ISSN 2063-5346

A UNIFIED AND DECISION METHODOLOGY FOR E-VOTING SYSTEM BASED ON PUBLIC BLOCKCHAIN - AN ETHEREUM WAY

[1]Dr.V. Gowri ,[2]A. Aijaz Ahamed Khan and [3]Ganga Prasad

[123]Department of Computer Science and Engineering,

SRM Institute of Science and Technology, Ramapuram, Chennai, India

Article History: Received: 01.02.2023 **Revised:** 07.03.2023 **Accepted:** 10.04.2023

Abstract

Citizens of democracies like India have the fundamental right to vote. Voters must be present to cast their ballots under a voting system based on ballots. Most citizens do not abide by this limit by avoiding their original duties. In such situations, electronic voting is often seen as one of the most effective solutions. Due to its immutable, transparent, anonymous, and decentralized nature, a new technology known as blockchain could offer a viable solution. We provide a base solution. Dial security and data integrity are given in theory. Another need that this system satisfies is voter privacy. Finally, the proposed blockchain voting technology significantly reduces the time spent waiting for results. The protocol uses smart contracts in electronic voting systems to address voter security, accuracy, and privacy issues. The protocol creates a visible, non-editable, independently verifiable approach that eliminates planned fraud during the election process while minimizing the involvement of third parties. Furthermore, it prevents double voting when used in conjunction with proper smart contract constraints. We go into great detail with our solution, emphasising the security assurances and design decisions that make it scalable to a high number of voters. The proof-of-concept version of the suggested framework is presented as our final product.

Keywords: Ballot-based voting, Electronic Voting, Decentralized nature, Blockchain Technology, Security and Data Integrity, Double Voting, accuracy.

INTRODUCTION

In a democracy, elections are important in choosing the leaders of each country. Voting must be conducted safely and quietly without the intervention of party representatives. Voting can be done in different ways in different countries. Voting is done on a piece of paper using conventional voting procedures. Invalid ballots, printing millions of ballots, transporting, storing, and distributing

ballots, stealing or tampering with ballot boxes, and lengthy manual counting are all drawbacks of this approach. Members of the armed forces, state police officers and other persons authorized to perform election-related duties in India have access to vote by mail. The ballot must be marked with the voter's choice, and the ballot will be mailed to elections officials for the appropriate convention. The downside of this system is that ballots may not be received on time and the paper may be torn in transit or improperly punched by voters, invalidating the ballot during the ballot counting process. This Indian situation is being transformed by Electronic Voting Machines (EVM). It helps overcome all the shortcomings of voting systems that use paper ballots. In this case, voters must go to the ballot box on polling day. There are other ways to vote online or via remote voting systems. Voter engagement has increased because people can vote from anywhere. The system is built via web-based or mobile applications. Blocks on the blockchain are kept up to date by a network of consensus nodes. A consensus node is a continuously growing distributed database (i.e. running a consensus protocol). New blocks are added to the blockchain after being approved by consensus nodes. Blocks keep a record of Bitcoin transfers made within the network and are cryptographically linked to ensure the immutability of the entire ledger. The network receives messages called transactions. This message contains instructions on how to send the money. In blockchain platforms that enable smart contracts, blocks can additionally contain application code written in a supported language. Transactions containing execution instructions trigger this code (i.e. smart contract function calls). A blockchain network functions as a decentralized computing platform when smart contract code is executed by blockchain nodes. Blockchain-based digital voting reduces the possibility of fraudulent voting while saving money. Blockchain technology is the latest innovation that is very safe and beneficial if used wisely. It can also increase trade traceability, which will make the reconciliation process more dependable and transparent. Blockchain is changeable, in contrast to traditional programming paradigms, where administrators can add, delete, or update data. If it is used for voting, anyone who has access to it is able to change it, add votes, or remove votes. Technology like blockchain is unique. Once being added to the chain, nodes cannot be altered or eliminated. The chain becomes immutable if an intrusive entity attacks a node, and other nodes notice it and fix the broken node. No one computing node on the blockchain controls the voting process since it is decentralised. Even if one or more nodes are attacked or rendered unreachable, the voting process still goes on.

LITERATURE SURVEY

John Crowccroft and Bassit Shahzad [1] Electronic voting has become more popular over time to eliminate duplicate voting and fraud. Due to security and privacy issues discovered over time, it has not been successful according to the historical perspective provided over the last 20 years. This research proposes a framework that makes use of effective hashing methods to guarantee data security. Block creation and sealing are concepts that are introduced in this work. The blockchain can be modified to meet the needs of the voting process by utilising the block ceiling concept. A consortium blockchain is something that we advise. By doing so, it is made sure that a governing entity (like an electoral commission) owns the blockchain and that

no unauthorised external access takes place. This paper describes a methodology that uses a flexible blockchain approach to collect data, create and seal blocks, declare results, and use hashing algorithms. This article claims to understand security and data management challenges in blockchain technology, in addition to providing a better explanation of the electronic voting process.

