Karnataka State Council for Science and Technology
(An autonomous organisation under the Dept. of Science & Technology, Govt. of Karnataka)
Indian Institute of Science Campus, Bengaluru – 560 012
Telephone: 080-23341652, 23348848, 23348849, 23348840
Email: office.kscst@iisc.ac.in, office@kscst.org.in ♦ **Website:** www.kscst.iisc.ernet.in, www.kscst.org.in

KSCST

SYNOPSIS REPORT

on

“Secured Digital Voting System Using Blockchain Technology”
Project Proposal Reference No. : 46S_BE_0671

Submitted By

Bhagya A Koushik – 1DS19CS037
Deekshitha R S – 1DS19CS044
Gowthami S – 1DS19CS053
Haritha Nandhini – 1DS19CS055

Eighth Semester
B.E(CSE) 2022-2023

Under the guidance of
Dr. Nagaraja J
Associate Professor
Dept. of CSE
DSCE, Bangalore

Co-guide
Mr. Sparsh Kesari

Department of Computer Science and Engineering
Dayananda Sagar College of Engineering Bangelore-78

KEYWORDS

Blockchain, Ethereum, Ganache, Hashing, Meta-mask, Smart contract, Truffle.

Blockchain

A blockchain is a growing collection of documents, or blocks, that are linked together via encryption. Each block includes trade information, a time stamp, and a cryptographic hash of the preceding block. Using blockchain, we can securely store information on a shared system that anybody can access but cannot modify.

Ethereum

The blockchain-based platform Ethereum is best known for the ether (ETH) cryptocurrency it uses. Ethereum's blockchain technology makes it possible to establish and maintain openly accessible secure digital ledgers.

Ganache

A blockchain may be created using Ganache, which then offers a secure testing ground for decentralised applications (dApps) and smart contracts.

Hashing

Blockchain hashing is the process of using input data of arbitrary length and an algorithm to produce an output string with a set length. On the blockchain, hashing facilitates address derivation, cryptographic signatures, transaction identification, and consensus building.

Meta-mask

MetaMask is used to communicate with the Ethereum network. Users can utilize a browser extension or mobile app to access their Ethereum wallet, which can then be used to connect with decentralized applications.

Smart contract

Smart contracts are self-executing contracts and they are programs stored on a blockchain that run when predetermined conditions are met.

Truffle

A blockchain-based digital asset known as a truffle uses distributed ledger technology to operate. It serves as a store of value and a unit of account that may be used to pay for goods and services.

INTRODUCTION

Voting to select one's leaders is one of a citizen's fundamental rights in a democratic society. Paper ballots were used for many years to vote in elections held all over the world. However, this method requires a lot of time and resources. It was a significant election scam that was reported. Electronic voting machines, which are currently an alternative to traditional paper ballots, have consistently changed the voting process. Despite being more beneficial, this strategy still has several flaws in terms of the validity of the votes. With the present technological developments come an increase in cybercrimes, such as the hacking of EVMs to tamper with election results.

The main flaw in the election process that allows for vote manipulation by influencing poll workers and producing a biased outcome is a lack of transparency. Unsupervised vote counting, a lack of audits, and the inability to challenge results can occasionally be detrimental. Peer-to-peer networking is used by blockchain, adding transparency. It is a distributed ledger that encrypts data using the SHA-256 algorithm. Additionally, the cast votes will be block-recorded and hashed. As a result, the system is unchangeable and the results of the voting are secure. One of the reasons why people are moving towards blockchain-based digital voting systems is because all of these aspects of blockchain serve to mitigate the drawbacks in the present system.

1. Features of free and fair elections

- **Anonymity**: Users' identity is preserved.
- **Fairness**: Vote casted by voters cannot be tampered due to usage of SHA-256.
- **Integrity**: Votes cast on a ballot should be confidential and unchangeable. A system for evaluating the ballot's integrity must exist.
- **Privacy**: Votes cast by voters should remain confidential to them and there shouldn't be any method to link votes with voters. Only the overall result is published at the end.
- **Mobility**: Individual can vote from anywhere once they are connected to the server.

2. Characteristics of a Blockchain

Blockchain is a decentralized digital ledger technology that makes transactions safe and transparent without the use of middlemen like banks or other financial organizations. The following are the key characteristics of blockchain:

Decentralization: There is no central authority in charge of the blockchain network, which implies it runs on a decentralized system. As a result, the network is more resistant to failures and assaults.

Immutable: Data added to a blockchain cannot be changed or removed after it has been added. As a result, the blockchain ledger is very secure and impenetrable.
Transparency: Every transaction made on the blockchain is visible to everyone on the network and is transparent. As a result, the network is extremely transparent, and fraud is also deterred.

Security: Blockchain is extremely secure and resistant to hacker threats because it employs cutting-edge cryptographic methods to safeguard transactions.

