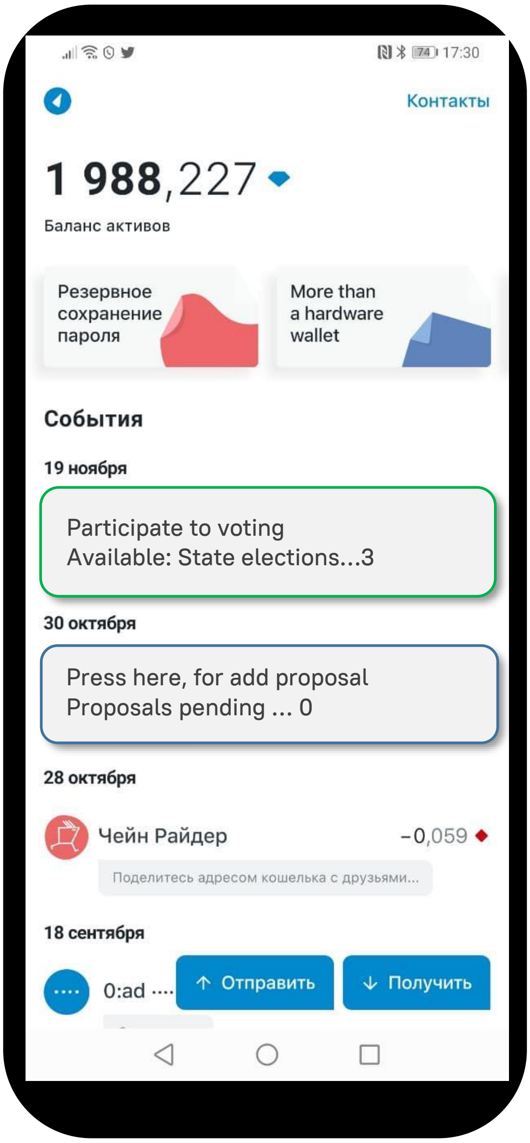
There should be no conflicts with the transparency of the system itself. Analogs of blockchain technology can be used to develop B2B trade products and optimize financial transactions in the blockchain (for example, Commonwealth Bank of Australia, Commonwealth Bank of Australia).

When registering and confirming your right to vote (it can be a one-time actual visit to a polling station or an entrance through a government service), you are given only a tool to activate any public key you create locally, and ZK-proof technology will allow you to do this anonymously. Subsequently, if you lose the private key from the authorized address, you can re-sign another address. In the event that this is an attempt to split the voice, then the smart contract will always find and cut off duplicates of such votes.

In any case, we need to avoid such vulnerabilities as SMS verification, registration through any site with many backdoors, centralized data processing servers, PoA mechanics, and so on.

The use of one SURF browser and a verified debot with an open source smart contract will increase trust in the network and increase the turnout rate and fair elections.