Getanjali Rathe , Ali Kashhif Bashir, Omar Waqar and Razi Iqubal [2] A smart city is an intelligent setting made possible by the coordinated and thoughtful application of all available resources and cutting-edge technologies. The needs of the user can be served more effectively when 5G technology and smart sensors (Internet of Things (IoT) devices) collaborate. One of the many IoT use cases and a crucial application that will advance IoT to the following level in the development of smart city technology is electronic voting. In conventional uses, all technology is frequently regarded as dependable and helpful. Nevertheless, malevolent users can actually hack your device and jeopardise network services. Hence, privacy and security concerns present a severe challenge because attackers can manipulate elections by engaging in a range of frauds, especially with computerised voting systems. In order to establish a trustworthy communication environment, it may be challenging to discern between trustworthy and dangerous IoT devices by computing trust values through social optimization. To prevent future manipulation of data collected from smart devices, a blockchain is also kept that stores blocks of all authorised IoT devices. This article offered a safe and transparent electronic voting system combining IoT devices and blockchain technology to identify and mitigate various threats posed by multi-level invasions. Also, the efficiency of the suggested mechanism is examined in light of several security considerations, such as message manipulation , DoS and DDoS attacks, and authentication delays.

Shiya Gao , Chenccheng Hu, Ruii Guo , Chunmming Jing and Dong Zheng [3] Being a crucial democratic decision-making process, voting has long been a socially significant issue. Because to its convenience, simplicity, and cost savings over traditional voting, electronic voting is frequently employed in a number of decision-making circumstances. To achieve true justice and transparency in e-voting, however, is challenging since the suggested e-voting protocol bears the risk of inflated authority and data tampering. Due to its decentralised and tamper-proof characteristics, combining blockchain technology can alleviate these issues. Election fraud, such as B, also threatens this fairness. It will be ruined if there are numerous ballots cast or if there are no candidates. As a result, it's critical to include auditing capabilities in electronic voting logs in order to confirm the validity of the voting process and maintain a fair voting environment. In order to make voting transparent, this paper suggests a blockchain-based electronic voting system. This method can check incorrectly handled votes while still being resistant to quantum attacks because it uses certificates and code-based cryptography. Our approach provides some advantages in terms of efficiency and security when there are few voters, according to performance studies, and is ideal for small elections.

Jiankun Huu, Benjamiin P. Turnbul , Hao-Ttian Wu , A. J. S. dee Silva , Kateerina Kormusheva and Quang Nhat Traan [4] Supply chain management, finance and banking, and cryptocurrency are just a few of the sectors that have been altered by blockchain and smart contracts during the

past ten years. The offered transparency, however, frequently jeopardises privacy. Blockchain contains characteristics that enhance privacy. This white paper uses examples from many fields and industries to discuss the present state of privacy using blockchain technology and smart contracts. It gives a brief introduction to blockchain, outlines the privacy problems it encounters, and organises themes that, when applied to this paradigm, can improve or defend privacy. Smart farming, the Internet of Things, electronic voting, data management and storage, and cryptocurrencies are some of these sectors. The next stage in this endeavour is to put forth PPSAF, a completely fresh privacy framework made specially to address the smart farming issue. Finally, the article offers potential research directions in the fields of blockchain, new technologies, and privacy.

Wei Liuu, Qi Liuu , Zhao Tiann , Jian-Sen Chenn , Bo Wanng and Wei Shee [5] Due to its great efficiency and real-time collaboration, the Internet of Things (IoT) is widely employed. The IoT's foundational technology is wireless sensor networks, but security concerns are taking on increasing significance. Current methods for detecting malicious nodes in wireless sensor networks concentrate on the fairness and traceability of the detection process, introducing the Blockchain Trust Model (BTM) for doing so. Initially, we show the general structure of the trust model, which addresses a problem that cannot be guaranteed. The next step is to create a blockchain data structure that will be employed to detect rogue nodes. Additionally, the decentralised blockchain's smart contract and WSN's quadrilateral measurement localization technique are used to achieve rogue node identification in 3D space, and the voting consensus results are saved there as well. Based on the results of the simulation, it can be concluded that the model is capable of detecting malicious nodes in WSNs and guaranteeing that the detection procedure is transparent.

Chienn-Chung Shen, Waanxin Li , Mark Nejjad and Hao Guoo [6] Autonomous vehicles can perceive their surroundings and navigate on their own. Accident forensics must, however, identify negligence when autonomous vehicles or pedestrians collide. Blockchain served as inspiration for the proposed technique of recording autonomous vehicle events in this study. By delivering trustworthy and verifiable event information, we especially build an event-proof method leveraging dynamic association consensus to accomplish uncontested accident forensics. We provide a dynamic association consensus method for quickly assessing and confirming fresh blocks of event data without the need for a centralised authority. We conduct a numerical analysis and experiments on a prototype based on the Hyperledger Fabric blockchain network and the suggested rapid executive election mechanism. The findings demonstrate that our system is capable of producing and storing accident information in car networks built on blockchain technology. Regarding various risks and attack scenarios, the security capability of the suggested architecture is also investigated.

