A Secure Electronic Voting System Using Blockchain Technology

K. Dhinakaran, P. M. Britto Hrudaya Raj, and D. Vinod

Abstract By voting, people can decide the direction of change and development since the people have a sense of "Ownership of Government". Voting is a very important process in any democratic country. For a secure voting, blockchain technology used by electronic voting is more effective and secure. Many digital services are being developed by the blockchain technology. The investigation on the blockchain topic is still proceeding; however, the research mainly focuses on its legal and technical issues, but this novel concept can be taken advantage of and can be used to create advanced digital services. This paper is going to grip the open-source blockchain technology, and we are going to propose an e-voting system based on this technology. We are using the SHA-256 hash function to keep the voter anonymous, and we are enabling the dual authentication process while the voters' cast their vote. This will result in the minimalization of malicious activities since it is safe, reliable, secure, and trustworthy.

Keywords Blockchain · Electronic voting system

1 Introduction

The most critical way that an individual can alter governmental decision is through voting. But in traditional ways of voting like ballot, EVM machines the casted votes

K. Dhinakaran · P. M. Britto Hrudaya Raj (✉)
Department of Computer Science and Engineering, Rajalakshmi Institute of Technology, Anna University, Chennai, India
e-mail: brittobosco1999@gmail.com

K. Dhinakaran
e-mail: maildhina.k@gmail.com

D. Vinod
Saveetha School of Engineering, Saveetha Institute of Medical and Technical Science, Chennai, India
e-mail: dvinopaul@gmail.com

D. Goyal et al. (eds.), *Proceedings of the Second International Conference on Information Management and Machine Intelligence*, Lecture Notes in Networks and Systems 166,
https://doi.org/10.1007/978-981-15-9689-6_34

are prone to alteration and electoral fraud. In addition, those who cannot reach the polling stations in their allocated time cannot cast a vote. The solution to all these problems is a safe, secure and easily accessible e-voting system supported by blockchain technology [1].

2 Literature Review

2.1 Electronic Voting Systems

David Shaum introduced the primordial electronic voting machine in ahead of time of eighties. Public key cryptography was used in this system through which the voters cast their votes and kept the voters anonymous [2]. Blind signature theorem was used. Polling stations were used for voting instead of the paper ballet voting system as the first system [3]. But the second system uses mobile and allows the users to cast their vote anytime and anywhere using their mobile phones or any other devices remotely which has an Internet connection. This will certainly increase the number of voters since the e-voting makes casting a vote a lot easier and more favourable [4].

- **Estonian I-Voting System**: The ID card allows for both secure authentication and legally binding digital signatures which was made compulsory. SHA1/SHA2 signatures were created using the ID card. Here, multiple times the voters can cast the vote, but only, the last one will be considered as valid. Vote buying can be prevented by using this method [5].
- **Norwegian I-Voting system**: The electronic voting system is used by Norway for its 2011 country council elections. Due to the security reason, the country discontinued its electronic voting system in 2014 [6].
- **New South Wales I-Voting System**: I-voting system has been used by the New South Wales election conducted in 2015. The system is different than that of the Norwegian I-voting system. For a voter to cast their vote, the voter must undergo a series of steps involving pin generation and authentication.
- **Malaysian I-Voting system**: Malaysia People's Justice Party conducted the leadership election with the electronic voting in 2018. It suffered numerous technological difficulties, and they had to postpone many polls due to the poor system.

2.2 Drawbacks and Security Issues

The major drawbacks of the Norwegian and the Estonian electing method are that the code used for casting a vote is prone to liability of critical parts of code. Transparency is also crucial in the Estonian I-voting since the code is close. A trusted election depends on an open-source e-voting system. There is no dual authentication

in the system. So, there is a lot of room for the voters to make error [7]. I-Voting systems make it unprotected to cyberattacks or (DOS) denial of service. Every earlier mentioned system is attacked by state level that is possible as the network traffic is controlled by the intelligence agencies all over the world [8, 9].

Our proposed system will overcome all these drawbacks by using open-source code which is used to develop the e-voting system using blockchain.

3 Proposed System Using Blockchain

Blockchain is distributed ledger technology (DLT) that allows to store data globally on thousands of available servers. Blockchain has high failure tolerance, so it can be used in our proposed voting system. Table 1 describes the structure of blockchain voting method.