Consensus: A network of nodes uses a consensus method to validate and verify transactions on the blockchain. This guarantees that there is no double spending and that all transactions are authentic.

Smart contracts: These are self-executing contracts where the terms of the agreement between the buyer and seller are directly encoded into lines of code, may be executed on a blockchain.

Interoperability: Blockchain networks are capable of being interoperable, which enables smooth data exchange and communication across them. This makes it simpler to develop international blockchain networks that can accommodate a variety of use cases and applications.

3. Working of Blockchain

A blockchain is made up of information-holding blocks arranged sequentially. Essentially, a blockchain is a distributed ledger. Blockchain has a strong, immutable linked list design. Each block contains a data hash of the block before it and a hash of its own contents. Here's an illustration: The sender-receiver information and transaction amount are stored on the Bitcoin blockchain. The hash value of a block can be compared to any form of biometric value. The block's content is always distinct. The hash is computed once the block has been formed. Since the hash is a key component of the blockchain, any modifications to the block will result in changes to the hash that is generated by the block. The hash value of the preceding block is the third element inside a block. By establishing a chain of blocks that each point to a preceding block, this practically renders it computationally impossible to change any block.

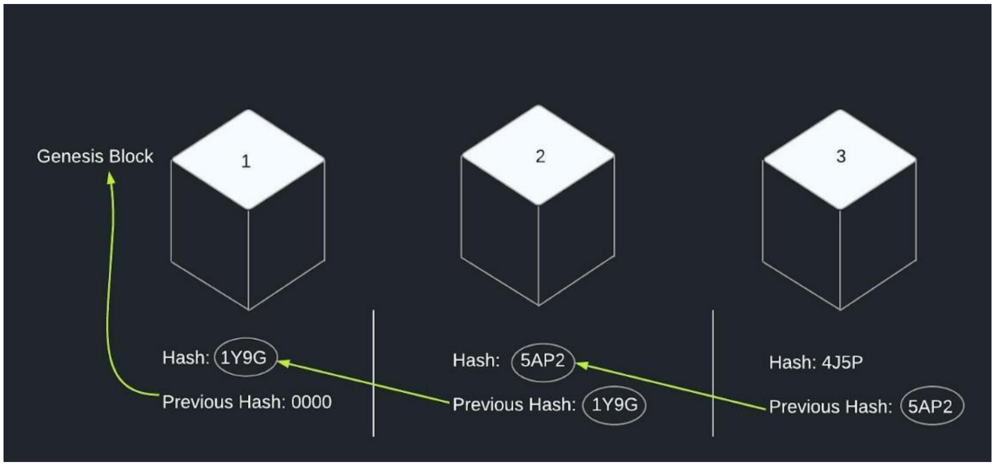


Figure 1: Block Structure

In the above figure three blocks are seen. The preceding block's hash is included in each block's hash. Blocks 3 and 2 are connected by a line, while block 1 is connected to block 2. The Genesis block is the initial block. Any attempt to alter a block will result in a change in the hash value, which compromises the integrity of the whole chain. Blockchain's security is provided by its inventive hashing, the proof-of-work process, and another way it protects itself: distribution.

