Blockchain Based E-Voting System: Open Issues and Challenges

Zarif Khudoykulov
Department of Cryptology
Tashkent University of Information Technologies
Tashkent, Uzbekistan
zarif.xudoyqulov@mail.ru

Umida Tojiakbarova
Department of Cryptology
Tashkent University of Information Technologies
Tashkent, Uzbekistan
umidatojiakbarova@mail.ru

Suhrob Bozorov
Department of Cryptology
Tashkent University of Information Technologies
Tashkent, Uzbekistan
bek.muminovich.95@mail.ru

Dilshoda Qurbonalieva
Department of Cryptology
Tashkent University of Information Technologies
Tashkent, Uzbekistan
dilshodavaliyevna@gmail.com

2021 International Conference on Information Science and Communications Technologies (ICISCT) | 978-1-6654-3258-0/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICISCT52966.2021.9670245

***Abstract*— Blockchain technology has become very trendy and penetrated different domains, mostly due to the popularity of cryptocurrencies. Blockchain technology offers decentralized nodes for e-voting and is used to create e-voting systems, mainly because of their end-to-end verification benefits. This technology is an excellent replacement for traditional e-voting solutions with distributed performance, reliability and security. The following article provides an overview of e-voting systems based on blockchain technology. The main purpose of this analysis was to examine the current state of blockchain-based voting systems, as well as any associated difficulties in predicting future events.**

Keywords*— *electronic voting, security, blockchain-based electronic voting, privacy, blockchain, voting, trust.

I. INTRODUCTION

Electronic voting is a term that defines the type of voting that involve electronic voting tools (electronic democracy) and technical electronic means of counting votes. In electronic voting, voters will be able to vote by downloading the hula, election applications that use the Internet.

The procedure for electronic voting varies by country, which may include voting machines on polling stations, centralized accounting of paper bills and voting on the Internet. In many countries, centralized calculations are used. Sometimes, however, they also use electronic voting machines in places of voting. However, there is little use of voting through the Internet. In particular, electronic approaches have been tested in several states, which have caused problems with security and reliability. Table I summarizes the general conclusions drawn from the implementation of electronic voting in the cross-section of states [1].

TABLE I. STATE-OF-THE-ART ANALYSIS OF ELECTRONIC VOTING

State name	Year	Voters number	Notes
Germany	2019	37807746	In electronic voting, it was found that there was no transparency in the recording with the voice of the caller and that problems with recalculation could be brought out.
Australia	2019	16419543	Electronic voting was favorable for the blind and disabled and was not considered negative.
Brazil	2018	146750529	In electronic voting, there was a lack of cables for the device and a shortage of electric current.
Canada	2018	27373058	Several cities used in the Federal Election opposed its use.
France	2019	22655174	France has announced that it will not be allowed to vote on the Internet (previously invited foreign citizens) in the legislative elections of 2017 year due to cybersecurity.
India	2019	1450000	The proposal was expressed not to use the new voting system because of concerns about the confidence of the population.

Electronic voting requires a number software, hardware-software computing tools. Table II below provides examples of them.

TABLE II. COMPARISON BETWEEN THE COUNTRIES OF THE ELECTRONIC VOTING SYSTEM

State name	Electoral system	Software used	Hardware used
India	FPP	EPROM	EVM
Brazil		GEMS	GX-1 integrated processor
Australia	PR-STV	eVACS	PCs
Spain	PR-List	SIRE	SIRE system
Canada	FPP	CanVote on Linux	CanVote Internet
UK	FPP	AVC	DRE
Belgium	Open PR-List	Digivote, Jites, Stesud	DEVS

E-voting system has its own advantages and disadvantages [3]:

Advantages of E-voting systems:
- only those who are eligible can vote;
- voters shall not vote more than once;
- it is impossible to know who a particular voter voted for (i.e., the secrecy of the vote is ensured);
- no voter can vote for another;
- no one can secretly change the result of a vote given by another.

The independence and integrity of election commission members are usually guaranteed by the supervision of observers at the proposed polling stations. Otherwise, it is impossible to guarantee the reliability of the election.

Disadvantages of E-voting systems:
- members of the election commission may vote instead of absent voters;
- hidden cameras can be installed in voting booths;

978-1-6654-3258-0/21/$31.00 ©2021 IEEE

- members of the election commission may cancel some ballots (for example, put a second checkmark on the ballot paper) or put a checkmark in front of the "necessary" candidate if there is no mark on the ballot paper;
- voting results may be considered incorrect (incorrect errors);
- voting results may be intentionally distorted;
- the voter cannot verify that his or her vote is taken into account, and especially that it is taken into account correctly;
- the average voter does not know who voted and who did not.
- voting results are considered for a relatively long time (especially since the final voting results are usually known within a few days).

