Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7750417

E-VOTING SYSTEM USING BLOCKCHAIN

S. Narayanan[1], Dr. V. Ramesh Babu[1], Dr. D. Usha[1]
Jayakrishna N[2], Sainath Reddy O[2], Jignesh N[2]
[1]Professor(s), Department of CSE, Dr. M.G.R. Educational and Research Institute
[2]Final Year, B. Tech CSE,Dr. M.G.R. Educational and Research Institute
[1]narayanan.cse@drmgrdu.ac.in, rameshbabu.cse@drmgrdu.ac.in, usha.cse@drmgrdu.ac.in
[2]jayakrishnanalamolu@gmail.com, sainathreddyobulareddy111@gmail.com,
nallamalajignesh@gmail.com

ABSTRACT
The voting process is the tool used to put the public opinion into action and improve system administration. Conventional voting hasn't been popular in recent years with either the public or the government. Given how easily ballots may be tampered with, they are not totally secure. It also raises concerns about transparency and voter safety. Additionally, it takes too long to count the votes. A fascinating topic in the current voting system is the modification of voting globally. To address these issues in many countries, the voting process involves digital technology. Digitalization cannot totally resolve the problems on its own. Additionally, there are several techniques to manipulate or alter digital technologies in order to obstruct voting. Fairness, independence and impartiality should all be present in the voting process. This research effort creates a voting system by examining the aforementioned issues and fusing digitalization with blockchain technology. Integrity, anonymity, privacy and security of voters are our voting system's primary objectives. In our proposed digital voting systems, the data integrity and voter anonymity, privacy, and security have been ensured through the usage of the Merkle tree and fingerprint hash.
Keywords: Voting; Blockchain; Fingerprint hash; Smart contract; Mining; Merkle tree

INTRODUCTION
In every place, democratic voting is a crucial and severe procedure. Countries often conduct elections using mechanical voting machines, paper ballots, and electronic voting machines. However, new digital technologies are required. E- voting and I-Voting are the two types of digital voting, both of which require the use of electronic voting machines. In e-voting, voters utilize a device to cast their votes at the polls, but in I-voting, a software interface is necessaryfor this purpose. Precision, resistance to unlawful behaviour, effectiveness, stability, and openness of the voting process are the key indicators of the democratic process's integrity. Digital voting methods can improve dependability, secrecy, integrity, and decrease investment in labour, supplies, and technological equipment. It only provides assurance that the votes cast and the final results are accurate [1].
Additionally, there are a few drawbacks to digital voting. Throughout the voting process, there are several malevolent tactics that include fake voting, cost savings, producing speedier results, etc. In fact, a number of intrusions may seriously affect voting or voting calculations, causing damage to smart or IoT (Internet of Things) systems in order to benefit themselves. A

consistent method of polling and counting must be guaranteed by a number of safety precautions. Different strategies have been proposed. However, these solutions may also make networks more complicated by raising the cost of testing, processing, bandwidth, and space. In order to provide consistent voting or counting procedures and prevent the aforementioned outlined issues, stronger protection systems or processes are needed [2].

A decentralised ledger that consistently understands the truth is maintained using blockchain technology. Blockchain technology has been employed in peer- to-peer networking platforms and mutual, tamper-proof ledgers like as Bitcoin [3] and Ethereum [4]. User anonymity is protected in this case by the public or private key identification. Security and privacy are provided by a number of blockchain-based models [5], [6]. While blockchain technology offers confidentiality, privacy, accountability, and durability, its implementation faces significant speed and scalability issues [7].

Our goal is to create a smart contract- based digital voting architecture that offers authentication, transparency, anonymity, accuracy, autonomy, singularity, integrity, and mobility while reducing the hurdles associated with the implementation of blockchain technology for voting. Our method creates a hash from the voter information and stores it in a chain. Given that the data is kept on the blockchain as a hash, this will offer scalability and voter anonymity. If the hash data is changed, any modifications will be obvious. Security and privacy are ensured by smart contracts operating in the chain. To increase transaction speed, a miner is selected by the smart contract. The nomination is based on a variety of factors, including energy usage and data transfer. Each block does its own vote tallying. After voting is complete, the final block's total vote may be simply examined. It cuts down on the time needed for counting.

The structure of the essay is as follows. Related Work section discusses relevant works on voting using EVMs, electronic voting, and mobile voting. The overall design of the proposed blockchain- based electronic voting system is described in Proposed Voting Mechanism section. The suggested system is examined from several angles in the next part, Section IV. Comparing the proposed system to the present system is shown in Comparative Analysis section. Future work on the system is detailed in Conclusions and Future Work section, which also contains the research's results.

