IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125109

IMPLEMENTATION OF THE ETHEREUM ALGORITHM TO MONITOR THE E-VOTING SYSTEM AND DATA STORAGE USING BLOCKCHAIN

Revathi TP[1], Sindhu M[2], Sivaranjani E[3]

Department of Computer Science, Anna University, Chennai[1-3]

Abstract: Electronic voting systems have gained significant attention due to their potential to streamline the voting process, increase accessibility, and reduce fraud. However, ensuring the integrity, security, and transparency of the voting process remains a critical challenge. Blockchain technology has emerged as a promising solution to address these concerns by providing a decentralized, immutable, and transparent ledger system.This abstract presents an e-voting system that leverages blockchain technology to enhance the security, transparency, and efficiency of the voting process. The proposed system utilizes a permissioned blockchain, ensuring that only authorized participants can participate in the consensus and validation process.Each eligible voter is assigned a unique cryptographic identity and can securely cast their vote through a user-friendly interface. The vote is recorded as a transaction on the blockchain, which includes a digital signature and timestamp to ensure its authenticity and immutability. The votes are anonymized to preserve voter privacy while maintaining the ability to verify the integrity of the overall election process.

Keywords: electronic voting, e-voting, blockchain, e-government, verifiable voting

I . INTRODUCTION

Elections are a fundamental pillar of a democratic system enabling the general public to express their views in the form of a vote. Due to their significance to our society, the election process should be transparent and reliable so as to ensure participants of its credibility. Within this context, the approach to voting has been an ever-evolving domain. This evolution is primarily driven by the efforts to make the system secure, verifiable and transparent. In view of its significance, continuous efforts have been made to improve the overall efficiency and resilience of the voting system. Electronic voting or e-voting has a profound role in this. Since its first use as punched-card ballots in the 1960s, e-voting systems have achieved remarkable progress with their adaptation using the internet technologies (Gobel et al, 2015). However, e-voting systems must adhere to specific benchmark parameters so as to facilitate its widespread adoption. These parameters include the anonymity of the voter, the integrity of the vote and non-repudiation among others. Blockchain is one of the emerging technologies with strong cryptographic foundations enabling applications to leverage these abilities to achieve resilient security solutions. A Blockchain resembles a data structure which maintains and shares all the transactions being executed through its genesis. It is primarily a distributed decentralized database that maintains a complete list of constantly germinating and growing data records secured from unauthorized manipulation, tampering and revision

II . LITERATURE SURVEY

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. This paper proposes an associated justify an adequate security model and criteria to judge comprehensibility. It additionally describes a web ballot theme, Pretty Graspable Democracy, showing that it satisfies the adequate security model which it’s a lot of graspable than Pretty Smart Democracy, presently the sole theme that additionally satisfies the planned security model.

2. Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, A. and Vora, P. (2008).“Scantegrity: End-to-end voter-verifiable optical- scan voting.", IEEE Security Privacy, vol. 6, no. 3, pp. 40-46, May 2008. This paper describes Scantegrity that minimally impacts election procedures and is the first independent E2E verification mechanism that preserves optical scan as the underlying voting system and doesn’t interfere with a manual recount.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.125109

3. Dalia, K., Ben, R. , Peter Y. A, and Feng, H. (2012). "A fair and robust voting system by broadcast.", 5th International Conference on E-voting, 2012. This paper proposes a recovery round to enable the election result to be announced if voters abort and also added a commitment round to ensure fairness. In addition, it also provided a computational security proof of ballot

4. 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

5 . S. Shukla, A. N. Thasmiya, D. O. Shashank, and H. R. Mamatha, "Online voting application using ethereum blockchain," in 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 873–880, Bangalore, India, September 2018.

6 . M. Achieng and E. Ruhode, "The adoption and challenges of electronic voting technologies within the South African context," International Journal of Managing Information Technology, vol. 5, no. 4, pp. 1–12, 2013.

7 . S. Nichter, "Vote buying or turnout buying? Machine politics and the secret ballot," American Political Science Review, vol. 102, no. 1, pp. 19–31, 2008.

8 . S. Komatineni and G. Lingala, "Secured E-voting system using two-factor biometric authentication," in Proceedings of the 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), pp. 245–248, Iccmc, Erode, India, March 2020.

9 . M. G. Gurubasavanna, S. Ulla Shariff, R. Mamatha, and N. Sathisha, "Multimode authentication based electronic voting kiosk using raspberry pi," in Proceedings of the International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC, pp. 528–535, Palladam, India., September 2018.