Minsoo Ryuu, Shuyanng Ren , Choonhawa Lee and Carllos Santiago [7] This study presents a unique, cheap, and leader-driven communication-free Byzantine fault-tolerant consensus approach for shared blockchain networks. In the proposed protocol, only one block proposal is selected at a time, and voting is carried out using threshold signatures to make sure that each block is trustworthy. Each node is capable of collecting and recovering group signatures in $mathrm O(logN)$ steps using a communication technique

comparable to gossip. There can never be any conflicting blocks because there is only one block proposer in each consensus round. According to our performance investigation, the proposed protocol enables negotiation between hundreds of nodes, with large blocks typically taking around 10 seconds to complete.

Changli Zhouu, Shaoobin Cai , Changllong Lin , Zuxxi Chen , Tiann Wang , Zhengguo Gao and Yuhaoo Wang [8] One of the most often used blockchain consensus techniques is PBFT (Practical Byzantine Fault Tolerance). To preserve data consistency, PBFT uses a lot of communication resources and struggles to effectively pique the interest of trusted nodes. Hence, Credit-Delegated Byzantine Fault Tolerance (CDBFT) is a novel consensus approach suggested in this paper. How CDBFT functions: 1) Voting incentive and punishment schemes and accompanying credit scoring schemes are suggested to boost the excitement of reliable nodes and decrease the involvement of aberrant nodes in the consensus process. In the system, this creates a positive feedback loop. 2) To improve the system's efficacy and adaptability, PBFT-based integrity and checkpointing techniques have been suggested. Based on the simulation findings, we can infer that it is possible to minimise the likelihood of anomalous nodes participating in the consensus process to 5%, which will have a long-term impact on the system's effectiveness and stability.

Mark Gohh, Yuhao Duu , Congjun Raao and Zhuo Huu [9] The majority of carbon emission trading schemes (ETS) rely on centralised systems, making them susceptible to security vulnerabilities. This article suggests a blockchain-enabled decentralised ETS to boost the system's effectiveness and security (BD-ETS). The centralised Carbon Emission Permit (CEP) trading mode is converted into a decentralised trading system by BDETS. This trading method is supported by Hyperledger Fabric-based smart contracts. The asking price and the issuer's reputation are taken into account in each smart contract transaction. The reputation score of an emitter, which is based on their efforts to lessen their carbon footprint, affects their voting privileges. We provide a delegated proof of consistency to guarantee the consistency of each node in a CEP transaction. In comparison to enhanced Delegated Proof of Stake, DPoR is more able to neutralise criminal enterprise attack intent and identify malicious miners more quickly, enhancing the security of BD-ETS. To illustrate how CEP trading operates and to support the DPoR mechanism, case studies and numerical simulations are created.

Guosheng Xuu, Jinwen Xii , Siyuan Wang , Yueeming Lu and Shihong Zoou [10] Mobile users may send and receive messages whenever and whenever they want, making it simple to collect useful feedback for smart city management. This is made possible by the widespread usage of internet-enabled gadgets. Unfortunately, few people think about or report these infractions of the law in their local context, and more and more people strive to ignore them. He generally attributes this phenomenon to two key causes. First of all, while we firmly advise you to report under your own name, it can be challenging to provide trustworthy and trustworthy communication without disclosing your identify. It usually isn't worth it because they frequently feel uncomfortable sharing information for fear of reprisal. We offer Report Coin, a blockchain-based anonymous reporting system for creative incentives, in this paper as a useful

anonymous reporting system. The confidentiality of user identities and the veracity of reporting messages are upheld by Report Coin throughout the reporting process. On the one hand, Report Coin enables non-deterministic mobile users to cast votes on reports by signing and transmitting anonymous announcements across a thinly veiled network of trust. With Report Coin, individuals are enticed to continue through rewards rather than fear of being punished for disclosing their identify. On the other side, Report Coin keeps an open, transparent, and impenetrable record of accounts and transactions. The efficacy and utility of Report Coin are demonstrated by theoretical analyses and significant experimental findings.

