

PROGRESS REPORT

ON

E-Voting System using Blockchain

SUBMITTED BY

- 1.Mohit Meena (2017UIT2604)
- 2.Bhavya Rustgi (2017UIT2564)
- 3.Mihir Singh(2017UIT2584)

UNDER THE GUIDANCE OF

Dr. Deepika Kukreja



NETAJI SUBHAS INSTITUTE OF TECHNOLOGY

UNIVERSITY OF DELHI

Introduction

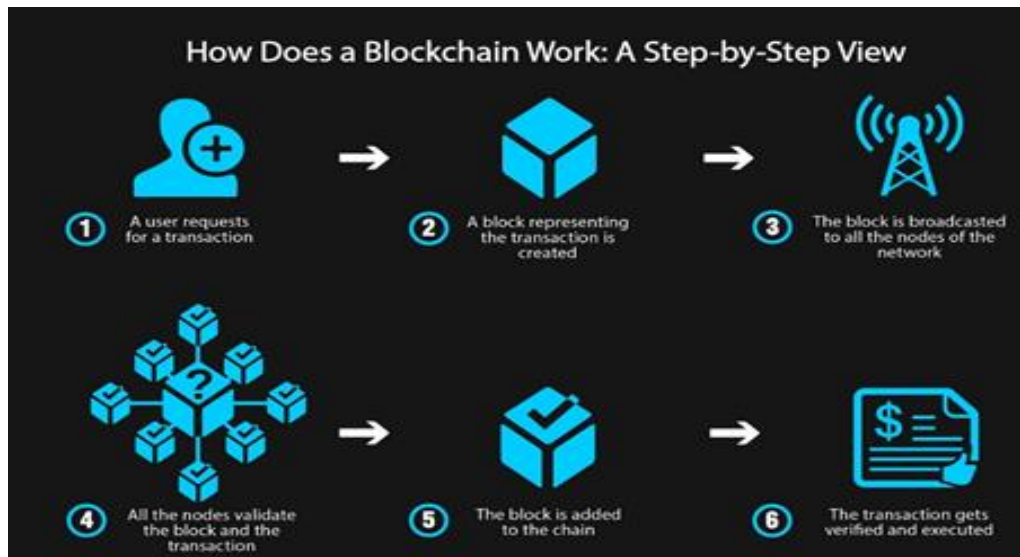
Blockchain is a series of changeless records of information managed by a group of comparable computers not by any single entity. Every block of information is secured and guaranteed to each other using cryptographic principles.

A no. of transactional records is represented by each “block” and the “chain” component links all of them beside a hash function. Once a record is formed, it is confirmed by a distributed network of computers and coupled with the previous entry in the chain, by doing so it creates a chain of blocks.

The information recorded on a blockchain can take on any form, whether it be; denoting a transfer of money, ownership, a transaction, someone's identity, an agreement between two parties. However, to do so requires a confirmation from several devices, such as computers, on the network.

The whole blockchain is kept stored on the large network of computers, which ensures that no single person can have control over its past records. It is an important thing, as it ensures that all the things done in the chain earlier can't be changed by any person by going back in records. It makes the blockchain a public record holder that can't be tampered easily.

In a blockchain network there will be nobody acting as one central authority. It's a shared and immutable ledger, the data in it is open for anyone and everybody to visualize. Everything among the blockchain is evident and everyone involved is responsible for their actions.



Working of Blockchain

Why Blockchain is suitable for E-Voting:

The inability to change or delete the information from the blocks make blockchain the best technology for voting systems. Blockchain technology is using a distributed network having many interconnected nodes. Every node has its own copy of information that contains the full history of all transactions that have been done.

For a strong and healthy e-voting scheme, several functional and security requirements are to be satisfied which includes

1. Transparency
2. Auditability
3. System and Data Integrity
4. Secrecy/Privacy
5. Availability
6. Distribution of authority

Comparison between Blockchain and Centralised Database:

Factor	Blockchain	Centralised Database
Disintermediation	X	
Trust	X	
Real time data	X	
Performance/Speed		X
Confidentiality		X
Robustness	X	
Codebase Maturity		X
Developer maturity	X	
Ecosystem breath	X	
Cost(hardware)	X	

Technologies employed in Blockchains:

Blockchain consists of 3 underlying technologies, that are combined to form better security of a blockchain:

Cryptographical keys:

When two or more persons are attempting to start a transaction among them, one non-public(private) and one public cryptographical key are going to be related to each of them. The mixture of those digital identities. On another side, this created digital identity ensures robust management of possession.

