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: 7.53
Volume 4, Issue 3, October 2024

Secure Digital Voting System based on Blockchain Technology

Prof. Rakesh Tannu
Department of Information Technology
JCEI's Jaihind Polytechnic Kuran, India

Abstract: *Since the 1970s, electronic voting, or e-voting, has been employed in a variety of forms and offers several advantages over paper-based systems, including more efficiency and fewer errors. Widespread acceptance of such systems is still difficult to accomplish, though, particularly when it comes to enhancing their resilience to potential flaws. Blockchain is a cutting-edge technology that has the potential to increase the general robustness of electronic voting systems. This paper outlines an attempt to use blockchain's advantages, namely its transparency and cryptographic underpinnings, to create a successful e-voting system. The suggested plan satisfies end-to-end verifiability and complies with the essential specifications for electronic voting systems. The suggested electronic voting system and its Multichain platform implementation are described in detail in this paper. The article provides thorough analysis of the plan that effectively shows how to create an end-to-end verified electronic voting system In summary: Since the 1970s, electronic voting, or e-voting, has been used in various forms. Its main advantages over paper-based systems include more efficiency and fewer errors. Widespread acceptance of such systems is still difficult to accomplish, though, particularly when it comes to enhancing their resilience to potential errors. Blockchain is a cutting-edge technology that has the potential to increase the general robustness of electronic voting systems. This study outlines an attempt to use blockchain's advantages—such as its transparency and cryptographic underpinnings—to create a successful electronic voting system. The suggested plan satisfies end-to-end verifiability and complies with the basic specifications for electronic voting systems*

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

I. INTRODUCTION

Elections are 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 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 1960's, e-voting systems have achieved remarkable progress with its adaption 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 anonymity of the voter, 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 manipulating, tampering and revision. Blockchain allows every user to connect to the network, send new transactions to it, verify transactions and create new blocks (Rosenfeld, 2017; Kadam et al, 2015; Nakamoto, 2009). Each block is assigned a cryptographic hash (which may also be treated as a finger print of the block) that remains valid as long as the data in the block is not altered. If any changes are made in the block, the cryptographic hash would change immediately indicating the change in the data which may be due to a malicious activity.

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: 7.53
Volume 4, Issue 3, October 2024

Therefore, due to its strong foundations in cryptography, blockchain has been increasingly used to mitigate against unauthorized transactions across various domains (Nakamoto, 2009; Kraft, 2015; Narayanan et al, 2015).

Bitcoin remains the most distinguished application of blockchain however researchers are keen to explore the use of blockchain technology to facilitate applications across different domains leveraging benefits such as non-repudiation, integrity and anonymity. In this paper, we explore the use of blockchain to facilitate e-voting applications with the ability to assure voter anonymity, vote integrity and end-to- verification. We believe e-voting can leverage from fundamental blockchain features such as self- cryptographic validation structure among transactions (through hashes) and public availability of distributed ledger of records. The blockchain technology can play key role in the domain of electronic voting due to inherent nature of preserving anonymity, maintaining decentralized and publicly distributed ledger of transactions across all the nodes. This makes blockchain technology very efficient to deal with the threat of utilizing a voting token more than once and the attempt to influence the transparency of the result.

The rest of the paper is organized as follows: the next section presents the requirements for an e-voting system as identified by (Rura et al, 2016) and explains how our proposed system fulfils them. Section 3 presents the state-of-the-art with respect to e-voting and how we contribute to it followed by a detailed description of the system design in section 4. Section 5 presents the implementation of our proposed system with Multichain and user interface along with evaluation of the system highlighting how it achieves the requirements presented in section 2. Section 6 concludes the paper identifying current progress and plans for further work.

II. 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

More recently, distributed ledger technologies such as blockchain have been used to achieve e-voting systems primarily due to their advantages in terms of end-to-end verifiability. With properties such as anonymity, privacy protection and non-repudiation, blockchain is a very attractive alternative to contemporary e-voting systems. The research presented in this paper also attempts to leverage these properties of blockchain to achieve an efficient e-voting system. A detailed analysis of such systems is presented in the next section along with the identification of comparison with these approaches.

e-Voting Requirements and Compliance by the Proposed System

The generic requirements for a typical e-voting system have been defined We present a brief description of each requirement along with an explanation of how the proposed system fulfils it.