II. Security Requirements for Voting System

Suitable electronic voting systems should meet the following electronic voting requirements. Fig. 1 shows the main security requirements for electronic voting systems [2].

A. Anonymity

Throughout the polling process, the voting turnout must be secured from external interpretation. Any correlation between registered votes and voter identities inside the electoral structure shall be unknown.

B. Auditability and Accuracy

Accuracy, also called correctness, demands that the declared results correspond precisely to the election results. It means that nobody can change the voting of other citizens, that the final tally includes all legitimate votes, and that there is no definitive tally of invalid ballots.

C. Democracy/Singularity

A "democratic" system is defined if only eligible voters can vote, and only a single vote can be cast for each registered voter. Another function is that no one else should be able to duplicate the vote.

D. Vote Privacy

After the vote is cast, no one should be in a position to attach the identity of a voter with its vote. Computer secrecy is a fragile type of confidentiality, which means that the voting relationship remains hidden for an extended period as long as the current rate continues to change with computer power and new techniques.

E. Robustness and Integrity

This condition means that a reasonably large group of electors or representatives cannot disrupt the election. It ensures that registered voters will abstain without problems or encourage others to cast their legitimate votes for themselves. The corruption of citizens and officials is prohibited from denying an election result by arguing that some other member has not performed their portion correctly.

F. Lack of Evidence

While anonymous privacy ensures electoral fraud safeguards, no method can be assured that votes are placed under bribery or election rigging in any way. This question has its root from the start.

G. Transparency and Fairness

It means that before the count is released, no one can find out the details. It avoids acts such as manipulating late voters' decisions by issuing a prediction or offering a significant yet unfair benefit to certain persons or groups as to be the first to know.

H. Availability and Mobility

During the voting period, voting systems should always be available. Voting systems should not limit the place of the vote.

I. Verifiable Participation/Authenticity

The criterion also referred to as desirability makes it possible to assess whether or not a single voter engaged in the election. This condition must be fulfilled where voting by voters becomes compulsory under the constitution (as is the case in some countries such as Australia, Germany, Greece) or in a social context, where abstention is deemed to be a disrespectful gesture (such as the small and medium-sized elections for a delegated corporate board) [10].

J. Accessibility and Reassurance

To ensure that everyone who wants to vote has the opportunity to avail the correct polling station and that polling station must be open and accessible for the voter. Only qualified voters should be allowed to vote, and all ballots must be accurately tallied to guarantee that elections are genuine.

K. Recoverability and Identification

Voting systems can track and restore voting information to prevent errors, delays, and attacks.

L. Voters Verifiability

Verifiability means that processes exist for election auditing to ensure that it is done correctly. Three separate segments are possible for this purpose: (a) uniform verification or public verification that implies that anybody such as voters, governments, and external auditors can test the election after the declaration of the tally; (b) transparent verifiability against a poll, which is a weaker prerequisite for each voter to verify whether their vote has been taken into account properly.

Fig. 1. Security requirements for electronic voting system

III. Electronic Voting on Blockchain

A. Background

Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible (a house, car, cash, and land) or intangible (intellectual property, patents, copyrights, branding). Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved [5].

Business runs on information. The faster it's received and the more accurate it is, the better. Blockchain is ideal for delivering that information because it provides immediate, shared and completely transparent information stored on an immutable ledger that can be accessed only by permissioned network members. A blockchain network can track orders, payments, accounts, production and much more. In addition, because members share a single view of the truth, you can see all details of a transaction end to end, giving you greater confidence, as well as new efficiencies and opportunities.

Blockchain is a relatively new technology that provides many benefits for information systems. The technology can be used in a wide variety of sectors. There is ongoing research applying blockchain-based solutions in healthcare, logistics, finances, and many others [4].

As mentioned, blockchain could be used to facilitate a modern voting system. Voting with blockchain carries the potential to eliminate election fraud and boost voter turnout, as was tested in the November 2018 midterm elections in West Virginia.Using blockchain in this way would make votes nearly impossible to tamper with. The blockchain protocol would also maintain transparency in the electoral process, reducing the personnel needed to conduct an election and providing officials with nearly instant results. This would eliminate the need for recounts or any real concern that fraud might threaten the election [6].

B. Core Components of Blockchain Architecture

These are the main architectural components of Blockchain as shown in Fig. 2.

