

Online Voting System using Ethereum in Blockchain Technology

¹V Srinadh, ²Chetan Sai Pyla, ³Desaraju Sri Rama Ganesh, ⁴Borra Kiran Kumar,
⁵Bheemerasetty Divya Sai

¹Computer Science and Engineering, GMR Institute of Technology, Rajam, India

²Computer Science and Engineering, GMR Institute of Technology, Rajam, India

³Computer Science and Engineering, GMR Institute of Technology, Rajam, India

⁴Computer Science and Engineering, GMR Institute of Technology, Rajam, India

⁵Computer Science and Engineering, GMR Institute of Technology, Rajam, India

DOI: <https://doi.org/10.5281/zenodo.7233830>

Published Date: 21-October-2022

Abstract: Modern digital technology has enhanced the lives of several people. Unlike to the election system, it makes heavy use of printed paper. Elections using the traditional method risk the security aspects and openness. The institution that oversees general elections continues to adopt a centralized approach. With an organization having complete control over the database and system, it is feasible to tamper with the database of significant opportunities. This is one of the issues that might arise in traditional election systems. Because it adopts a decentralized structure and the full database is held by multiple people, blockchain technology has been one of the solutions. The methodology outlined in this work examines the usefulness of hashing algorithms, the construction and sealing of blocks, the accumulation of data, and the declaration of results using an adaptable blockchain approach. Electronic voting or e-voting has fundamental benefits over paper-based systems such as increased efficiency and reduced errors. The electronic voting system tends to maximize user participation, by allowing them to vote from anywhere and from any device that has an internet connection. The blockchain is an emerging, decentralized, and distributed technology with strong cryptographic foundations that promises to improve different aspects of many industries. Expanding e-voting into blockchain technology could be the solution to alleviate the present concerns in e-voting. Here we propose a blockchain-based voting system that will limit the voting fraud and make the voting process simple, secure and efficient.

Keywords: Blockchain, Online voting, Decentralization, Privacy, Security, Ethereum.

I. INTRODUCTION

Voting is a way for a group, gathering, or electorates to decide something together or voice their opinion. Election campaigns, debates, and discussions are often followed by voting. Typically, a voter has the option to select candidates from the list or any additional candidates they so want. Voters must mark their ballots in secret voting booths, unsigned, so that no one else can see who they are voting for.

Many traditional offline services, including voting, postal delivery, and payment, are moving online due to the Internet's and information technologies' fast expansion. Voting is done online, a voter may cast their ballots from any place and transmit them electronically to the election officials. E-voting using blockchain, which is replacing traditional voting, is gaining more and more attention because of its great efficiency and flexibility. It has the advantages of being data-rich, real-time, and requiring high security, is a quick and affordable way to execute a voting operation.

Any form of digital system that incorporates blockchain experiences several advantages, especially on the security and business sides of any digital system. For security and accounting reasons, blockchain can be included into an online voting system. There are several aspects to integrating blockchain technology, from planning and design to producing nodes for distribution across various organizations. Additionally, blockchain technology may be used in a variety of commercial sectors. This illustrates how blockchain technology functions when consumers receive their health records electronically rather than on paper. This makes it possible for us to determine the advantages of utilising blockchain technology in an online procurement system.

Diverse mathematical equations with various scenarios and techniques to obtain commodities and goods are used to depict the procedure and technical elements of procurement, from purchase through announcement of winners. Online procurement systems will never be completely functional; there will always be some restrictions.

Blockchain technology makes e-voting cheaper, easier, and much more secure to implement. It is a considerably new paradigm that can help to form decentralized systems, which assure the data integrity, availability, and fault tolerance. This technology aims to revolutionize the systems. The blockchain systems are formed as decentralized networked systems of computers, which are used for validating and recording the pure online transactions. They also constitute ledgers, where digital data is tied to each other, called the blockchain. The records on the blockchain are essentially immutable.

Our work focuses on looking at important topics including end-to-end verification, vote secrecy, and voter anonymity. These difficulties serve as the cornerstone of a voting system that is effective while maintaining the fairness of the electoral process. In this work, we outline our efforts to investigate the potential of using blockchain technology to address these problems.

