Abhilash Gaddam, 2023, 11:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

The Transformative Power Of Block chain Technology And Its Application To Voting and Cyber Security

Abhilash Gaddam
MET, College of Computer Science, Mumbai

Abstract- Many have looked to block chain technology as a way to make online voting more trustworthy and open. Electronic voting systems may avoid manipulation and fraud, make voting more anonymous, and boost confidence in the election process by using blockchain technology's decentralization, immutability, and transparency. Electronic voting solutions built on the blockchain also have the potential to cut down on the time and money needed for conventional voting procedures. The reliance on centralized organizations in traditional voting processes might leave them open to vulnerabilities like election fraud or results manipulation. Blockchain technology's intrinsic decentralization and immutability provide a potential remedy to the problems associated with conventional and alternative electronic voting methods. An immutable and open platform for electronic voting may be built using blockchain technology. By combining cryptographic methods with consensus protocols, blockchain-based electronic voting systems provide voting processes that are safe, verifiable, and auditable. To develop a successful voting mechanism, this study tries to make use of blockchain's cryptographic underpinnings and transparency. The suggested technique accomplishes end-to-end verifiability and complies with the basic criteria for electronic voting systems. This paper lays out the specifics of the proposed electronic voting system and how it would be implemented on the Multichain platform. To establish an end-to-end verifiable e-voting method, the article offers an in-depth review of the technique, which effectively confirms its efficacy.

Keywords-blockchain; e-voting systems; security; scalability; digital transformation;

I. INTRODUCTION

The safety of the election is a legitimate concern for voters. There is widespread concern about the reliability of elections due to news reports of potential meddling from foreign powers, instances of illegal voting, voter disenfranchisement, and technological malfunctions [1]. In recent years, the expansion of the IoT has resulted in numerous technical advancements, one of which is the concept of the smart city. Improving inhabitants' lives in numerous sectors, including health, economy, business, farming, and transportation, is the goal of developing a smart city, which in turn necessitates the integration of IoT devices as well as information and communication technology [2]. Emerging as a game-changing technology, blockchain has the potential to solve problems in fields as diverse as electronic voting and the security of smart cities. Even while blockchain was first developed for use with bitcoin, a digital money, it is already having and will continue to have far-reaching effects on many industries and communities [3].

To evaluate the efficacy and safety of blockchain technology in electronic voting systems, a comparison was made with a centralized system. As a distributed, decentralized database system, blockchain technology is one of the newer innovations that promises to increase openness and decrease cybersecurity threats. Two electronic voting systems were created and tested for security and performance: one that relies on blockchain technology (BEVS) and the other that uses a centralized database (CEVS) [4]. An enticingly disruptive technology, blockchain can revolutionize companies. Companies may be at a disadvantage in the market if they choose to ignore it. The most popular proposed uses for cryptocurrencies have expanded beyond their initial financial use to include supply chain administration and electronic voting systems. Nevertheless, blockchain's potential information and cyber security uses are under-discussed, particularly from an enterprise viewpoint [5], [11], [12], [13].

II.RELATED WORK

The article debunks the assertions that "voting over the Internet" or "voting on the blockchain" would make elections more secure, arguing that such claims are deficient and deceiving. Internet and blockchain-based voting would substantially raise the possibility of undetectable, national-scale election failures, even though present election methods are not flawless. To others, the idea of casting a ballot from the comfort of their own home or on the go with a mobile device can be alluring. Online voting may not improve participation in actual elections and may even lead to more people not exercising their right to vote, according to mixed research. To add insult to injury, the present level of computer security makes it impossible to say with any certainty that votes have been accurately counted and not tampered with or deleted, even if turnout increases due to voting over the Internet or blockchain.

As long as tried-and-true methods like denial-of-service assaults, malware, and zero-day vulnerabilities are viable, the current situation will persist. Researchers looked at how blockchain's four characteristics transparency, democratization, decentralization, and security can enhance smart city services and examined various blockchain uses in smart cities in [7]. To demonstrate the potential of blockchain technology to enhance smart city security, this study will aid in the development of an electronic voting model built on the Ethereum blockchain through the use of a smart contract. To combat both existing and emerging problems, including the proliferation of cybercrimes and attacks, [8] provides an in-depth analysis of the many ways blockchain technology is being used to secure online transactions. As part of the evaluation, we look into the potential effects of blockchain technology on online data and information.

