IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 7.105 ⁜ Vol. 9, Issue 4, April 2022

DOI: 10.17148/IARJSET.2022.94114

ONLINE VOTING SYSTEM USING BLOCKCHAIN

Ajay Tiwari[1], Bharat Goma[2], Bharti Suraj[3]

*[1]Professor, Computer Science And Engineering Department, Maharaja Agrasen Institute OfTechnology, Rohini, New Delhi 110086 India.

*[2,3]B.Tech Scholar, Computer Science And Engineering Department, Maharaja Agrasen Institute OfTechnology, Rohini, New Delhi 110086 India.

ABSTRACT

Technology is changing very rapidly and with new tools and technology comes alternate and better ways of doing things. Security and transparency are some of the threats which the world faces. Similarly, the elections are held by a centralized party and there is always a possibility of data tampering. Blockchain is one such technology that can deal with such threats. Blockchain is a digital information recording system that is created in such a way that makes it very difficult to tamper with data. Blockchain is a technology that decentralizes the whole system and the database is owned by every node. It offers immutable distributed ledger technology which is an exciting advancement in the field of the information technology world in this research we aim to discuss a decentralized online voting system using blockchain technology. Using this we create a decentralized, secure and easy way of voting.

Keywords: Smart Contract, Etherium, Blockchain, Solidity, E-Voting, SHA-256.

I. INTRODUCTION

Blockchain is a decentralized system that serves as a decentralized database that provides new tools for creating a truthless system. Blockchain is a trustless decentralized system, where each node in a blockchain holds data locally. Initially, blockchain was designed for a money transfer but with advancements in technology, blockchain is now used in many fields for example Internet of Things, the healthcare sector, etc. The real boom in the industry came after the discovery of Ethereum. Contains a complete programming language and users can work with smart contracts in the Ethereum network.

Blockchain is a technology that is gaining momentum faster in the 4.0 era. With high-quality provision and transparency, it is widely used in procurement management systems, health care, payments, business, IoT, voting systems, etc. Current voting systems such as ballot box voting or electronic voting meet various security threats such as DDoS attacks, voting booth capturing, vote-rigging and fraud, malware attacks, etc., and also require large amounts of paperwork, human resources, and time. This creates a sense of mistrust between existing systems[1]. Using the blockchain, the voting process can be made more secure, transparent, consistent, and Reliable. Suppose you are an eligible voter who goes to the polls and casts your vote using EVM (Electronic Voting Machine). But since it's a roundabout behind it all and if someone interrupts a microchip, you might not know that your vote has reached the person you voted for or was diverted to someone else's account? Since there is no way to track it back. However, if you use blockchain- it processes everything as transactions therefore, gives you a receipt for your vote (in the form of a transaction ID) and you can use it to make sure thatyour vote is counted securely. Now let's say a digital voting system (website/application) has been introduced to make the process digital and all personal data is stored on a single server. If someone tries to hack, they can change the number of votes - from 10 to 100! We can never know whether a hacker installs some malware or performs click jacking attacks to steal or negate your vote or simply attacks the central server. This is avoided with the help of immutability. Consider SQL, PHP, or other database programs. You can add, modify, or delete votes. But in blockchain, you can just enter data but you can't modify or delete it. So, when you add something, it stays there forever and no one can control it- thus the name immutable ledger. But only building a blockchain system is not enough. It should still be decentralized so if one server goes down or something happens to a particular node, other nodes may operate normally and do not have to wait for the victim's node recovery.

Types of Blockchain:-

Blockchain technology can be classified into three types of blockchain a public blockchain, private blockchain, and consortium based on network design. Blockchain network construction depends on the performance,

analysis, and accessibility of data by network users. The three types of blockchain play an important role in the development of any organization depends on its use. The organization shifts data from their databases to the blockchain as it is more reliable and secure.

Public Blockchain:-

A public blockchain works without restrictions. As long as you have an internet connection you can access the network and start the transaction. In general, such networks often offer some form of incentive for users who verify blocks. However, this network tends to use Proof of Work or Proof of Stake to verify Transactions. Public blockchain architecture allows you to download protocol anytime without anyone’s permission. The public blockchains present a viable model that makes the technology industry more profitable. It is completely decentralized and no one can change it. The downside of a blockchain is the transaction costs incurred by joining a blockchain network and measurement issues network.

