

Blockchain-Based Electronic Voting System

Samarth Malik¹, Umesh Kaushik², Anu Rathee³, Shikha Gupta⁴

B.Tech Scholar, Information Technology Department, Maharaja Agrasen Institute Of Technology, Rohini, New Delhi
110086 India^{1,2}

Assistant Professor, Information Technology Department, Maharaja Agrasen Institute Of Technology, Rohini, New
Delhi 110086 India^{3,4}

Abstract: Blockchain technology has the potential to address a number of challenges in the field of elections, particularly in terms of security and transparency. A decentralized online voting system using blockchain could provide a secure and tamper-proof way of conducting elections, as the decentralized nature of the technology would make it difficult for any single entity to manipulate the data. The use of a distributed ledger would also ensure that the results of the election are transparent and verifiable, as all nodes in the network would have access to the same data. Additionally, such a system could potentially make the voting process more convenient and accessible for voters, as they would be able to cast their ballots online from anywhere. Overall, the adoption of blockchain technology in the electoral process has the potential to greatly improve the integrity and fairness of election

Keywords: Blockchain, Ethereum, Smart Contract, Solidity, Electronic-Voting, SHA-256.

I. INTRODUCTION

Blockchain is a decentralized technology that allows for the creation of a distributed database or ledger. It was originally developed for use in financial transactions, but has since been adopted for a variety of applications, including the Internet of Things and the healthcare sector. One key feature of blockchain is that it is trustless, meaning that nodes in the network hold data locally and do not need to rely on a central authority to verify transactions. The Ethereum network, which includes a complete programming language and allows for the use of smart contracts, has further expanded the potential uses for blockchain. Overall, blockchain offers a range of benefits, including increased security and transparency, as well as the ability to create decentralized systems.

Blockchain technology is rapidly gaining popularity in a variety of industries, including procurement management, healthcare, payments, business, Internet of Things (IoT), and voting systems. One reason for its success is its ability to provide high levels of transparency and security. Traditional voting systems, such as ballot box voting or electronic voting machines (EVMs), can be susceptible to various security threats such as DDoS attacks, voting booth capturing, vote-rigging and fraud, and malware attacks. These systems can also require significant amounts of paperwork, human resources, and time, which can create a sense of mistrust among users

By using blockchain technology in the voting process, it is possible to make the system more secure, transparent, consistent, and reliable. For example, when an eligible voter casts their vote using an EVM, there is no way to track whether the vote was counted properly or if it was diverted to someone else's account. However, if the voting process is conducted using blockchain technology, each vote is processed as a transaction and the voter is given a receipt (in the form of a transaction ID) that can be used to verify that their vote was counted correctly.

Another advantage of using blockchain in voting systems is its ability to provide immutability, which makes it difficult for anyone to modify or delete data. This is in contrast to database programs like SQL or PHP, where it is possible to add, modify, or delete data. In a blockchain system, once data is entered, it remains there permanently and cannot be controlled by any single entity.

However, it is important to note that simply building a blockchain system is not enough to ensure the security and transparency of a voting process. The system must also be decentralized, meaning that if one server goes down or there is an issue with a particular node, other nodes can continue to operate normally without waiting for the affected node to be recovered. This ensures that the system remains reliable even in the event of technical problems or attacks. Types of Blockchain:-

Blockchain technology can be classified into three types based on its network design: public, private, and consortium. The type of blockchain chosen for a particular organization depends on its performance, data analysis, and accessibility

requirements. Public blockchain networks are open to all users and offer the highest level of transparency and security, while private blockchain networks are restricted to specific users and offer a higher level of control over data. Consortium blockchain networks fall between these two extremes and are governed by a group of organizations. Organizations may choose to shift data from their databases to the blockchain in order to take advantage of its security and reliability.

Public Blockchain:-

Public blockchain networks are open to all users and do not have any restrictions on access. These networks typically use Proof of Work or Proof of Stake algorithms to verify transactions and may offer incentives for users who participate in block verification. Public blockchain architectures allow users to download the protocol at any time without the need for permission. This decentralization makes public blockchains highly secure and resistant to tampering, but they can also incur higher transaction costs and may have issues with scalability. Despite these drawbacks, public blockchains offer a viable model that can make the technology industry more profitable.

