Blockchain based E-voting System

PRABAL MALIK[1], GARIMA GUPTA[2], ARNAV JAIN[3], LUVJEET SINGH[4]
[1, 2, 3, 4] *Maharaja Agrasen Institute of Technology*

Abstract- ***E-voting, or electronic voting, refers to the use of electronic systems to facilitate the casting and counting of votes. One way to implement e-voting is through the use of blockchain technology, which can provide a secure and transparent way to record and tally votes. In a blockchain-based e-voting system, voters can cast their votes electronically using a device such as a computer or smartphone. The votes are then recorded on a distributed ledger, which is a database that is shared and maintained by multiple parties. Each vote is recorded as a transaction on the ledger, and the ledger is secured using cryptographic techniques to ensure that it cannot be altered. There are various possible benefits of using blockchain technology in e-voting. For one thing, it can aid in the prevention of voter fraud by giving a tamper-evident record of the votes cast. Furthermore, because the ledger is visible to everybody, it can strengthen the transparency of the voting process. This can contribute to increased trust in the voting process and results. Overall, the application of blockchain technology in e-voting has the potential to increase the integrity and transparency of the voting process, potentially leading to a global acceptance of e-voting systems. Smart contracts are significant bits of code that must be inserted into the blockchain and executed as scheduled in each phase of the blockchain update process. E-voting is another hot, but important, subject in the world of internet services. The blockchain, along with smart contracts, appears to be a promising option for application in the construction of safer, cheaper, more secure, transparent, and easier-to-use e-voting systems. Ethereum and its network are among the most ideal because to their stability, extensive use, and supply of smart contracts logic. An e-voting system must be safe, since it should not allow duplicate votes and be completely visible, all while respecting the participants' privacy. We built and tested an e-voting system in this project. Application as a smart contract for the Ethereum network written in Solidity.***

Indexed Terms- ***Blockchain, Ethereum, Decentralized, Digitalization***

I. INTRODUCTION

Extensive research has been conducted on electronic voting systems that allow people to vote whenever and wherever they choose using a cell phone, computer, or other electronic device. Nonetheless, because to the inherent security threats/concerns that these systems may pose to the integrity of the voting process, none of these technologies have been used on a wider scale. In this work, we present electronic voting systems that use blockchain, a safe and resilient technology that provides voter anonymity, transparency, and reliable operation.

Blockchain- A blockchain is a decentralized, distributed ledger that records transactions on multiple computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network. Each block in the chain contains a record of multiple transactions, and once a block is added to the chain it cannot be altered. This makes blockchains secure by design, as any attempt to alter a transaction would require the alteration of all subsequent blocks in the chain, which would be detected by the network.

Blockchains can be used for a wide range of applications, such as recording financial transactions, tracking the movement of goods, or even as a platform for smart contracts, which are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code.

One of the most well-known applications of blockchain technology is in the cryptocurrency Bitcoin, which uses a blockchain to track and verify transactions made with the digital currency. However, the potential uses for blockchains are

nearly limitless, and they are being explored in many different industries and applications.

II. LITERATURE SURVEY

A. The Blockchain Technology

The term "blockchain" refers to a chain of blocks, which are interconnected nodes that each have their own copy of the distributed ledger, which stores the history of all transactions. Mining is the method through which data is processed and stored in a block. Every block contains a hash of the preceding block, forming a chain, with the first block referred to as the genesis block. As a result, it generates a linked list structure. Blockchain includes many ledgers where data may only be appended but not erased or altered with. As a result, it is unchangeable. Blockchain can be either public (everyone can read or write data onto the blockchain) or private (restricted), in which case only a limited number of people can read or write data onto the blockchain.

B. Existing E-Voting Systems and Betterment using Blockchain

Since 2005, Estonia has used electronic voting (I-voting system). The foundation of this system is a national ID card issued to all people. These cards are encrypted files that uniquely identify the user and may be used for document signing, financial services, and other purposes. To vote, the voter must first enter their card into a card reader, following which they will be provided access to the voting website. Furthermore, the voter's eligibility is confirmed once they provide their information when requested on the internet interface. Once verified, the voter has until four days before election day to cast his or her vote and also change the casted vote.

Once a vote is cast, it is routed from the publicly visible vote forwarding server to the vote storage server, where it is encrypted and held until the online voting session expires. The vote information is transported from the vote storage server to an isolated vote counting server using DVDs. This server decrypts and counts the votes before generating the election results. However, malicious attacks that compromise the client-side machine by modifying the voters' votes without the voters' knowledge are possible. Another conceivable concern is that an attacker will directly infect the servers via malware planted on the DVDs used for vote transmission.