Privacy - Keeping an individual's vote secret

The system leverages cryptographic properties of blockchain to achieve privacy of a voter. More specifically, as voter is registered into the system, a voter hash is generated by blockchain which is the unique identifier of a voter into the blockchain, and is protected from misuse due to 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

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: 7.53
Volume 4, Issue 3, October 2024

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 strong authentication mechanism using finger printing technology to assert that only authorized voters can access the system. Furthermore, the use of biometrics also enables the system to protect against double voting.

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 extract information about the way voter has voted.

Convenience - Voters must be able to vote easily, and everyone who is eligible must be able to vote

The system has been implemented using a user friendly web based interface with the voting process requiring minimal input from the user. For instance, fingerprinting is implemented for authentication mechanism to avoid the requirement to remember username/passwords. Furthermore, the overall process is integrated which enables the user to interact with it in a seamless manner.

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.

The analysis presented above highlights the performance of the proposed system with respect to the specific requirements of e-voting. It also highlights the significance of defining characteristics of blockchain and their profound role in achieving the cornerstones of an efficient e-voting system.

Therefore, we believe the work presented here makes significant contribution to the existing knowledge with respect to the application of blockchain technology to achieve a secure digital voting system.

III. RELATED WORKS

In a two round protocol is proposed that computes the tally in two rounds without using a private channel or a trusted third party. The protocol is efficient in terms of amputation and bandwidth consumption but is neither robust nor fair in certain conditions .In a protocol is proposed to improve the robustness and fairness of the two round protocol

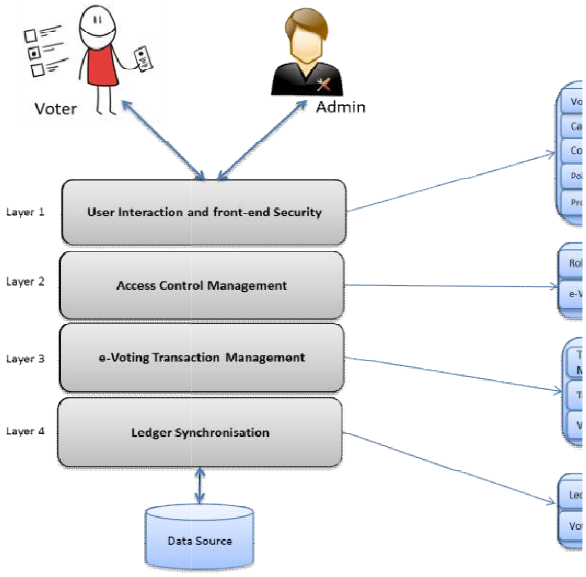

Fig. 1 Architecture for proposed e-voting system.

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: 7.53
Volume 4, Issue 3, October 2024

The existing approaches perform well for end-to-end verifiability without compromising the privacy of voters. In the implementation of decentralized and self-tallying internet voting protocol over the blockchain using Ethereum. e-voting approach as their baseline.

The focus of our research is to explore the exciting opportunities presented by blockchain technologies by investigating their application in diverse application domains. Within this context, this paper presents our efforts to develop an e-voting system by leveraging blockchain technology. To this end, our proposed scheme fulfils the specific requirements for e-voting .

IV. PROPOSED SYSTEM

The proposed e-voting system is based on the well-established Prêt à Voter e-voting approach identified in .The system has been designed to support a voting application in the real world environment taking into account specific requirements such as privacy, eligibility, convenience, receipt- freeness and verifiability. The proposed system aims to achieve secure digital voting without compromising its usability. Within this context, the system is designed using a web-based interface to facilitate user engagement with measures such as finger printing to protect against double voting. With a clear need to administer the voters, constituencies and candidates for constituencies, a user-friendly administrator interface is implemented to enable ease of access. Furthermore, the system allows all voters equal rights of participation and develops a fair and healthy competition among all the candidates while keeping the anonymity of the voters preserved. The cryptographic hash of the transaction (ID) is emailed to the voter as a proof that the vote has been casted which may later on be tracked outside the premises of the constituency.