The following were among our contributions: (i) providing an overview of the Blockchain technology and models as they pertain to cybersecurity; (ii) categorizing and addressing current and pertinent works on blockchain-based cyber countermeasures; (iii) assessing the primary hurdles and difficulties of blockchain technology in relation to cybersecurity and cyber defense; and (iv) proposing solutions and directions for future research regarding the integration of blockchain-based cyber defense. In the 2022 Kenyan election, researchers looked at data collection, outcomes transmission servers (RTS), and management concerns related to information security in the context of biometric voter registration (BVR) technology, a hybrid system for voting and results transmission, and the process of authenticating voter

registration. Additionally, this research examines voting platforms in the US and provides evidence of cyberattacks on local and state networks, as well as attempts to compromise election cybersecurity. In comparison to blockchain-secured BVR and virtualized platforms, conventional data centers are shown to be both expensive and inefficient. Filling this informational void, the authors of [10] investigate blockchain technology in the context of an organization's identity management system. This paper provides a thorough introduction to the topic in an effort to help readers grasp it better. It seeks to clarify if the claims made about blockchain technology, in particular about its ability to solve problems with identity management, are grounded in reality or merely hype. The research methodology of meta-synthesis was employed to synthesize the 69 publications that were chosen qualitatively from reputable academic sources. Theoretical evidence is showing up to back up some of the claims, but it's not always helpful in an industrial setting. The research shows that blockchain is still in its early stages, which makes one wonder if it's really practicable for organizations to use blockchain-based distributed identity management. In order to direct future studies, the authors propose a research model named TOE-BDIDM.

III.PROPOSED WORK

Concerning identification in a public blockchain structure, the binding of electronic identities within the blockchain a pair of public and private keys is vital. The private key creates the public key address, and the actual identity of the person or individuals behind those pairings is what matters most. Users are very concerned about the security of private keys.

The difficulty with using blockchain technology for electronic voting is that it cannot verify the identities of participants, which is necessary for an electronic voting system to ensure that only eligible voters can cast ballots. In the meantime, voting must be anonymous so that no one knows who voted for whom, and voters should be able to see how they voted without having to reveal their identity or explain their decision to prevent any kind of manipulation [16], [17].

As a solution, we propose an off-chain voter administration system that authorities may use to confirm voters' identities before they cast their ballots. We used cutting-edge identity verification technologies based on facial biometrics while liveness detection since voters are required to register in the voting phase and provide authorities with identification for this verification to be done automatically. Applicants will be required to provide a national electronic identification card (NEIC) as identification. This card will include a photo of the applicant as well as their qualifications, which can be easily verified by authorities. We opted for facial recognition as a biometric since almost everyone has a digital camera on their phone or PC. There may be other biometrics that need for specialized tools that are hard to come by.

1. Proposed System Deisgn

An already-established electronic voting method, Prêt à Voter, forms the foundation of the suggested system. Privacy, eligibility, ease, lack of receipts, and verifiability are some of the particular needs that went into designing the system to enable a voting application in a real-world setting. Reliable digital voting without sacrificing usability is the goal of the suggested solution. Within this framework, the system is built with a web-based interface that allows users to easily interact with security mechanisms like fingerprinting that prevent duplicate voting. A straightforward administrator interface is put in place to provide easy access in order to manage the voters, constituencies, and candidates for constituencies. In addition, the approach ensures that all voters have equal opportunities to participate, fosters a level playing field among all candidates, and protects voters' confidentiality. In order to verify the casting of a vote, which may thereafter be traced even when the constituency is not in session, the voter is sent an email with the digital hash of the transaction (ID).