Interface of the home page



17:30

Контакты

1 988,227

Баланс активов

Резервное сохранение пароля

More than a hardware wallet

События

19 ноября

Participate to voting
Available: State elections...3

30 октября

Press here, for add proposal
Proposals pending ... 0

28 октября

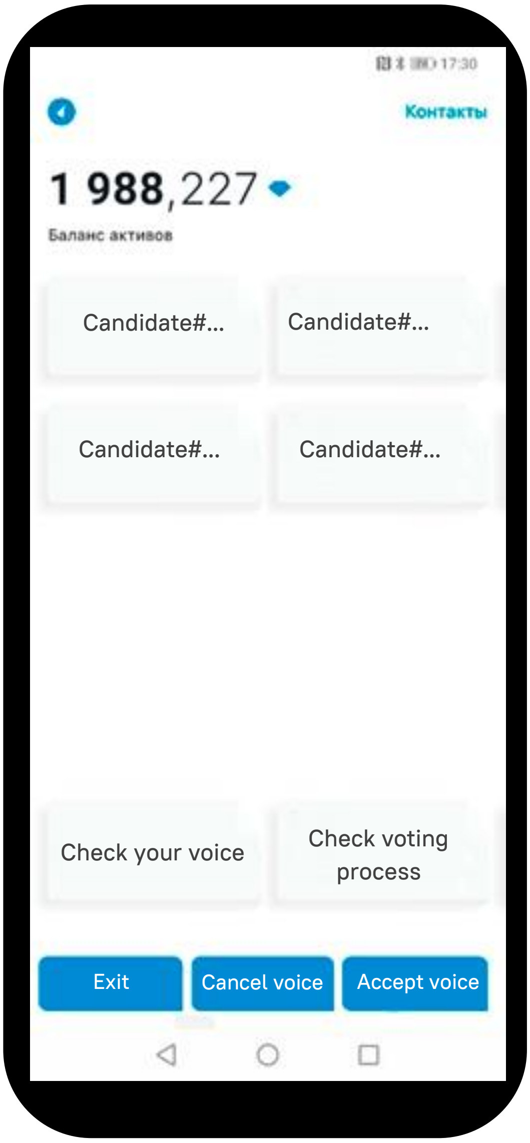
Чейн Райдер −0,059

Поделитесь адресом кошелька с друзьями...

18 сентября

0:ad ....

Interface for voiting



17:30

Контакты

1 988,227

Баланс активов

Candidate#...

Candidate#...

Candidate#...

Candidate#...

Check your voice

Check voting process

Voting system can be implemented in about 1 year including all tests.
Development of a sustainable decentralized blockchain - completed
Development of a browser for interacting with the blockchain - completed
Development of a smart contract for debot - 150000 ton crystal
Debot interface development - 100000 ton crystal
Development of a workchain and / or a bridge for backup - 100,000 ton crystal
Introduction of zk-snark - 90,000 ton crystal
Smart contract audit from 5,000 to 30,000 ton crystal
Gas for maintaining the operation of the system no more than 5000 tons of crystal
Further expenses include salaries for ordinary employees.

According to a recent announcement, about $ 20 mln was spent on the Russian presidential election.[22]

If we compare these numbers and amounts for the development and maintenance of the voting system on the Free TON Blockchain, then the choice is obvious.
Today the Free TON community has all the necessary skills and resources to build this system.

Conclusions

To liberalize and create a democratic voting system, opportunity analytics based on blockchain technologies are necessary. First of all, in terms of predictability, security and decentralization.

The analysis done in our work is the "zero turn of the evolutionary spiral", a possible part of the basis for the development of a self-developing system ("self-voting" system) based on blockchains.

