# An e-voting application

Aashay Garg
Department of Computer Science and Information Systems
BITS Pilani, Pilani, India
aashaygarg2000@gmail.com

*Abstract* – **Scaling, cost, transparency have all been a key ingredient in the exercise of electing a representative through voting. The application built aims to solve these issues while being highly scalable and secure.**

## I. INTRODUCTION

Electoral integrity is essential not just for democratic nations but also for state voter's trust and liability. Political voting methods are crucial in this respect. From a government standpoint, electronic voting technologies can boost voter participation and confidence and rekindle interest in the voting system. As an effective means of making democratic decisions, elections have long been a social concern. As the number of votes cast in real life increases, citizens are becoming more aware of the significance of the electoral system. The voting system is the method through which judges judge who will represent in political and corporate governance. Democracy is a system of voters to elect representatives by voting. The efficacy of such a procedure is determined mainly by the level of faith that people have in the election process. The creation of legislative institutions to represent the desire of the people is a well-known tendency. Such political bodies differ from student unions to constituencies. Over the years, the vote has become the primary resource to express the will of the citizens by selecting from the choices they made.

The traditional or paper-based polling method served to increase people's confidence in the selection by majority voting. It has helped make the democratic process and the electoral system worthwhile for electing constituencies and governments more democratized. There are 167 nations with democracy in 2018, out of approximately 200, which are either wholly flawed or hybrid. The secret voting model has been used to enhance trust in democratic systems since the beginning of the voting system.

It is essential to ensure that assurance in voting does not diminish. A recent study revealed that the traditional voting process was not wholly hygienic, posing several questions, including fairness, equality, and people's will, was not adequately quantified and understood in the form of government.

Engineers across the globe have created new voting techniques that offer some anticorruption protection while still ensuring that the voting process should be correct. Technology introduced the new electronic voting techniques and methods, which are essential and have posed significant challenges to the democratic system. Electronic voting increases election reliability when compared to manual polling. In contrast to the conventional voting method, it has enhanced both the efficiency and the integrity of the process. Because of its flexibility, simplicity of use, and cheap cost compared to general elections, electronic voting is widely utilized in various decisions. Despite this, existing electronic voting methods run the danger of over-authority and manipulated details, limiting fundamental fairness, privacy, secrecy, anonymity, and transparency in the voting process. Most procedures are now centralized, licensed by the critical authority, controlled, measured, and monitored in an electronic voting system, which is a problem for a transparent voting process in and of itself.

On the other hand, the electronic voting protocols have a single controller that oversees the whole voting process. This technique leads to erroneous selections due to the central authority's dishonesty (election commission), which is difficult to rectify using existing methods. The decentralized network may be used as a modern electronic voting technique to circumvent the central authority.

Blockchain technology offers a decentralized node for online voting or electronic voting. Recently distributed ledger technologies such blockchain were used to produce electronic voting systems mainly because of their end-to-end verification advantages. Blockchain is an appealing alternative to conventional electronic voting systems with features such as decentralization, non-repudiation, and security protection. It is used to hold both boardroom and public voting. A blockchain, initially a chain of blocks, is a growing list of blocks combined with cryptographic connections. Each block contains a hash, timestamp, and transaction data from the previous block. The blockchain was created to be data-resistant. Voting is a new phase of blockchain technology; in this area, the researchers are trying to leverage benefits such as transparency, secrecy, and nonrepudiation that are essential for voting applications. With the usage of blockchain for electronic voting applications, efforts such as utilizing blockchain technology to secure and rectify elections have recently received much attention.

## II. Background

The first things that come to mind about the blockchain are cryptocurrencies and smart contracts because of the well-known initiatives in Bitcoin and Ethereum. Bitcoin was the first crypto-currency solution that used a blockchain data structure. Ethereum introduced smart contracts that leverage the power of blockchain immutability and distributed consensus while offering a crypto-currency solution comparable to Bitcoin. The concept of smart contracts was introduced much earlier by Nick Szabo in the 1990s and is described as "a set of promises, specified in digital form, including protocols within which the parties perform on these promises". In Ethereum, a smart contract is a piece of code deployed to the network so that everyone has access to it. The result of executing this code is verified by a consensus mechanism and by every member of the network as a whole.

Today, we call a blockchain a set of technologies combining the blockchain data structure itself, distributed consensus algorithm, public key cryptography, and smart contracts [18]. Below we describe these technologies in more detail.