II. RELATED WORKS

A framework based on the adjustable blockchain that can apprehend the problems in the polling process, selection of the suitable hash algorithm is used. The effectiveness of the polling process is increased using hashing algorithms' utility, block creation and sealing, data accumulation, and result declaration by using the adjustable blockchain method [1]. The code-based Niederreiter technique is used to defend against quantum assaults. It realizes anonymous voters and provides the feature of audit by combining with traceable ring signature [2]. SeVEP, a cast-as-intended verifiability based on cryptographic primitives, which are used to design a complex voting interaction between the voting device. It satisfies the desirable security properties and offers computationally feasible solution [3]. PriScore, a secure decentralised self-tallying election system that allows voters to give each candidate on the ballot an arbitrary assessment score. The security analysis and formal security proof indicate that it achieves maximal ballot secrecy, multiple-voting detection and dispute freeness [4]. The applicability of the foraging theory to the context of a community where members cast ballots to sway others in their preferred community [5].

The traditional voting method and the benefits of implementing a blockchain-based electronic voting system using a case study of a manual voting procedure are analysed [6]. An electronic voting system using blockchain that uses voting data encryption in the same way that voting data is disclosed in electronic voting using the existing blockchain platform. It satisfies all the security requirements of the system and improves the performance of the algorithm by about 50 times than the existing algorithm [7]. A comprehensive review on the current state of the art of e-voting systems is presented. It tackles the problems like coercion-resistant, coercion-evident [8]. Assess the use of blockchain technology as a tool to create distributed electronic voting systems. Voters are masked behind an encrypted key, this offers greater privacy and security than traditional ballot boxes and could reduce voter suppression [9]. Research on blockchain-based voting systems will be reviewed and evaluated. Blockchain-supported voting systems may provide different solutions than traditional e-voting: coin-based, privacy and consensus [10].

Blockchain-based self-tallying voting systems and decentralised IoT architecture are combined in order to address the difficulties in self-tallying systems and give a practical structure. Self-tallying schemes are used which do not need a third party to tally the ballots and reveal the final result [11]. Signcryption and Ring Signature are used to ensure anonymity and a fair vote, and passwords are used to create a blank door to thwart attempts at pressure and bribery. The scheme protects against bribery and coercion behaviors, including getting all ballot information, checking the encrypted ballot [12]. k-anonymity, an unconditionally secure electronic voting system in which the voting system creates a polynomial in accordance with voter intent, calculates and distributes the shares among candidates and VS [13]. Understanding the unexplored topic by applying a practical evaluation framework to Helios Voting, one of the most widely used e-voting tools till date. It is fully-

operative, open source and auditable e-voting system, Helios Voting is a valid, almost free of charge option for minor elections in low-risk and low coercion environments [14]. A framework that can be implemented to conduct voting activity digitally through blockchain without involving any physical polling stations by using consensus algorithms. The usability of this system performs well by using the more effective approach of implementing a flexible consensus algorithm to reduce extensive computing resources in the blockchain [15].

A secure voter verifiable e-voting system is used, which incorporates the distributed ElGamal cryptosystem. Each cast ballot is encrypted before submission and remains encrypted at all times. The voters can cast their ballots by assigning arbitrary numbers of points to different candidates [16]. An end-to-end verifiable Internet-voting system (E2E-VIV), in which each voter is authenticated using a unique identifier issued by the appropriate authority and his biometric information. The system is secured against the existential forgery attack under chosen message and ID [17]. A two-round self-tallying Borda count e-voting scheme is proposed. This scheme does not require any trusted party to compute the tally. This scheme ensures the maximum voter privacy, and upon the successful completion of the protocol, the voters are strictly limited to learn only the tally of the election and their own inputs [18]. The most revealing e-voting solutions based on blockchain technology is reviewed. The use of blockchain as a voting method seems like an intriguing option [19]. d-BAME, a novel remote e-voting model for large-scale elections by proposing the participation of two conflicting parties to ensure election integrity and accountability. It is secure, preserves voter privacy, protects voters against coercers, and maintains the integrity of election results and is designed to run large-scale elections [20].

A secure and transparent e-voting mechanism through IoT devices using Blockchain technology is developed with the aim of detecting and resolving the various threats caused by an intruder at various levels. The proposed framework shows better success rate in all simulation results against DDoS threats and authentication mechanisms [21]. CrowdBC, a decentralised crowdsourcing framework built on blockchain technology, and assessed how the old centralised system suffers from privacy disclosure, single points of failure, and expensive service costs. The cases of meddling and infringement are reduced to enhance transparency in the voting process and establish faith in the democratic institutions crucial for working of modern societies [22]. The creation of an online procurement system and the use of blockchain technology is addressed. The integration of blockchain results to different benefits in digital signature, multi signature protocol, and blockchain notarization [23]. Details of the proposed e-voting scheme is presented along with its implementation using Multichain platform. The integration of e-voting with blockchain provides voter anonymity, vote confidentiality and end-to-end verification [24]. A blockchain-based electronic voting system is developed that satisfies all of the criteria for electronic voting. The system involves electronic voting theory, cryptography. It solves the problem on forgery of votes during e-voting along with non-repudiation [25].