Existing System: Widespread scepticism about traditional voting methods has increased the importance of democratic elections in all countries. Individuals have witnessed violations of their fundamental rights. Some digital voting systems suffer from a lack of transparency. It is very difficult for governments to win public trust because most voting procedures are not sufficiently public. Both traditional and current digital voting systems are ineffective because they are so easy to abuse. The main goal is to fix problems in traditional and digital voting systems, such as errors and fraud that can occur during the voting process. Blockchain technology can be integrated into election processes to ensure fair elections and reduce fraud. Both analogy and digital voting systems have too many shortcomings for widespread use. Analog voting procedures have many drawbacks. Assess the need for solutions to protect people's democratic rights. Blockchain-based platforms available today offer the highest level of system transparency and trust, fostering trust between voters and election officials. Modern technology offers a framework that can be utilised to execute voting operations digitally via blockchain without needing actual polling places. Our present design offers a scalable blockchain by utilising a flexible consensus method. The security of voting transactions is increased by implementing a chain security algorithm in a voting system. By carrying out on-chain transactions, smart contracts offer a safe connection for users and networks. It is also up for discussion whether voting systems based on blockchains are secure. We also covered how to secure the blockchain from assaults and encrypt transactions using cryptographic hashes. A method was created to conduct blockchain transactions during the voting process utilising the blockchain. The system can be employed for huge populations, according to the performance assessment. Blockchain is changeable, unlike other programming frameworks where administrators can add, remove, or update data. If someone has access to such a system and is accustomed to voting, they can alter or remove votes. Blockchain technology prevents this from happening. Once inserted, nodes cannot be modified or eliminated from the chain. The chain becomes immutable if a node is attacked by an attacker because nearby nodes will notice the attack and fix the damaged node. The voting procedure is independent of the computer nodes on the blockchain because it is decentralised. Even if one or more nodes are attacked or malfunction, voting operations continue to run smoothly. It ensures dependability in all challenging circumstances. Voter Identification Agencies (IAs) and Election Commission Administrative Agencies (AAs) are key participants in the proposed system. The current system process consists of several steps. The first step is the application's user interface, which also requires front-end security. This is where users enter their credentials, so it should be

safe and easy. During voting activities, the system grants each user equal and complete access rights. It can be tracked even after voting. Voters enter their credentials to register with the system. To enrol voters in the system, VMS uses voter ID information and verifies it with online IA data. For logging into the system, the user receives a special OTP. Voters must generate an OTP each time they attempt to log into VMS. VMS has stored all voter information. Voting Coins (VC) will be added to each voter's wallet upon successful registration in the system. Each voter is given 1 VC, preventing her from voting twice. This mechanism ensures that voters will not vote a second time even if their voting coin balance is not updated due to a technical error. The miner instantly rejects any malicious requests or nodes from voters by determining whether the transaction's hash matches the voter's digital national ID. An SMS will be sent to the voter's registered phone number and an email will be sent to her registered email address after the transaction is finished and the node is successfully added to the voting chain. Voter identities, however, could not be ensured, and intricate calculations were needed. Users could cast their ballots in the system, but when user rates climbed owing to computing complexity, delay started to become a problem. Voter identities were at risk. The system could not be implemented on a large scale because it could not compute large amounts of data. In contrast, the proposed voting system manages latency through the flexible use of consensus algorithms. Using cryptographic hashes on the blockchain eliminates the risk of voter identities being compromised.

Existing System Issues:

- Your implementation will determine your strengths.
- There are scaling issues and new technologies.
- Frequent use may degrade performance.
- Internal processes and voting are less transparent.
- Motivation may be hampered by previous failed attempts.
- It consumes more processing power because the hashing method has to be repeated until the pattern is matched, but if a malicious party creates a hash and tries to chain and add blocks of it, the hash pattern can be given Security which is also better because of its privacy.

Proposed Architecture: In this study, we offer a comprehensive and expandable architecture for creating safe electronic voting systems. Signatures—which have been shown to be secure—allow for voter accuracy and anonymity, while specialised smart contracts on the blockchain offer voting decentralisation, transparency, determinism, and immutability. For the purposes of electronic voting systems, blockchain serves as a reliable data repository. It also supports smart contracts, which define the computations that must be made at each voting stage. Blockchain has eliminated the necessity for a centralised system of verified message boards. Next, a linkable ring signature is placed on the ballot. Only registered voters are able to sign this document using cryptography, which also detects duplicate signers without disclosing the signers' names or the ballot's contents. Voting processes are broken down into various actors playing various parts. Each actor is intended to operate independently for convenience of usage, but actors can also be groups of cooperating parties using blockchain and smart contract capability, alternate contracts, or other limitations. No one is stopping you from Our system guarantees voter privacy and

prevents the early disclosure of unfavourable results. To do this, a variety of doable tactics might be used. Anyone can see more ballots in a voting box made with blockchain technology because it is transparent and has its paper spread out. In most application scenarios, real-time results are not a preferred option since they may have an impact on voters who have not yet cast their ballots. It's well knowledge that voting outcomes are gradual during the voting phase. As a result, during the voting process, we need a way to conceal the vote's substance. Because to the verifiability property, each party can confirm that their votes were counted. The two basic categories of verifiability that are often stated are individual and universal. Every voter has the option of individually verifying their vote after casting it. Election results should be publicly available for everyone to be able to verify them. Voting must be transparent throughout and after, and the entire process must be verifiable. In this situation, the blockchain offers an add-only register abstraction that permits auditing of all method calls of the subsystems used to build smart contracts.