RELATED WORK

A. EVM

In [8], a voting system is introduced. Voters cast their vote using electronic voting machines. The system in question is centralised. In this manner, vote data is readily altered. There is no way for voters to verify that their vote was actually counted. [9] Provide a voting method based on blockchain in which each EVM is directly connected to a network. The three components of this system—fingerprint authentication, peer verification transactions, and chain manipulation detection—ensure system integrity. It is vulnerable to DoS (Denial- of-Service) attacks and snooping. It requires updating for a number of nodes.

B. E-Voting

Santhosh et al. [10] introduce the idea of online voting systems that emphasise the setup of voting counters utilising the internet. On the Internet, voters can participate in this process. Because to the possibility of system failure and the manipulation of vote data, this system

has some limitations. They have created a fresh sample of the voting procedure in India in [11]. Voters can use any voting machine after completing the authentication process. There hasn't been any discussion of the technical and protection specifications for electronic voting with regard to confidentiality, credibility, privacy, fairness, simplicity, and accountability. [2] present an architecture that focuses on enhancing security using Blockchain in the IoT- based e-voting infrastructure. In order to create an account on a smart device and successfully verify it, the user will need to utilise their voting ID and other biometric methods throughout the programme. Voting operations are handled by smart contracts. The equipment operates slowly due to workload even if the procedure is busy and extremely safe.

C. Mobile Voting

In [12], mobile voting methods are utilised to cast a secure vote for their candidate using SMS (Short Message Service) and smartphone applications. It ensures that the ballots may be kept safely safeguarded until the conclusion of the election in respective districts. In the absence of the mobile owner, anyone with a phone may cast a vote. Thus, it is feasible to cast a bad vote. It is advised to use an m-voting platform [13] that uses blockchain technology to securely handle cast votes. Voters are authenticated using a multi-factor authentication method during the voting process. They haven't conducted any security research. It may be open to several attacks, including a quantum assault and a 51% attack.

PROPOSED VOTING MECHANISM

As most people live in abject poverty, they lack gadgets. So, legitimate voters may cast votes from a designated voting location or through mobile gadgets. Figures 2 and 3 depict the voting system's specifics in detail. Figures 2 and 3 depict the registration and casting and counting procedures, respectively. System Data Management, first huge data quantities are produced throughout the election process. Hence, data should be logged in a methodical manner. There are two different types of storages employed in our system:

A. Data Management of the system Massive data volumes

are generated throughout the electoral process. The systematic recording of data is therefore necessary. Our system employs two different kinds of storage.

1) Election Commission’s Database : The database will contain all the information connected to voter registration, candidate registration, party registration, and other election-related information.

2) Blockchain Storage : A hash value created from the voter information will be placed in the genesis block as a list of voters in the voting blockchain, and each vote will be saved as a block in the chain.

B. Voter Registration

Voters Registration Process showed in fig. 2 are explained below:

- Each person must visit their local voter registration office and provide the necessary information in order to cast a valid vote.
- A key generation method will be utilized to create a public key and private key pair.
- With the blockchain network, voter identification is done via public keys. Voters who have mobile devices receive the private key. They can take part in the voting process and cast a vote using this private key.

- A voter's provided fingerprint is utilized to create a hash using a fingerprint hash creation method [14]. Fig. 1 depicts the complete process of hash creation from the data provided by voters.
- A new hash value will be created by combining the generated hash with information from other voters.
- As a voter list, the final hash value will be saved in the blockchain's genesis block. where hash value = membership evidence.

C. Candidate Registration

As a candidate is also a voter, the registration process is identical to that for voters. The blockchain's genesis block will have the candidate number, party name, and public key.

D. Candidate Registration

The following list outlines the function of a smart contract operating on a blockchain :

- **Verification of a voter :**
  - Using a device that is linked to the internet, the voter logs into the voting system using their private key.
  - NID, fingerprints, and other data should be submitted.
  - When a voter submit the information, smart contracts incorporated into the blockchain compare it to the information of genuine voters in the genesis block.
  - If the information matches, the smart contract gives the voter a list of candidates.