Research on the security risks of online and electronic voting is reviewed, and shows the risks that persist in blockchain-based voting systems. Security is guaranteed if a majority of the mining hash power adheres to the protocol [26]. A blockchain-based voting system is proposed that uses blind signatures to ensure both the voters' privacy and the accuracy of their votes. To lessen the need on trust in our system, we replace TTP in the original FOO voting method with smart contracts. This voting system has many functional attributes and high efficiency, and it is suitable for large-scale voting [27]. A hybrid consensus model (PSC-Bchain) is suggested in which Proof of Credibility (PoC) and Proof of Stake (PoS) cooperate (PoS). Due to this, a safe hybrid blockchain was developed, which, when used with the e-voting system, guarantees comprehensive security [28]. An innovative blockchain-based traceable self-tallying e-voting mechanism is used to assist the consolidation of AI ecosystems. The proposed system satisfies features like multi-choice and self-tallying [29]. An Ethereum-based electronic voting system was developed. This system resolves the issue of fraudulent voting by enhancing the safety and reliability of the electronic voting system. This system has improved the counting error, tampering, cryptographic complexity [30].

III. METHODOLOGY

Unlike other programming frameworks where an administrator may add, delete, or change the data, blockchain is malleable. Anyone with access might tamper with the system and alter or remove the votes if such a system was utilised for voting. The blockchain technology changes this. A node cannot be changed or removed after it has been added to the chain, under any circumstances. The chain becomes immutable if a node is attacked by an attacker and the related nodes recognise it and repair the injured node. The voting method is independent of any specific computing node thanks to the decentralised nature of the blockchain. Even if one or more nodes are attacked or go down, the voting process still goes on as usual.

3.1 VOTING SYSTEM ARCHITECTURE

In Fig.1, a high-level architecture of the proposed system has been presented. It shows how the main stakeholders; Voters, VMS, AA, work together to perform certain voting tasks. All voters are connected to VMS directly through dAPP; it is either a mobile application or a web portal. The authority verifies voters registering in the system. Any voter who is verified and eligible to vote is allowed in the application to take part in voting.

The user interface of the programme is the initial component of the whole system process, and it also needs front-end security. Because the user inputs his credentials on that interface, it is crucial and should be safe and straightforward. Every user has full and equitable access to the system throughout voting activity. Additionally, it offers traceability once a vote has been cast. By using his credentials, the voter registers in the system. In order to register a voter in the system, VMS uses the information on their ID and confirms it against IA's online database. A distinct OTP is sent to the user to enable system access. Every time a voter tries to log into the VMS, an OTP is generated. The voter's complete information is kept in the VMS. Each voter receives one Ethereum Voting Coin after properly registering with the system. Each voter is prevented from double voting by storing the Hash value generated.

