A Survey on Vote Vault-Blockchain-Based System Using SHA-256 Algorithm and Smart Contract

Shyamala Gowri B[1], Sai Krishna R[2], Saketh Raman R[3], Yuteesh S[4]

[1]*Computer Science and Engineering, Easwari Engineering College, Anna University, Chennai, India*

[2,3,4]*Students, Computer Science and Engineering, Easwari Engineering College, Anna University, Chennai, India*

Abstract:

One of the most important indications of how residents participate in their country's administration is voter turnout. Since the 1990s, the number of countries that hold national elections has increased substantially. However, the global average voter turnout has decreased significantly over the same period. We propose a Blockchain-based Voting System to solve the above-mentioned issue. We argue that our system is more secure, reliable, and can protect voter privacy which will help boost the number of voters and their trust in the electoral system as well as reduce considerably the cost of national elections. Since it is an online voting system, it allows citizens to vote from the comfort of their homes. The system makes use of the SHA-256 Algorithm for voter authentication and Smart Contract for the voting process.

Keywords: Blockchain, SHA-256, Smart Contract.

1. Introduction:

Voting systems have been used for over decades in various democracies helping in letting voters choose their leaders. But for the most part, the systems are unchanged for a long period of time. The majority of the systems are devoid of the security of the voter and the votes which can be tampered with. There has been a decline in the number of voters in recent elections in various parts of the world. For example, the Tamil Nadu State Legislative Assembly Elections held in 2021 recorded only a 72.8% voter turnout, which is 2% lesser than the preceding 2016 elections. As stated in the study conducted by IDEA on the recent Voter Turnout Trends, Institutional factors such as Electoral systems, Registration, and Voting Arrangements play an important role.

We have proposed a blockchain-based voting system that succeeds in securing the privacy of the voter and their votes. Blockchain was first developed as a cryptocurrency financial services company where an immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. But as time passed, blockchain has been used in multiple domains and now we are proposing it to be used in the voting systems.

In the proposed system, the voter logs into the system via their UserID and password which is encrypted using the SHA-256 algorithm and compared with the encrypted hash in the database for authentication. After they complete the authentication process, they enter the voting system where they are provided with multiple parties they wish to vote. When they are done selecting the party and casting their vote, a blockchain is created to store the vote data. Smart Contract is used during the blockchain creation process and the created blockchains are immutable. Thus, the votes cannot be changed and since it is an online voting system, people can vote from the comfort of their homes which will increase the number of voters in the elections. Compared to other state-of-the-art blockchain-based voting systems it respects voters' privacy and has user-friendly terminals, which will boost the confidence of people in the voting system and therefore increase the number of participants in the election.

2. Literature Survey:

The authors of **Dongliang Xu et al., (2021) [1]** propose a "k-out-of-m" multi-candidate voting model based on blockchain technology that ensures: 1) the preservation of anonymity during the voting process through ECC encryption and a signature mechanism; and 2) the prevention of forgery of voting information by combining blockchain technology, automatic statistics, and the display of voting results through a smart contract. In addition, this research introduces an anonymity-preserving voting (APV) algorithm to address the shortcomings of the blockchain voting technique. They conduct experiments on the suggested paradigm using the Hyperledger Fabric technology. Hyperledger Caliper is used to evaluate the model's performance. Experiments are planned and thoroughly tested in terms of the model's security criteria as well as the proposed APV algorithm's efficacy and efficiency. They confirm that the model is especially well-suited for small-scale voting circumstances and that it solves the shortcomings of traditional electronic voting, such as lack of anonymity, excessive centralization, and ease of forging, through these trials.

The authors of **Geetanjali Rathee et al., (2021) [2]** introduced the concept of E-voting attacks, which occur during the polling mechanism in smart cities. The privacy and security vulnerabilities are addressed by computing each entity's trust and then storing it in a Blockchain to compare their continuous conduct. Furthermore, when compared to the baseline scheme, the proposed phenomena exhibit a substantial improvement because the provided technique ensured security by employing blockchain and trust computation instead of checking certificates and using cryptographic algorithms. By comparing numerous security metrics, our suggested method is comprehensively evaluated against the baseline mechanism. Furthermore, by tracking the activity of each election process, the proposed mechanism outperformed the baseline mechanism. However, the system's drawback is that it is merely a simulation (theory) that can only be employed in smart cities that use IoT.

The primary takeaway of **Saurabh Singh et al., (2021) [3]** is that the authors have thoroughly studied many attacks on blockchain and the security vulnerabilities with blockchain using real-world scenarios. Furthermore, this study explored the many security difficulties, challenges, weaknesses, and assaults that restrict the increased adoption of blockchain technology from a range of perspectives. They also went over various blockchain applications and benefits, as well as a variety of business options. Finally, they outlined existing security solutions for various situations as well as ongoing research projects.