As a result of the presence of a susceptible centralised authority and database server to store and handle the votes, such an electronic-voting system raises security problems. To improve dependability and alleviate worries about manipulation from the client system, a system comprised of two blockchains—the vote blockchain and the voter blockchain—can be offered. This includes voter registration, followed by the voting procedure. During the registration procedure, the voter fills out a form with all of his or her personal information.

The system can be created using a three-tier architecture to simplify and scale the design: national, constituency, and local. The local layer includes all polling stations and is linked to a constituency node. All nodes in the constituency level are contained in the constituency tier. National nodes are in charge of mining votes and adding blocks to the voting blockchain. As part of the design, there is an encryption mechanism based on public and private keys, as well as a structure in which the data is logically separated and isolated. This segregation was accomplished by instructing the various constituency level nodes to produce unique key pairs.

The public key of a constituency node is then transmitted to polling station nodes linked to that constituency node, which utilise the public key to encrypt any votes cast at that polling stations. The votes and voter data from all constituency nodes are then encrypted and kept within the blockchain before being distributed to the whole network. As a result, even if a hacker obtains a constituency private key, he or she will only be able to decode a portion of the blockchain, namely the votes coming from that particular constituency node. As a result, this architecture makes the system more self-sufficient and secure. However, due to the high complexity associated with encrypting all votes, this method is not practically feasible for large-scale deployment.

C. Requirements

The existing e-voting systems suggested for use with blockchain technology may be characterised as having the following needs and features.

Verifiability by the general public: All players in the election process (including those observing the voting process) may verify the whole method and result.

Individual Verifiability: Each voter has the ability to confirm that his or her vote was correctly recorded and evaluated.

Reliability and dependability: To guard against assaults, asymmetric-key cryptography and different blockchain methods are used. To ensure that only genuine and confirmed votes are added to the blockchain network, digital signatures (blind signatures or short-linkable ring signatures) are employed to validate votes.

Consistency: Using blockchain consensus methods, all nodes have the same copy of records (same copy of blockchain) at any one moment, and all of them will have the same end outcome when the election process is through.

Auditability: If required, the entire operation may be audited after the election.

Anonymity: There is no link between voters and votes. Cryptography and the use of zero knowledge proofs to validate ballots assure complete voter anonymity.

Transparency: The entire procedure is available to the public. It is both secure and transparent.

Scalability: The digital signature process uses a short-linkable ring signature, which may handle a high number of voters.

Making certain that only qualified candidates get access to the system. Authentication: Authenticating people who want to use the e-voting system by using a unique voter ID and other credentials.
Fairness: The election results are not available in real time. Because there is no centralised authority, counting votes can only be done after the entire election process is completed, by decrypting the encrypted blocks in the blockchain network.

D. Blockchain Methodology for E-Voting System

Any blockchain-based e-voting system will consist of the following entities:

- Smart Contract Admin
- Voting Process Admin/Authorization
- Organization
- Smart Contract
- Voters

The operation of a rudimentary blockchain-based e-voting system is as follows: The block's first transaction is a special transaction that represents the candidate. It contains information on the candidate and serves as a basis for adding votes to that candidate. Creating one chain for each candidate, on the other hand, imposes a bigger overhead for storage and processing, making it more complex. Alternatively, crypto-voting has been investigated for implementation utilising sidechain technology, which connects two sidechains to a parent blockchain. Furthermore, one sidechain keeps voter and vote information, while the other sidechain stores the vote count, or results. This, however, makes the election outcomes visible throughout the voting process and undermines the idea of fairness in a democratic election.

An alternative architecture for the e-voting system might include a district node and a boot node, with the district node managing the boot node's smart contract. The system is decentralised since the district nodes collectively agree on whether a vote is valid or not.

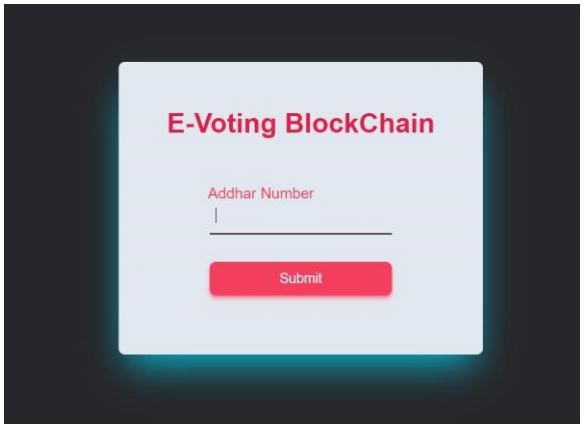
Smart contracts may be implemented using the frameworks listed below: Exonium, which employs the Rust programming language, Quorum, which is built on the Ethereum infrastructure, and Geth, which is an abbreviation for Go-Ethereum.
Ethereum is a platform for developing decentralised apps on either a public or private network.To utilise the public