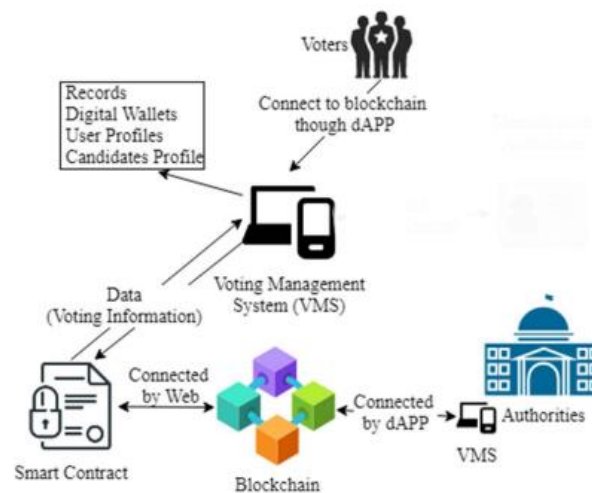


Fig.1. Voting System Architecture

3.2 WORKFLOW OF THE PROPOSED MODEL

The voter is added to the Voting Management System after completing the verification. On the blockchain, a single chain system is put into use. To maintain the integrity of the voter's vote, the system is also connected with the nation's national database. A transaction is created against the voter's National ID for each vote. The miners then mine the transaction and store it in the blockchain. Vote Coin from the voter's wallet is also used throughout the voting process. Once one vote coin has been used, the voter cannot cast another vote. As soon as the voter signs in using his or her credentials, the voter is sent to the election interface, where all of the candidates running in his constituency are listed. When a voter requests to vote, VMS checks the voting status of the voter on the blockchain by comparing the hash of all previous transactions with the voter's computerised National ID. If a transaction hash matching the voter's computerised National ID is discovered, the request will be rejected and the voter will be logged out of the system. The request to add the node is given to the miner if a voter hasn't cast their ballot yet. The miner chooses his preferred candidate and casts his ballot. The transaction is carried out by the miner and is tracked with the aid of a transaction hash. The node is then connected to the voting chain. To cast a ballot, a voter must have access to a smartphone or online browser. In order to make the voter's interface accessible to all users, many languages would be offered. At the time of voting, the suggested system has the capacity for a sizable number of voters. A voter may cast their ballot from anywhere in the globe thanks to a decentralised blockchain technology. A person can vote from anywhere, including from abroad, as long as his or her computerised National ID is validated against the national database before the vote is cast.

Voting transactions are forwarded to a pool, where miners study them and take the consensus from the other nodes before adding the malicious request to the chain. A cryptographic hash is used to completely safeguard the votes. A new block is added to the chain for each vote cast. By employing the vote coin, the system also ensures that each user may only cast one vote. The method makes guarantee that no voter has cast a duplicate vote, even if for some technical reason the balance of the voting coin does not change. Any node or request from a voter that the miner determines to be malicious is automatically rejected by examining whether the transaction hash is created against the voter's computerised National ID or not. The voter of that specific voting transaction is alerted through SMS to his registered phone number and email when the transaction completes and a node is successfully added to the Vote Chain. The voter has given a distinct transaction hash with which he may validate his vote using a web portal, and when the transaction has been properly completed, the vote has been included in the overall voting activity.

The voting process is managed by our system, which is supported by the blockchain. Every voter's transaction hash is kept on the chain, and all election results are likewise saved there. From there, users may access the election results dashboard to observe the outcomes of the election. The voting system first confirms that the voter is the nationality holder of the country and determines whether or not the voter has already cast a vote. If the voter still has a vote coin, the voting system permits him to cast a vote. After verifying the voting details i.e. voter identifier, vote, and timestamp was stored in the chain which saves vote details. The many parts of the voting management system are covered in this section. Voters can engage securely with the system using a user interface that also provides front-end security.

3.3 dAPP Setup

The front end of the VMS has been given a dAPP interface. A decentralised application built on blockchain technology is known as a dAPP. It utilises a blockchain network to operate. Because the user submits their credentials on that interface, user identification is crucial and must be uncompromised. Every voter has unequal access to the system, which also enables traceability of votes cast. The voter uses their credentials to log into the system. In order to register a user in the system, the system takes the user's ID information and verifies it against the database. The dAPP technology is used to guarantee VMS stability since decentralisation makes processing effective at all nodes. The other nodes in the system are not damaged if one becomes susceptible during the voting process. The other nodes reestablish the susceptible node.

3.4 ELECTION AS A SMART CONTRACT

While carrying out a transaction in the chain, smart contracts offer a safe connection between the user and the network. These are the regulations that apply to the whole blockchain and cannot, under any circumstances, be disregarded. To effectively save the vote in the system, all nodes must adhere to the smart contracts. The Can-Cast-Vote function, which verifies that the provided voter is eligible to cast a vote, is used in the first smart contract to verify users between AA and the VMS. It enters the voter information record after verification for further usage. A voting smart contract that defines which candidates will be displayed to the voter is tied to the voter. Voting is permitted if the consensus reached by the node and the chain is in agreement. It determines if the voter is eligible to cast a ballot by looking at the Vote Coin in his or her wallet. a feature Voters' National IDs and wallet addresses are inputted while casting a ballot, and a check is made to see if the user voting coin is available. The voter may only cast a vote if they have a voting currency; otherwise, the vote request is refused by the smart contract.