Blockchain creates a series of blocks replicated on a peer-to-peer network. Any block in blockchain has a cryptographic hash and timestamp added to the previous block, as shown in Figure 1. A block contains the Merkle tree block header and several transactions [19]. It is a secure networking method that combines computer science and mathematics to hide data and information from others that is called cryptography. It allows the data to be transmitted securely across the insecure network, in encrypted and decrypted forms.

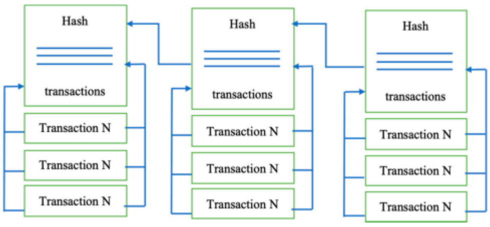

Fig. 1. Structure of a blockchain

As was already mentioned, the blockchain itself is the name for the data structure. All the written data are divided into blocks, and each block contains a hash of all the data from the previous block as part of its data. The aim of using such a data structure is to achieve provable immutability. If a piece of data is changed, the block's hash containing this piece needs to be recalculated, and the hashes of all subsequent blocks also need to be recalculated. It means only the hash of the latest block has to be used to guarantee that all the data remains unchanged. In blockchain solutions, data stored in blocks are formed from all the validated transactions during their creation, which means no one can insert, delete or alter transactions in an already validated block without it being noticed [24]. The initial zero-block, called the "genesis block," usually contains some network settings, for example, the initial set of validators (those who issue blocks). Blockchain solutions are developed to be used in a distributed environment. It is assumed that nodes contain identical data and form a peer-to-peer network without a central authority. A consensus algorithm is used to reach an agreement on blockchain data that is fault-tolerant in the presence of malicious actors. Such consensus is called ByzanFigure 1. The blockchain structure.

As was already mentioned, the blockchain itself is the name for the data structure. All the written data are divided into blocks, and each block contains a hash of all the data from the previous block as part of its data. The aim of using such a data structure is to achieve provable immutability. If a piece of data is changed, the block's hash containing this piece needs to be recalculated, and the hashes of all subsequent blocks also need to be recalculated. It means only the hash of the latest block has to be used to guarantee that all the data remains unchanged. In blockchain solutions, data stored in blocks are formed from all the validated transactions during their creation, which means no one can insert, delete or alter transactions in an already validated block without it being noticed. The initial zero-block, called the "genesis block," usually contains some network settings, for example, the initial set of validators (those who issue blocks).

Blockchain solutions are developed to be used in a distributed environment. It is assumed that nodes contain identical data and form a peer-to-peer network without a central authority. A consensus algorithm is used to reach an agreement on blockchain data that is fault-tolerant in the presence of malicious actors. Such consensus is called Byzantine fault tolerance, named after the Byzantine Generals' Problem. Blockchain solutions use different Byzantine fault tolerance (BFT) consensus algorithms: Those that are intended to be used in fully decentralized self-organizing networks, such as cryptocurrency platforms use algorithms such as proof-of-work or proof-of-stake, where validators are chosen by an algorithm so that it is economically profitable for them to act honestly. When the network does not need to be self-organized, validators can be chosen at the network setup stage. The point is that all validators execute all incoming transactions and agree on achieving results so that more than two-thirds of honest validators need to decide on the outcome.

Public key cryptography is used mainly for two purposes: Firstly, all validators own their keypairs used to sign consensus messages, and, secondly, all incoming transactions (requests to modify blockchain data) have to be signed to determine the requester. Anonymity in a blockchain context relates to the fact that anyone wanting to use cryptocurrencies just needs to generate a random keypair and use it to control a wallet linked to a public key. The blockchain solution guarantees that only the keypair owner can manage the funds in the wallet, and this property is verifiable. As for online voting, ballots need to be accepted anonymously but only from eligible voters, so a blockchain by itself definitely cannot solve the issue of voter privacy.

Smart contracts breathed new life into blockchain solutions. They stimulated the application of blockchain technology in efforts to improve numerous spheres. A smart contract itself is nothing more than a piece of logic written in code. Still, it can act as an unconditionally trusted third party in conjunction with the immutability provided by a blockchain data structure and distributed consensus. Once written, it cannot be altered, and all the network participants verify all steps. The great thing about smart contracts is that anybody who can set up a blockchain node can verify its outcome.