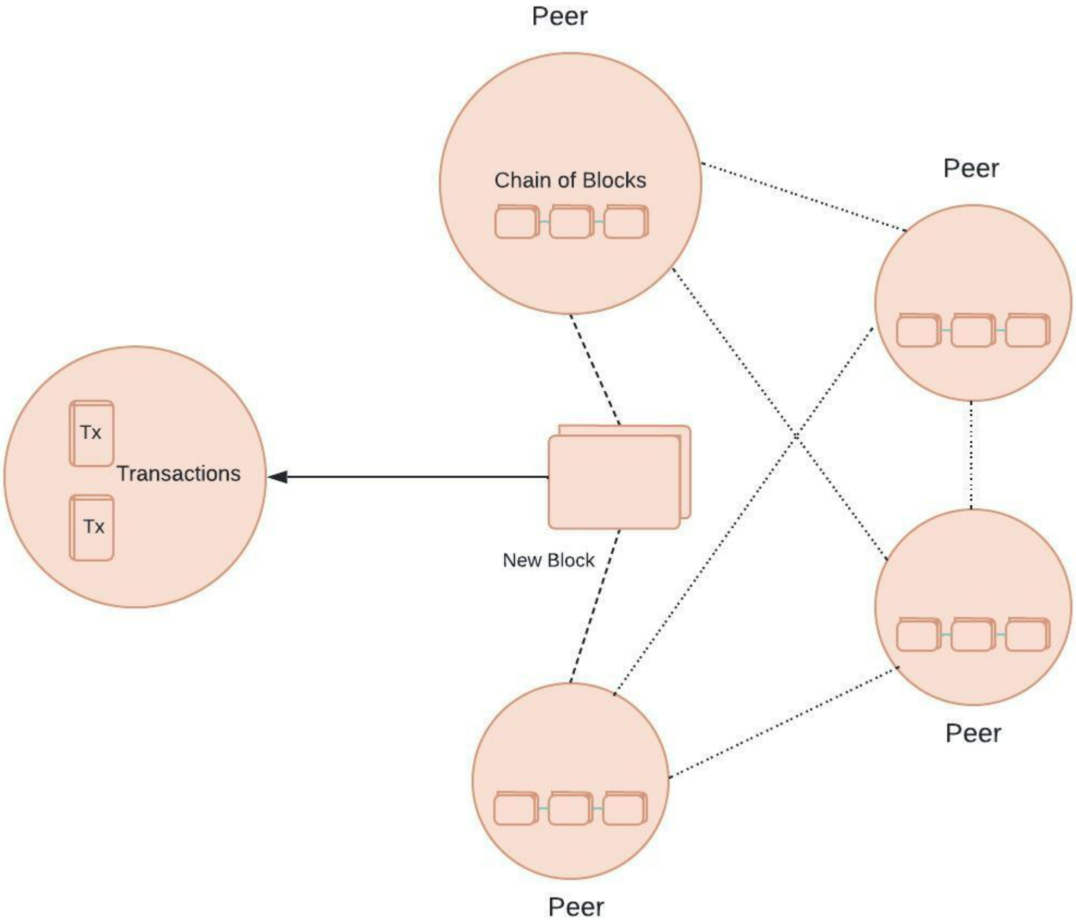


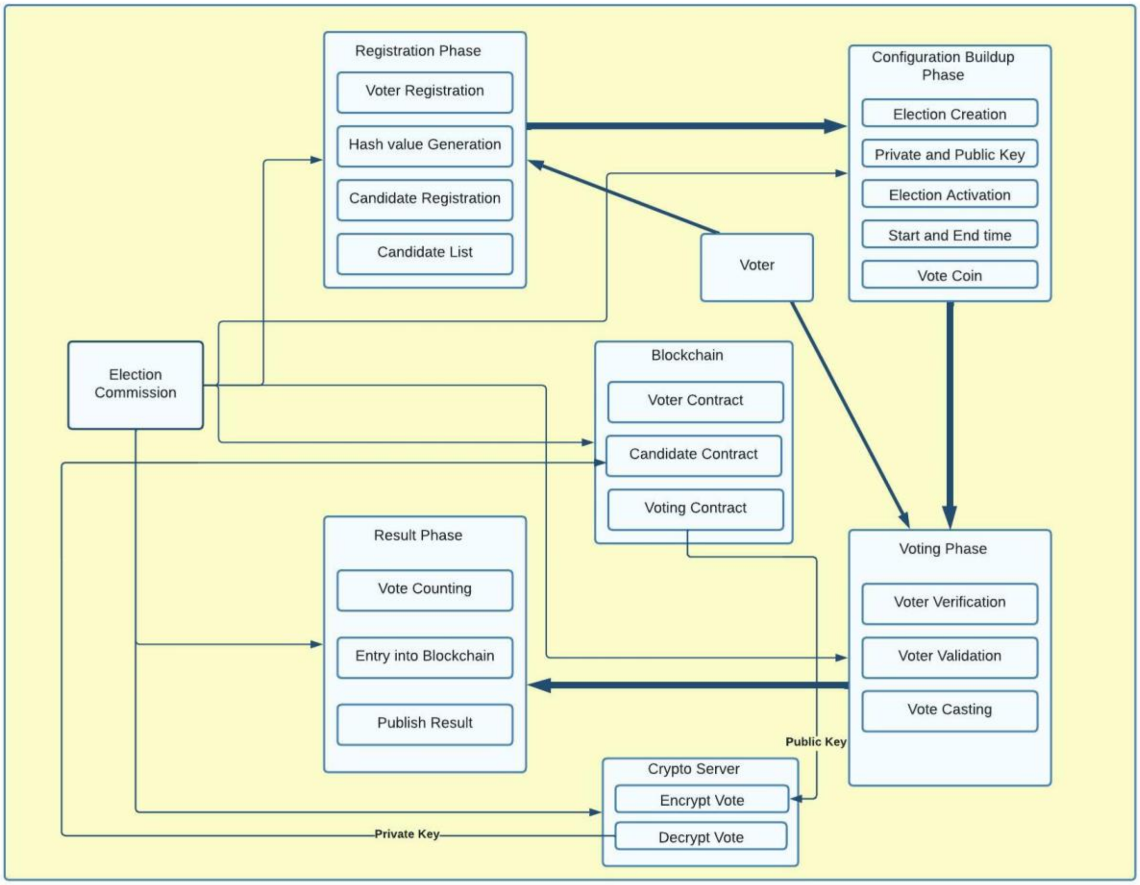
Figure 2: Distributed network between peers.