Private blockchain:-

A private blockchain is an authorized blockchain. Private blockchains operate based on access controls that limit people who can participate in a network. There are one or more businesses that control the network and this leads to trust for other people to do something. Private blockchains are often run by some organization. Private blockchain only allows participating organizations to access the blockchain, others are not allowed to do so.

Consortium blockchain:-

A consortium blockchain is your combination of both public and private blockchain. The consortium blockchain allows users to join the network without permission as in the public blockchain but when users join the network, ownership of the network does not fall into the hands of a single owner or similar company a private blockchain rather than a few users out of all users who can be assigned a task of regulators or verifiers who can verify transactions made by network users also own the authorized network rules[2]

Advantages Of Blockchain

Each action is recorded in the Blockchain and the data for Records are available to all Blockchain participants nor can they be altered or deleted. Consequences of this recording provide Blockchain transparency, consistency, and reliability The credibility of Blockchain is based on the belief of two or more participants, who do not know each other. The main idea is to trade real and not useless in between of these unknown people. Confidence can be increased continuously because there can be many processes that are shared with records

[6] The transaction takes up a lot of time while processing but the blockchain can reduce that time to several minutes and seconds.[8] Blockchain technology.

Disadvantages of Blockchain

Blockchains are not completely secure. If a group of people manages to get hold of 51% of the nodes on a blockchain then they can control what goes in. Although attaining hold of these many computers is almost impossible on large and popular networks but on small networks it is possible. Signature verification is one of the most challenging tasks in the blockchain. It uses up a lot of power and big computing is needed to process the sign.[5] Another big disadvantage associated with blockchain is that its transaction cost is very high, each transaction on average takes around 75-80 dollars. This is due to the high initial capital of blockchain[3]

II. LITERATURE SURVEY

Some of the work that has been done in the aforementioned field to achieve common sense and to capture the few key ideas needed for this study. Refer to the paper for a complete overview of the problem-solving process using blockchain. We refer to the paper [12] and verification strategies. There are various strategies to ensure voters. According to Kriti Patidar and Dr Jain, voter verification can be done using cryptography of the secret key that should be provided to voters before the election process [13]. Voters must be registered by certain authorities while voter keys must be registered and distributed to incumbent voters. There are different thoughts of Friðrik Þ. Hjálmarsson has plans to use a 6-digit PIN for voters who can use it for voter verification [14]. Each person is identified and approved by the system by presenting an electronic ID from Auokenni and a corresponding 6-digit PIN at the polling station. Without surveillance, one can vote for more people.

How to: -

Blockchain is a distributed site that is shared between computer network nodes. As a database, blockchain stores information in a digital format electronically. Blockchains are best known for their important role in cryptocurrency systems. The innovation of blockchain is that it ensures the integrity and security of the data record and creates trust without the need for a trusted third party. One important difference between a standard website and a blockchain is the way data is structured. Blockchain collects information together in groups, known as blocks containing information sets. Blocks have some storage capacity and, when completed, are closed and connected to a pre-filled block, forming a series of data known as a "blockchain." All new information following that newly installed block is integrated into a newly constructed block which will be added to the series once completed. The blockchain allows the data stored in that database to be distributed between several network nodes in different locations. This not only creates duplication but also maintains the integrity of the data stored there: if someone tries to change the record at the same time on the site, other nodes will not be changed and that may prevent the bad character from doing so. Blockchain technology achieves the security and trust that is shared by people in many ways. First, new blocks are always kept in chronological order. After the block is added at the end of the blockchain, it is very difficult to go back and change the blockchain content unless the majority of the network has reached an agreement to do so. This is because each block contains its own hash, with the block hash before it, and the time stamp specified earlier. Hash codes are made by a mathematical function that converts digital information into a series of alphanumerics. If that information is organized in any way, the hash code also changes. Each block in the blockchain is given a hash value and maintains a record of the previous block hash that changes or disrupts data in the blockchain will result in mine another block hash value and will create an avalanche that breaks a series of blocks. The result of an avalanche is a term associated with certain behavioral mathematical operations used for encryption. The Avalanche effect is considered one of the most desirable for any encryption algorithm. A slight change in a key or blank text should result in a significant ciphertext change. This structure is called the avalanche effect.