As is the case with any other technology, blockchain technology has its drawbacks. Unlike other distributed solutions, a blockchain is hard to scale: An increasing number of nodes does not improve network performance because, by definition, every node needs to execute all transactions, and this process is not shared among the nodes. Moreover, increasing the number of validators impacts performance because it implies a more intensive exchange of messages during consensus. For the same reason, blockchain solutions are vulnerable to various denial-of-service attacks. If a blockchain allows anyone to publish smart contracts in a network, then the operation of the entire network can be disabled by simply putting an infinite loop in a smart contract. A network can also be attacked by merely sending a considerable number of transactions: At some point, the system will refuse to receive anything else. In cryptocurrency solutions, all transactions have an execution cost: the more resources a transaction utilizes, the more expensive it will be, and there is a cost threshold, with transactions exceeding the threshold being discarded. In private blockchain networks, this problem is solved depending on how the network is implemented via the exact mechanism of transaction cost, access control, or something more suited to the specific context.

Blockchain technology fixed shortcomings in today's method in elections made the polling mechanism clear and accessible, stopped illegal voting, strengthened the data protection, and checked the outcome of the polling. The implementation of the electronic voting method in blockchain is very significant. However, electronic voting carries significant risks such as if an electronic voting system is compromised, all cast votes can probably be manipulated and misused. Electronic voting has thus not yet been adopted on national scale, considering all its possible advantages. Today, there is a viable solution to overcome the risks and electronic voting, which is blockchain technology. In traditional voting systems, we have a central authority to cast a vote. If someone wants to modify or change the record, they can do it quickly; no one knows how to verify that record. One does not have the central authority; the data are stored in multiple nodes. It is not possible to hack all nodes and change the data. Thus, in this way, one cannot destroy the votes and efficiently verify the votes by tally with other nodes.

If the technology is used correctly, the blockchain is a digital, decentralized, encrypted, transparent ledger that can withstand manipulation and fraud. Because of the distributed structure of the blockchain, a Bitcoin electronic voting system reduces the risks involved with electronic voting and allows for a tamper-proof for the voting system. A blockchain-based electronic voting system requires a wholly distributed voting infrastructure. Electronic voting based on blockchain will only work where the online voting system is fully controlled by no single body, not even the government. To sum-up, elections can only be free and fair when there is a broad belief in the legitimacy of the power held by those in positions of authority. The literature review for this field of study and other related experiments may be seen as a good path for making voting more efficient in terms of administration and participation. However, the idea of using blockchain offered a new model for electronic voting.

## III. Related Work

Several articles have been published in the recent era that highlighted the security and privacy issues of blockchain-based electronic voting systems. Reflects the comparison of selected electronic voting schemes based on blockchain.

The open vote network (OVN) was presented by [1], which is the first deployment of a transparent and self-tallying internet voting protocol with total user privacy by using Ethereum. In OVN, the voting size was limited to 50–60 electors by the framework. The OVN is unable to stop fraudulent miners from corrupting the system. A fraudulent voter may also circumvent the voting process by sending an invalid vote. The protocol does nothing to guarantee the resistance to violence, and the electoral administrator wants to trust.

Furthermore, since solidity does not support elliptic curve cryptography, they used an external library to do the computation [2]. After the library was added, the voting contract became too big to be stored on the blockchain. Since it has occurred throughout the history of the Bitcoin network, OVN is susceptible to a denial-of-service attack.

Lai et al. [3] suggested a decentralized anonymous transparent electronic voting system (DATE) requiring a minimal degree of confidence between participants. They think that for large-scale electronic elections, the current DATE voting method is appropriate. Unfortunately, their proposed system is not strong enough to secure from DoS attacks because there was no third-party authority on the scheme responsible for auditing the vote after the election process. This system is suitable only for small scales because of the limitation of the platform [4]. Although using Ring Signature keeps the privacy of individual voters, it is hard to manage and coordinate several signer entities. They also use PoW consensus, which has significant drawbacks such as energy consumption: the "supercomputers" of miners monitor a million computations a second, which is happening worldwide. Because this arrangement requires high computational power, it is expensive and energy-consuming.

Shahzad et al. [5] proposed the BSJC proof of completeness as a reliable electronic voting method. They used a process model to describe the whole system's structure. On a smaller scale, it also attempted to address anonymity, privacy, and security problems in the election. However, many additional problems have been highlighted. The proof of labor, for example, is a mathematically vast and challenging job that requires a tremendous amount of energy to complete. Another problem is the participation of a third party since there is a significant risk of data tampering, leakage, and unfair tabulated results, all of which may impact end-to-end verification. On a large scale, generating and sealing the block may cause the polling process to be delayed [4].