An algorithm has been designed by the National Security Agency (NSA) in 2001 which is widely being used and known as (SHA-256) Secure Hash Algorithm. The hash function is a one-way cryptographic. SHA-256 is a fixed size for any size of source text. The SHA-256 may take any size of plain text as an input, and it is encrypted to a 256-byte binary value.

Figure 1 shows that when you input any type of data like password, text it goes through the hash algorithm/function and comes out as a new value.

The requirements of our e-voting system are demonstrated below,

Authentication—The system will validate voters' identities with the database that has been already verified. While discharging a vote, the user needs to undergo dual verification process so that there is very little room for error and the casting of vote is done only once for every user.

Obscurity—The voter will remain obscure during and after the election. No one can establish a link between the voter and the ballot.

Table 1 Structure of the voting blockchain

Field	Description	Size
Block size	The size of the whole block	4 bytes
Block header	Encrypted hash	60 bytes
Vote transaction	Number of transactions	1–9 bytes
Transaction	Contains the transactions saved in the block	Depends on the transaction size

Fig. 1 Working of SHA-256 hash

Precision—Every vote should be precise, as it was unable to modify, remove or duplicate.

Verifiability—The system should be testable as to check whether it counts all votes properly. The voter will get a SMS to his registered mobile number about the details of his vote.

3.1 Representation of Overall Process

- **Registration**: The user needs to enrol into the system with the accreditation which had already been provided by the government authorities like his voter ID. The credentials will go through the blockchain to the verification phase.
- **Verification**: The system will verify all the details that had been entered by the user, and only if all the information is correct, his/her name will be added to the voter's list which again will go through the hash function and will get published.
- **Vote casting**: The voters will cast their vote using their devices which are supported by the internet. The users must go through a dual authentication process while casting their vote.
- **Encrypting and Counting votes**: The votes that are casted will go through the SHA-256 as to remain anonymous to who cast the vote. We use one-way hash function SHA-256. So, no voters information can be retrieved. The received votes will go to an analytical machine which analyses valid votes and count them.

Result: The validated and counted votes from the analytical machine will securely be transmitted through the blockchain and will have the results to the conducted election, and the results will be published. The overall process is shown in Fig. 2.

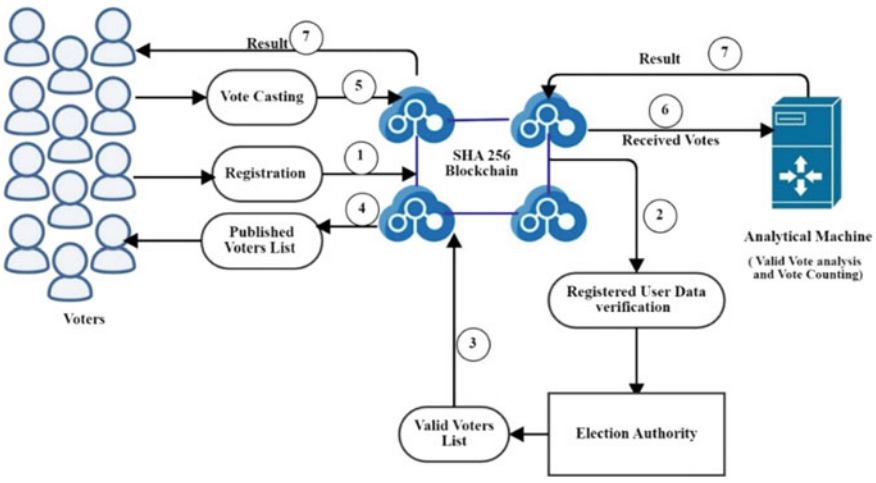

Fig. 2 Architecture of the overall process

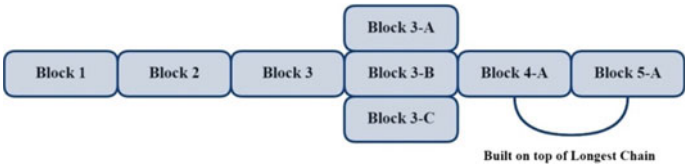

Fig. 3 Longest chain rule

4 Concusses in the Blockchain

Our proposed system based on e-voting and blockchain is a decentralized system. So, the problem of concuss may occur. The concuss occurs when the system obtains tremendous votes from different users at the same time. This problem can be solved with the help of the longest chain rule.