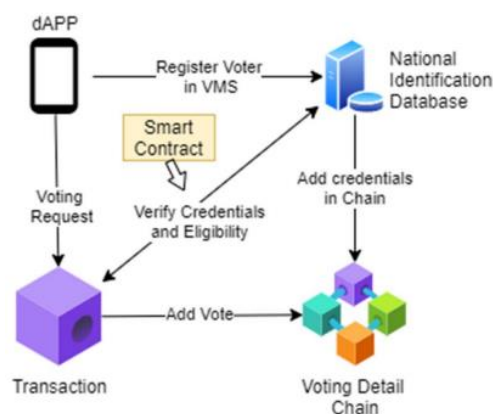
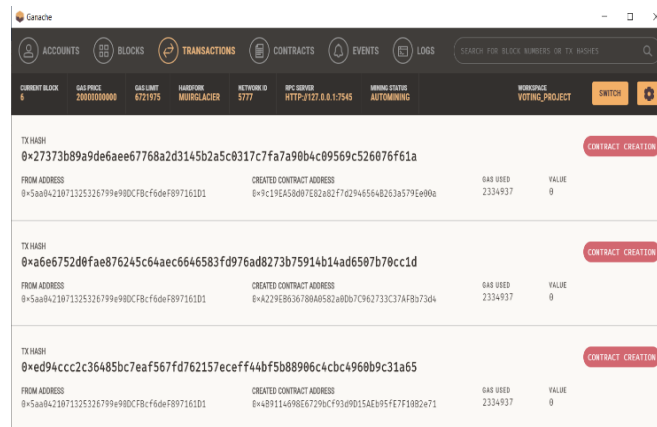


Fig.2. Smart Contract used in Proposed Model

Every vote is stored in the transaction and each voter gets a Transaction ID for his/her vote. Using a cryptographic hash, all the data contained in the transaction is highly encrypted. Each voter has a wallet that was provided by the government and is filled with voting coins. When a transaction is completed, the wallet is depleted by 0.04669874 ETH. It guarantees the voter won't be allowed to cast another ballot. The block in which the transaction is being executed is listed under the Block column; this is where the transaction is transmitted. The TX Hash is the transaction ID of a specific transaction. The information, including who received the vote, is what makes the transaction valuable.



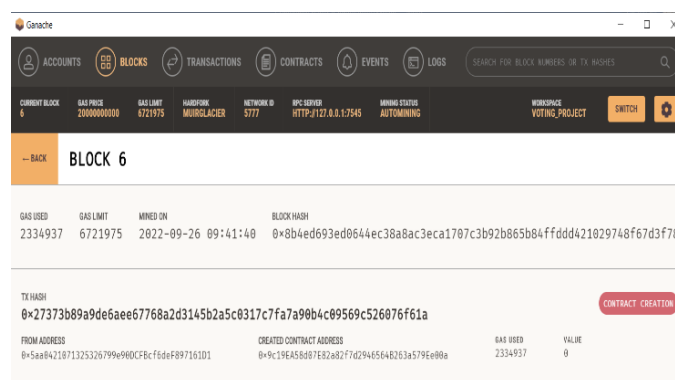
TX HASH	FROM ADDRESS	CREATED CONTRACT ADDRESS	GAS USED	VALUE
0x27373b89a9de6aee67768a2d3145b2a5c8317c7fa7a90b4c09569c526076f61a	0x5aa0421071325326799e90dcfbcf6daF897161D1	0x9c19E458d87E82a82F7d29465648263a579Ee00a	2334937	0
0xa6e6752d0fae876245c64aec6646583fd976ad827b75914b14ad6597b70cc1d	0x5aa0421071325326799e90dcfbcf6daF897161D1	0x4229E8036780A8582a8D07C962733C7AF8b7364	2334937	0
0xed94ccc2c36485bc7eaf567fd762157ecff44bf5b88906c4cbc4960b9c31a65	0x5aa0421071325326799e90dcfbcf6daF897161D1	0x48911469867290CF9d9D15AEb95FE7F1082a71	2334937	0

Fig.3. Transactions containing TX Hash and Gas used

When adding a new user to the system, a smart contract is shown. A voter cannot register to vote in the voting system more than once, according to this smart contract. The system uses a smart contract to confirm for each new registration request that the requested voter does not already exist in the chain. If a National ID is missing, the system transfers some Ethereum voting currency to the new voter's wallet and registers him as a voter. In a separate check, this smart contract also confirms the user's age to avoid flooding the network with unnecessarily numerous registrations. With the aid of Identification Authorities and his National ID, the age is confirmed.

3.5 CRYPTOGRAPHIC HASH

The data is kept secret from any system intruders thanks to cryptographic hashes, which also protect user identity privacy. Only the authorised owner of the transaction may use his private key to decode the transaction and read the content. Cryptographic hash employs encryption to make the transaction safe as it is transported over the network to be added to a node. By giving the voter the address of his transaction, the user's vote may be tracked, and the voter will be alerted as soon as the vote is cast. Voters can track their vote. The voting data consists of all the data that was recorded throughout the voting process. The information is still concealed, safe, and secure. The voter is the only one with access to the tracking data, and he or she may see and confirm his or her voting records. The voter's public key is used to lock the transaction once it has been stored in a block. The voter's public key is used to identify the node while monitoring the vote. To examine the transactions his wallet has done, the voter uses his private key. Voters can only watch their votes; after they've been cast, they can never go back and edit or remove them. Cryptography encrypts all user data sent during a transaction. The hash value is the tracking address of this block given to the voter to verify his vote.



