In-depth Analysis of Securing E-voting through Blockchains

Amay Sandanshiv
Vivek Salve
Tejas Muthe
Sameer Shaikh
Prof. Balaji Bodkhe
Computer Engineering Dept., MESCOE, Pune.
[1]

Abstract

Democratic governance of a state is governance in which voters choose their chosen leader from a group of candidates in the hopes of improved expression and leadership. The procedure should be comprehensive and follow best practices, including being free and without aggression, and treating each individual's interests equitably. With an increasing number of voters as well as a large number of polling places designed to help everyone who has reached the voting age in exercising their ballot, the vast bulk of the inspectors tasked with overseeing these polls have been put under strain. In order to execute functional elections, every one of these votes from individuals should always be obtained. As a consequence, the Blockchain architecture is being proposed as a way to increase vote integrity while simultaneously cutting election costs. The blockchain are some of the most reliable technologies for ensuring tamper-proof results due to its robust construction. The results of earlier studies have shown to be useful in deciding on a blockchain technique for efficiently safeguarding post-voting data. In future revisions of this study piece, this technique will be expanded upon..

Keywords: *Electronic voting, Blockchain Framework, Post voting Data Security.*

I INTRODUCTION

The impact of information technology on our general societal political and social lifestyles has piqued our involvement, as scientists and engineers look for new ways to enhance things on a regular basis, including that of the selection of a leader through investigation and the incorporation of scientifically centered research into the political frame. Undoubtedly, as society progresses, people's demands vary, and this includes the selection of leadership that will match their aspirations. The disciples are interested in authority from all perspectives. This has prompted researchers in the fields of humanities and social studies to devise techniques for selecting leaders that are free of deception.

Every person has the democratic right to vote, which permits them to elect tomorrow's administrators. Polling not only allows individuals to express their political preferences, but it also teaches them to appreciate the importance of democracy. Many individuals do not vote because they believe that one vote will not make a significant impact, except it does. The democratic foundations of the country are built by implication of elections. Voting is an important tool for maintaining a country's political system. Individuals have the ability to challenge the government as a result of this. In a democratic society, polling is a mechanism for citizens to voice their opinions. Voting is essential for a democratic system to be initiated. Ballot papers, new regulations to simplify elections, and the deployment of technological tools to accelerate the operation are all instances of advancements that have taken place over time.

Liberal democracies are established on voting, whether through conventional ballet voting or computerised voting. Voter indifference has been growing rapidly in recent decades, particularly amongst the youthful computer/tech aware population. E-voting is being promoted as a means of attracting young voters. A variety of

[1]

security and performance characteristics are defined for a strong e-voting mechanism, encompassing accessibility, correctness, traceability, system and data integrity, secrecy/privacy, scalability, and authorization distribution.

For years, electronic voting technologies have become the focus of ongoing research, with the objective of lowering ballot costs while maintaining election legitimacy by meeting security, anonymity, and stringent guidelines. The use of a new voting system to replace the existing pen and paper method offers the capability to minimize fraud while also keeping the voting process accesible and verifiable.

Polling has indeed evolved from the conventional, highly error-prone ballot papers approach to a more dependable, less error-prone E system, in which a voter may cast a vote by demonstrating their identification and appearance at a voting centre. Even though this sort of scheme has made great strides and has shown to be a dependable mechanism, it may be confronted in terms of privacy, intrusion durability, counterfeiting, and manipulation by diverse groups of users owing towards certain inherent problems such as blind faith and centralization.

With the aid of the blockchain data architecture, the move to a decentralized system from a centralized system in numerous industries has emphasized the necessity for electronic signatures in numerous technology-based alternatives. The blockchain is a decentralized peer-to-peer digital ledger which has offered its consumers with the benefits of traditional relational repository as well as additional capabilities such as data protection, authenticity, accountability, and verification without relying on a centralized trusted intermediary. As a result, blockchain technology is now being used in a range of industries, including banking, medicine, and supply chain management.

Numerous studies show that in the era of Blockchain, a streamlined transition from a crucial centralized approach to a decentralized network can be achieved to achieve a secure election process without centralized authenticity, as the blockchain has the capacity to make all transactions highly secure and tamper-proof. This approach can be applicable for an accountable E-voting system which will be elaborated in the future.

This literature survey paper segregates the section 2 for the evaluation of the past work in the configuration of a literature survey, and finally, section 3 provides the conclusion and the future work.

1. II RELATED WORKS

F. P. Hjalmarsson et al. [1] presented a blockchain-based electronic voting system that uses smart contracts to allow for safe and cost-effective elections while protecting voters' privacy. The authors demonstrated that blockchain technology provides a new way to overcome the limits and adoption obstacles of electronic voting systems, ensuring election security and integrity and laying the groundwork for transparency. It is feasible to transfer hundreds of transactions per second into an Ethereum private blockchain, employing every component of the smart contract to reduce the load on the blockchain.