Detailed Description of the Layered Approach

The proposed e-voting system architecture is presented in Fig. 1 and has been divided into several layers to achieve modular design. These layers are described below;

User Interaction and Front-end Security layer is responsible for interacting with a voter (to support vote casting functions) and the administrator (to support functions pertaining to administering the election process). It encapsulates two key functions i.e. authentication and authorization of the users (voters and administrators) to ensure that the access to the system is restricted to legitimate users in accordance with the predefined access control policies. A number of different methods can be applied to achieve this function ranging from basic username/password to more advanced such as fingerprinting or iris recognition. Therefore these are rendered specific to individual implementation of the proposed architecture. Overall, this layer serves as the first point of contact with the users and is responsible for validating user credentials as governed by the system-specific policies.

Access Control Management layer is envisaged to facilitate layer 1 and layer 3 by providing services required for these layers to achieve their expected functions. These services include roles definition, their respective access control policies and voting transaction definitions. The role definition and management provides core support for the access control functions implemented by layer 1 whereas the voting transaction definitions support the blockchain based transaction mapping and mining performed at the layer 3. Overall, this layer enables a coherent function of the proposed system by providing the foundations required by individual layers.

e-Voting Transaction Management layer is the core layer of the architecture where the transaction for e- voting constructed at Role Management / Transactions layer is mapped onto the blockchain transaction to be mined. This mapped transaction also contains the credentials provided by a voter at layer 1 for authentication. An example of such data can be the fingerprint of the voter. This data is then used to create the cryptographic hash and contributes towards creating the transaction ID. The verification of such credentials is envisioned to be achieved at User Interaction and Front-end Security layer (layer 1). A number of virtual instances of nodes are involved in the process of mining to get this transaction finally enter into the chain.

Ledger Synchronization layer synchronizes Multichain ledger with the local application specific database using one of the existing database technologies. Votes cast are recorded in the data tables at the backend of the database. Voters are able to track their votes using the unique identifier provided to them as soon as their vote is mined and added into the blockchain ledger. The security considerations of the votes are based on block-chain technology using cryptographic

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: 7.53
Volume 4, Issue 3, October 2024

hashes to secure end-to-end communication. Voting results are also stored in the application's database with the view to facilitate auditing and any further operations at a later stage.

The Voting Process

We now describe a typical interaction of a user with the proposed scheme based on our current implementation of the system. Typically, a voter logs into the system by providing his/her thumb impression. If the match is found, the voter is then presented with a list of available candidates with the option to cast vote against them. On the contrary, if the match is unsuccessful, any further access would be denied. This function is achieved using appropriate implementation of the authentication mechanism (fingerprinting in this case) and predefined role based access control management. Furthermore, it is also envisioned that a voter is assigned to their specific constituency and this information is used to develop the list of candidates that a voter can vote for. The assignment of voter to a constituency is rendered an offline process and therefore out of scope of this research.

After a successful vote-cast, it is mined by multiple miners for validation following which valid and verified votes are added into public ledger. The security considerations of the votes are based on blockchain technology using cryptographic hashes to secure end-to-end verification. To this end, a successful vote cast is considered as a transaction within the blockchain of the voting application.

Therefore, a vote cast is added as a new block (after successful mining) in the blockchain as well as being recorded in data tables at the backend of the database. The system ensures only one-person, one-vote (democracy) property of voting systems. This is achieved by using the voter's unique thumbprint, which is matched at the beginning of every voting attempt to prevent double voting. A transaction is generated as soon as the vote is mined by the miners which is unique for each vote. If the vote is found malicious it is rejected by miners.

After validation process, a notification is immediately sent to the voter through message or an email providing the above defined transaction id by which user can track his/her vote into the ledger. Although this functions as a notification to the voter however it does not enable any user to extract the information about how a specific voter voted thereby achieving privacy of a voter. It is important here to note that cryptographic hash for a voter is the unique hash of voter by which voter is known in the blockchain. This property facilitates achieving verifiability of the overall voting process. Furthermore, this id is hidden and no one can view it even a system operator cannot view this hash therefore achieving privacy of individual voters.