10 . A. Khelifi, Y. Grisi, D. Soufi, D. Mohanad, P. V. S. Shastry, and " M-Vote, "M-Vote: a reliable and highly secure mobile voting system," in 2013 Palestinian International Conference on Information and Communication Technology, pp. 90–98, Gaza, Israel, April 2013.

III . E-VOTING BACKGROUND AND REQUIREMENTS

Electronic voting has been an area of research focus for many years by using computing machines and equipment for casting votes and producing high quality and precise results in accordance with the sentiments of the participating voters. Various attempts have been adopted in practice to support election process. Initially computer counting system allowed the voter to cast vote on papers. Later on, those cards went through the process of scanning and tallying at every polling cell on a central server . Direct Recording Electronic (DRE) voting systems were put in place later on which were admired and acknowledged greatly by the voters in-spite of the resistance from computer scientists. If the voting system is well understood by the voters, the system's usability can be increased remarkably. DRE systems in particular have gathered a lot of successes in bringing the voters to use this technology. These systems work more or less in the same way as any conventional election system does. In the case of DRE, a voter begins his journey by going to their polling place and get their token to vote where he utilizes his token at the voting terminal to vote for his candidate. When the candidate selection procedure is completed, DRE systems present the final selection to the voter before actually casting it (in case if the voter wants to change his opinion) and after the final selection, the ballot casting is completed.

IV . EXISTING SYSTEM

Anonymous vote-casting: Each vote may or may not contain any choice per candidate, should be anonymous to everyone including the system administrators, after the vote is submitted through the system.

Individualized ballot processes: How a vote are depicted within the involving net applications or databases continues to be AN open discussion. whereas a transparent text message is that the worst plan, a hashed token is wont to offer obscurity and integrity. Meanwhile, the vote ought to be non-reputable, that can't be bonded by the token resolution.

Ballot casting verifiability by (and only by) the voter: The elector ought to be ready to see and verify his/her own vote, when he/she submitted the vote. this is often vital to realize so as to forestall, or a minimum of to note, any potential malicious activity. This counter live, except for providing suggests that of non repudiation, can sure boost the sensation

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.125109

of trust of the voters. These issues area unit partly self-addressed in some recent applications. Yet, suggests that of e-voting is presently in use in many countries together with Brazil, uk, Japan, and Republic of Estonia. Republic of Estonia 2 ITM Web of Conferences 32, 03001 (2020)

High initial setup costs: Though sustaining and maintaining on-line selection systems is way cheaper than ancient elections, initial deployments could be pricy, particularly for businesses.

V . PROPOSED SYSTEM

Privacy - Keeping an individual's vote secret
The system leverages the cryptographic properties of blockchain to achieve the privacy of a voter. More specifically, as a voter is registered into the system, a voter hash is generated by the blockchain which is the unique identifier of a voter into the blockchain and is protected from misuse due to the collision resistance property of the cryptographic hash. Due to this, the traceability of a vote is also non-trivial thereby protecting the voter when under duress.

Eligibility - Allowing only registered voters to vote, with each such voter voting only once
All eligible users are required to register using unique identifiers such as government-issued documents to assert their eligibility. In addition to this, our system implements a strong authentication mechanism using

Receipt Freeness - Voters should be unable to prove to a third party that they voted in a particular way
The proposed system enables a voter to vote as per their choice and creates a cryptographic hash for each such event (transaction). This is important to achieve verifiability i.e. to verify if a certain vote was included in the count. However, possession of this hash does not allow to the extraction of information about the way the voter has voted.

Verifiability - The ability to trust the vote tallying process
Upon casting their vote successfully, a user is provided with their unique transaction ID in the form of a cryptographic hash. A user can use this transaction ID to track if their vote was included in the tallying process. However, this process does not enable a user to view how they voted which has been adopted to mitigate threats when under duress.

VI . IMPLEMENTATION

The implementation of the proposed system has been carried out within a controlled environment with a web page created to serve as the front end application enabling the users to interact in a convenient manner. This application is implemented within the Netbeans platform with native Glassfish server used for hosting the application. Glassfish managed server side container for holding the application's EJBs and the data source. The application uses a MySQL as the backend database for the application and contains the data entered manually by an admin such as the voter details, constituency details and the information about different political parties running for the election. An application screenshot demonstrating the admin function to view list of eligible voters is presented in Fig. 2. In addition to manual entries, the application also supports importing data using MS Excel spread sheets to perform bulk import in view of the size of the data in real-world voting scenarios. We have used Multichain as the blockchain platform to create a private blockchain for this application which is used for recording the voting transactions. This choice is influenced by the ease of use provided by this platform and therefore it was easily integrated into our proposed architecture.

