International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Self-tallying E-Voting Protocol Based Using Blockchain

Reshma Totare[1], Aakanksha Kulkarni[2]

[1]Assistant Professor, Department of Information Technology, AISSMS's Institute of Information Technology, Pune- 411001,INDIA
[2]TE. BE (Information Technology), AISSMS's Institute of Information Technology, Pune-411001, INDIA

A B S T R A C T

Blockchain is a means of storing information that makes it difficult or impossible to change, hack, or cheat the system. Blockchain technology may play a vital part in electronic voting, as it is inherent in maintaining anonymity

and maintaining a decentralized, distributed register of transactions between nodes.

In this study, we will discuss how blockchain can support a Trusted E- voting system for a Democracy. I will describe my efforts to explore blockchain technology to solve critical issues such as voter anonymity, election secret, and end-to-end verification. The system generates a robust cryptographic hash of every vote based on information from a particular voter to protect the anonymity and integrity of the vote.

Keywords: Electronic Voting System, e-Voting, AI (Artificial Intelligence), Traceability, Self-tallying.

1. Introduction

Elections are a vital pillar of a democratic system allowing the general people to choose their representatives via elections. Due to their relevance to our society, the election process should be transparent and reliable. Within this environment, the method of voting has been an ever- developing subject. This development is mainly driven by the attempts to make the system safe, verifiable and transparent. Constant efforts have been undertaken to increase the overall efficiency and robustness of the voting system. Electronic voting or e-voting plays a deep significance in this. Since its earliest usage as punched-card ballots in the 1960s, e-voting systems have advanced remarkably in their adaptability to internet technologies. However, e-voting systems must comply with particular benchmark requirements to permit its broad acceptance. These requirements include anonymity of the voter, integrity of the vote and non-repudiation, among others.

Blockchain is one of the developing technologies with solid cryptographic techniques allowing applications to secure these abilities to build resilient security solutions. A Blockchain, the decentralised ledger- based system, keeps a comprehensive list of continually sprouting and increasing data records guarded against unwanted manipulation, tampering, and alteration. Each block is issued a cryptographic hash (which may alternatively be viewed as a block's fingerprint) that stays valid as long as the data in the block is not changed. If any modifications are made in the blocks, the cryptographic hash will change quickly, revealing the change in the data, which may be due to malicious activity.

1.1 Motivation

Elections may readily be rigged or controlled, particularly in small towns and even in major cities situated in corrupt nations. Also, large- scale conventional polls are pretty costly in the long run. My primary objective is to offer a safe voting environment and establish that a viable e-voting mechanism is achievable by utilizing blockchain. These methods will ultimately bring humanity to actual direct democracy.

1.2 Aim and Objective

To provide a healthy environment for e-voting we need to achieve the following goals:

 Improve voter privacy: Votes information should be anonymous.

 Prevent vote tampering.

 Maintaining accuracy: Tally of votes should be accurate.

 Reduce vote-counting time: This will eventually result in cutting costs for conducting elections.

* Corresponding author. Tel.: +918208598779.
E-mail address: aakankshak31102@gmail.com

2. Literature Review

Current e-voting systems rely heavily on centralized architectures with little regard for reliability, security, and transparency, making them vulnerable to distributed denial of service attacks and single points of failure. Such things have an impact on voters' minds and eventually, lead to a loss of trust in democracy. The emerging blockchain technology introduced a novel approach to overcoming the majority of the challenges associated with traditional e-voting systems.

A secure and trusted platform can be built using protocols such as Zero-knowledge Proof-of-knowledge and Signature of Knowledge, linear encryption, time-lock puzzle, event-oriented linkable group signature, and smart contracts on the blockchain increasing voter trust.

The "Open Vote Network" is a decentralized two-round protocol designed for supporting small-scale boardroom voting. It costs as low as $0.73 per voter to vote in an election [3]. In the first round, all voters indicate their intent to vote in the election, and in the second round, all voters vote. The systems assume that all voters have access to an authenticated broadcast channel. The self-tallying property enables anyone (including non-voters) to compute the tally based on messages from other voters.