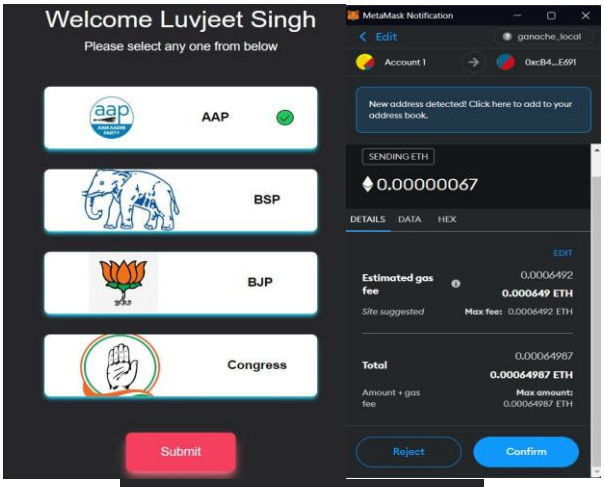
Ethereum platform, ethers are required. It validates and stores votes using a smart contract. The Ethereum framework, on the other hand, is a heavyweight framework.

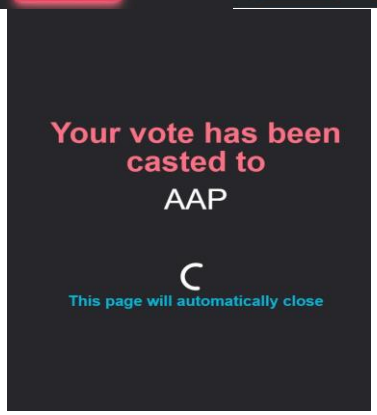
Private blockchain networks may be built using the Multichain architecture. Unlike the Ethereum network, it uses less computer power and is free to use. An e-voting system's key characteristic is anonymity—no one should know who the voter voted for. TTP (Trusted Third Party) can be utilised for this purpose. An authenticating institution, comparable to an electoral commission, is also required. Because multichain has both of these properties, it may be utilised as a blockchain network. In the multichain, each vote is viewed as an asset.

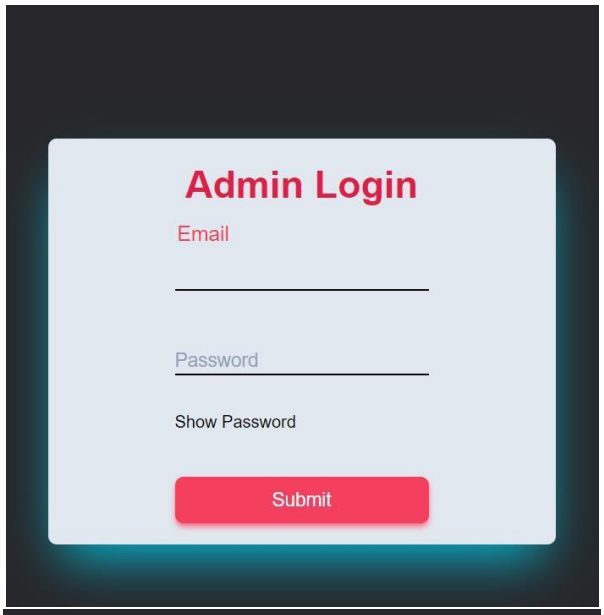
The voter must intend to vote before casting a ballot. Following the registration of voters, the authorization organisation issues each voter an identifying number to be used in the voting process, generates a public address in the multichain network, and saves it against the voter. During the voting procedure, the voter must provide his or her identity number as well as his or her secret message (vote). The vote is verified by a Trusted Third Party (TTP). The TTP produces a public key for the voter over the network and stores the information against the hash of the secret message and the voter's identity number. Multichain also limits the voter to only one vote.

Voters use their voter ID and credentials to access the system and examine the list of candidates during the evoting process. When a logged-in voter votes for a candidate, TTP verifies the voter's information and the vote cast and securely adds it to the blockchain network.









III. FUTURE RESEARCH DIRECTION

In terms of architecture and design, the blockchain-based e-voting systems reviewed and explained have several important aspects. However, significant system enhancements are conceivable, notably in terms of enhancing system scalability, in order to handle actual large-scale voting situations. The research presented on e-voting systems using blockchain not only demonstrates the benefits of such a system in terms of security, reliability, dependability, and transparency of the entire election process, but also encourages further research on utilising frameworks such as Hyperledger Sawtooth in designing an e-voting system to support scalability and practical application in realistic election scenarios. Table I outlines the research given.