2. Detailed Description of the Layered Approach

In order to achieve a modular design, the suggested electronic voting system, as shown in Fig. 1, has been separated into many levels. What follows is a description of these tiers; Interaction with Users and Front End It is the responsibility of the security layer to communicate with both the administrator (to facilitate the administration of the election) and the voter (to facilitate the casting of votes). To make sure that only authorized users (such as administrators and voters) may access the system, it combines two important functions: authentication and authorization. These regulations dictate who can and cannot use the system. From the most basic username/password system to more complex ones like fingerprint or iris

recognition, there is a wide range of options for accomplishing this task. In light of this, they become implementation-dependent aspects of the proposed design. Verifying user credentials by system-specific standards is the responsibility of this layer, which acts as the initial point of interaction with users. To ensure that layers two and three can carry out their intended tasks, the Access Control Management layer is designed to provide the necessary services. Definitions of roles, access control restrictions for those roles, and voting transactions are all part of these services. Layer 3's blockchain-based transaction mapping along with mining is supported by voting transaction definitions, whereas layer 1's access control operations are supported by role definition and maintenance.

In sum, this layer provides the necessary foundations for individual levels, allowing the proposed system to work coherently. At its foundational level, the e-Voting Transaction Management layer maps the voting transactions built at the Role Management / Transactions layer onto the blockchain transactions that are ready to be mined. An additional piece of information included in this mapped transaction is the voter's layer 1 authentication credentials. Data such as a voter's fingerprints is one example. This information is then used to generate the cryptographic hash and add to the transaction ID.

At the User Interaction with the Front-end Security layer (layer 1), it is intended to do the credential verification. For this transaction to be added to the chain, mining involves an assortment of virtual nodes. A preexisting database technology is used by the Ledger Synchronization layer to synchronize the Multichain ledger using the local application-specific database. The database's backend data tables keep track of votes. The moment a voter's vote is mined and recorded to the blockchain ledger, they are given a unique identification that they may use to trace their vote. Blockchain technology, which uses cryptographic hashes to safeguard end-to-end communication, is the basis for the votes' security concerns. The application's database also stores voting results for future use in audits and other processes.

3. Voting Process

Based on our present system implementation, we will now detail a typical user interaction with the suggested approach. In most systems, a voter's thumb imprint serves as the login. Following the discovery of a match, the voter is given the opportunity to cast their vote against any of the offered candidates. If the match doesn't work, however, you won't be able to visit again. To do this, we use a combination of a specified role-based access control system and an authentication technique (fingerprinting in our example). In addition, the idea is to utilize a voter's designated constituency to compile a list of candidates for whom they might cast a ballot. This study does not include the process of assigning voters to constituencies as it is an offline operation. Multiple miners validate each vote once it has been successfully cast, and only then are the legitimate and validated votes added to the public ledger.

Blockchain technology, which employs cryptographic hashes to provide end-to-end verification, is the foundation of the votes' security concerns. Based on this logic, the voting app's blockchain records a valid vote as a transaction. Consequently, a vote is recorded in the database's backend tables and uploaded to the blockchain as a fresh block (after successfully mining). The system guarantees that voting methods adhere to the notion of "one person, one vote" (democracy). In order to avoid the possibility of duplicate votes, this is accomplished by comparing each voter's distinct fingerprint at the start of each voting attempt.

The miners, who are distinct for every vote, immediately create a transaction upon mining the vote. Miners will reject a vote if they determine it is harmful. Once the validation procedure is complete, the voter will get a quick notice by message or email. This communication will include the transaction ID that was set before, allowing the user to trace their vote in the ledger. This serves as a notice for the voter, but it prevents others from accessing their voting information, ensuring their privacy. To be clear, a voter's cryptographic hash is their distinct hash that is used to identify them on the blockchain. The total voting process may be more easily verified using this attribute. The anonymity of individual voters is further ensured by the fact that not even the system operator has access to this hash.

III.RESULTS & DISCUSSION

1. Implementation

An online application was developed to facilitate user interaction and operate as the front end for the proposed system, which has been tested in a controlled setting. The application is hosted by a native Glassfish server and is developed using Java EE inside the Netbeans environment. The application's

EJBs and data source were housed in a server-side container that Glassfish maintained. Information on voters, their constituencies, and the various political parties participating in the election is stored in MySQL, the application's backend database.