Blockchain employs a peer-to-peer network, where anybody may join and receive a full copy of the blockchain. This eliminates the need for a central organization to govern the chain. This may be used by the node to verify that everything is in working order and hasn't been tampered with. whenever a new block is made. To every peer in that network, the block is sent. The block is then corrected by each node to ensure that it has not been changed. A consensus is produced once all the nodes have completed the verification. Since all the blocks in the chain must be altered, it is impossible to alter blockchain with CPU power alone. The development of smart contracts is another intriguing aspect of the blockchain. They have a variety of forms and applications in different kinds of blockchain. Smart Contracts must be created Ethereum is being utilized. Chaincode is written in Hyperledger.

OBJECTIVES

- To validate the system to ensure only the legitimate voters are allowed to cast their vote.
- To protect voter identity by providing unlinkability between voter and their casted vote.
- To reduce the transaction cost compared with the existing systems.
- Usage of three smart contracts to control the voter’s registration process, voter authentication, and voting which are done directly between the voter and the blockchain.
- The casted vote is encrypted using a public key which Election Commission generates in a crypto server.
- The encrypted ballot is sent to the voting contract and added as a block in the chain.
- The total votes of each candidate and the winning candidate are shown. Then the final result is published in the result panel.

METHODOLOGY



The proposed voting mechanism includes four phases:

First Phase: Registration Phase

(i) ***Voter's registration:*** It is first stage in the model and is needed as part of the identity verfication phase in keeping a track of which individuals who are going to take part in the election process. It also serves as a control mechanism to prevent unregistered individuals from participating in the election by preventing them from casting a ballot.

(ii) ***Candidate Registration:*** A candidate is also a voter. The candidate registration procedure is similar to voter registration. They must complete several additional steps following key generating in order to be considered a candidate.

Second Phase: Configuration Buildup Phase

(i) ***Election Creation:*** The election is created by Election Commission. Election Commissioon joins Blockchain using a key pair of public and private keys. The transfer of vote coins and keypair of public key and private key to the crypto server for vote encryption and decryption.

(ii) ***Election Activation:*** Voter contract sends a transaction to all registered voter's public key of 1 vote coin, starting time and ending time of election. All the vote transactions are added to Blockchain.

Third Phase: Voting Phase

(i) ***Voter Verification and Validation:*** Voters must first sign into their wallets using the private key in order to complete the verification procedure. After that, the voter must enter their credentials for validation. In this case, the voter contract receives the credentials and generates a hash value from them in order to compare the hash value with other hash values already present in the blockchain. If both hash values are found equal, the voter is valid for voting.

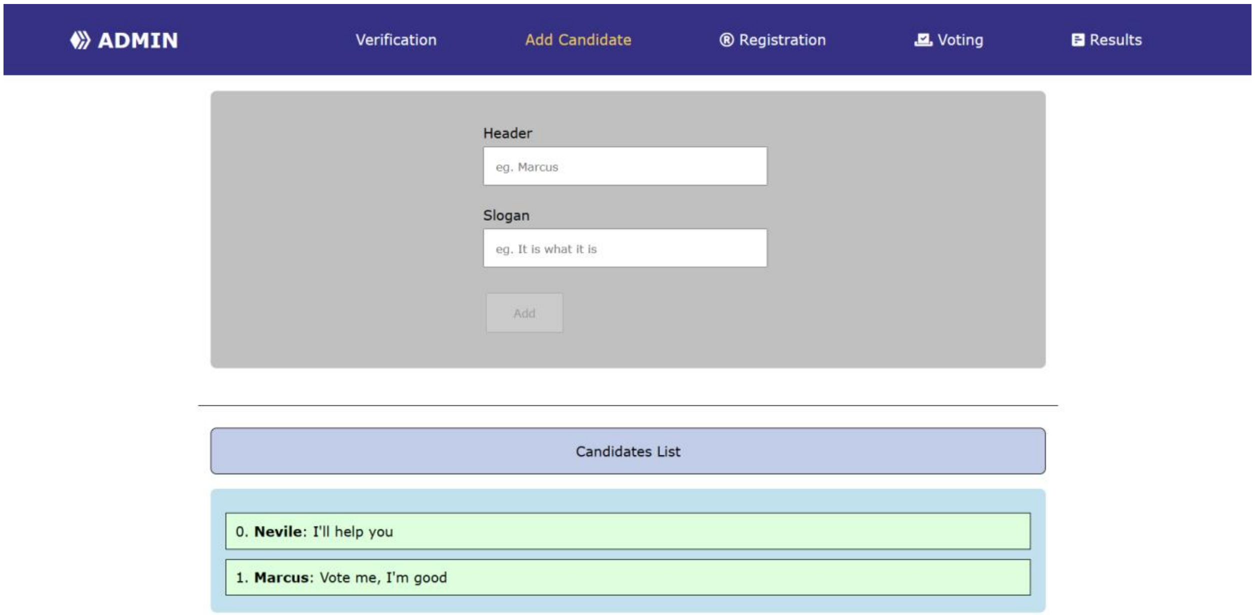
(ii) ***Vote Casting:*** Each participant is given a digital wallet by the authority after the registration process. After the verification procedure is completed, the voter receives a ballot containing a list of candidates. Voters can select candidates from the list of candidates and vote using the vote coin. Then the voter will get the vote id and the casted vote is encrypted using the election commissioner's public key and saved on the blockchain.