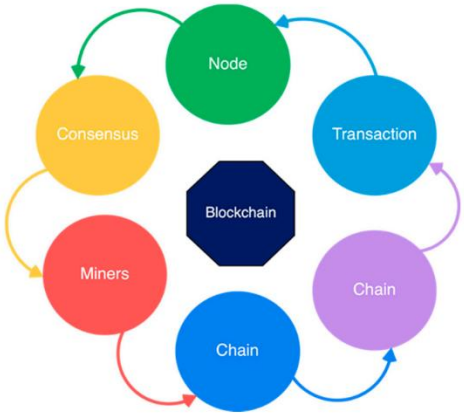

Fig. 2. Core components of blockchain architecture

- *Node:* user or computer within the blockchain architecture (each has an independent copy of the whole blockchain ledger);
- *Transaction:* smallest building block of a blockchain system (records, information, etc.) that serves as the purpose of blockchain;
- *Block:* a data structure used for keeping a set of transactions which is distributed to all nodes in the network;
- *Chain:* a sequence of blocks in a specific order;
- *Miners:* specific nodes which perform the block verification process before adding anything to the blockchain structure;
- *Consensus:* a set of rules and arrangements to carry out blockchain operations.

C. How Blockchain Can Transform the Electronic Voting System

In its basic form, blockchain is a decentralized digital ledger, which exists on the chain supported by millions of nodes simultaneously. It means any hacker with access to a terminal will not be able to attack other nodes. The decentralized functionality of blockchain makes it one of the most secure technology. There are many methods through which blockchain can address the issues of current election systems.

The traditional election system is vulnerable to post-election fraud because it relies on third parties like humans or centralized databases to collect, count, and audit votes. While a centralized database is vulnerable to hacking, humans are vulnerable to bribery (Fig. 3).

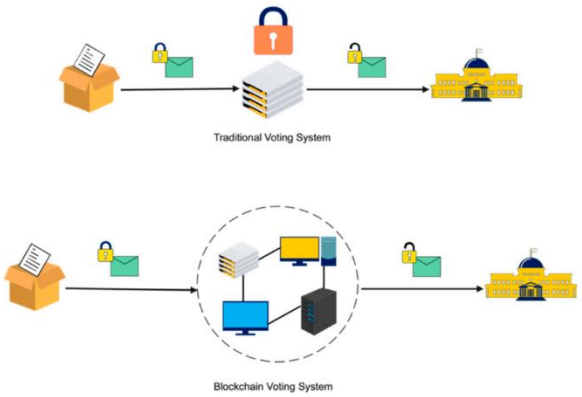

Fig. 3. Traditional vs. blockchain voting system

Blockchain systems store data on a peer-to-peer network, which makes it more secure than traditional data management systems. Voter registration databases will be immutable with the help of blockchain.

Blockchain could help store voter identity data, which is collected during voter registration in a secure database. The data can then be used to identify the voter with the help of biometrics like iris, fingerprint, and face.

Blockchain will make the third parties like a centralized database and humans meaningless as its transparency will allow voters to track their votes in real-time. Blockchain's transparency will prevent the fraud that occurs during the post-election audit.

A blockchain-based voting system handles voter privacy and security as it is a transparent and traceable system. Looking at the benefits of blockchain for elections, many companies are investing in building blockchain software for voting. For example, a blockchain software has been designed that uses a webcam and government-issued ID to allow voters to log in before they vote. After casting their

votes, voters can also look whether their vote is correctly inserted in the ballot box or not. It can be said that the use of blockchain for elections will inevitably change the way we vote.

IV. Open problems in blockchain based E-voting systems

Many problems with e-voting can be solved with blockchain technology, which makes e-voting more cost effective, enjoyable and secure than any other network. Over time, studies have identified specific issues such as the need for further work on blockchain-based e-voting and that blockchain-based e-voting schemes have serious technical problems [2].

A. Scalability and Processing Overheads

For a small number of users, blockchain works well. However, when the network is used for large-scale elections, the number of users increases, which leads to an increase in the cost and time to complete the transaction. The growing number of nodes on the blockchain network exacerbates scalability problems. In this situation, the scalability of the system is already a serious problem [8].

B. User Identity

The blockchain uses pseudonyms as the username. This strategy does not provide complete confidentiality and secrecy. Since transactions are publicly available, the identity of the user can be discovered by examining and analyzing them. The blockchain functionality is not very suitable for national elections [9].