SHA-256 is a highly secure and innovative cryptographic hash function developed in 2000 as a new version of SHA functions and adopted as a FIPS standard in 2002. It is permitted to use a hash production tool to produce SHA256 hash in any character unit. or input value. Also, it produces 256 hash values, and the internal size is 256 bits and the actual message size reaches 264-1 bits.

Hashing:-

Hashing is a process in which information is processed in such a way that it is not able to produce back the original information. It takes the data and passes it to a function that performs mathematical and new and encrypted information is generated. This is called a hash function. This function is designed to be irreversible and will provide the same output value if the input remains unchanged.

There are two types of hashing:

Password hashing: This removes the possibility of any unauthorized access to the database and avoids tampering with the same. Here hashing does a one-way transformation on a password and transforms it into a string called a hashed password. The hashed password value is stored in the database. When someone tries to login, hash is again generated from the password entered by the user. If new hash is equal to the stored value then the login is successful.

Integration Verification: Hash-based verification confirms that the file is corrupted by comparing the hash file value with the predefined value. If these values match, the file is considered unedited. Because of the nature of hash functions, hash conflicts may result in untruths, but the chances of conflict often do not matter to random corruption.

Smart Contract:

A smart contract is a computer program that works on blockchain technology. A smart contract can be considered a reliable external company among unscrupulous participants. Smart contracts consist of contract storage, a balance, and program code. It can be created and made available for use by any node in the network, simply by posting a transaction to the blockchain.

DOI: 10.17148/IARJSET.2022.94114

The smart contract program code is fixed and cannot be updated once included in the blockchain. Smart contracts are run by a network of miners who are responsible for maintaining the blockchain. Miners reach a consensus on the execution outcome of the smart contract and accordingly update the blockchain. Once deployed, each smart contract is assigned to a 160-bit address and is executed whenever a transaction is created using this address. In between the creation of a smart contract whose storage can be updated.[15]

Types of smart contracts:-

Smart Legal Contracts: A smart legal contract is a legally binding contract that is fully available in the native language, and is only available with a computer code. The native language component compiles the party's agreement and the computer code automatically activates the contractual features. The original language and code can interact with the language of 'laying down' dynamics accessible by code or by embedding code in a contract in the same way as formulas are sometimes included in contracts. An important feature of smart legal contracts is that in the event of non-compliance, the native language contract will be valid. As a legally binding contract, all common dispute resolution mechanisms will be available in the event of a dispute.

Decentralized Autonomous Organizations: The Independent Non-Governmental Organization (DAO) is a business without central leadership. Decisions are made from bottom to top, governed by a community organized by a set of rules that are enforced on the blockchain.

DAOs are online organizations owned and operated by their members. They have built-in savings accounts that are accessible only with the consent of their members. DAO operates without phase management and can have a large number of objectives. DAO was a project launched in 2016 that ultimately failed and led to a significant split in the Ethereum network.

Application Logic Contracts: Logical Performance Contracts (ALCs) contain code based on an application that is consistent with other blockchain contracts. They allow you to connect to all different devices, such as the integration of the Internet of Things (IoT) and blockchain technology. ALCs are an important part of a multi- functional smart contract and are primarily operating under a management system.

Gas in Ethereum:

Gas refers to the payment, or price, required for a successful operation or contract on the Ethereum blockchain platform. With a small number of particles of cryptocurrency ether (ETH), commonly called gwei and sometimes also called nanoeth, the gas is used to distribute Ethereum virtual (EVM) machine resources so that applications are assigned to areas such as smart contracts can operate on their own. in a secure but distinct way. The actual price of gas is determined by the supply and demand among network miners, who can refuse to process the work if the gas price does not meet their limit, and network users who want processing power. Gas payments are payments made by users to compensate for the computer power required to process and verify transactions in the Ethereum blockchain. "Gas limit" refers to the maximum amount of gas (or energy) you intend to use for a specific purpose. A high gas limit means you have to do extra work to get the job done using ETH or a smart contract.