GAS USED	GAS LIMIT	MINED ON	BLOCK HASH
2334937	6721975	2022-09-26 09:41:40	0x8b4ed693ed0644ec38a8ac3eca1707c3b92b865b04ffddd421029748f67d3f78

TX HASH	FROM ADDRESS	CREATED CONTRACT ADDRESS	GAS USED	VALUE
0x27373b89a9de6aee67768a2d3145b2a5c8317c7fa7a90b4c09569c526076f61a	0x5aa0421071325326799e90dcfbcf6daF897161D1	0x9c19E458d87E82a82F7d29465648263a579Ee00a	2334937	0

Fig.4. A Block in VMS

Blockchain technology emphasises secrecy and integrity. The blockchain communications are locked and unlocked by the system using signatures. As a result, only the voter has access to the message. A signature is produced using the user's private key and message. The results of the vote may be seen by election officials on the VMS dashboard after voting. The dashboard displays information about eligible candidates, registered voters, and election results.

IV. RESULTS

We created an online voting contract and put it on the voter's electronic voting system in order to create an online voting system based on the Ethereum platform. Table 1 presents a comparison and analysis of the blockchain-based electronic voting system and the existing voting method. This experiment evaluated whether the function of distributed ledger in a blockchain-based online voting system can provide voting credibility through the implementation of the Ethereum platform environment and the self-developed online voting contract. E-voting and blockchain-based e-voting improved turnout for voters who are handicapped or have limited mobility as compared to offline voting.

Table 1: Comparison and Analysis of other Voting Methods

Category	Offline Voting	Electronic Voting	Blockchain based Electronic Voting	Ethereum based Electronic Voting
Voter turnout	Low	High	High	High
Election cost	High	Low	Low	Low
Counting error	Possible to occur	Possible to occur	Impossible to occur	Impossible to occur
Tampering	Possible to occur	Possible to occur	Impossible to occur	Impossible to occur
Confidentiality	Low	High	High	High
Extendibility	Low	Low	Middle	High

Long-distance travel did not reduce voter participation, thanks to e-voting. Compared to the current paper voting system, election expenses can be reduced in several incidental expenditures, including labour costs. Each node must keep every vote registered using the blockchain technique in order for the blockchain to function decentralised.

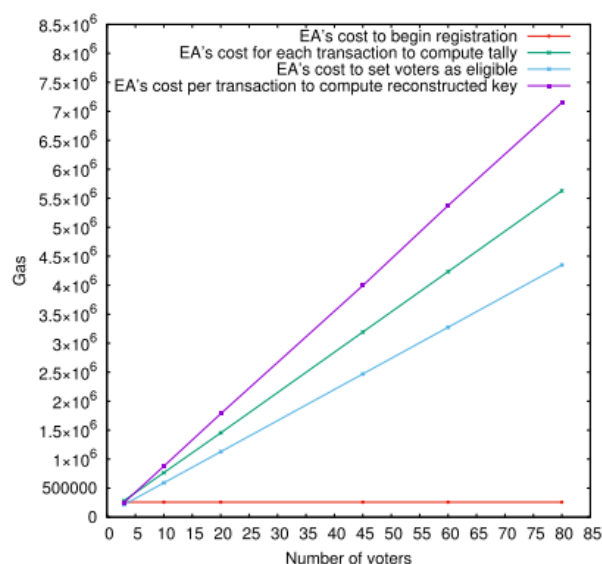


Fig 5. Gas cost for different tasks based on the number of voters participating in the elections.

As a result, a proof-of-work consensus mechanism like Bitcoin that demands financial remuneration for block production when running a voting system is inappropriate. It was created on the basis of earlier research on how to distribute and agree, or how to manufacture blocks in a certain order to prevent collisions. The blockchain-based electronic voting technique prevents this from happening. In terms of counting mistakes, the electronic voting method may be influenced by hackers and the server administrator changing their mind.