The author of **Anusha Vangala et al., (2021) [4]** presents smart contract authentication for a smart farming architecture that leverages hybrid blockchain and edge computing. The suggested scheme (SCBAS-SF) includes anonymity and traceability as security elements. Using the well-known ROR model, SCBAS-SF is proven to be provably secure. Furthermore, using informal security analysis, it is proven to be resistant to a variety of hypothetical assaults. AVISPA, an automated validation tool, is also used to formally verify SCBAS-SF against replay and man-in-the-middle attacks. The planned SCBAS-SF is demonstrated in practice on the Sawtooth Hyperledger platform as well as the MIRACL-based Raspberry PI 3 testbed. In comparison to other existing competitive authentication systems, a detailed comparison reveals that the proposed SCBAS-SF has greater security, comparable computing cost, and low communication cost.

The authors of **Somnath Panja et al., (2020) [5]** proposed a two-round self-tallying Borda count e-voting mechanism in their paper. The tally is not computed by any trustworthy party in this approach. Instead, the approach assures that anyone with access to the bulletin board can calculate the total using public data. The technique protects voter privacy, with voters only being able to discover the election tally and their individual inputs after the procedure is completed successfully. They presented security proofs to demonstrate the protocol's security. Furthermore, the scheme is publically verifiable. Every voter generates NIZK proofs to demonstrate that they have followed the protocol specification to the letter while keeping their secret input hidden. For implementation, blockchain is employed. The findings of both the theoretical and experimental analyses demonstrate that this technique can be employed in practice. However, this approach has the drawback of not being designed for a traditional voting process. Instead, it's designed for the Borda count method of voting.

The findings of **Santeri Paavolainen et al., (2020) [6]** refute many conventional assumptions about light client security. While light clients may be regarded as secure against adversarial invalid block injections in "typical" settings, these are optimistic scenarios that include a brief attack window, an honest majority, and no network partitioning. However, if one gets away from these optimistic assumptions, the reality changes dramatically. Under partial network isolation, an adversary has a statistically substantial chance of success even with modest hashing power. They also find that if an opponent can undermine an existing mining pool on the Ethereum network, their chances of succeeding skyrocket. When adversaries who can change the target node's operating environment are considered, light clients' security is further weakened. The attacker may have access to the device, and it could modify its network accessibility or power availability even if it did not meddle with the device itself. Jammers for GSM and Wi-Fi are reasonably easy to buy and deploy, allowing a hostile actor to manipulate the availability of the network to which a client is connected. Finally, their assumptions constrain the analysis. For example, Ethereum allows for gradual adjustments to the cryptographic puzzle's difficulty in reaction to changes in network hashing power. This indicates that a partitioned network will adjust over time to reach a block interval similar to the complete network. They don't take this into consideration and believe it has minimal impact; this is a significant departure from the Ethereum protocol. Similarly, they believe the adversary's strategy is likely to be ineffective.

The author of **Huilin Li et al., (2020) [7]** proposes a blockchain-based traceable self-tallying e-voting protocol to reconcile the anonymity and accountability of existing e-voting systems while also achieving a trade-off between voting scale and computing performance. Furthermore, the suggested protocol supports e-voting system features such as multi-choice and self-tallying. By presenting extensive security proofs, they demonstrated that the proposed protocol satisfies the requisite security. They also published a proof-of-concept implementation to demonstrate the protocol's efficacy. The e-voting technology will be used in real-world applications in the future.

The writers of **Basit Shahzad et al., (2019) [8]** provide a viewpoint on the electronic voting process. This study suggested a framework based on an adjustable blockchain that can address issues in the polling process, such as the selection of an appropriate hash algorithm, the selection of blockchain changes, the voting data management process, and the voting process' security and authentication. The flexibility of blockchain has allowed it to adapt to the dynamics of the electronic voting process. However, the suggested system makes a few assumptions. Notably, the voter is well-educated and knowledgeable about his constitutional rights and the polling procedure. It is critical that each voter be able to vote within the time limit, (ii) all voter data be available and accessible for verification, and (iii) the data be provided by the national agency that manages the data. It is also anticipated that connectivity is available at all times, with no communication delays and no interruptions due to internet outages, and that the polling staff is knowledgeable about technology and can properly lead voters through the voting process.