Private blockchain:-

Private blockchain networks are restricted and can only be accessed by authorized users. These networks are often run by a single organization or group of organizations and operate based on access controls that limit participation. Private blockchains offer a high level of trust, as they are controlled by a known entity and only allow participating organizations to access the network. However, private blockchains may not offer the same level of transparency and decentralization as public blockchain networks. They may also be less secure, as they rely on the trustworthiness of the controlling organization rather than the decentralized consensus of the network as a whole.

Consortium blockchain:-

A consortium blockchain is a hybrid of public and private blockchain networks, offering a combination of their respective features. Like public blockchain networks, consortium blockchain networks allow users to join the network without permission. However, unlike public blockchain networks, ownership of the network does not fall into the hands of a single entity or company. Instead, a group of users who are responsible for verifying transactions and enforcing network rules are designated as regulators or verifiers. Consortium blockchain networks offer a level of decentralization and trust similar to that of public blockchain networks, while also providing the control and access restrictions of private blockchain networks.

Advantages Of Blockchain

Blockchain technology is known for its ability to provide transparency, consistency, and reliability through the recording of every action in a distributed ledger that is available to all participants in the network. This type of recording ensures that data cannot be altered or deleted, which enhances the credibility of the blockchain. The credibility of a blockchain is based on the trust of two or more participants who do not know each other, but are able to engage in real transactions. This trust can be continuously strengthened through the sharing of multiple processes and records. Additionally, blockchain technology can significantly reduce the time it takes to process transactions, making it a more efficient option compared to traditional methods. Overall, the use of blockchain technology can greatly improve the speed, security, and transparency of various processes.

Disadvantages of Blockchain

While blockchain technology is generally considered to be secure, it is not completely immune to attacks. One potential vulnerability is the possibility of a group of individuals gaining control of 51% of the nodes on a blockchain network. While this may be difficult to accomplish on large and popular networks, it could be more feasible on smaller networks. Another challenge with blockchain technology is the power-intensive process of signature verification, which requires significant computing resources. Additionally, one of the drawbacks of using blockchain is the high cost of transactions, which can average around \$75-\$80 per transaction. This is largely due to the high initial capital required to set up a blockchain network. Despite these challenges, blockchain technology continues to be a promising solution for a variety of applications due to its ability to provide secure and transparent record-keeping.

II. LITERATURE SURVEY

Blockchain technology has been extensively researched for its potential use in secure and transparent voting systems. There are various strategies for ensuring the integrity of the voting process, including the use of cryptography and secret keys for voter verification, as well as the implementation of PINs and electronic IDs for identification at polling stations. It is important for voters to be registered and for voter keys to be distributed to eligible voters in order to prevent fraud and ensure that only authorized individuals are able to cast their ballots. In order to further ensure the

security and transparency of the voting process, it is necessary to have a thorough understanding of the problem-solving process and the various verification strategies that can be employed using blockchain technology. By implementing these measures, it is possible to create a decentralized and secure voting system that can be trusted by all participants.

How to: -

Blockchain is a decentralized network of computers that share and store data in a digital format. It was originally developed for use in cryptocurrency systems, but has since been applied to a variety of other fields as well. One of the key features of blockchain technology is its ability to ensure the integrity and security of data records, creating trust without the need for a central authority. This is accomplished through the use of blocks, which are groups of information that are connected in a chain, forming a series of data known as a "blockchain." Each block contains its own unique hash code, as well as a record of the previous block's hash, and is added to the chain in chronological order. This makes it difficult to alter the data in the blockchain without the consensus of the majority of the network.

In addition to its security features, blockchain also offers other benefits such as transparency and decentralization. Data stored in a blockchain is distributed among multiple nodes in different locations, which not only creates duplication but also helps to maintain the integrity of the data. If someone tries to change the data on one node, the other nodes will not be affected, which can prevent bad actors from tampering with the information.