Advantages of Proposed System:

- Immutable record.
- Deletion of records is nearly impossible, and even if successful, the deletion of evidence may stop.
- A sense of openness while maintaining privacy. cheap in the long run.
- Enable flexible elections with different timeframes, requirements, and target groups.
- Instant results.

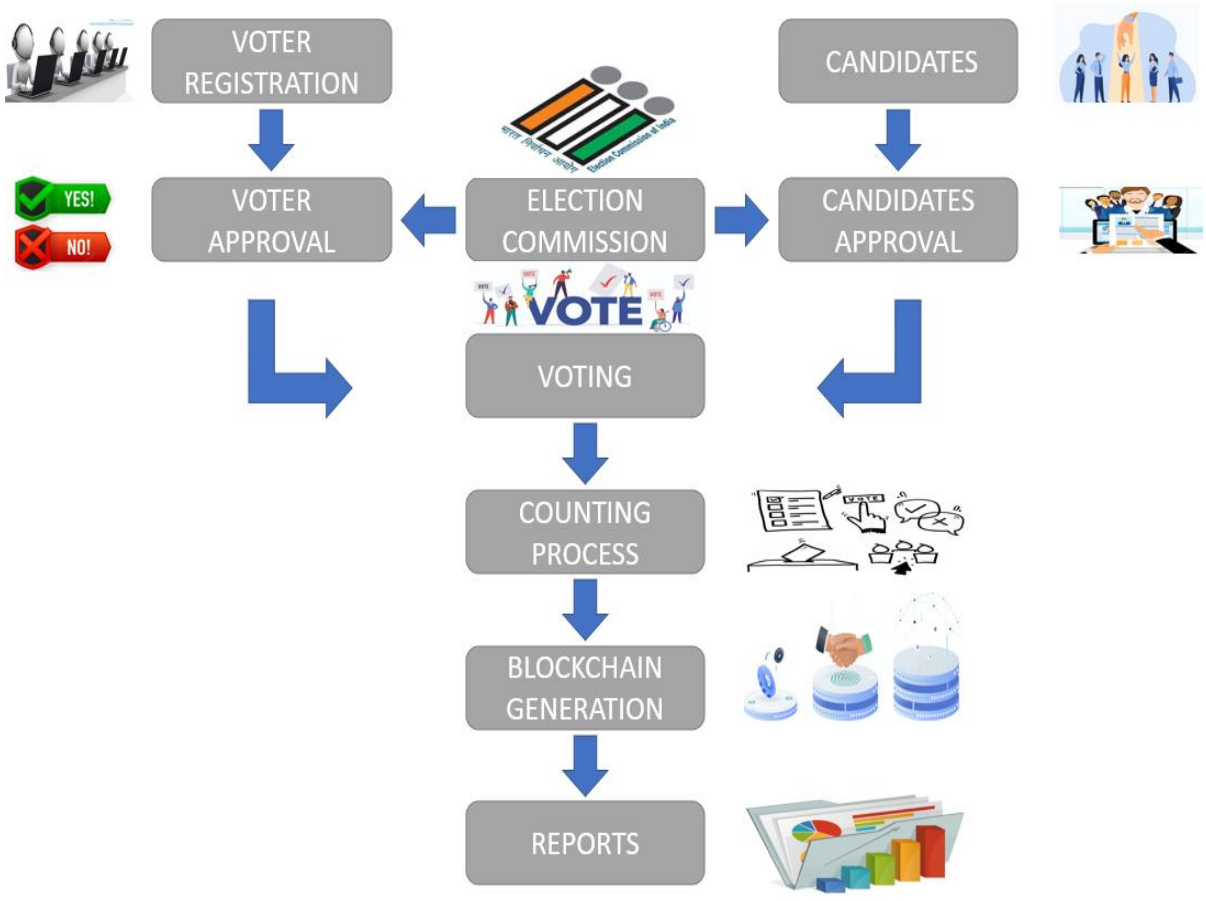


Fig. 1: Proposed Architecture Diagram

Algorithms:

(1) SHA256 Algorithm for Hashing - The industry standard for safety, collisions are very rare, when the input changes, the output changes.

(2) Proof-of-Stake for Voting - Greater scale and throughput, increase transaction volume and throughput (speed) with less energy consumption, reduces the need for complex calculations, anyone can join a participating peer-to-peer network without the need to purchase and set up expensive and powerful computers or cooling systems.