In recent times, industry interest has shifted to second-generation blockchain applications, which include digital assets, intellectual property, and smart contracts. [9] A smart contract is a computer program that encodes a code between unscrupulous participants and is based on pre-defined rules.[10] . A smart contract is deployed or executed on blockchain systems as part of a blockchain transaction. Miners are responsible for deploying new contracts and executing existing ones. Miners are paid for this work based on the transaction costs required to contract. [11]).

Table 1: Gas used in our project

Operation	Gas
factory deploy	2131913
create election	1394070
add party	23160

DOI: 10.17148/IARJSET.2022.94114

start election	21380
cast vote	21344
end election	21064

The flow of execution:-

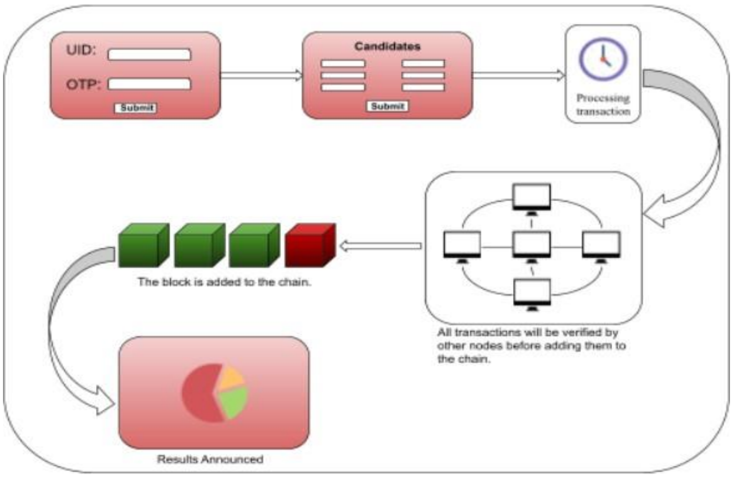
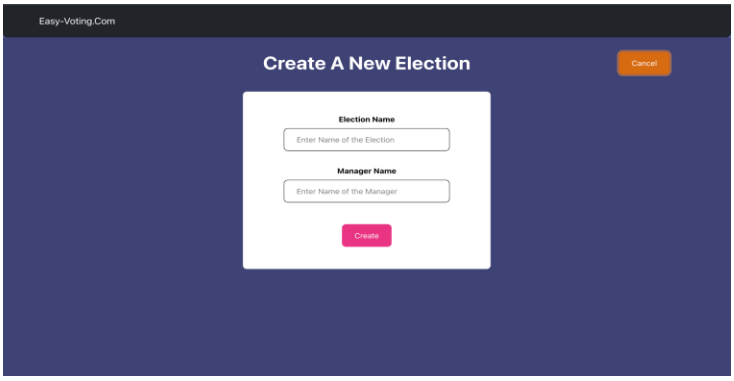

UID:
OTP:
Submit
Candidates
Submit
Processing transaction
The block is added to the chain.
All transactions will be verified by other nodes before adding them to the chain.
Results Announced

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.



Create A New Election

Election Name

Enter Name of the Election

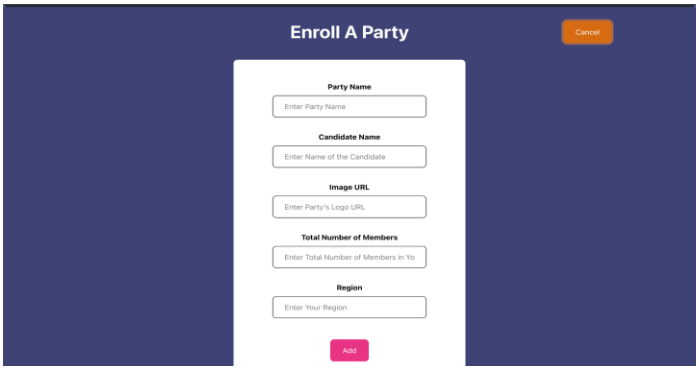
Manager Name

Enter Name of the Manager

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



Enroll A Party

Party Name

Enter Party Name

Candidate Name

Enter Name of the Candidate

Image URL

Enter Party's Logo URL

Total Number of Members

Enter Total Number of Members in Yo

Region

Enter Your Region

DOI: 10.17148/IARJSET.2022.94114

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.

