IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 16, May 2023

A Voting System with Blockchain Technology

Aashif K[1], Anjana V[2], Vrishab N[3], Shimna P T[4]
Students, Department of Computer Science & Engineering[1,2,3]
Asst. Professor, Department of Computer Science & Engineering[4]
KMCT College of Engineering, Calicut, Kerala, India

Abstract: *A voting system based on blockchain technology is an innovative method to ensuring secure and transparent elections. As a distributed ledger technology, blockchain can do away with the need for middlemen and offer a decentralised architecture that makes secure and open vote counting possible. Each vote in a voting system based on a blockchain is recorded as a transaction on the blockchain, which cannot be changed or interfered with. Through the use of cryptography, the voter's identity is made anonymous, and the blockchain's consensus algorithm ensures the validity of the vote. In addition, a blockchain-based voting system can be made even more secure by incorporating biometric authentication, which guarantees that only authorised users are permitted to cast ballots. To identify a person, biometric identification uses distinctive physical or behavioural traits like fingerprints, iris scans, or facial recognition. Voters in a blockchain-based voting system can securely authenticate their identity and guarantee that their vote is counted correctly by employing biometric authentication. Because their identity can be checked in real-time against the recorded biometric data, the use of biometric authentication can also deter people from trying to cast multiple ballots or pose as other voters.*

Keywords: Blockchain, Voting System, Biometric Authentication, Security

I. INTRODUCTION

A democratic system's core component, elections allow the entire people to express their opinions by voting. Elections are important to our society, so the process should be open and trustworthy to reassure participants of its legitimacy. The method of voting has been a dynamic area within this setting. The main force behind this progress is the goal to make the system visible, verifiable, and secure. Given its importance, ongoing attempts have been made to increase the voting system's overall effectiveness and robustness. E-voting, often known as electronic voting, is crucial in this. E-voting systems have advanced significantly since they were originally implemented as punched-card ballots in the 1960s because to the use of internet technologies.To ensure widespread acceptance, e-voting systems must abide by a set of baseline standards. These criteria include, among others, the voter's anonymity, the validity of the vote, and non-repudiation. One of the cutting-edge technologies, blockchain has solid cryptographic underpinnings that enable apps to take advantage of these capabilities to produce robust security solutions. A blockchain is similar to a data structure that stores and distributes all of the transactions that have been carried out since its inception. It functions primarily as a distributed decentralised database that keeps an exhaustive list of continuously accumulating and expanding data records protected from unauthorised manipulation, tampering, and alteration. at core.ac.uk, you may find blockchain CORE metadata, citations, and related studies. Every user can join to the network, transmit new transactions there, and validate transactions thanks to UWL Repository's provision. and add additional blocks (Nakamoto, 2009; Kadam et al., 2015; Rosenfeld, 2017). As long as the content in a block is not changed, a cryptographic hash that can also be thought of as a fingerprint of the block is assigned to each block. If the block is altered in any way, the cryptographic hash will immediately change, indicating that the data has changed, possibly because of malicious activity. As a result, blockchain has been utilised more frequently to prevent unauthorised transactions across a variety of areas due to its solid cryptographic foundations (Nakamoto, 2009; Kraft, 2015; Narayanan et al, 2015). Although the most notable blockchain application is still Bitcoin, researchers are eager to investigate how blockchain technology might be used to assist applications across various areas are making use of advantages like non-repudiation, integrity, and anonymity. In this article, we examine how blockchain technology can be used to support e-voting applications that can guarantee voter anonymity, vote integrity, and end-to-end verification. We think that basic blockchain properties like the self-

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 16, May 2023

cryptographic validation structure of transactions (via hashes) and the openness of the distributed ledger of records can be used to benefit e-voting. Due to its intrinsic ability to preserve anonymity, maintain a decentralised and publicly distributed record of transactions across all nodes, and play a significant role in the field of electronic voting, blockchain technology can be extremely useful. Due to this, blockchain technology is particularly effective at addressing the risk of using a voting token more than once as well as attempts to sway the outcome's transparency.