Modules:

(1) Voter Registration & Authenticate Voter - Voters are people who participate in the voting process and vote. Thanks to the wealth of information, voters are sufficiently identifiable. All persons entitled to vote must register directly with the election authorities with the required documentation. Judging criteria help determine whether a voter is eligible. The code verifies the smart contract's ability to execute executable code by calling a function that validates whether the voter entered is authorized. As a result, the voting authority list is kept in the genesis block. After confirming their identity, each voter receives access data in the form of a user ID or password. Credentials hide the identity of voters from the public. Each voter is verified with their credentials when voting, thus preventing repeated voting. Because voters do not know when to vote, the likelihood of voter manipulation and coercion by unauthorized supporters is reduced. Only the time allotted to vote for each group was randomly generated when the code was run. Voters are therefore not intimidated or intimidated by manipulators or the general public of a particular political party. A list of candidates is handed out to the voters represented by the logo. Voters then decide which candidate to support. A representative logo for each candidate is a binary representation. Candidate representative logos will be used to represent them. Each logo has a binary value that is used when it is selected.

(2) Casting Vote - The ballot contains a list of candidates, and each voter must select one. Voting results cannot be proven because there is no connection between voters and their ballots. There ought to be two layers of protection for each voice. To avoid double voting, votes cast are compared with previously cast votes. Votes are recorded on the blockchain upon verification. Voters can vote during the designated hours. Data protection conditions are met if voters' votes are not attributed to any person, including electoral authorities. All ballots are private, so it is impossible to determine which candidate voters chose during the voting process.

(3) Vote Tallying - Voting Attributes and Voting Rights Election Commission, an institution that configures and chooses the characteristics that constitute a specific voting event. He is in charge of organising the popular vote session. The number of votes cast by each voter is counted at the conclusion of the voting period. If not, you will receive a prompt notification asking you to complete your vote within the specified time frame. Otherwise, votes will not be considered. Otherwise, it will be cast the same as in the voting phase. Once all sibling blocks have been submitted, peer nodes start computing results using block and voter data to determine candidates for each block. All nodes should have the same result in this case, since no blocks are wasted thrown in between and the blockchain does not allow changes. As a result, peer nodes or voters count votes independently and broadcast the results,

eliminating the need for a third party to do the counting. Blockchain transparency ensures accuracy as everything is public. Once the voting phase is complete, the system will start counting the votes stored in the system. The results will be recorded on the blockchain for auditing purposes before the election results are announced. Each vote is currently extracted from the blockchain, decrypted, and added to a distinct account. The outcomes are decided when the voting process is finished, and the blockchain records everything so that the entire process can be validated. Rejected blocks and votes can later be tracked to determine how frequently fraud attempts are undertaken. The blockchain permanently stores the code for smart contracts, making changes to it impossible. Yet it is still possible to add some. The force function is employed in these circumstances. The code cannot be changed without the support and agreement of all party representatives; hence enforcement procedures have been altered.

RESULTS AND DISCISSION:

In this section, we evaluate the performance of the proposed framework using data from a real-world scenario using the blockchain tool Remix, a browser-based application. Proposed models are evaluated using Solidity as the programming language.