One of the key tools used to ensure the security and integrity of data in a blockchain is the use of hash functions. A hash function is a mathematical function that converts digital information into a series of alphanumeric characters, known as a hash code. If the input data is altered in any way, the resulting hash code will also change, making it easy to detect tampering. One example of a widely used hash function is SHA-256

Hashing:-

Blockchain technology is rapidly gaining popularity in a variety of industries, including procurement management, healthcare, payments, business, Internet of Things (IoT), and voting systems. One reason for its success is its ability to provide high levels of transparency and security. Traditional voting systems, such as ballot box voting or electronic voting machines (EVMs), can be susceptible to various security threats such as DDoS attacks, voting booth capturing, vote-rigging and fraud, and malware attacks. These systems can also require significant amounts of paperwork, human resources, and time, which can create a sense of mistrust among users. By using blockchain technology in the voting process, it is possible to make the system more secure, transparent, consistent, and reliable. For example, when an eligible voter casts their vote using an EVM, there is no way to track whether the vote was counted properly or if it was diverted to someone else's account. However, if the voting process is conducted using blockchain technology, each vote is processed as a transaction and the voter is given a receipt (in the form of a transaction ID) that can be used to verify that their vote was counted correctly.

Another advantage of using blockchain in voting systems is its ability to provide immutability, which makes it difficult for anyone to modify or delete data. This is in contrast to database programs like SQL or PHP, where it is possible to add, modify, or delete data. In a blockchain system, once data is entered, it remains there permanently and cannot be controlled by any single entity.

Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein are stored and replicated on a blockchain network. Smart contracts allow for the automation of certain processes, which can save time and reduce the potential for errors.

One type of smart contract is a "smart legal contract," which is a legally binding contract that is written in both natural language and code. The natural language component outlines the terms of the agreement, while the code automatically activates the contract's provisions. In the event of non-compliance, the contract is still legally binding and all common dispute resolution mechanisms can be utilized.

Another type of smart contract is a decentralized autonomous organization (DAO). A DAO is a type of online organization that is owned and operated by its members. It operates without a central leadership and decisions are made from the bottom up, governed by a set of rules enforced on the blockchain. DAOs can have various objectives and include built-in savings accounts that can only be accessed with the consent of the members. One example of a DAO is the project launched in 2016, which ultimately failed and led to a significant split in the Ethereum network.

Once a smart contract is deployed, it is assigned to a unique 160-bit address and is executed whenever a transaction is made using that address. The execution of the contract is carried out by a network of miners who are responsible for maintaining the blockchain. They reach a consensus on the outcome of the smart contract and update the blockchain accordingly. It is important to note that once a smart contract is included in the blockchain, the program code is fixed and cannot be updated.

Application Logic Contracts (ALCs) are a type of smart contract that contain code based on an application that is consistent with other blockchain contracts. They enable the integration of the Internet of Things (IoT) and blockchain

technology by allowing connections to various devices. ALCs are a vital part of a multi-functional smart contract and operate under a management system.

In the Ethereum blockchain platform, the payment required for a successful operation or contract is known as "gas." Gas is paid in small amounts of cryptocurrency called ether, also known as gwei or nanoeth, and is used to allocate Ethereum virtual machine (EVM) resources so that applications such as smart contracts can operate securely but independently. The price of gas is determined by the supply and demand among network miners, who can choose not to process the work if the gas price does not meet their threshold, and network users who want processing power. Gas payments are made by users to compensate for the computer power needed to process and verify transactions in the Ethereum blockchain. The "gas limit" refers to the maximum amount of gas (or energy) intended to be used for a specific purpose. A high gas limit means that more work needs to be done using ETH or a smart contract.

Recently, there has been increasing interest in second-generation blockchain applications such as digital assets, intellectual property, and smart contracts. Smart contracts are computer programs that encode the terms of an agreement between untrusting parties and are based on predefined rules. They are deployed or executed on blockchain systems as part of a blockchain transaction. Miners are responsible for deploying new contracts and executing existing ones, and they are compensated for this work based on the transaction costs required for the contract.