Fourth Phase: Result Phase

(i) ***Vote Counting Unit:*** Election Commission enters the private key into the system as part of the counting procedure. Each vote will be decrypted, and the voting contract will transfer the voting currency to the public key of each of the candidates who have been chosen. Through candidate contract, the number of coins in each candidate's wallet is found which represents the number of votes casted on him.

(ii) ***Publish Result:*** After voting, every vote will form a block and add it to the chain. The vote will be counted instantaneously after the vote is submitted, as there will be no risk of vote tampering and vote manipulation. The winner is found by checking the account of the candidates. The result is also published in tabular format which contains the total votes of each candidate and the winning candidate are shown for different regions.

RESULTS AND CONCLUSIONS



Header

eg. Marcus

Slogan

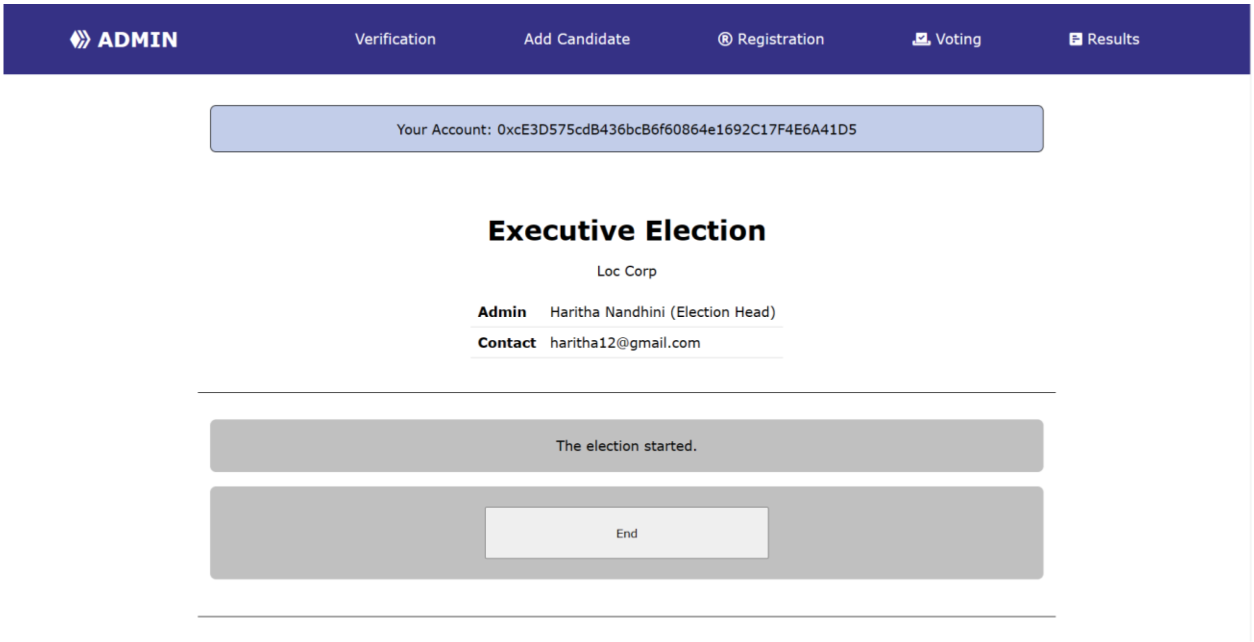
eg. It is what it is

Candidates List

0. **Nevile**: I'll help you