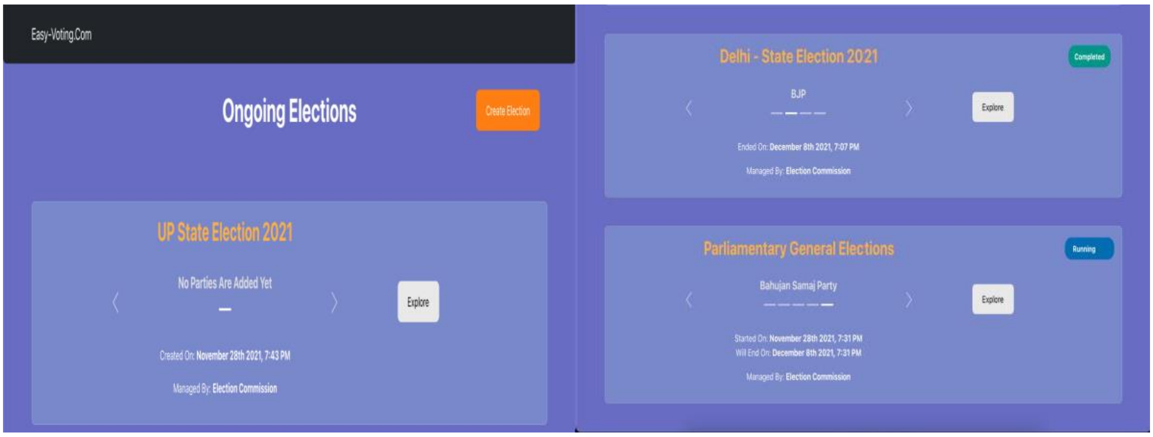

Easy-Voting.Com
Ongoing Elections
Create Election
UP State Election 2021
No Parties Are Added Yet
Explore
Created On: November 28th 2021, 7:43 PM
Managed By: Election Commission
Delhi - State Election 2021
Completed
BJP
Explore
Ended On: December 8th 2021, 7:07 PM
Managed By: Election Commission
Parliamentary General Elections
Running
Bahujan Samaj Party
Explore
Started On: November 28th 2021, 7:31 PM
Will End On: December 8th 2021, 7:31 PM
Managed By: Election Commission

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 webpage of any ongoing election, all the participating parties are displayed in form of cards with their candidate information in them.

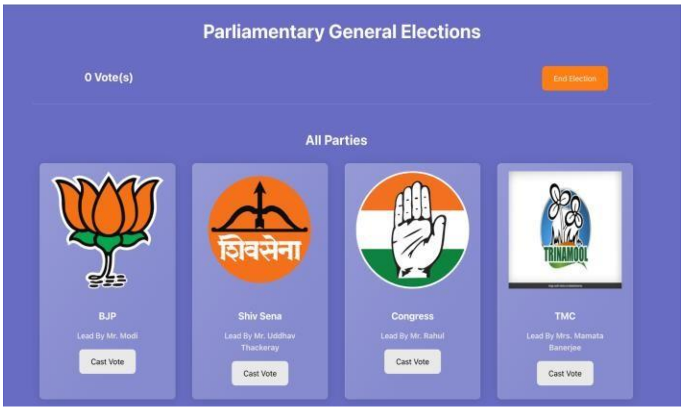


Fig 5: Parties to Select From The voter then chooses the party he wants to vote for and enters the Aadhar number to verify themselves.

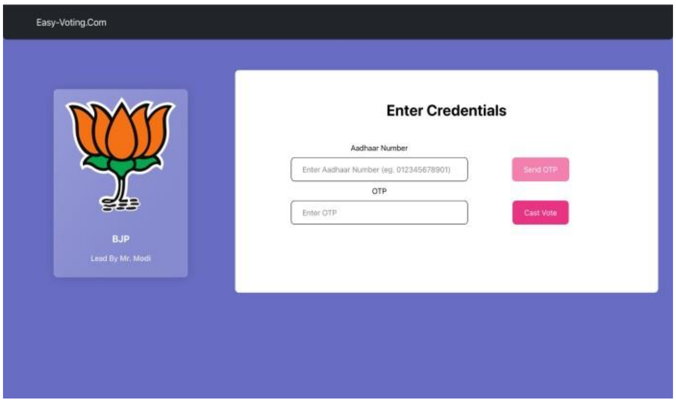


Fig 6: Authentication

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.