Table 1: Gas used in our project

Operation	Gas
factory deploy	2131913
create election	1394070
add party	23160
start election	21380
cast vote	21344
end election	21064

The flow of execution:-

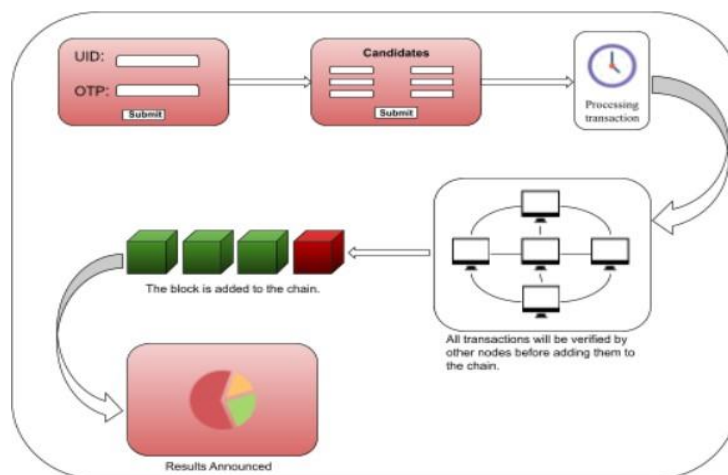


Fig 1: Basic Functioning

In our project, there are two types of users, one is the manager and the other is the voter. The manager is the one who created a particular election and he is the only one who can control that election.

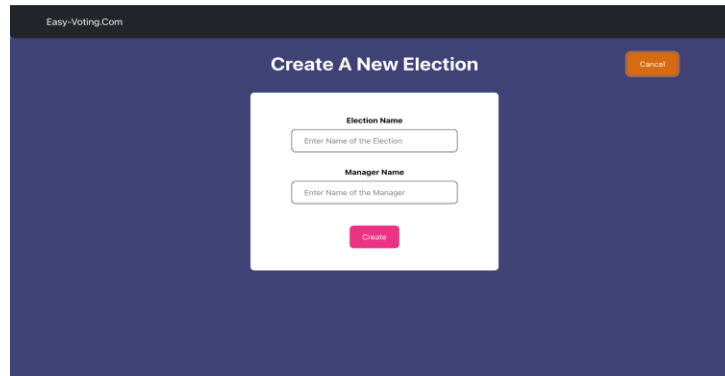


Fig 2: New Election Creation

The election has 3 phases, the one is when an election is created, the second one is when it starts, and the third is when it gets over, and the result is declared. The Manager has to add parties or candidates by providing information like the Party's Name, Candidate's Name, Logo of their party, Total number of Members in their party, etc.

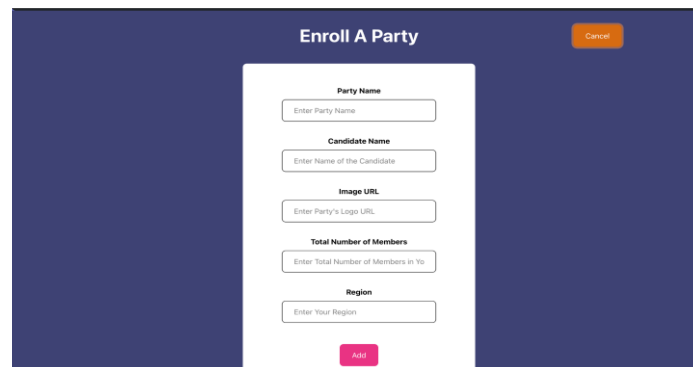


Fig 3: Entering Party Details

All the parties should be added before the starting of the election as after the election is started, no party can be added. When all the parties are added, then the election is started by the manager and has 10 days before the results of that election are announced. On the main page, all the elections are listed including the ones which are over and the ones which are not started yet.