1. **Marcus**: Vote me, I'm good

Candidate Registration



Your Account: 0xcE3D575cdB436bcB6f60864e1692C17F4E6A41D5

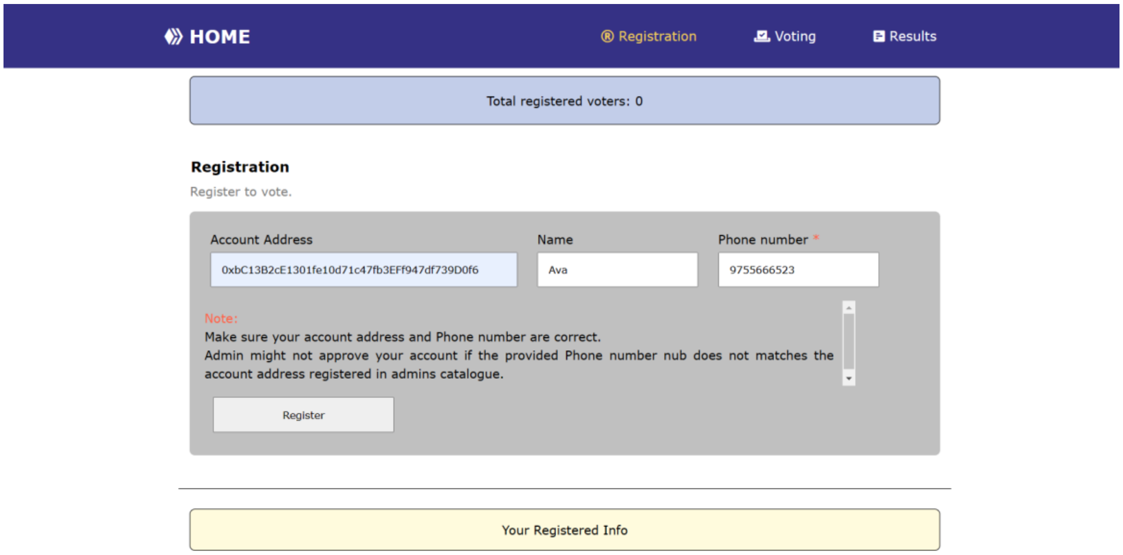
Executive Election

Loc Corp

Admin	Haritha Nandhini (Election Head)
Contact	haritha12@gmail.com

The election started.

Election Activation



Total registered voters: 0

Registration

Register to vote.

Account Address: 0xbC13B2cE1301fe10d71c47fb3EFf947df739D0f6

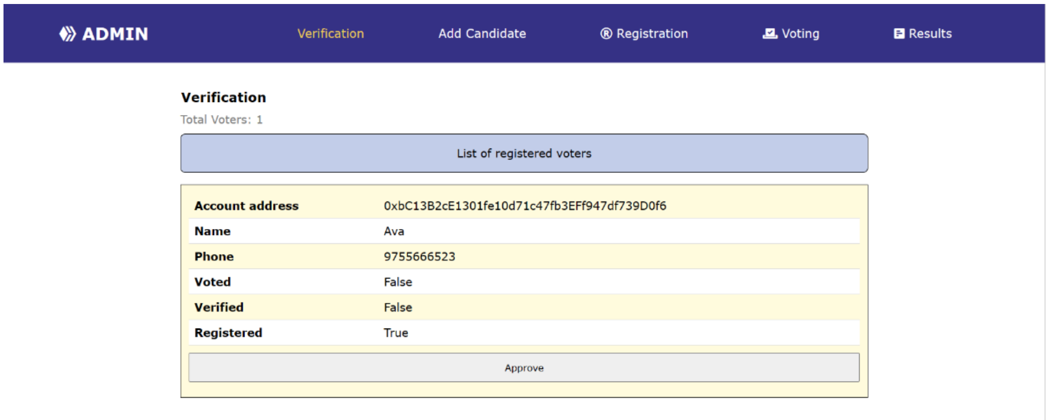
Name: Ava

Phone number *: 9755666523

Note:
Make sure your account address and Phone number are correct.
Admin might not approve your account if the provided Phone number nub does not matches the account address registered in admins catalogue.

Your Registered Info

Voter Registration



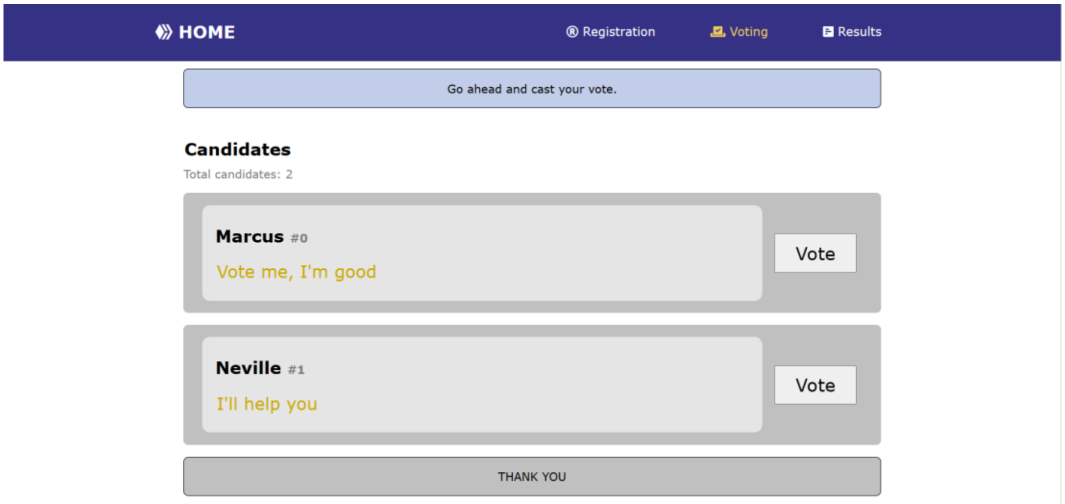
Verification

Total Voters: 1

List of registered voters

Account address	0xbC13B2cE1301fe10d71c47fb3EFf947df739D0f6
Name	Ava
Phone	9755666523
Voted	False
Verified	False
Registered	True

Verification of Voter by Admin



Go ahead and cast your vote.