Gao et al. [4] has suggested a blockchain-based anti-quantum electronic voting protocol with an audit function. They have also made modifications to the code-based Niederreiter algorithm to make it more resistant to quantum assaults. The Key Generation Center (KGC) is a certificateless cryptosystem that serves as a regulator. It not only recognizes the voter's anonymity but also facilitates the audit's functioning. However, an examination of their system reveals that, even if the number of voters is modest, the security and efficiency benefits are substantial for a small-scale election. If the number is high, some of the efficiency is reduced to provide better security [6].

Yi [7] presented the blockchain-based electronic voting Scheme (BES) that offered methods for improving electronic voting security in the peer-to-peer network using blockchain technology. A BES is based on the distributed ledger (DLT) may be employed to avoid vote falsification. The system was tested and designed on Linux systems in a P2P network. In this technique, counter-measurement assaults constitute a significant issue. This method necessitates the involvement of responsible third parties and is not well suited to centralized usage in a system with many agents. A distributed process, i.e., the utilization of secure multipart computers, may address the problem. However, in this situation, computing expenses are more significant and maybe prohibitive if the calculation function is complex and there are too many participants. [8,9].

Khan, K.M. [10] has proposed block-based e-voting architecture (BEA) that conducted strict experimentation with permissioned and permissionless blockchain architectures through different scenarios involving voting population, block size, block generation rate, and block transaction speed. Their experiments also uncovered fascinating findings of how these parameters influence the overall scalability and reliability of the electronic voting model, including interchanges between different parameters and protection and performance measures inside the organization alone. In their scheme, the electoral process requires the generation of voter addresses and candidate addresses. These addresses are then used to cast votes from voters to candidates. The mining group updates the ledger of the main blockchain to keep track of votes cast and the status of the vote. The voting status remains unconfirmed until a miner updates the main ledger. The vote is then cast using the voting machine at the polling station.

However, in this model, there are some flaws found. There is no regulatory authority to restrict invalid voters from casting a vote, and it is not secure from quantum attach. Their model is not accurate and did not care about voter's integrity. Moreover, their scheme using Distributed consensus in which testimonies (data and facts) can be organized into cartels because fewer people keep the network active, a "51This attack is potentially more concentrated and did not discuss scalability and delays in electronic voting, which are the main concerns about the blockchain voting system. They have used the Multichain framework, a private blockchain derived from Bitcoin, which is unsuitable for the nationwide voting process. As the authors mentioned, their system is efficient for small and medium-sized voting environments only.

## IV. Proposed Application

The application makes use of the ethereum blockchain network to ensure transparency while being highly scalable and secure. The application has been built with the use of javascript to ensure a smooth UI which can be further improved so as to ensure a smoother and richer experience.

The Aadhaar based voting system is developed to overcome the flaws of EVM system. The authority must login first with the provided session ID. The voter can now begin the process of voting with proper authentication through OTP(one time password) on the respective linked mobile number. If the voter is valid then the system will check for for the voters age and the address to which he can give vote. The voting pallete will be opened with candidate names,their parties and logos. Now the voter can give his vote by clicking vote button. One voter can vote only once,i.e after one time voting buttons are disabled and the vote is automatically loged out. Same process continues for many more voters irrespective of their voting wards.

The authority login is to ensure security to prevent piracy, harassment and corruption from candidates standing in election. OTP generation is to authenticate the right aadhar card owner. Button disabling and automatic logout is to prevent multiple voting by single candidate.

The code for the same can be found at https://github.com/aashaygarg/E-voting

## V. Application Dependencies

To implement the application we must have the following dependencies installed. Below are the list of dependencies which have been used to develop the application. Detailed information about each can be found on their respective websites and corresponding Github repositories.

*1) JavaScript:* JavaScript, often abbreviated JS, is a programming language that is one of the core technologies of the World Wide Web, alongside HTML and CSS. Over 97percent of websites use JavaScript on the client side for web page behavior, often incorporating thirdparty libraries. This is the main framework which the application uses to get integrated to web3, web2, IPFS, metamask, localhost, etc.

*2) Metamask:* Metamask is a plugin for browsers which allows to make Ethereum transactions. It allows to run Ethereum Dapps (Decentralised applications) without having to run the full Ethereum node, manage identities and sign Blockchain transactions. This is a wallet node on the blockchain which enables us to use our funds in the Dapp provided with proper authentication from the user.

*3) Ganache:* Ganache is an Ethereum Blockchain emulator. Ganache is in-memory Ethereum node that allows to test all components locally. It also lets users deploy contracts, develop application and run tests. This tool has been used to test the functionality of the application over the blockchain environment and proper working of the smart contracts.