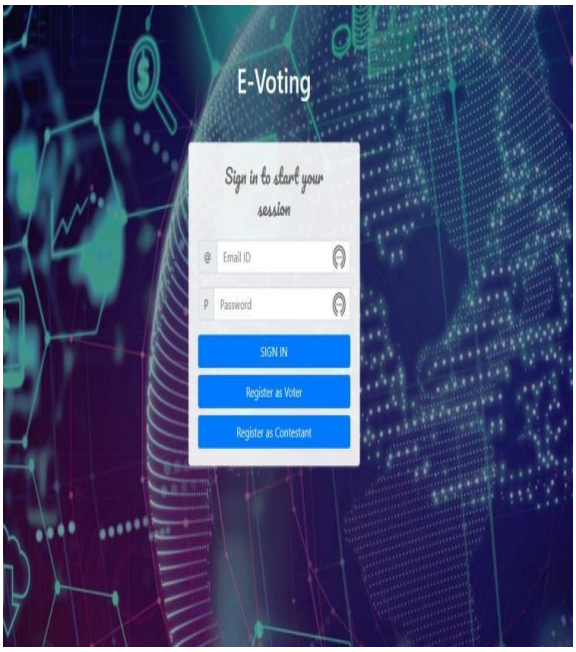


Fig. 2: Login/Registration

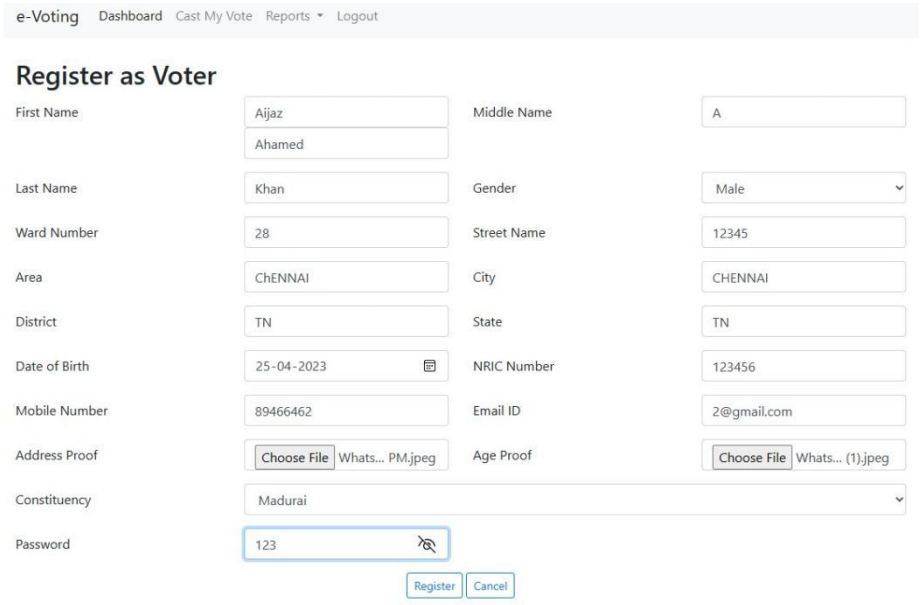
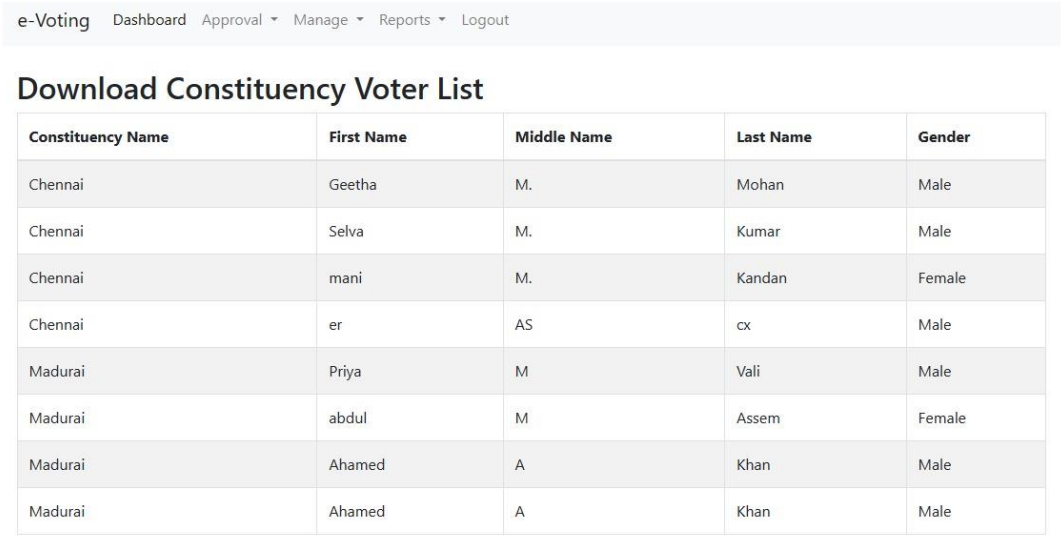


Fig. 3:Voter Registration

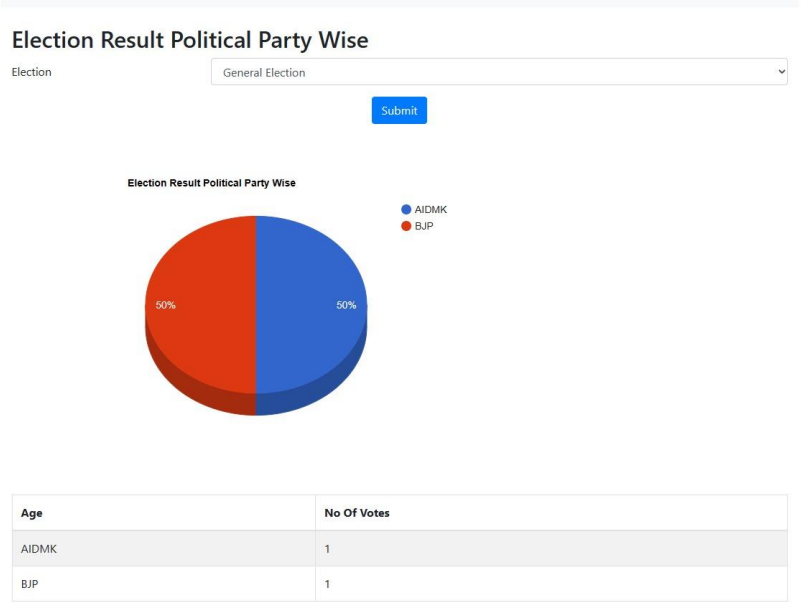


e-Voting Dashboard Approval Manage Reports Logout

Download Constituency Voter List

Constituency Name	First Name	Middle Name	Last Name	Gender
Chennai	Geetha	M.	Mohan	Male
Chennai	Selva	M.	Kumar	Male
Chennai	mani	M.	Kandan	Female
Chennai	er	AS	cx	Male
Madurai	Priya	M	Vali	Male
Madurai	abdul	M	Assem	Female
Madurai	Ahamed	A	Khan	Male
Madurai	Ahamed	A	Khan	Male