Candidates

Total candidates: 2

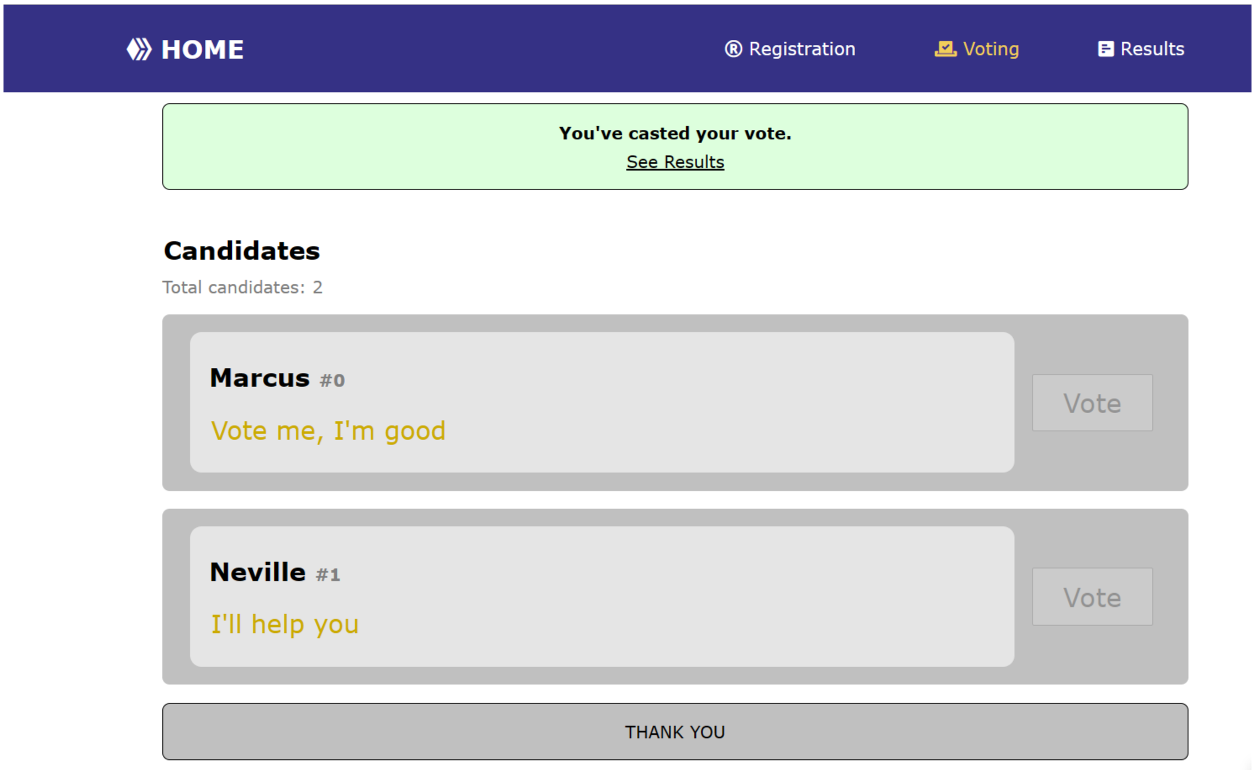
Marcus #0

Vote me, I'm good

Neville #1

I'll help you

Voting



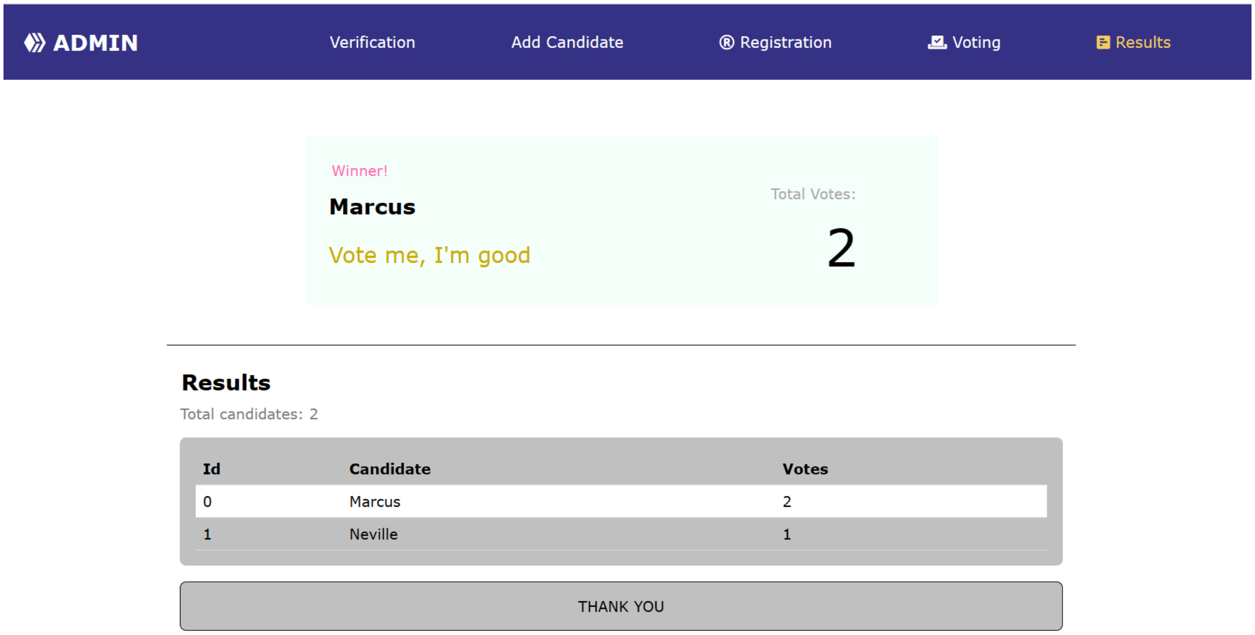
You've casted your vote.
See Results

Candidates
Total candidates: 2

Marcus #0
Vote me, I'm good

Neville #1
I'll help you

Confirmation after vote cast



Winner!
Marcus
Vote me, I'm good

Total Votes:
2

Results
Total candidates: 2

Id	Candidate	Votes
0	Marcus	2
1	Neville	1

Election Results

Since the 1970s, many versions of digital voting have been utilized, and they have many advantages over paper-based methods, including more efficiency and fewer mistakes. Numerous efforts have been made to investigate the viability of utilizing blockchain to provide an efficient solution to digital-voting in light of the phenomenal development in the use of blockchain technology. This project, "Secured Digital Voting System using blockchain technology" will explain how we may overcome the constraints of centralized voting methods and address the issues with security, transparency, fairness, and anonymity. To prevent corruption, the blockchain technology will help as it is widely distributed and publically verified.

This framework demonstrates blockchain technology which provides a new way to overcome the limits and adoption of digital voting systems, ensuring election security and honesty, as well as laying the groundwork for openness. It is feasible to transmit hundreds of transactions per second into an Ethereum private blockchain, using every component of the smart contract to reduce the load on the blockchain. Additional steps would be required for larger nations to accommodate higher transaction volume per second.

There will always be the issue of user authentication, which will need the usage of a biometric device or a unique id. We can suggest that a Blockchain-based solution is a superior choice, but our goal is always to create a safe and reliable system, regardless of platform, and to make the voting mechanism more transparent and error-free. So, we proposed a blockchain-based digital voting system that uses smart contracts to ensure safe and cost-effective elections while protecting voters' privacy and also blockchain will help to lower the computing costs. It also counts votes instantaneously, reducing the time required for the election process.