The basic foundation for a secure and reliable e-voting system based on blockchain technology, as well as a security and performance analysis of the proposed system architecture, were introduced by D. Rathore[2]. An eligible and authenticated voter has the right to vote in this system by authenticating with the AS and thereby utilizing the granted virtual identity throughout the voting procedure. The proposed system solves the problem of remote voting without requiring physical presence in the polling booth by encrypting the choice made with its own public key and then re-encrypting it with the RKey before providing it to the permissioned blockchain communicating DgS, resulting in a strong randomized variation in the ciphertexts generated for the same plaintext using the same EO key.

M. Ibrahim et al. illustrate the effectiveness of an online voting system as well as the answers it gives to typical challenges in online voting systems through the development of a blockchain-based voting system. This solution is not based on any current blockchain network and merely employs blockchain-related ideas such as SHA-256 encryption, immutability, and anonymity. Voter fraud may be greatly reduced by implementing the ElectionBlock technology, which also provides total transparency and an easy-to-use interface [3]. Because of blockchain technology, vote anonymity and security are also greatly improved. The authors have made the source code of prototype implementation publicly available to encourage the incorporation of new ideas into the system.

F. Sheer Hardwick et al. suggest an e-voting mechanism, which is eventually put into action. The research describes the implementation and related performance metrics, as well as the obstacles offered by the blockchain platform when developing a sophisticated application such as e-voting. The study identifies certain problems and proposes two potential next steps to upgrade the underlying platform of blockchain technology to accommodate e-voting and other similar applications [4].

E. Bellini et al. introduced an e-Vote-as-a-Service based on Blockchain that overcomes the constraints of existing initiatives by utilizing a cloud-based approach. Even while several cloud providers, like IBM and Oracle, provide ready-to-use blockchain installations in the cloud for a charge based on the volume of transactions, the difficulty of dynamic and on-demand system design and optimization based on end users' business requirements persists [5]. The current model enables end-users to specify functional and non-functional service needs, as well as the cloud infrastructure where services are delivered on-demand, to optimize costs and service performance.

A. Kaudare et al. developed and constructed a blockchain-based electronic voting system based on Hyperledger to conduct safe elections while protecting users' privacy. When ethereum and hyper ledger are compared, it is discovered that hyperledger is more efficient than ethereum in most performance measures, and because it is a permissioned chain, it allows the voter's anonymity to be preserved [6].

To establish a stable and efficient E-voting system design, the concepts of blockchain and machine learning are presented by M. A. Cheema et al. to give protection and integrity to the voting system [7]. As an E-voting station network, this suggested system not only ensures the integrity of votes but also protects people's data. The authors employed two machine learning models, each with its own set of parameters. The Gaussian Vector Support Machine is one, while the linear Vector Support Machine is another. These two classifiers are compared by calculating their accuracy and AUC. The concept of a smart contract is utilized to both register voters and receive votes. The Merkle root technique was used to obtain the root hash to verify the integrity of the data kept in the citizen's data center.

To overcome the challenges that electronic voting systems encounter, S. N. Odaudu et al. proposed to use Blockchain technology in conjunction with electoral voting systems to establish a distributed yet irreversible electoral collation process. The suggested technique of result collation is an attempt to provide electorates with confidence and dependability, hence preventing vote theft at the level of result collation. A vulnerability assessment of blockchain technology, block processing capability, smart contracts, and use of the technology on the result collation stage is provided [8].

H. Li et al. present a concrete blockchain-depend self-tallying e-voting system that does not require a central entity to tally votes and broadcast the voting results. To achieve self-tallying, the proposed approach utilizes a homomorphic time-lock problem, which also secures the anonymity of votes. Furthermore, the protocol enables large-scale voting and multi-choice voting in the sense that the time it takes for each voter to decode the voting result is unaffected by the number of voters. As a result, the approach strikes a satisfactory compromise between voting size and computing efficiency. The authors create a novel event-oriented linkable group signature to safeguard voter privacy and avoid multiple voting, where a malicious voter may be publicly connected and exposed by the tracing authority, to balance anonymity and accountability in e-voting [9].

D. Pramulia [10] introduced a blockchain-based e-voting system using Ethereum and Metamask which serve as a solution to the e-voting system's security and trust issues. Because it allows smart contracts and has a variety of development tools, the blockchain network is popular. Ballot Manager and Voter are the two key systems that make up its core architecture. Metamask, an Ethereum meta-transaction implementation in the form of a browser, connects both systems to the Ethereum Blockchain network. According to the findings of the performance evaluation, the time necessary to verify a transaction, particularly Vote, ranges between 10 and 47 seconds, which is acceptable given that this is a non-real-time transaction.