Fig. 1. Hash generation from voter credential

Fig. 2. Architecture Of Registration Process

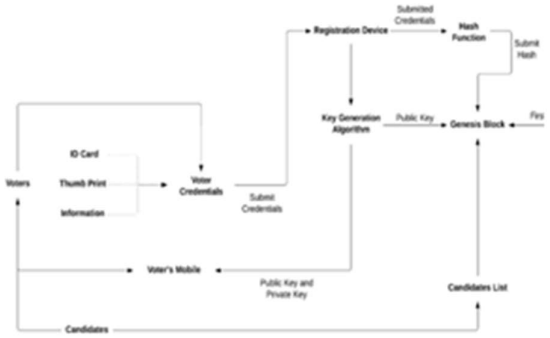

Fig. 3. Architecture Of Vote Casting and Counting

- Create Block for Casted Vote :
  - Voters select a candidate from the list of contenders and then cast their votes.
  - Vote is signed with digital signature and transaction is sent to the SC.
  - SC creates a VID (Vote ID) for the voter's vote.
  - Increase the candidate's vote total.
  - Create a block of transaction with the voter's VID and Candidate Vote number included.
- Miner Selection:
  - A miner selection algorithm is run by the SC and
  - Choose a miner to produce the block's target hash.
- Generate Hash:
  - The SC-nominated miner modifies the block by adding the hash of the most recently mined block and increasing the nonce.
  - By raising a variable known as the block's nonce, the miner starts producing the desired hash, which includes several noticeable zeros and is known as Proof of Work.
  - After creating the desired hash, the miner sends the block to the blockchain network in exchange for payment.

In order to prevent record meddling, all Bitcoin miners compete to be the first to compute the block's target hash, which consumes a significant amount of computational power. Under the suggested voting architecture, a Miner would be chosen based on heuristics extrapolated from their accomplishments. The SC collects information based on [15] criteria, like as node capacity, latency, and energy consumption.

- Verify Block :
  - The block is added to the existing Blockchain after being verified by all Blockchain nodes.
  - To avoid the casting of duplicate votes, the SC will delete the hash value from the voter list after adding the vote to the chain.
  - And add it to another list called Already voted.
  - Give the voter their VID back so they may check their vote on the blockchain.

E. Vote Counting

Voting totals for each block will be tracked by the smart contract. When a vote is cast, it is promptly counted, eliminating any possibility of voting fraud or manipulation.

Fig. 4. R e s u l t D e c l a r a t i o n

EXPERIMENTAL ANALYSIS

A. Concusses in the Blockchain

There might be a concussion issue with decentralised systems, especially with blockchain-based electronic voting. When several voters cast their votes at roughly the same moment, this occurs. When a voter casts a vote that is related to the previous vote, an obvious line will be formed [16]. As the vote transaction is first sent to a smart contract, there is no concussion issue in our system. Hence, after a predetermined amount of time, the miner will receive the information for each block.

B. Integrity

To ensure data integrity, Merkle trees are constructed utilising blockchain technology [17]. The Merkle tree idea was created for Ethereum in order to offer a quick and reliable evidence that a transaction had took place in a node. All of the transactions in a block are hashed and included in the Merkle tree. A Merkle tree must be created in the transaction if a node wants to determine if a transaction has been changed or not. As a result, it is quite simple to validate or invalidate a vote [18]. To make sure the electoral process is fair.

C. Anonymity and Privacy

The suggested approach gives voters privacy and anonymity. Voters' entries onto the blockchain are made anonymously in the voting mechanism. The blockchain network preserves voter anonymity and privacy by using the public key as the voter's identity and the hash value created during the registration process as the voter's information.

D. Verifiability

Every vote adds a block to the chain. Every time a voting block is generated, the Smart Contract (SC) sends the voters a VID (Voter ID) and the position of the block so they can confirm if their vote was added to the chain and counted without alteration.

E. Security Analysis

Following are some of the assaults that our model has successfully thwarted:

- In the Sybil assault, which targets centralized networks, a person creates a sizable number of nodes in an effort to sabotage network operations by intercepting or dropping messages [19]. Only users who have registered may vote in our system, and since each voter’s hash value is distinct, no one has access to manufacture one.
- It addresses the 51% attack [20], a serious flaw in blockchains based on Bitcoin and Ethereum. The 51% assault is defeated by randomly selecting miner nodes from [21].

COMPARATIVE ANALYSIS

Properties	[8]	[9]	[10]	[2]	[12]	[13]	C
Anonymity	×	✓	×	✓	×	✓	✓
Integrity	×	✓	×	×	×	✓	✓
Privacy	×	✓	×	×	×	✓	✓
Security	✓	✓	×	✓	×	✓	✓
Verifiability	×	×	×	×	×	×	✓
Decenralization	×	✓	×	✓	×	✓	✓
Singularity	✓	✓	×	✓	✓	×	✓
Authentication	✓	✓	✓	✓	×	×	✓

Fig. 5. C om p a r i s o n b e t w e e n r e l a t e d a n d p r o p os e d w o r k s

By this analysis, it can be shown that [8], [10], and [12] do not offer decentralisation, anonymity, integrity, or privacy. Integrity, privacy, and

verifiability are not provided by [2]. Verifiability is not provided by [9] and [13]. Security is not provided by [10] or [12]. Singularity is not provided by [9] and [13]. There is no authentication mechanism in [12]. The proposed system offers anonymity, integrity, privacy, security, verifiability, decentralisation, singularity, and authentication.