II. PROPOSED SYSTEM DESIGN

The system has been created to support a voting application in a real-world context while taking into account specific needs like as privacy, eligibility, convenience, receipt-freeness, and verifiability. With the suggested approach, safe digital voting is achieved without sacrificing usability. In this regard, the system is created with a web-based interface to simplify user interaction with security features like finger printing to prevent double voting. A user-friendly administrator interface is designed to facilitate ease of access because there is an obvious need to administer the voters, constituencies, and candidates for constituencies. Additionally, the approach maintains voter privacy while granting all voters equal participation rights and encouraging fair and healthy competition among all the candidates.

Text Font of Entire Document

The entire document should be in Times New Roman or Times font. Type 3 fonts must not be used. Other font types may be used if needed for special purposes.
Recommended font sizes are shown in Table 1.

Title and Author Details

Title must be in 24 pt Regular font. Author name must be in 11 pt Regular font. Author affiliation must be in 10 pt Italic. Email address must be in 9 pt Courier Regular font.
All title and author details must be in single-column format and must be centered. Every word in a title must be capitalized except for short minor words such as “a”, “an”,“and”, “as”, “at”, “by”, “for”, “from”, “if”, “in”, “into”, “on”, “or”, “of”, “the”, “to”, “with”.
Author details must not show any professional title (e.g. Managing Director), any academic title (e.g. Dr.) or any membership of any professional organization (e.g. Senior Member IEEE).
To avoid confusion, the family name must be written as the last part of each author name (e.g. John A.K. Smith).
Each affiliation must include, at the very least, the name of the company and the name of the country where the author is based (e.g. Causal Productions Pty Ltd, Australia).

III. DETAILED DESCRIPTION OF APPROACH

Front-end interaction with users The security layer is in charge of communicating with the voter (to facilitate voting operations) and the administrator (to assist election administration duties). It combines two essential tasks, namely user authentication and authorization (for voters and administrators), to guarantee that only authorised users have access to the system in accordance with established access control regulations. This function can be accomplished using a variety of techniques, from straightforward username/password authentication to more sophisticated techniques like fingerprint or iris recognition. As a result, they become unique to each implementation of the suggested architecture. Overall, this layer acts as the first point of contact with users and is in charge of authenticating their credentials in accordance with applicable laws.
By offering the services necessary for layer 1 and layer 3 to perform as expected, the access control management layer is intended to facilitate these layers. Role’s definition, the corresponding access control rules, and voting transaction definitions are all included in these services. The layer 1 access control functions are fundamentally supported by role definition and maintenance, whereas layer 3 mining and transaction mapping on a blockchain are supported by voting transaction definitions. Overall, by providing the support needed by other layers, this layer enables the proposed system to work coherently.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 16, May 2023

The transaction for evoting created at the Role Management / Transactions layer is mapped onto the blockchain transaction that needs to be mined at the e-Voting Transaction Management layer, which is the fundamental layer of the design. The authentication credentials supplied by a voter at layer 1 are also included in this mapped transaction. The Voter's fingerprint is one example of this data. The transaction ID is then generated using this data, which is also used to generate the cryptographic hash. The User Interaction and Front-end Security layer (layer 1) is where it is intended to be possible to verify such credentials. To finally add this transaction to the chain.

Using one of the current database technologies, the Ledger Synchronisation layer synchronises the Multichain ledger with the local application-specific database. The data tables at the database's backend keep track of votes cast. As soon as a vote is mined and uploaded to the blockchain ledger, voters are given a unique identification that allows them to track their votes. Voting security is built on block-chain technology, which secures end-to-end communication using cryptographic hashes. In order to enable audits and any subsequent procedures, voting results are also saved in the application's database.

IV. VOTING PROCESS

By entering his or her thumbprint, a voter logs into the system. If a match is discovered, the voter is then shown a list of potential opponents and given the chance to vote against them. On the other hand, any additional access would be refused if the match is unsuccessful. The proper implementation of the authentication technique (in this example, fingerprinting) and role-based access control management are used to accomplish this purpose. Additionally, it is also envisioned that each voter will be assigned to a certain constituency, and that this data will be utilised to create a list of candidates for that voter to choose from. Voter assignment to a constituency is now an offline operation, making it outside the purview of this study.