This data is input manually by an administrator. Figure 2 shows a snapshot of the program that shows the administrator feature that allows them to examine the list of qualified voters. Given the magnitude of the data involved in actual voting situations, the program allows for both human input and bulk import via Microsoft Excel spreadsheets. For this application's private blockchain that records voting transactions, we have employed Multichain as the blockchain platform. This platform's user-friendliness was a deciding factor, and it fit right in with our suggested design.

2. Evaluation and Experimentation

Evaluating the system's performance in light of the e-voting system demands laid forth in section 2 and spotting any issues related to its practical implementation were the main goals of the assessment. The experiment included many phases, such as mining transactions into the blockchain, verifying transactions, completing numerous transactions, reflecting changes made to the public ledger to all nodes in the network, and evaluating the system's usefulness. Starting with asset generation, a test run was conducted immediately at Multichain. As shown in Figure 3, this has an effect. It is possible to call these assets votes. We built our APIs with voting in mind since Multichain is naturally well-suited to cryptocurrencies. In order to complete a Multichain transaction, we found the address and balance of the Multichain node that would send the asset (vote).

The transaction hash, which contains the vote transfer, was produced as the asset was being sent to the address. One vote (asset) was added to the receiving node's balance. The mining process is shown by the transaction's inclusion in the public ledger. As shown in Figure 2, the proposed system includes an example transaction. An address can only have one vote (asset) via our specialized API for asset generation. Therefore, a voter cannot cast multiple votes unless the node gets them from another address, which is only permitted for candidates.

The following are the characteristics of a transaction:

(1) From: The account that starts the transaction, which is the sender's 20-byte address (user on the Ethereum network).

(2) To: The account that gets the money—the 20-byte recipient addresses—which may be an EOA, a smart contract account, or nothing at all

(3) The value is the sum of all Wei funds that may be transferred to an EOA or smart contract account, where 1 ether is equal to 1018 Weis. Wei stands for the lowest possible denomination of ether, the virtual token that users may deal with on the Ethereum network. An other perspective holds that a single wei is equivalent to a quintillionth of an ether.

(4) Information: This is for the purpose of launching and carrying out the contract.

(5) Gas prices: The total of Wei per gas unit.

(6) The gas limit is the maximum amount of gas that may be spent on a single transaction.

But there are a few problems and restrictions with this search that might lead to interesting new directions for research. To begin, there's the matter of whether or not all qualified voters can use blockchain-based electronic voting. Voters with impairments, limited access to new technologies, or no prior experience using the Internet should have this given greater weight. In addition, all types of voters should be able to easily and positively engage with the electronic voting system. Secondly, there is the matter of verifying and registering to vote.

There is some discussion about this issue in several blockchain-based electronic voting systems. In the context of blockchain-based electronic voting systems, it would be fascinating to talk about biometrics, the internet of things, and other safe and practical methods of voter registration with verification. As a third point, the scalability of online voting is an important consideration.

The transaction confirmation time for a blockchain-based electronic voting system is negatively correlated with the number of voters, hence a system with a low number of voters will be cheaper. In the article, we covered this topic by discussing how Hyperledger sharding can be used to divide a blockchain network into smaller networks. This helps prevent longer transaction confirmation times. However, when analyzing the cost of blockchain-based e-voting systems, scalability is still a crucial factor to consider. Lastly, it would be interesting to investigate a different critical problem; including how well it works with other systems, if all types of voters can use it, and how voters trust it in comparison to other technology for voting and conventional methods.

IV.CONCLUSION

There have been several versions of electronic voting since the 1970s, and the main advantages over paper-based systems, such as enhanced efficiency and decreased mistakes, remain. The tremendous rise of blockchain technology has prompted many efforts to investigate the possibility of applying blockchain to assist an efficient solution to electronic voting. An efficient solution to electronic voting may be achieved by using the features of blockchain technology, such as its cryptographic underpinnings and transparency. This article presents one such endeavor. After implementing the technique using Multichain, it was thoroughly evaluated to ensure it effectively meets the core criteria of an electronic voting system.