V. IMPLEMENTATION AND EVALUATION

Implementation

The implementation of the proposed system has been carried out within a controlled environment with a web-based application created to serve as the front end application enabling the users to interact in a convenient manner. This application is implemented via Java EE 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

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.

VI. CONCLUSION AND FUTURE WORK

Since the 1970s, electronic voting has been utilized in various ways, offering basic advantages over paper-based systems like more efficiency and fewer mistakes. Numerous efforts have been undertaken to investigate the viability of employing blockchain technology to support an efficient solution to electronic voting, given the remarkable development in its use. This study has described one such attempt that makes use of blockchain's advantages, including

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: 7.53
Volume 4, Issue 3, October 2024

its transparency and cryptographic underpinnings, to provide an efficient e-voting solution. The suggested strategy has been put into practice with Multichain, and a thorough analysis of the strategy demonstrates how well it meets the essential needs for an electronic voting system.

A thorough analysis of the strategy demonstrates how well it meets the essential needs for an electronic voting system.

As we continue our effort, we are working to make blockchain technology more resilient to the "double spending" issue, which translates to "double voting" for electronic voting systems. Even though blockchain technology is quite effective at identifying changeable changes in transactions, successful demonstrations of these events have been made, which encourages us to look into it more. In light of this, we think that establishing a reliable provenance model for e-voting systems will be essential to achieving an end-to-end verifiable e-voting scheme. To help the current blockchain-based infrastructure, an extra provenance layer is being developed in order to do this.

REFERENCES

[1]. 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.

[2]. 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.

[3]. 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.

[4]. Chaum, D. (2004) Secret-ballot receipts: True voter-verifiable elections, IEEE Security Privacy, vol. 2, no. 1, pp. 38{47, Jan 2004.

[5]. Chaum, D. (1981) Untraceable electronic mail, return addresses, and digital pseudonym', Commun. ACM, vol. 24, no. 2, pp. 84{90, Feb. 1981.

[6]. Chaum, D., Ryan, P. Y. A. and Schneider, P. Y. A. (2005). A practical voter-verifiable election scheme, in Proceedings of the 10th European Conference on Research in Computer Security, ser. ESORICS'05. Berlin, Heidelberg: Springer-Verlag, 2005, pp. 118- 139.

[7]. 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.

[8]. Hao, F., Kreeger, M. N., Randell, B., Clarke, D., Shahandashti, S. F. and Lee, P. H.-J. (2014). Every vote counts: Ensuring integrity in large-scale electronic voting, in 2014 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 14). San Diego, CA: USENIX Association, 2014.

[9]. 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.

[10]. 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.

[11]. Kadam, M., Jha, P. Jaiswal, S. (2015) Double Spending Prevention in Bitcoins Network, International Journal of Computer Engineering and Applications, August 2015.

[12]. Kiayias, A. and Yung, M. (2002) Self-tallying Elections and Perfect Ballot Secrecy. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002, pp. 141{158.

[13]. Kraft, D. (2015) Difficulty Control for Blockchain-Based Consensus System, Peer-to-Peer Networking and Applications by Springer, March 2015.

[14]. McCorry, P., Shahandashti, S. F. and Hao. F. (2017) A smart contract for boardroom voting with maximum voter privacy in the proceedings of FC 2017.

[15]. Multichain (2017) Open platform for blockchain applications. Available at: www.multichain.com last accessed: December 2017.

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: 7.53
Volume 4, Issue 3, October 2024

[16]. Nakamoto., S. (2009) Bitcoin: A peer-to-peer electronic cash system, 2009 [Online]. Available: http://bitcoins.info/bitcoin-a-peer-to-peer-electroniccash-system-satoshi-nakamoto. Last accessed: December 2017.

[17]. Narayanan, A., Bonneau, J., Felten, E., Miller, A. and Gold, S. (2015) Bitcoin and Cryptocurrency Technologies, Chapter 2 and 3, Draft October 2015.