After a vote is successfully cast, it is validated by several miners, and then the valid and verified votes are added to the public ledger. Blockchain technology is the foundation for the security considerations of the votes, and cryptographic hashes are used to guarantee end-to-end verification. To this aim, a valid vote cast is regarded as a transaction within the voting application's blockchain. A vote is thus stored in data tables in the database's backend and added as a new block (after successful mining) on the blockchain. Only the one-person, one-vote principle is guaranteed by the system. This is accomplished by using the individual fingerprint of each voter, which is compared at the start of each voting attempt to prevent double voting.As soon as a vote is mined by the miners, a transaction is generated that is specific to each vote. The vote is discarded by miners if it is determined to be fraudulent.

Following the confirmation procedure, the voter is immediately notified through text message or email with the above-described transaction id, allowing them to follow their vote as it is recorded in the ledger. Although this serves as a notification to the voter, it prevents any user from being able to extract information about how a given voter voted, ensuring the voter's privacy.It is crucial to remember that a voter's cryptographic hash is the only way for that voter to be identified on the blockchain. The total voting process may be verified more easily because to this characteristic. Additionally, this ID is concealed and inaccessible—not even a system administrator can see it—ensuring voter anonymity..

V. CONCLUSION

Electronic voting has been used in various forms since the 1970s, with significant advantages over paper-based systems such as enhanced efficiency and fewer errors. Numerous efforts have been made to investigate the viability of using blockchain to support an efficient solution to e-voting in light of the phenomenal development in the use of blockchain technologies. This paper describes one such endeavor that makes use of blockchain's advantages, including its transparency and cryptographic underpinnings, to find a workable solution to e-voting. The proposed method has been implemented with Multichain, and a thorough analysis of the method shows that it is effective in satisfying the essential conditions for an electronic voting system. We are continuing our effort with the goal of strengthening blockchain technology's resilience to "double spending"andfor e-voting systems, this will translate as "dual voting." Although detecting malleable change in a transaction using blockchain technology is very successful, successful demonstrations of such events have been made, which encourages us to look into it more. In order to accomplish an end-to-end verifiable e-voting scheme, we believe an efficient approach to establish reliable provenance for e-voting systems will

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 16, May 2023

be essential. This goal is being worked upon by creating an additional provenance layer to support the current blockchain-based infrastructure.

REFERENCES

[1] Adida, B.; 'Helios (2008). Web-based open-audit voting, in Proceedings of the 17th Conference on Security Symposium, ser. SS'08. Berkeley, CA, USA: USENIX Association, 2008, pp. 335{348.

[2] Adida B. and Rivest, R. L. (2006). Scratch & vote: Self-contained paper-based cryptographic voting, in Proceedings of the 5th ACM Workshop on Privacy in Electronic Society, ser. WPES '06. New York, NY, USA: ACM, 2006, pp. 29-40.

[3] Bell, S., Benaloh, J., Byrne, M. D., Debeauvoir, D., Eakin, B., Kortum, P., McBurnett, N., Pereira, O., Stark, P. B., Wallach, D. S., Fisher, G., Montoya, J., Parker, M. and Winn, M. (2013). Star-vote: A secure, transparent, auditable, and reliable voting system, in 2013 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 13). Washington, D.C.: USENIX Association, 2013.

[4] Bohli, J. M., Muller-Quade, J. and Rohrich, S. (2007). Bingo voting: Secure and coercion- free voting using a trusted random number generator, in Proceedings of the 1st International Conference on E-voting and Identity, ser. VOTE-ID'07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 111-124.

[5] Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, A. and Vora, P. (2008) Scantegrity: End-to-end voter-veri_able optical- scan voting, IEEE Security Privacy, vol. 6, no. 3, pp. 40- 46, May 2008