Fig. 4: constituency Voter list



Age	No Of Votes
AIDMK	1
BJP	1

Fig. 5: Result political party wise

CONCLUSION AND FUTURE WORK

Conclusion:

The architecture of a blockchain-based voting system for mass elections should be secure, reliable, trustworthy, robust, and free of security vulnerabilities. Systematic processes should be user-friendly and systems should be easy to use and accessible to the general public. Still, blockchain-based remote voting is in the research and development stage with a sizeable population, and we need to discover different ways to prevent coercion and conduct smooth elections. Voting logs can be made transparent to all voters and external observers thanks to blockchain technology. Blockchain technology offers a decentralized method of storage and processing (if it also represents accounts, wallets, etc.). We provide a reliable system for everyone. This trust is based on more

than just recognition. It also relies on logical and analytical mathematical security measures provided by blockchain technology. According to our research, using a blockchain technology like Ethereum that natively supports on-chain decentralized applications can be a great solution. Ethereum supports smart contracts (or equivalent) and other blockchain technologies. Authentication, the uniqueness and integrity of voter accounts, and the immutability and traceability of all records are included in the aforementioned security phrases.

Future work:

We plan to address safety issues in our next work and may consider other generalizations. We even want to address minor problem which occur during establishment of e-voting system.

REFERENCES

[1]. S. Wolchok et al., Security analysis of India's electronic voting machines, in Proc. 17th ACM Conf. Comput. Commun. Secure., 2010, [10] R. L. Rivest, The three-ballot voting system, Tech. Rep., 2006, p. 15.

[2]. M. Pilkington, 11 Blockchain Technology: Principles and applications, in Research Handbook on Digital Transformations. 2016, p. 225.

[3]. S. Baig, U. Ishtiaq, A. Kanwal, U. Ishtiaq, and M. H. Javed, Electronic voting system using fingerprint matching with Gabor filter, in Proc. Int.

[4]. Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, Consortium blockchain for secure energy trading in the industrial Internet of Things, [40] SpringerLink. Security Accessed: Aug. 2, 2018. com/chapter/10.1007/978-3-540-24654-1_13 Analysis Sisters. SHA-256

[5]. F. Al-Turjman, 5G-enabled devices and smart-spaces in social-IoT: Mar. 2019.

[6]. P. Tarasov and H. Tewari, The future of E-voting, IADIS Int. J. Comput.

[7]. M. A. Khan and K. Salah, IoT security: Review, blockchain solutions, May 2018.

[8]. M. Swan, Blockchain: Blueprint for a New Economy. Sebastopol, CA, USA: OReilly Media, 2015.

[9]. S. S. Al-Riyami and K. G. Paterson, Certicateless public key cryptography, in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secure. Berlin, Germany: [10] T.-Y. Wang, J.-F. Ma, and X.-Q. Cai, The postprocessing of quan- 2017.

[10]. T.-Y. Wang and Z.-L. Wei, One-time proxy signature based on quan- 2012.

[11]. N. Hackius and M. Petersen, "Blockchain in logistics and supply chain: Trick or treat?," in Proc. Digitalization Supply Chain Manage. Logis- tics: Smart Digit. Solutions Ind. 4.0 Environ. Proc. Hamburg Int. Conf. S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," Int.

[12]. J. H. Park and J. H. Park, "Blockchain security in cloud computing: Use 164.

[13]. O. Jacobovitz, "Blockchain for identity management," The Lynne William Frankel Center Comput. Sci. Dept. Comput. Sci. Beer Sheva: Ben-Gurion University, 2016.

[14]. A. Rejeb, J. G. Keogh, and H. Treiblmaier, "How blockchain technology can benet marketing: Six pending research areas," Front.

[15]. D. L. Chaum, Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups. Electronics Research Laboratory, Univ. California, California, USA, 1979.

[16]. A. Mohsin et al., "Based blockchain-PSO-AES techniques in finger vein biometrics: A novel verification secure framework for patient 103343.

[17]. Y. Ji, J. Zhang, J. Ma, C. Yang, and X. Yao, "BMPLS: Blockchain-based multi-level privacy-preserving location sharing scheme for tele- Art. no. 147.

[18]. M. Jones, M. Johnson, M. Shervey, J. T. Dudley, and N. Zimmerman, "Privacy-preserving methods for feature engineering using blockchain: no. 8, 2019, Art. no. e13600.

[19]. Z. Lu, Q. Wang, G. Qu, H. Zhang, and Z. Liu, "A blockchain-based Dec. 2019.

[20]. K. Salah, N. Nizamuddin, R. Jayaraman, and M. Omar, "Blockchain- [80] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, and W. Ni, "PrivySharing: A blockchain-based framework for privacy-preserving Art. no. 101653.