Our current efforts are focused on enhancing blockchain technology's resilience against the "double spending" issue, which may be seen as "double voting" in electronic voting systems. We are motivated to examine blockchain technology further because, while it has shown to be quite effective at detecting transactions with changeable changes, there has been successful proof of such occurrences. In order to accomplish an end-to-end traceable e-voting scheme, it is important to have a reliable model for establishing the provenance of e-voting systems. In order to do this, an extra provenance layer is being developed to supplement the current blockchain-based infrastructure.

References

[1] Matulevicius, N., & Cordeiro, L.C. (2021). Verifying Security Vulnerabilities For Blockchain-Based Smart Contracts. 2021 Xi Brazilian Symposium On Computing Systems Engineering (Sbesc), 1-8.

[2] Khalane, P.S., Tupe, B., Patil, P., Bhardwaj, S., & Wagh, M. (2023). Survey On Decentralized Democracy: Blockchain Voting System. Interantional Journal Of Scientific Research In Engineering And Management.

[3] Manukonda, K.R. (2022). Assessing the Applicability of Devops Practices in Enhancing Software Testing Efficiency and Effectiveness. Journal of Mathematical & Computer Applications.

[4] Manukonda, Kodanda. (2020). Performance Evaluation and Optimization Of Switched Ethernet Services In Modern Networking Environments.

[5] Manukonda, Kodanda. (2020). Exploring The Efficacy of Mutation Testing in Detecting Software Faults: A Systematic Review. 7. 71-77. 10.5281/zenodo.11408273.

[6] Selvarajan, S., & Mouratidis, H. (2023). A quantum trust and consultative transaction-based blockchain cybersecurity model for healthcare systems. Scientific Reports, 13.

[7] Manukonda, Kodanda. (2020). Efficient Test Case Generation using Combinatorial Test Design: Towards Enhanced Testing Effectiveness and Resource Utilization. 7. 78-83.

[8] Park, S., Specter, M.A., Narula, N., & Rivest, R.L. (2021). Going from bad to worse: from Internet voting to blockchain voting. J. Cybersecur., 7.

[9] Chentouf, F.Z., & Bouchkaren, S. (2023). Security and privacy in smart city: a secure e-voting system based on blockchain. International Journal of Electrical and Computer Engineering (IJECE).

[10] Manideep, Y. Examining Partitioned Caches Performance in Heterogeneous Multi-Core Processors. International Journal of Communication and Information Technology, 3, 31-35.

[11] Singh, d. P. (2022). An efficient system for customer relationship management on churn prediction using machine learning technique. International journal of core engineering & management, 7(04), 19–34.

[12] Yenugula, M., Kodam, R., & He, D. (2019). Performance and load testing: Tools and challenges. International Journal of Engineering in Computer Science, 1, 57-62.

[13] Yenugula, M. Data Center Power Management Using Neural Network. International Journal of Advanced Academic Studies, 3, 320-25.

[14] Sethy, N. K., Yenugula, M., Goswami, S. S., Bhola, A., & Behera, D. K. (2023). Selection of Ideal IoT-Based Overhead Conductor for Optimizing the Performance of a Small Hydropower Project.

[15] Singh, d. P. (2023). Forecasting of supermarket sales using big data analytics and machine learning techniques in business sector. International journal of core engineering & management, 7(06), 18–30.

[16] Yenugula, M. Examining partitioned caches performance in heterogeneous multi-core processors.

[17] Kshetri, N., Bhushal, C.S., Pandey, P.S., & Vasudha (2022). BCT-CS: Blockchain Technology Applications for Cyber Defense and Cybersecurity: A Survey and Solutions. International Journal of Advanced Computer Science and Applications.

[18] Irungu, J., & Girma, A. (2023). Cybersecurity and Electoral Processes. An Analysis of Block Chain Enabled Biometric Voter System and Risk Control

in Kenya's 2022 Electoral Process and the United States Election System Infrastructure. 2023 14th International Conference on Information and Communication Technology Convergence (ICTC), 687-694.

[19] Mulaji, S.M., & Roodt, S. (2021). The Practicality of Adopting Blockchain-Based Distributed Identity Management in Organisations: A Meta-Synthesis. Security and Communication Networks.