Finally, the electronic voting system based on blockchain increases voting accuracy by making it nearly difficult to rig or fake votes. Electronic voting based on Bitcoin has a higher level of cryptographic complexity than electronic voting based on Ethereum, which lowers performance. While offline voting does not require encryption, the complexity of encryption is relatively high in the current electronic voting system. While previous techniques of electronic voting demand a high level of confidentiality, Ethereum-based electronic voting does not. In particular, compared to the other techniques, only the Ethereum-based electronic voting system is extremely highly extensible. The current E-Voting system can only be extended to a certain extent because of the need for more management servers and TTPs (Tactics, Techniques, and Procedures) to handle the growing number of voters. This causes problems with interdependence and SPoF (Single Point of Failure), and in the case of a system based on Bitcoin, separate Bitcoin blocks. The extendability is constrained by the use of incompatible cryptographic technologies that requires each participant to install a separate software.

V. CONCLUSION

In this paper, we chose Ethereum, one of the blockchain technologies, as the foundation for our online voting system. In order to test if the online voting system can be developed while maintaining the credibility of vote counting, a Solidity-based smart contract was constructed and distributed among voters. However, since a contract cannot be changed after a Solidity-based smart contract is deployed to a blockchain account, future issues with system upkeep may occur. The secrecy of the vote's substance, the validity of the results, and the transparency of the voting process must all be guaranteed in any voting. These characteristics of voting system secrecy, trustworthiness, and transparency necessitate a high level of security. To ensure voter trust in the voting process and its outcomes, this initiative used extremely secure blockchain technology to create an online voting system with few location restrictions. The most widely used technique for bitcoin transactions—blockchain technology—was used in the study. Voters get voting coins from the server; they use the coins to cast their ballots and then return them. The voting results are stored in a database and transferred to the voting result database by the server that receives the voting coins. Voters may keep an eye on the entire process in real-time, which gives the voting process and results a high level of legitimacy. Voters will thus have more faith in the concept of online voting as a result of the high degree of security that has been established in the electronic voting system and the high level of credibility in the votes. This approach will make online voting easier and promote voting, helping to raise voter turnout and enabling a more democratic manner of decision-making for our modern society.

VI. FUTURE SCOPE

In the future, we intend to analyse the differences between the development languages now in use and Solidity, the smart contract programming language used by Ethereum, in order to enhance the accessibility and maintainability of smart contract development. One of the most difficult characteristics for a verified electronic voting system is coercion resistance, which we will take into account in our future work. Even while some current solutions employ the re-voting paradigm or phoney credentials to avoid coercion, they nevertheless have large computing costs or strict security requirements. We want to address these issues in the upcoming design.

REFERENCES

- [1] Shahzad, B., & Crowcroft, J. (2019). Trustworthy electronic voting using adjusted blockchain technology. *IEEE Access*, 7, 24477-24488.
- [2] Gao, S., Zheng, D., Guo, R., Jing, C., & Hu, C. (2019). An anti-quantum e-voting protocol in blockchain with audit function. *IEEE Access*, 7, 115304-115316.
- [3] Qureshi, A., Megías, D., & Rifà-Pous, H. (2019). SeVEP: Secure and verifiable electronic polling system. *IEEE Access*, 7, 19266-19290.
- [4] Yang, Y., Guan, Z., Wan, Z., Weng, J., Pang, H. H., & Deng, R. H. (2021). PriScore: blockchain-based self-tallying election system supporting score voting. *IEEE Transactions on Information Forensics and Security*, 16, 4705-4720.
- [5] Xu, L., Shen, Y., & Chan, H. C. (2017). Understanding content voting based on social foraging theory. *IEEE Transactions on Engineering Management*, 64(4), 574-585.
- [6] Pathak, M., Suradkar, A., Kadam, A., Ghodeswar, A., & Parde, P. (2021). Blockchain Based E-Voting System. *IEEE Transactions on Neural Networks and Learning Systems*.