According to [4] IoT is pervasive in people's daily lives, according to experts. Integration of blockchain-based self-tallying voting systems with decentralized IoT architecture solves fairness issues in self-tallying systems with two distinct mechanisms and provides a concrete structure.

In an e-voting system, malpractice such as signal jamming in the polling area is a concern. To prevent jamming attacks, "Reinforcement Learning (RL)" techniques can be used. The solution includes a secure mobile offloading solution that is resistant to smart attacks, lightweight authentication, and a caching collaboration scheme that is resistant to wiretaps [2]. Secure mobile edge caching based on RL can improve the security and user privacy of mobile edge caching systems. This security solution may aid in the prevention of signal jamming in the voting area.

3. Algorithms and Techniques

3.1.1 Zero-knowledge Proof-of-knowledge and Signature of Knowledge:

ZKPok is a protocol in which a prover convinces a verifier that he knows a certain quantity satisfying but revealing nothing about it.

3.1.2 Linear encryption:

Linear encryption is a semantically secure extension of ElGamal encryption under the decision linear assumption. Three polynomial-time algorithms are used in the linear encryption scheme: key generation KeyGen, encryption Enc, and decryption Dec.

3.1.3 Time-Lock puzzle:

A time-lock puzzle, which consists of two polynomial-time algorithms: puzzle generation and puzzle-solving, allows one to encrypt messages for a specific amount of time.

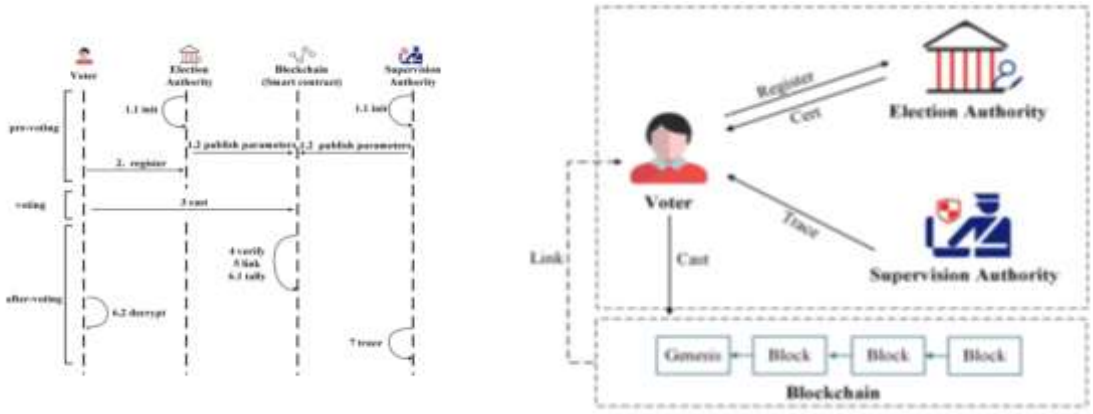
3.1.4 Event-oriented linkable group signature:

An event-oriented linkable group signature (ELGS) states that two signatures for the same event can be linked if they are signed by the same signer, even if the signer is signing on behalf of different groups.

3.1.5 Smart contract:

A smart contract is a set of code and data that is executed on the Ethereum virtual machine.

3.2 Stages of e-voting system in the blockchain



Workflow of an e-voting system on blockchain

3.2.1 Pre-voting:

Setup:

The Setup step takes a security parameter, the number of candidates, the number of voters, a time-related hardness parameter, and the identifier of the voting event as input and returns the system public parameters EA's key pair (EPK, ESK) and SA's key pair.

Register:

This is an interactive step between a voter and EA that accepts the system public parameter, a voter's identifier, and EA's private key as input and returns the voter's key pair and the corresponding certificate as output.

3.2.2Voting:

Cast:

This step includes puzzle generation and sign operations, and it takes the system public parameter, a voter's ballot for n candidates, and outputs the encrypted ballot, signature, and NIZK proof.