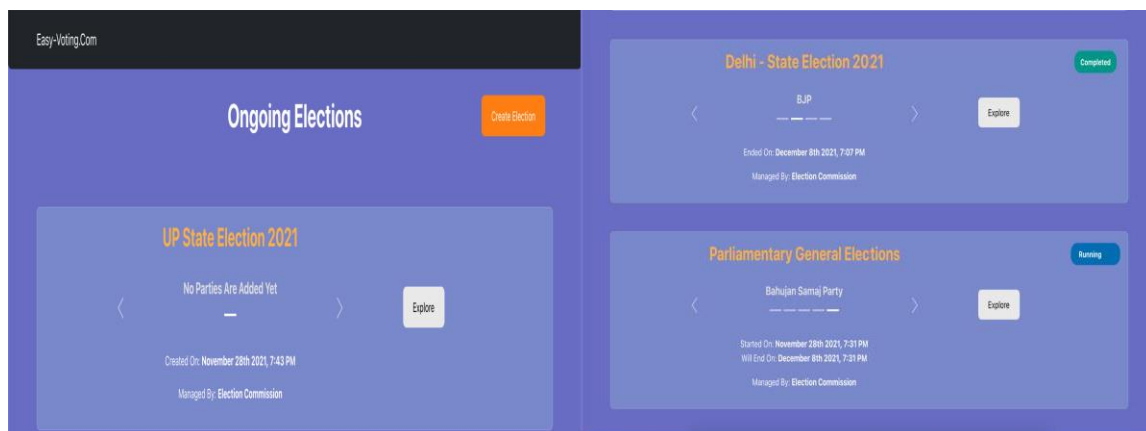


Fig 4: Previous and Current Election

The voter can view any election, and if that election is ongoing then he can take part and can vote but if it is already over and the result is already announced, then he can just see the result. On opening the web page of any ongoing election, all the participating parties are displayed in form of cards with their candidate information in them.



Fig 5: Parties to Select From

The voter then chooses the party he wants to vote for and enters the Aadhar number to verify themselves.



Fig 6: Authentication

If the aadhar number is invalid, then an error will be displayed on the screen and if the aadhar number is correct, an OTP will be sent to their mobile number which is linked to that Aadhar number for authentication. After the aadhar authentication is done, it will be checked if a vote was already cast by that aadhar number, and if so, the vote will not be cast and the error will be displayed and the user will be returned to the home page of that election but if there is no vote cast yet through that aadhar number, then vote count of that particular party in that particular election will be increased by one. After the manager ended the election and the result gets declared, a pie chart shows all the statistics, and a winner party is declared.

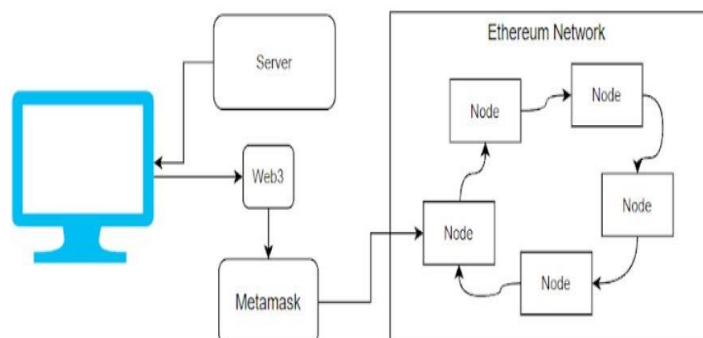


Fig 7: Winning Party and Current Stats

Each vote is saved as a transaction and is added to the blockchain. The program makes sure one vote per aadhar number. In the end, a successful vote cast is considered a transaction within the blockchain of the voting application.



III. INDEX OF FUNCTIONALITIES

Election Factory: It is deployed as our primary way of communication with the data on the blockchain. With the help of this contract, we can create new elections. It also stores some metadata of all the elections that are either running, completed, or are yet to be started. Creating a new election requires the title of the election, the name of the manager, and the time at which the election is created.

Contract Election: This is the contract that will hold all the details of the election starting from details of the parties to the election results. It also incorporates all the logic to prevent frauds/ multiple entries of votes/ manager access etc.

Modifier Restricted: This modifier when applied to other functions prevents non-manager users to access these functions, thus adding an additional layer of security.

Constructor: For creating an election, one needs to pass in Election name/title and time of creation.

Struct Party: This structure allows storing all the details of a party in one place.

Function Add Party: This function is used to add a new party to an existing election. It requires details of the party such as the name of the party, name of the leader/candidate, number of members in the party, region of the party, and a URL of an image representing the logo of the party. To use this function it is required that the election has not yet been started, once an election starts no more parties can be added. Once a new object of the Party is successfully created it is then added to the parties list of that election.

Function get Parties: It returns the list of parties in the election. Since it contains the view modifier, calling this function does not require any gas. **Function cast Vote:** This function is used to add a vote to a party. It requires the Aadhaar number and index of the party to be voted in reference to the parties list. It has three security checks, first, one being that election must have been started by the manager before someone tries to vote, the second one is that the user must have not voted before, and the last one is that the election must have not ended. Once it passes all the checks that user is marked as voted and the vote count is increased for that party.