VII . EVALUATION AND EXPERIMENTATION

The primary objective of evaluation was to assess the performance of the system in view of the e-voting system requirements presented in section 2 and to identify any considerations with regards to its application in a real world scenario. The experimentation consisted of multiple steps i.e. conducting multiple transactions, verification of transactions, mining transactions into blockchain, reflection of the changes made in the public ledger to all the nodes in the network and the usability of the system.

 This work is licensed under a Creative Commons Attribution 4.0 International License

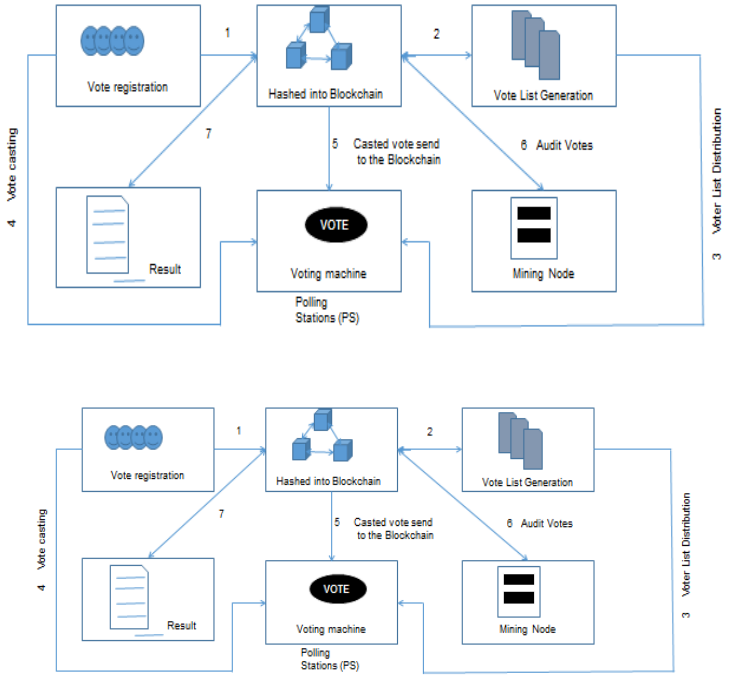
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125109

VIII . SYSTEM ARCHITECTURE



IX . CONCLUSION AND FUTURE WORK

Electronic voting has been used in varying forms since 1970s with fundamental benefits over paper based systems such as increased efficiency and reduced errors. With the extraordinary growth in the use of blockchain technologies, a number of initiatives have been made to explore the feasibility of using blockchain to aid an effective solution to e-voting. This paper has presented one such effort which leverages benefits of blockchain such as cryptographic foundations and transparency to achieve an effective solution to e-voting.

The proposed approach has been implemented with Multichain and in- depth evaluation of approach highlights its effectiveness with respect to achieving fundamental requirements for an e-voting scheme. In continuation of this work, we are focused at improving the resistance of blockchain technology to 'double spending' problem which will translate as 'double voting' for e-voting systems. Although blockchain technology achieves significant success in detection of malleable change in a transaction however successful demonstration of such events have been achieve which motivates us to investigate it further. To this end, we believe an effective model to establish trustworthy provenance for e-voting systems will be crucial to achieve an end-to-end verifiable e-voting scheme. The work to achieve this is underway in the form of an additional provenance layer to aid the existing 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.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.125109

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
6 . Hao, F., Ryan, P. Y. A., and Zielinski, P. (2010) Anonymous voting by two-round public discussion, IET Information Security, vol. 4, no. 2, pp. 62-67, June 2010.
7 . Gobel, J., Keeler, H. P., Krzesinski, A.E. and Taylor, P.G. (2015). Bitcoin Blockchain Dynamics: the Selfish-Mine Strategy in the Presence of Propagation Delay, May 2015.
8 . Kadam, M., Jha, P. Jaiswal, S. (2015) Double Spending Prevention in Bitcoins Network, International Journal of Computer Engineering and Applications, August 2015.
9 . Kiayias, A. and Yung, M. (2002) Self-tallying Elections and Perfect Ballot Secrecy. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002, pp. 141{158.
10 . Kraft, D. (2015) Difficulty Control for Blockchain-Based Consensus System, Peer-to-Peer Networking and Applications by Springer, March 2015.

 This work is licensed under a Creative Commons Attribution 4.0 International License