3.2.3Post-voting:

Verify:

Any participant on the blockchain can perform this step, which takes as input the system public parameter, a tuple consisting of the encrypted ballot, signature, and NIZK proof. If the tuple is valid, it returns 1; otherwise, it returns 0.

Link:

Any participant on the blockchain can perform this step, which takes the system public parameter, any two tuples consisting of the encrypted ballot, signature, and NIZK proof, and any two tuples consisting of the encrypted ballot, signature, and NIZK proof as input. If two ballots were signed by the same voter, it returns 1; otherwise, it returns 0.

Tally:

Smart contracts and voters perform this step. It accepts the system's public parameter as well as tuples containing the encrypted ballot, signature, and NIZK proof as input and outputs the final voting result.

Trace:

SA is in charge of this step. It accepts as input the system public parameter, the SA's private key, and a tuple consisting of the encrypted ballot, signature, and corresponding NIZK proof. It returns the appropriate certification as well as the voter's public key.

4. Conclusion

I studied the idea of adopting a blockchain-based electronic voting system that utilizes smart contracts to enable secure and cost-efficient elections while guaranteeing voters' privacy. Blockchain can replace the traditional voting system because Blockchain is more secure than the current system and the cost of conducting an election on the blockchain is comparatively less. Despite being many advantages of conducting a whole election process on the blockchain, the implementation requires lots of expertise to make it secure and cost-efficient. Currently, blockchain technology is comparatively new. In countries like India where there is only 38% of total digital literacy rate (in the year 2020-21) implementing this kind of election process is currently difficult or rather impossible. In addition to digital literacy, basic needs for conducting this kind of election plays a very crucial role, this includes wide coverage of network accessibility. Also, it's hard to hack Blockchain, but it may not be that difficult to hack individuals' phones, and network switch off is another concern in the polling area. Considering all the current statistics, there is no chance that this kind of election is feasible in near future, or roughly a decade or two. At last, I would like to mention that I'm very excited to try to implement a blockchain-based e-voting system as a real-world application in near future.

Acknowledgments

I'm greatly appreciative of all who gave valuable support in getting the seminar report completed. I owe Mrs. Reshma Totare, my guide, a debt of gratitude for her guidance and encouragement with this work. Her expert suggestions added depth to this seminar study. I would also like to recount my appreciation to Mrs. Meenakshi Thalor, Head of Department, Information

Technology, as well as Mrs. Resha Totare, PBS coordinator who provided insightful feedback by considering a broader point-of-view and understanding how important it is to broaden one's perspective while embracing new ideas and visions.

I want to express appreciation and thanks to all my colleagues and family members who knowingly or unknowingly have assisted and encouraged me throughout my work.

References

[1] H. Li, Y. Li, Y. Yu, B. Wang and K. Chen, "A Blockchain-Based Traceable Self- Tallying E-Voting Protocol in AI Era," in *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 1019-1032, 1 April-June 2021, doi: 10.1109/TNSE.2020.3011928.

[2] L. Xiao, X. Wan, C. Dai, X. Du, X. Chen, and M. Guizani," Security in mobile edge caching with reinforcement learning," *IEEE Wirel. Commun.*, vol. 25, no. 3, pp. 116-122, Jun. 2018.

[3] P. McCorry, S.F. Shahandashti, and F. Hao," A smart contract for boardroom voting with maximum voter privacy," in *FC*, Sliema, Malta, Apr. 2017, pp. 357-375.

[4] Y. Li, W. Susilo, G. Yang, Y. Yu, D. Liu, X. Du, M. Guizani," A Blockchain-Based Self-Tallying Voting Protocol in Decentralized IoT," *IEEE Trans Dependable Secure Comput*. DOI: 10.1109/TDSC.2020.2979856, 2020.

[5] S. Panja, S. Bag, F. Hao and B. Roy," A Smart Contract System for Decentralized Borda Count Voting," *IEEE Trans. on Eng. Manag.*, DOI: 10.1109/TEM.2020.2986371, 2020.

[6] https://www.ijrar.org/viewfull.php?&p_id=IJRAR19J3551