Let us take the three Blocks 3-A, 3-B, and 3-C. The system will add Block 3-A to the descendant to the Block 3, and when Block 3-B is inaugurated, the system waits. When Block 4-A is initiated to the system, then the Block 3-A will be considered as the valid block in the blockchain which keeps on building the chain. Block 3-B and Block 3-C are considered as orphan blocks [10]. Since the orphan blocks (Block 3-B and Block 3-C) have the details/votes as same as the other blocks, they will be examined when votes are counted. Figure 3 is described as the chain rule of blockchain.

5 Implementation and Result

The simulation of our system was done with the help of Python programming using software called PyCharm Community. The receiving of votes, the storage, counting, and publishing of votes remained anonymous and secure because of the blockchain technology. The blocks (votes) contain ID of node, ID of the next node, votes record, digital signature, preceding hash, and timestamp. On any network, if the node is down, then the system succeeds with the next node by continuing the sequence. Overall, the system is secure and ingenious.

Every number of nodes present has undergone reliability testing with essential capacity parameters. Let us assume that the number of nodes represents the place where the election is being conducted and the number of nodes verified ranging from 1 to 500,000. The generated data is shown in the below graph Fig. 4; many numbers of nodes are commensurate to the volume required in the recording process of this e-voting.

The system took longer time to work as the nodes increased. ID of node, ID of the next node, votes record, preceding hash, digital signature, and timestamp were the attributes of the data block containing all nodes. In this reproduction, if the node becomes down on the network, then it cannot transmit the block and disables the nodes. Then, the system has succeeded with the next node by continuing the

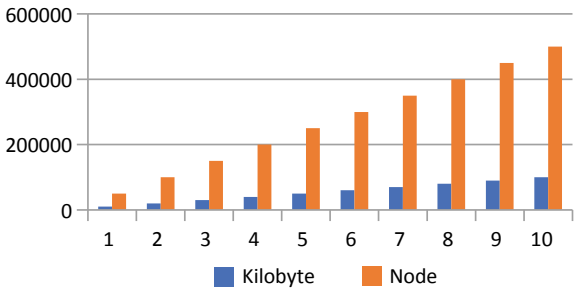

Fig. 4 Possibility of data storage in database

sequence. The counter time for every node expires, and then, the node knows its turn has arrived "My Turn = TRUE". Figure 4 shows the possible data processing in number of nodes in the proposed system.

6 Conclusion

The electoral voting system is the best way to cast a vote; using the blockchain technology like proposed in our paper, we can make the voting process secure. Reliability of the system is considered, and as the nodes increased, the time for the system to work was also increased in the simulation. The system continued the sequence even if a node is down to the following node due to the counter time. The dimensions necessary for the recording process can be known by the number of nodes as they are proportionate. The recording of voting result by using hash values makes the system more secure. The limitations given will be addressed in the future reference papers.

References

1. Shahzad B, Crowcroft J (2019) Trustworthy electronic voting using adjusted blockchain technology. IEEE Access 7:24477–24488
2. Chaum DL (1981) Untraceable electronic mail, return addresses, and digital pseudonyms. Commun ACM 24(2):84–90
3. Hanifatunnisa R, Rahardjo B (2017) Blockchain based e-voting recording system design. In: 11th International conference on telecommunication systems services and applications (TSSA), Lombok, pp 1–6
4. Trueb Baltic, Estonian electronic ID—card application specification prerequisites to the smart card differentiation to previous version of EstEID card application. http://www.id.ee/public/TBSPEC-EstEID-Chip-App-v3_5-20140327.pdf
5. Christian K, Rodrigues B, Matile R, Scheid E, Stiller B (2020) Design and Implementation of cast-as-intended verifiabilityfor a blockchain-based voting system. In: SAC '20: the 35th ACM/SIGAPP symposium on applied computing Brno Czech Republic Mar (2020)
6. Ministry of local government and modernisation. Internet voting pilot to be discontinued. https://www.regjeringen.no/en/aktuelt/Internet-voting-pilot-to-be-discontinued/id764300/

7. Can Çabuk U, Adıguzel E, Karaarslan E (2018) A survey on feasibility and suitability of blockchain techniques for the e-voting systems. Int J Adv Res Comput Commun Eng 7(3):124–134
8. Maesa D, Paolo M (2020) Blockchain 3.0 applications survey. J Parall Distrib Comput
9. Zhang J, Zhong S, Wang T, Chao H-C, Wang J (2020) Blockchain-based systems and applications: a survey. J Internet Technol 21(1):1–14
10. Ayed AB (2017) A conceptual secure blockchain—based electronic voting system. Int J Netw Secur Appl (IJNSA) 9(3)