CONCLUSIONS AND FUTURE WORK

The protection of voting system security is a key challenge for many nations. A blockchain-based voting system employing smart contracts has been suggested to guarantee voter participation and validity, the accuracy of the vote-counting results, and the absence of voter fraud. In order to lower the computational cost, this approach uses the SC to carry out voter authentication and to choose a miner in the blockchain. The election procedure takes less time since the votes are counted right away. This system gives voters the ability to cast their votes from any location utilising mobile devices. This will contribute to increasing the number of voters, which is necessary for democracy in any nation. This research project aims to develop an encryption method in the future to increase the security of our system.

REFERENCES

[1] Casado-Vara R and Corchado J. M., “Blockchain for Democratic Voting: How Blockchain Could Cast off Voter Fraud”, Oriental journal of computer science and technology, 11(1), 03 2018.

[2] R. Krishnamurthy et al., “An Enhanced Security Mechanism through Blockchain for Epolling/Counting Process using IoT Devices”, Wireless Networks, 26:2391-2402, 08 2019.

[3] Satoshi Nakamoto, “Bitcoin: A peer- to-peer electronic cash system”. http://bit.ly/3Ica7Nq, 2009.

[4] Vitalik Buterin, “A Next-Generation Smart Contract and Decentralized Application Platform”. http://bit.ly/3XH0rAf, 2014.

[5] V. Suma, “Security and Privacy Mechanism using Blockchain”, Journal of Ubiquitous Computing and Communication Technologies, 01:45- 54, 09 2019.

[6] Sivaganesan, “Block Chain Enabled Internet of Things”, Journal of Information Technology and Digital World, 01:1-8, 09 2019.

[7] Md. Ashraf Uddin et al., “A Decentralized Patient Agent Controlled Blockchain for Remote Patient Monitoring”, 2019

International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pages 1-8, 10 2019.

[8] Srikrishnaswetha. K et al., "A Study on Smart Electronics Voting Machine Using Face Recognition and Aadhar Verification with IoT", Innovations in Electronics and Communication Engineering, pages 87-95, 01 2019.

[9] Sudharsan B et al., "Secured Electronic Voting System Using the Concepts of Blockchain", 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), pages 0675-0681, 102019.

[10] M.Santhosh et al., "Electronic Voting Machine Using Internet", International Journalof Communication and Computer Technologies, 4(2): 72-75, 2016.

[11] Swati Gawhale et al., "IoT Based E-Voting System", International Journal for Research in Applied Science and Engineering Technology (IJRASET), 5(5), 05 2017.

[12] X. Ignatius Selvarani et al., "Secure voting system through SMS and using smart phone application", 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET), pages 1-3, 02 2017.

[13] T. P. Abayomi-Zannu et al., "A Proposed Mobile Voting Framework Utilizing Blockchain Technology and Multi-Factor Authentication", Journal of Physics: Conference Series, 1378(3):032104, 12 2019.

[14] K. Krishna Prasad and P. S. Aithal, "A Study on Fingerprint Hash Code Generation Based on MD5 Algorithm and Freeman Chain code", International Journalof Computational Research and Development (IJCRD), 3(1):13-22, 01 2018.

[15] M. A. Uddin et al., "An EfficientSelective Miner Consensus Protocol in Blockchain Oriented IoT Smart Monitoring", 2019 IEEE International Conference on Industrial Technology (ICIT), pages 1135-1142, 02 2019.

[16] Ahmed Ben Ayed, "A Conceptual Secure Blockchain-Based Electronic Voting System", International Journal of Network Security Its Applications, 9(3):01-09, 05 2017.

[17] Brian Rogers et al., "Using Address Independent Seed Encryption and Bonsai Merkle Trees to Make Secure Processors OS- and Performance- Friendly", 40th Annual IEEE/ACM International Symposium on Microarchitecture (MICRO 2007), pages 183-196, 12 2007.

[18] R. Bosri et al., "Towards a Privacy- Preserving Voting System Through Blockchain Technologies", 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), pages 602-608, 08 2019.

[19] Ronald Cramer et al., "A Secure and Optimally Efficient Multi-Authority Election Scheme", European Transactions on Telecommunications, 8(5):481–490, 09 1997.

[20] Iuon-Chang Lin and Tzu-Chun Liao, "A Survey of Blockchain Security Issues and Challenges", International Journal of Network Security, 19(5):653-659, 09 2017.

[21] Rumeysa Bulut et al., "Blockchain- Based Electronic Voting System for Elections in Turkey", 2019 4th International Conference on Computer Science and Engineering (UBMK), pages 183-188, 09 2019.