- [7] Roh, C. H., & Lee, I. Y. (2020). A study on electronic voting system using private blockchain. *Journal of Information Processing Systems*, 16(2), 421-434.
- [8] Wang, K. H., Mondal, S. K., Chan, K., & Xie, X. (2017). A review of contemporary e-voting: Requirements, technology, systems and usability. *Data Science and Pattern Recognition*, 1(1), 31-47.
- [9] Patil, H. V., Rathi, K. G., & Tribhuwan, M. V. (2018). A study on decentralized e-voting system using blockchain technology. *Int. Res. J. Eng. Technol*, 5(11), 48-53.
- [10] Taş, R., & Tanrıöver, Ö. Ö. (2020). A systematic review of challenges and opportunities of blockchain for E-voting. *Symmetry*, 12(8), 1328.
- [11] Li, Y., Susilo, W., Yang, G., Yu, Y., Liu, D., Du, X., & Guizani, M. (2020). A blockchain-based self-tallying voting protocol in decentralized IoT. *IEEE Transactions on Dependable and Secure Computing*.
- [12] Hsiao, T. C., Wu, Z. Y., Liu, C. H., & Chung, Y. F. (2017). Electronic voting systems for defending free will and resisting bribery and coercion based on ring anonymous signcryption scheme. *Advances in Mechanical Engineering*, 9(1), 1687814016687194.
- [13] Liu, Y., & Zhao, Q. (2019). E-voting scheme using secret sharing and K-anonymity. *World Wide Web*, 22(4), 1657-1667.
- [14] Alonso, L. P., Gasco, M., del BLANCO, D. Y. M., Alonso, J. Á. H., Barrat, J., & Moreton, H. A. (2018). E-voting system evaluation based on the Council of Europe recommendations: Helios Voting. *IEEE Transactions on Emerging Topics in Computing*, 9(1), 161-173.
- [15] Farooq, M. S., Iftikhar, U., & Khelifi, A. (2022). A Framework to Make Voting System Transparent Using Blockchain Technology. *IEEE Access*, 10, 59959-59969.
- [16] Kumar, M., Chand, S., & Katti, C. P. (2020). A secure end-to-end verifiable internet-voting system using identity-based blind signature. *IEEE Systems Journal*, 14(2), 2032-2041.
- [17] Yang, X., Yi, X., Nepal, S., Kelarev, A., & Han, F. (2018). A secure verifiable ranked choice online voting system based on homomorphic encryption. *IEEE Access*, 6, 20506-20519.
- [18] Panja, S., Bag, S., Hao, F., & Roy, B. (2020). A smart contract system for decentralized borda count voting. *IEEE Transactions on Engineering Management*, 67(4), 1323-1339.
- [19] Benabdallah, A., Audras, A., Coudert, L., El Madhoun, N., & Badra, M. (2022). Analysis of Blockchain Solutions for E-Voting: A Systematic Literature Review. *IEEE Access*.
- [20] Zaghoul, E., Li, T., & Ren, J. (2021). d-BAME: distributed blockchain-based anonymous mobile electronic voting. *IEEE Internet of Things Journal*, 8(22), 16585-16597.
- [21] Rathee, G., Iqbal, R., Waqar, O., & Bashir, A. K. (2021). On the design and implementation of a blockchain enabled e-voting application within iot-oriented smart cities. *IEEE Access*, 9, 34165-34176.
- [22] Li, M., Weng, J., Yang, A., Lu, W., Zhang, Y., Hou, L., ... & Deng, R. H. (2018). CrowdBC: A blockchain-based decentralized framework for crowdsourcing. *IEEE Transactions on Parallel and Distributed Systems*, 30(6), 1251-1266.
- [23] Thio-ac, A., Domingo, E. J., Reyes, R. M., Arago, N., Jorda Jr, R., & Velasco, J. (2019). Development of a secure and private electronic procurement system based on blockchain implementation. *arXiv preprint arXiv:1911.05391*.
- [24] Khan, K. M., Arshad, J., & Khan, M. M. (2018). Secure digital voting system based on blockchain technology. *International Journal of Electronic Government Research (IJEGR)*, 14(1), 53-62.
- [25] Yi, H. (2019). Securing e-voting based on blockchain in P2P network. *EURASIP Journal on Wireless Communications and Networking*, 2019(1), 1-9.

- [26] Park, S., Specter, M., Narula, N., & Rivest, R. L. (2021). Going from bad to worse: from internet voting to blockchain voting. *Journal of Cybersecurity*, 7(1), tyaa025.
- [27] Zhou, Y., Liu, Y., Jiang, C., & Wang, S. (2020). An improved FOO voting scheme using blockchain. *International Journal of Information Security*, 19(3), 303-310.
- [28] Abuidris, Y., Kumar, R., Yang, T., & Onginjo, J. (2021). Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding. *Etri Journal*, 43(2), 357-370.
- [29] H. Li, Y. Li, Y. Yu, B. Wang and K. Chen, "A Blockchain-Based Traceable Self-Tallying E-Voting Protocol in AI Era," in *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 1019-1032, 1 April-June 2021, doi: 10.1109/TNSE.2020.3011928.
- [30] Ahn, B. (2022). Implementation and Early Adoption of an Ethereum-Based Electronic Voting System for the Prevention of Fraudulent Voting. *Sustainability*, 14(5), 2917.