C. Transactional Privacy

In blockchain technology, it is difficult to ensure the anonymity of transactions and confidentiality. However, an electoral system requires transaction secrecy and anonymity due to the presence of transactions. For this purpose, a third-party body is required, but not centralized, this third-party body must review and balance confidentiality.

D. Energy Efficiency

Blockchain includes energy-intensive processes such as protocols, consensus, peer-to-peer communication, and asymmetric encryption. Appropriate energy efficient consensus methods are required for blockchain-based e-voting. Researchers have proposed modifications to existing peer-to-peer protocols to make them more energy efficient [11].

E. Immatureness

Blockchain is a revolutionary technology that symbolizes a complete transition to a decentralized network. It can revolutionize business in terms of strategy, structure, processes and culture. The current blockchain implementation is not without flaws. The technology is currently useless and there is little public or professional understanding of it, making it impossible to assess its potential. All the existing technical problems in blockchain implementation are usually caused by the immaturity of the technology.

F. Acceptableness

Although blockchain is accurate and secure, people's confidence and trust are critical components of effective electronic voting on the blockchain. The complexity of the blockchain can make it difficult for people to accept blockchain-based e-voting and could pose a major obstacle to the ultimate adoption of blockchain-based e-voting as mainstream. This requires a major marketing campaign to educate people about the benefits of blockchain voting systems so that they can easily embrace this new technology.

G. Political Leaders' Resistance

Central governments such as electoral bodies and government bodies will be diverted from blockchain-based e-voting. As a result, political leaders who profit from the existing electoral process are likely to oppose the technology because blockchain will increase social resistance through decentralized autonomous organizations.

Conclusion

The purpose of this study is to analyze current research on blockchain-based electronic voting systems and identify open issues in it. The article discusses the electronic voting procedure, security requirements, advantages and disadvantages of electronic voting using blockchain technology. It then presents the open problems that exist in electronic voting systems based on blockchain technology. Further research will focus on finding solutions to these problems.

References

[1] S. Sridharan, "Implementation of authenticated and secure online voting system," 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), 2013, pp. 1-7, doi: 10.1109/ICCCNT.2013.6726801.

[2] U. Jafar, M. Aziz and Z. Shukur, "Blockchain for Electronic Voting System—Review and Open Research Challenges", Sensors, vol. 21, no. 17, p. 5874, 2021. Available: 10.3390/s21175874 [Accessed 24 September 2021].

[3] "Учебная и научная деятельность Анисимова Владимира Викторовича - Протоколы", Sites.google.com, 2021. [Online]. Available: https://www.sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema15/tema15_3. [Accessed: 24- Sep- 2021].

[4] D. Berdik, S. Otoum, N. Schmidt, D. Porter and Y. Jararweh, "A Survey on Blockchain for Information Systems Management and Security", Information Processing & Management, vol. 58, no. 1, p. 102397, 2021. Available: 10.1016/j.ipm.2020.102397.

[5] "What is Blockchain Technology? - IBM Blockchain | IBM", Ibm.com, 2021. [Online]. Available: https://www.ibm.com/topics/what-is-blockchain. [Accessed: 27- Sep- 2021].

[6] "Blockchain Explained", Investopedia, 2021. [Online]. Available: https://www.investopedia.com/terms/b/blockchain.asp. [Accessed: 27- Sep- 2021].

[7] K. Khan, J. Arshad and M. Khan, "Secure Digital Voting System Based on Blockchain Technology", International Journal of Electronic Government Research, vol. 14, no. 1, pp. 53-62, 2018. Available: 10.4018/ijegr.2018010103.

[8] J. Song, S. Moon and J. Jang, "A Scalable Implementation of Anonymous Voting over Ethereum Blockchain", Sensors, vol. 21, no. 12, p. 3958, 2021. Available: 10.3390/s21123958.

[9] I. Javed, F. Alharbi, B. Bellaj, T. Margaria, N. Crespi and K. Qureshi, "Health-ID: A Blockchain-Based Decentralized Identity Management for Remote Healthcare", Healthcare, vol. 9, no. 6, p. 712, 2021. Available: 10.3390/healthcare9060712.

[10] D. Irgasheva and S. Rustamova, "Development Of Role Model For Computer System Security," 2019 International Conference on

Information Science and Communications Technologies (ICISCT), 2019, pp. 1-5, doi: 10.1109/ICISCT47635.2019.9012058.

[11] A. Bakhtiyor, A. Orif, B. Ilkhom and K. Zarif, "Differential Collisions in SHA-1," 2020 International Conference on Information Science and Communications Technologies (ICISCT), 2020, pp. 1-5, doi: 10.1109/ICISCT50599.2020.9351441.