*4) Truffle:* Truffle is used to compile, test, build smart contracts and provides a development framework to increase speed in the development process. Used to compile the smart-contracts and deploy them over the Ethereum blockchain.

*5) Node.js:* : Node.js is an open-source, cross-platform, backend JavaScript runtime environment that runs on the V8 engine and executes JavaScript code outside a web browser. Used for running the application, provides a runtime environment and executes the JavaScript code.

*6) Bootstrap:* Bootstrap is a free and open-source CSS framework directed at responsive, mobile-first frontend web development. It contains HTML, CSS and JavaScript-based design templates for typography, forms, buttons, navigation, and other interface components. User to code a user friendly front-end interface.

## VI. CONCLUSIONS

The goal of this application is to analyze and evaluate current research on blockchain based electronic voting systems. The article discusses recent electronic voting research using blockchain technology. The blockchain concept and its uses are presented first, followed by existing electronic voting systems. Then, a set of deficiencies in existing electronic voting systems are identified and addressed in the application. The blockchain's potential is fundamental to enhance electronic voting, current solutions for blockchain-based electronic voting, and possible research paths on blockchain-based electronic voting systems. Numerous experts believe that blockchain may be a good fit for a decentralized electronic voting system.

Furthermore, all voters and impartial observers may see the voting records kept in these suggested systems. On the other hand, researchers discovered that most applications on blockchain-based electronic voting identified and addressed similar issues. There have been many study gaps in electronic voting that need to be addressed in future studies. Scalability attacks, lack of transparency, reliance on untrustworthy systems, and resistance to compulsion are all potential drawbacks that must be addressed. As further research is required, we are not entirely aware of all the risks connected with the security and scalability of blockchain-based electronic voting systems. Adopting blockchain voting methods may expose users to unforeseen security risks and flaws. Blockchain technologies require a more sophisticated software architecture as well as managerial expertise. The above-mentioned crucial concerns should be addressed in more depth during actual voting procedures, based on experience. As a result, electronic voting systems should initially be implemented in limited pilot areas before being expanded. Many security flaws still exist in the internet and polling machines. Electronic voting over a secure and dependable internet will need substantial security improvements. Despite its appearance as an ideal solution, the blockchain system could not wholly address the voting system's issues due to these flaws. This research revealed that blockchain systems raised difficulties that needed to be addressed and that there are still many technical challenges. That is why it is crucial to understand that blockchain-based technology is still in its infancy as an electronic voting option.

## VII. References

1. McCorry, P.; Shahandashti, S.F.; Hao, F. A smart contract for boardroom voting with maximum voter privacy. In Proceedings of the International Conference on Financial Cryptography and Data Security, Sliema, Malta, 3–7 April 2017.

2. Woda, M.; Huzaini, Z. A Proposal to Use Elliptical Curves to Secure the Block in E-voting System Based on Blockchain Mechanism. In Proceedings of the International Conference on Dependability and Complex Systems, Wrocław, Poland, 28 June–2 July 2021

3. Lai, W.J.; Hsieh, Y.C.; Hsueh, C.W.; Wu, J.L. Date: A decentralized, anonymous, and transparent e-voting system. In Proceedings of the 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, China, 15–17 August 2018

4. Gao, S.; Zheng, D.; Guo, R.; Jing, C.; Hu, C. An Anti-Quantum E-Voting Protocol in Blockchain with Audit Function. IEEE Access 2019, 7, 115304–115316.

5. Shahzad, B.; Crowcroft, J. Trustworthy Electronic Voting Using Adjusted Blockchain Technology. IEEE Access 2019, 7, 24477–24488

6. Fernández-Caramés, T.M.; Fraga-Lamas, P. Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. IEEE Access 2020, 8, 21091–21116.

7. Yi, H. Securing e-voting based on blockchain in P2P network. EURASIP J. Wirel. Commun. Netw. 2019, 2019, 137

8. Torra, V. Random dictatorship for privacy-preserving social choice. Int. J. Inf. Secur. 2019, 19, 537–543.

9. Alaya, B.; Laouamer, L.; Msilini, N. Homomorphic encryption systems statement: Trends and challenges. Comput. Sci. Rev. 2020, 36, 100235

10. Khan, K.M.; Arshad, J.; Khan, M.M. Investigating performance constraints for blockchain based secure e-voting system. Future Gener. Comput.Syst. 2020, 105, 13–26.