Ethereum blockchain has been used as a part of the network along with Ganache. Without the aid of a central database, the prototype's ability to record each voting transaction on the network was demonstrated by the Ganache (local blockchain) network design. The voter can examine each voting transaction on the local blockchain to confirm the outcome of the election. This technology allows individuals to vote using smart devices from anywhere in the world. Together, these factors make it possible for businesses, organizations, or institutions to conduct voting procedures that meet high criteria for auditability and security.

SCOPE FOR FUTURE WORK

OTP (One Time Password) generation is not implemented in our registration process which is a limitation which can be considered formerly in the on-going future work. Therefore, we target to use of sidechains in our proposed method as using duplicate currency, and sidechains expand the capabilities of blockchains by executing some activity outside them and returning the outcome to the mainchain for usage. So, we can store the encrypted vote in the sidechain and can use the decrypted result in the mainchain, which will reduce the cost.

The above framework can be scaled up to be able to handle election process on a large scale such as for a whole country so that we can obtain unbiased and faster result.

Using blockchain, even though security is a key advantage, gas consumption is a concerning issue. While fulfilling security properties like anonymity, privacy, integrity, there is a need to create a framework which will consume less gas and still produce efficient result.

This framework can be designed to include biometric encryption algorithm with improved False Rejection Rate as well as to design DRE-based voting solution without tallying authorities for more complex voting systems such as single transferable vote (STV) and Condorcet.