Literature

1. Alekseev R.A., Abramov A.V. Problems and prospects of application of electronic voting and technology of electoral blockchain in Russia and abroad // Citizen. Elections. Power. 2020. No.1(15). –pp.12-20.
2. Davydov D.A. Internet voting as an electoral political technology // Bulletin of Perm University. 2010. No.1(9). -pp.59-63.
3. Titovskaya A.V. Electronic secret ballot in Russia and abroad: comparative legal analysis // Legal science. 2012. No.4. -pp.106-108.
4. Grachev M.N. Electronic voting "for" and "against " // Izvestia Tula State University. 2011. No.1. pp.360-366.
5. Alekseev R.A. Probation of blockchain technology in the elections to the Moscow City Duma in 2019: results and prospects for application for the federal election process // J. of Political Studies. 2019. vol.3. No.4. -pp.12-23.
6. Zvorykina E.V. Prospects for the use of blockchain technology in elections in Russia // Citizen. Elections. Power. 2018. No.4. -pp.179-183.
7. Evangelos Benos, Rodney Garratt, Pedro Gurrola-Perez. The Economics of Distributed Ledger Technology for Securities Settlement // LEDGER, 2019, vol. 4, pp.121−156. DOI 10.5195/LEDGER.2019.144.
8. Tapscott D., Tapscott A. Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world. –N.Y.: Penguin, 2016. –324p.
9. Yolokhova I.V., Akhmetova M.I., Krutova A.V., Tetenova A.V. Approaches to determining the legal status of cryptocurrencies in leading countries of the world // PNIPU Bulletin. Socio-economic sciences, 2019, No.1. -pp.201-209. DOI: 10.15593/2224-9354/2019.1.17
10. Mishustin about cryptocurrency and the digital economy. The main quotes. URL: https://www.rbc.ru/crypto/news/5e2038f29a7947423ddeab0f (case date: 24.01.2021).
11. Korchagin S.A. On current trends in the development of blockchain technology // Free thought. 2018. No.4. –pp.31-38
12. Sunoo Park, Michael Specter, Neha Narula, Ronald L. Rivest. Going from Bad to Worse: From Internet Voting to Blockchain Voting. November 6, 2020 (DRAFT), URL: https://people.csail.mit.edu/rivest/pubs/PSNR20.pdf
13. Genkin A., Mikheev A. Blockchain. How it works and what awaits us tomorrow/A. Genkin, A. Mikheev. -M.: Alpina Pablisher, 2018. -592p.
14. Babkin A.V., Burkaltseva D.D., Pshenichnikov V.V., Tyulin A.S. Cryptocurrency and blockchain technology in the digital economy: development genesis // Scientific and technical statements of St. Petersburg State Polytechnic University. Economic sciences. 2017, vol.10, No.5. -pp.9-22. URL: https://doi.org/10.18721/JE.10501.

15. Babkin S., Meleshenko A. Naklikali victory. The results of electronic voting in Moscow confirmed - the future is behind him. URL: https://rg.ru/2019/09/09/reg-cfo/v-moskve-podveli-itogi-eksperimenta-s-elektronnym-golosovaniem.html (case date: 25.01.2021).
16. Study on the benefits and drawbacks of remote voting solutions to support the preparation of a best practice guide for the use of digital tools to facilitate the exercise of EU citizens' political rights. URL: https://ec.europa.eu/info/sites/info/files/remote_voting_main_findings.pdf (case date: 25.01.2021).
17. Kaziev V.M., Kaziev K.V., Kazieva B.V. Fundamentals of legal informatics and informatization of legal systems: a textbook (2nd ed.). -M.: University textbook. INFRA-M. 2017. -336p. ISBN 978-5-16-104376-9 (online).
18. Andrew W.Appel, Philip B.Stark. Evidence-based elections: create a meaningful paper trail, then audit. GEO. L. TECH. REV. 2020. No. 523. -pp.523-541. URL: https://georgetownlawtechreview.org/wp-content/uploads/2020/07/4.2-p523-541-Appel-Stark.pdf
19. McCorry P., Shahandashti S. F., Hao F. A smart contract for boardroom voting with maximum voter privacy //International Conference on Financial Cryptography and Data Security. – Springer, Cham, 2017. – С. 357-375.
20. B Smyth, S. Frink and M. R. Clarkson, Election Verifiability: Cryptographic Definitions and an Analysis of Helios and JCJ, Cornell's digital repository, Feb. 2017
21. Jeremy Clark, Aleks Essex, and Carlisle Adams. On the Security of Ballot Receipts in E2E Voting Systems IAVoSS Workshop on Trustworthy Elections 2007.
22. https://tass.ru/politika/5259952 Article "14 billion rubles were spent on organizing presidential elections"

About author

My name is Alex R

Forum name
https://forum.freeton.org/u/encipher/summary

TG name
https://t.me/enbit88

My story (short biography):
https://medium.com/@encipher/the-cryptocurrency-that-i-build-myself-b04d0605088b

Wallet:
0:f6466adf8b0490dda4fd7d217cfe3d4267fd296fa7ed6af5640a5b31c7f2a898