Function get Party Details: It returns the details of a specific party at the given index with reference to the list of parties.

Function get Results: Once an election is ended this function can be called to get the results of the election. It returns an integer array with each element at index *i* representing the number of votes for the party at index *i* in the parties list.

Function end Election: Since this function has restricted access only the manager can call this function to end the election. Once the election is ended users can see the results of the election.

Function start Election: This function is also restricted and can only be called by the manager and it requires two arguments one being the current time that will represent the time this election is started and the other being the time when this election is supposed to be ended. Although the ending of the election is completely dependant on the manager this time gives users an idea of the election schedule. Once an election starts no more entries for parties will be accepted and users can cast their votes.

IV. FUTURE WORK AND DISCUSSION

Blockchain technology has the potential to revolutionize the way we vote by providing a secure and transparent method for recording and verifying votes. However, the current process of voting through blockchain can be costly due to the various processes involved, such as encryption, hashing, and protocols. These processes are necessary to ensure the security and integrity of the voting system, but they can also increase the overall cost.

One solution to this problem is to design a new network that is specifically optimized for voting. This network could incorporate features such as more efficient encryption and hashing algorithms, or more streamlined protocols, in order to minimize the cost of voting. Additionally, using a currency other than etherium, such as one with lower transaction fees, could help to reduce the overall cost of voting through blockchain.

An android app could also be developed to make it easier for people to access and use the voting system. This app could

provide a user-friendly interface and allow users to cast their votes directly from their mobile devices. Overall, by designing a new network and developing an android app, the cost of voting through blockchain could be significantly reduced, making it more accessible and practical for wider use.

V. CONCLUSION

The use of technology in voting systems has evolved over time, from ballot paper to electronic voting machines (EVMs) to the latest proposal of using blockchain technology. blockchain has the potential to greatly improve the current voting system by providing a secure and tamper-proof method for casting and counting votes. The proposed research paper has implemented the use of blockchain to build a voting application. The proposed system uses solidity for contract creation, HTML, CSS, ReactJs, NodeJs for a user-friendly voting website, and aadhar API for authentication. One of the key benefits of using blockchain is its decentralized nature, which allows anyone with the proper credentials to vote from anywhere with internet access, eliminating the risk of outside threats. Additionally, blockchain's distributed data and SHA-256 hashing make it extremely secure and resistant to corruption.

REFERENCES

- [1] Prof. Mrunal Pathak, Amol Suradkar, Ajinkya Kadam, Akansha Ghodeswar, Prashant Parde, BlockchainBased E-Voting System.
- [2] Yogesh Sharma, B. Balamurugan, "A Survey On Privacy Preserving Methods Of Electronic Medical Record Using Blockchain"
- [3] Julija Golosova, Andrejs Romanovs, "The Advantages and Disadvantages of the Blockchain Technology".
- [4] J.Light, "The differences between a hard fork, a soft fork, and a chain split, and what they mean for the future of bitcoin"[online].
- [5] W. Fauvel, "Blockchain Advantages and Disadvantages" [online]
- [6] Dataflair team, "Advantages and disadvantages of Blockchain Technology" [online].
- [7] Woorchul Song, Stone Shi, Victoria Xu, Gursahib Gill, "Advantages & Disadvantages of Blockchain Technology" [online].
- [8] P. Ezhilchelvan, A. Aldweesh, and A. van Moorsel, "Non-blocking two-phase commit using blockchain,"
- [9] Gareth W. Peters, Efstathios Panayi, "Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money."
- [10] V. Buterin, "A next-generation smart contract and decentralized application platform."
- [11] Maher Alharby, Amjad Aldweesh, Aad van Moorse, "Blockchain-based Smart Contracts: A Systematic Mapping Study of Academic Research"
- [12] Yash Dalvi, Shivam Jaiswal, Pawan Sharma (2021), "E-Voting using Blockchain."
- [13] Kashif Mehboob Khan, Junaid Arshad, Muhammad Mubashir Khan, "Secure Digital Voting System based on Blockchain Technology."
- [14] Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson, "Blockchain-Based E-Voting System."
- [15] Maher Alharby, Amjad Aldweesh, "Blockchain-based Smart Contracts: A Systematic Mapping Study of Academic Research"(2018).