A. M. Al-Madani et al. propose the electronic voting mechanism based on Ethereum's Blockchain. Using Blockchain technology, this application can solve the limits and security difficulties of the centralized voting method. This research demonstrated how a blockchain secures data [11]. The researchers created a decentralized voting tool using a smart contract. Then, for this application, a smart contract was published on a local blockchain. The software uses Ethereum Blockchain technology to serve as both a network and a decentralized database for recording voter accounts, votes, and candidate information. Blockchain creates a decentralized network that is

dependable, secure, versatile, and capable of supporting real-time services. Because the architecture does not allow for duplicate votes, the voter recognizes that his vote is going to the appropriate candidate and that he only has one vote.

III CONCLUSION AND FUTURE SCOPE

Democracy is built on the foundation of elections. Most countries around the globe consider relatively frequent and periodic elections to be a key feature of democracies. To provide substance to democracy's essential objectives of political fairness and citizen responsibility, the process should take place within settings that satisfy international standards. Manual voting through ballot boxes is outdated and inefficient, resulting in a huge deal of pollution and other environmental damage. Additionally, voters would have to be present physically to participate for their contender, which may require standing in line for an extended amount of time; this may discourage prospective participation because of additional dedication is not seen beneficial sufficiently. As a consequence, voter turnout falls and, as an outcome, the election's overall efficacy suffers. As a consequence, this article has explained how to use an E-voting alternative as well as the various tasks that go along with it. These essential investigations have contributed to the creation of a successful blockchain-based method that will be outlined in future iterations.

REFERENCES

[1] F. P. Hjalmarsson, G. K. Hreioarsson, M. Hamdaqa, and G. Hjálmtýsson, "Blockchain-Based E-Voting System," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), 2018, pp. 983-986, DOI: 10.1109/CLOUD.2018.00151.

[2] D. Rathore and V. Ranga, "Secure Remote E-Voting using Blockchain," 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), 2021, pp. 282-287, DOI: 10.1109/ICICCS51141.2021.9432249.

[3] M. Ibrahim, K. Ravindran, H. Lee, O. Farooqui, and Q. H. Mahmoud, "ElectionBlock: An Electronic Voting System using Blockchain and Fingerprint Authentication," 2021 IEEE 18th International Conference on Software Architecture Companion (ICSA-C), 2021, pp. 123-129, DOI: 10.1109/ICSA-C52384.2021.00033.

[4] F. Sheer Hardwick, A. Gioulis, R. Naeem Akram and K. Markantonakis, "E-Voting With Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy," 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018, pp. 1561-1567, DOI: 10.1109/Cybermatics_2018.2018.00262.

[5] E. Bellini, P. Ceravolo, and E. Damiani, "Blockchain-Based E-Vote-as-a-Service," 2019 IEEE 12th International Conference on Cloud Computing (CLOUD), 2019, pp. 484-486, DOI: 10.1109/CLOUD.2019.00085.

[6] A. Kaudare, M. Hazra, A. Shelar, and M. Sabnis, "Implementing Electronic Voting System With Blockchain Technology," 2020 International Conference for Emerging Technology (INCET), 2020, pp. 1-9, DOI: 10.1109/INCET49848.2020.9154116.

[7] M. A. Cheema, N. Ashraf, A. Aftab, H. K. Qureshi, M. Kazim, and A. T. Azar, "Machine Learning with Blockchain for Secure E-voting System," 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH), 2020, pp. 177-182, DOI: 10.1109/SMART-TECH49988.2020.00050.

[8] S. N. Odaudu, U. J. Imeh, and U. Abubakar, "BIDS: Blockchain-Based Intrusion Detection System for Electoral Process," 2019 15th International Conference on Electronics, Computer and Computation (ICECCO), 2019, pp. 1-15, DOI: 10.1109/ICECCO48375.2019.9043292.

[9] 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.

[10] D. Pramulia and B. Anggorojati, "Implementation and evaluation of blockchain-based e-voting system with Ethereum and Metamask," 2020 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS), 2020, pp. 18-23, DOI: 10.1109/ICIMCIS51567.2020.9354310.

[11] A. M. Al-Madani, A. T. Gaikwad, V. Mahale, and Z. A. T. Ahmed, "Decentralized E-voting system based on Smart Contract by using Blockchain Technology," 2020 International Conference on Smart Innovations in Design, Environment, Management, Planning, and Computing (ICSIDEMPC), 2020, pp. 176-180, DOI: 10.1109/ICSIDEMPC49020.2020.9299581.

*****