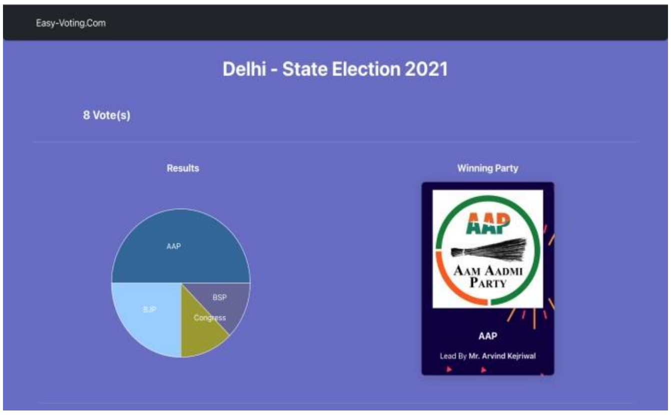
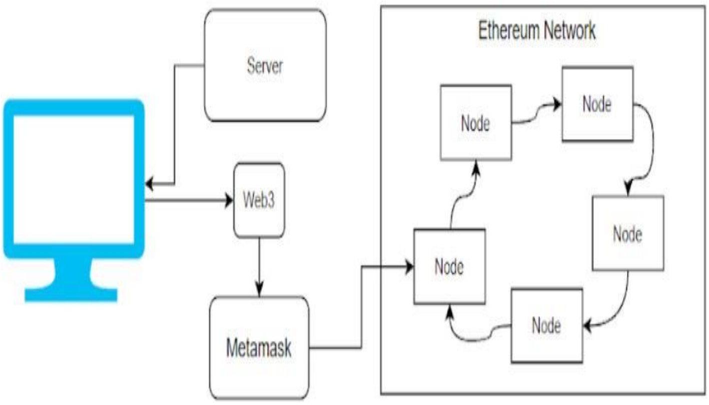


Fig 7: Winning Party and Current Stats

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.

Fig 8: Architecture



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 is election is started and the other being the time when this is 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

Voting through blockchain is very expensive as it involves a lot of processes such as encryption, hashing, protocols hence there is a need to design a different type of network so that overall cost can be minimized. The transaction is done using Ethereum which increases the cost, so there is a need to create a new currency that decreases the overall cost. We would like to make an android app for the same for easy use.

V. CONCLUSION

With the change of technology comes to a change in methods, we used ballot paper for election then we shifted to electronic voting machines(EVM), now we have a more secured and easy technology for voting i.e. blockchain technology. The proposed research paper has implemented the use of blockchain in improving the current voting system. Securing every vote in blockchain and making it difficult to tamper has given this technology an edge over others. According to the proposed research paper blockchain is the best fit and is recommended for online voting systems. The project uses solidity for creating contracts, HTML, CSS, ReactJs, NodeJs to create a website for easy voting, and aadhar API for authentication. Blockchain is decentralized and doesn't work on trust. Anyone with proper credentials and vote from anywhere with access to the internet thus eliminating any outside threats. Blockchain distributes data on every node and uses SHA -256 for hashing making it extremely secure and incorruptible.

ACKNOWLEDGEMENT

This paper is made possible through the help of everyone. We would like to dedicate our acknowledgement of gratitude towards our mentor Ajay Tiwari. Finally, we sincerely thank our parents, family, and friends who provide advice and support.

VI. REFERENCES

[1] Prof. Mrunal Pathak, Amol Suradkar, Ajinkya Kadam, Akansha Ghodeswar, Prashant Parde, Blockchain-Based E-Voting System.

[2] Yogesh Sharma, B. Balamurugan, "A Survey On Privacy Preserving Methods Of Electronic MedicalRecord 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] Woochul Song, Stone Shi, Victoria Xu, Gursahib Gill, "Advantages & Disadvantages of Blockchain

DOI: 10.17148/IARJSET.2022.94114

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 basedon 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).