The authors of **Xuechao Yang et al., (2018) [9]** present a secure voter-verifiable e-voting system that allows voters to cast ballots by allocating unlimited numbers of points to various candidates. This means that voters can give each candidate the same number of points, or they can give each contender a different number of points. The distributed ElGamal cryptosystem is used in the system. Before being submitted, each cast ballot is encrypted and stays encrypted at all times. The exponential ElGamal cryptosystem's additive homomorphic characteristic allows for efficient ciphertext processing throughout these procedures. Furthermore, anyone can check the legitimacy of voters and their submissions without revealing the contents of the ballots. The security and performance research not only verifies the online voting system's practicality for real-world elections but also reveals that it outperforms other systems previously studied. However, the system's shortcoming is that it must assume that at least one authority is trustworthy; otherwise, the system is insecure.

The authors of **Xiwang Yung et al., (2017) [10]** introduced a variety of MF-based and NN-based online social voting systems. They discovered that both social network information and group affiliation information can improve the accuracy of popularity-based voting recommendations, especially for cold users, in real-world experiments, and that social network information dominates group affiliation information in NN-based approaches. This study found that for cold users, social and group information is far more beneficial than for heavy users when it comes to improving recommendation accuracy. This is because chilly users are more likely to vote in popular polls. In the studies, simple meta path-based NN models outperformed computation-intensive MF models in hot-voting suggestions, however, MF models can better mine users' interests for nonhot voting.

3. Conclusion:

In today's world, the idea of adapting digital voting techniques to make the public political process cheaper, faster, and easier is appealing. This paper is thus made to give the readers a survey of various papers on blockchain-based voting systems. Making the voting process inexpensive and quick normalizes it in the eyes of voters, lowers a power barrier between the voter and the elected official, and puts pressure on the elected official. We presented a novel blockchain-based electronic voting system in this study that provides secure and cost-effective elections. To protect the privacy of the voter, we employed the SHA-256 hashing mechanism. The vote data of each voter is stored using an Ethereum-based blockchain system, and the vote data is protected in the blockchain.

In the future, we would like to make the voting system attack proof by immunizing it from Malware, DDOS, and Phishing attack to name a few. We would also like to take our project mainstream by using it in real-life election processes.

4. References:

[1] Dongliang Xu, Wei Shi, Wenshang Zhai, Zhihong Tian, 2021 ‘Multi-Candidate Voting Model Based on Blockchain’, IEEE/CAA Journal of Automatica Sinica, Vol.8, Issue: 12, Page(s): 1891 - 1900.

[2] Geetanjali Rathee, Razi Iqbal, Omer Waqar, Ali Kashif Bashir, 2021, ‘On the Design and Implementation of a Blockchain-Enabled E-Voting Application Within IoT- Oriented SmartCities’, IEEE Access, Vol. 9, Issue-10 Page(s): 34165 - 34176.

[3] Saurabh Singh, A.S.M. Sanwar Hosen, Byungun Yoon, 2021 ‘Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network’, IEEE Access, Vol.9, Page(s): 13938 - 13959.

[4] Anusha Vangala, Anil Kumar Sutrala, Ashok Kumar Das, Minho Jo, 2021 ‘Smart Contract-Based Blockchain-Envisioned Authentication Scheme for Smart Farming’, IEEE Internet, Vol.6, Issue: 4, Page(s): 20506 - 20519.

[5] Somnath Panja, Samiran Bag, Feng Hao, Bimal Roy, 2020 ‘A Smart Contract System for Decentralized Borda Count Voting’, IEEE Transactions on Engineering Management, Vol.67, Issue: 4, Page(s): 1323 – 1339.

[6] Santeri Paavolainen, Christopher Carr, 2020 ‘Security Properties of Light Clients on the Etherium Blockchain’, IEEE Access, Vol.8, Page(s): 124339 - 124358.

[7] Huilin Li, Yannan Li, Yong Yu, Baocang Wang, Kefei Chen, 2020 ‘A Blockchain-Based Traceable Self-Tallying E-Voting Protocol in AI Era’, IEEE Transactions on Network Science and Engineering, Vol.8, Issue: 2, Page(s): 1019 - 1032.

[8] Basit Shahzad, Jon Crowcroft, 2019 ‘Trustworthy Electronic Voting Using Adjusted Blockchain Technology’, IEEE Access, Vol.7, Page(s): 24477 - 24488.

[9] Xuechao Yang, Xun Yi, Surya Nepal, Andrei Kelarev, Fengling Han, 2018 ‘A Secure Verifiable Ranked Choice Online System Based on Homomorphic

Encryption’, IEEE Access, Vol.6, Issue: 4, Page(s): 20506 - 20519.

[10] Xiwang Yung, Chao Liang, Miao Zhao, Hongwei Wang, Hao Ding, Yong Liu, Yang Li, Junlin Zhang, 2017 ‘Collaborative Filtering-Based Recommendation of Online Social Voting’, IEEE Transactions on Computational Social Systems, Vol.4, Issue: 1, Page(s): 1 - 13.