Ensure total anonymity of the election process by removing any links between voters and votes. There is no need for separate blockchains for voter information and vote information, which would need additional storage and processing cost.

CONCLUSION

In this project, we presented a blockchain-based electronic voting system that uses smart contracts to enable safe and cost-effective elections while protecting voters' privacy. We have demonstrated that blockchain technology provides a new way to overcome the limits and adoption obstacles of electronic voting systems, ensuring election security and integrity and laying the groundwork for transparency. Using an Ethereum private blockchain, it is feasible to transmit hundreds of transactions per second onto the blockchain, employing every part of the smart contract to reduce the load on the blockchain. Some extra steps would be required for larger nations to provide higher transaction volume per second.

The openness of the block chain allows for increased auditing and understanding of elections. These are some of the characteristics of the needs of a voting system. These qualities emerge from decentralised networks and have the potential to bring more democratic procedures to elections, particularly direct election systems. A potential approach for making e-voting more open, transparent, and independently auditable would be to build it on blockchain technology.

This study investigates the possibilities of blockchain technology and its application in an e-voting method. The blockchain will be publicly verified and distributed in such a way that it cannot be corrupted.

REFERENCES

[1] *Kirillov, Denis, Vladimir Korkhov, Vadim Petrunin, Mikhail Makarov, Ildar M. Khamitov,*

and Victor Dostov. "Implementation of an EVoting Scheme Using Hyperledger Fabric Permissioned Blockchain." In International Conference on Computational Science and Its Applications, pp. 509-521. Springer, Cham, 2019.

[2] *Wang, Baocheng, Jiawei Sun, Yunhua He, Dandan Pang, and Ningxiao Lu. "Large-scale election based on blockchain." Procedia Computer Science 129 (2018): 234-237.*

[3] *Moura, Teogenes, and Alexandre Gomes. "Blockchain voting and its effects on election transparency and voter confidence." In Proceedings of the 18th Annual International Conference on Digital Government Research, pp. 574-575. ACM, 2017.*

[4] *"BlockchainTutorial." Weka, Solidity, Org.Json, AWS QuickSight, JSON.Simple, Jackson Annotations, Passay, Boon, MuleSoft, Nagios, Matplotlib, Java NIO, PyTorch, SLF4J, Parallax Scrolling, Java Cryptography. Accessed September 11, 2019. https://www.tutorialspoint.com/blockchain/index.htm*

[5] *Barnes, Andrew, Christopher Brake, and Thomas Perry. "Digital Voting with the use of Blockchain Technology." Plymouth University. Accessed Dezembro 15 (2016): 2017.*

[6] *Hardwick, Freya Sheer, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis. "EVoting with blockchain: an E-Voting protocol with decentralisation and voter privacy." In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1561-1567. IEEE, 2018.*

[7] *Ayed, Ahmed Ben. "A conceptual secure blockchainbased electronic voting system." International Journal of Network Security & Its Appli- cations 9, no. 3 (2017):01-09.*

[8] *Liu, Yi, and Qi Wang. "An E-voting Protocol Based on Blockchain." IACR Cryptology ePrint Archive 2017 (2017): 1043.*

[9] *Yu, Bin, Joseph K. Liu, Amin Sakzad, Surya Nepal, Ron Steinfeld, Paul Rimba, and Man Ho Au. "Platform-independent secure blockchain-based voting system." In International Conference on Information Secu- rity, pp. 369-386. Springer, Cham, 2018.*

[10] *Harsha V. Patil, Kanchan G. Rathi and Malati V. Tribhuwan. "A Study on Decentralized E-Voting System Using Blockchain Technology". International Research Journal of Engineering and Technology (IRJET). Volume: 05, Issue: 11, (Nov 2018).*

[11] *Fusco, Francesco, Maria Ilaria Lunesu, FILIPPO EROS Pani, and Andrea Pinna. "Crypto-voting, a Blockchain based e-Voting System." In KMIS, pp. 221-225. 2018.*

[12] *Hja´lmarsson, Fririk., Gunnlaugur K. Hreiarsson, Mohammad Hamdaqa, and G´ısli Hja´lmty´sson."Blockchain-based e-voting system." In 2018 IEEE 11th*

[13] *International Conference on Cloud Computing (CLOUD), pp. 983-986. IEEE, 2018. 13. Ganji, Raghavendra, and B. N. Yatish. "ELECTRONIC VOTING SYS- TEM USING BLOCKCHAIN." (2018).*

[14] *Yi, Haibo. "Securing e-voting based on blockchain in P2P network." EURASIP Journal on Wireless Communications and Networking 2019, no. 1 (2019): 137.*