A distributed network with a shared ledger:

Another technology used is distributed network that have the blockchain. The cryptographical key's not enough to ensure the protection of the digital relationship between the 2 persons. This is where the "distributed network" comes into play.

We conclude that the massive size of the network, in a way, contributes to its security. When the distributed network is used with cryptographical keys, the result brings a few helpful varieties of digital interactions. For instance, by using his/her private key User 1 announces an event of some type and links that announcement to User 2's public key. As a result, a segment, better known as "block" is generated and distributed to all participants within the network. This block contains a digital identity likewise other relevant data.

A network servicing protocol:

A major objective of the network servicing protocol is to neutralize the chance that one and therefore the same coin of the various cryptocurrency is employed in many completely different transactions at one and the same time. So as to possess value and be owned by users, Bitcoins and their severable units, known as"

satoshi”, ought to be distinctive. For this to be accomplished, a history of transactions is formed and maintained for every single coin by all the nodes that service the Bitcoin network. What nodes do is use their CPU capability to vote, or they agree on new blocks that are created or reject blocks they think about as being invalid. As shortly as most of the network’s participants reach one and the same resolution, a new block will then be added to the chain. Each new block will have a timestamp and should embody messages or alternative info.

Consensus Algorithm:

A consensus algorithm is a method in computer science used to reach to an agreement on single data value among distributed processes or systems. Consensus [algorithms](#) are designed to attain dependability in a network involving multiple unreliable nodes. Resolving that issue which is referred as the consensus problem is vital in [distributed computing](#) and multi-agent systems.

To accommodate this reality, consensus algorithms essentially assume that some processes and systems are unavailable and that some communications will be lost. As a result, consensus algorithms should be [fault-tolerant](#). They usually assume, for instance, that solely some of nodes will respond but require a response from that portion, like 51%, at a minimum.

Applications of consensus algorithms include:

- Deciding whether or not to commit a distributed [transaction](#) to a info.
- Designating [node](#) as a leader for few distributed task.
- Synchronizing [state machine](#) replicas and guaranteeing consistency among them.

[Blockchain](#), the [distributed ledger](#) most ordinarily related to [Bitcoin](#), conjointly depends on consensus algorithms to achieve agreement among nodes. A blockchain will be thought of as a decentralised database that's managed by distributed computers on a peer-to-peer ([P2P](#)) network. Every peer maintains a replica of the ledger to stop a single point of failure ([SPOF](#)). Updates and validations are reflected in all copies at the same time.

Bitcoin uses the proof of work algorithm (PoW) to confirm security during a trust less network, by having a mechanisms that make sure that the effort of [mining](#) is drawn among the block submitted by the miner. Software on the computers of miners accesses their processing capability to resolve transaction-related algorithms. The block is an encrypted [hash](#) proof of work that's created during a compute-intensive method. Though any party will submit a chain of blocks to the ledger, the quantity of computing resources needed to fake consensus is simply too great to form it worthy to a dishonest party.

Other common consensus algorithms include the practical Byzantine fault tolerance algorithm (PBFT), the proof-of-stake algorithm (PoS) and also the delegated proof-of-stake algorithm (DPoS).

SHA256 Cryptographic Hash Algorithm:

A **cryptographical hash** is a type of 'signature' for a data or text file. SHA-256 generates an almost-unique 256-bit signature for a text.

SHA-256 (Secure Hash Algorithm), is one amongst the cryptographic hash functions that has digest length of 256 bits. It is a keyless hash function, means that an MDC (Manipulation Detection Code).



SHA256 Cryptographic Hash algorithm

In addition, SHA-256 has parameters:

Size of block (byte): 64.

Max length allowed(message) (bytes): 33.

characteristics of the message digest size (bytes): 32.

size of word (bytes): 4.

internal position length parameter (bytes): 32.

the number of iterations in one cycle: 64.

the speed achieved by the Protocol (MiB/s): approximately 140.

RSA Algorithm:

RSA algorithm is asymmetric cryptography algorithm. Asymmetric implies that it works on two different keys i.e. **Public Key** and **Private Key**. As the name describes that the Public Key is given to everybody and Private key is kept private.

The idea of RSA relies on the fact that it's tough to factorise a large integer. The public key consists of two numbers where one number is multiplication of two large prime numbers. And private key is also derived

from the equivalent two prime numbers. Therefore, if someone can factorize the large number, the private key is compromised. Therefore, encryption strength completely lies on the key size and if we tend to double or triple the key size, the strength of encryption will increase exponentially. RSA keys can be usually 1024 or 2048 bits long, however experts believe that 1024-bit keys might be tamed soon. But until now it looks to be an impossible task.

Mechanism behind RSA algorithm:

a. Key Generation Algorithm:

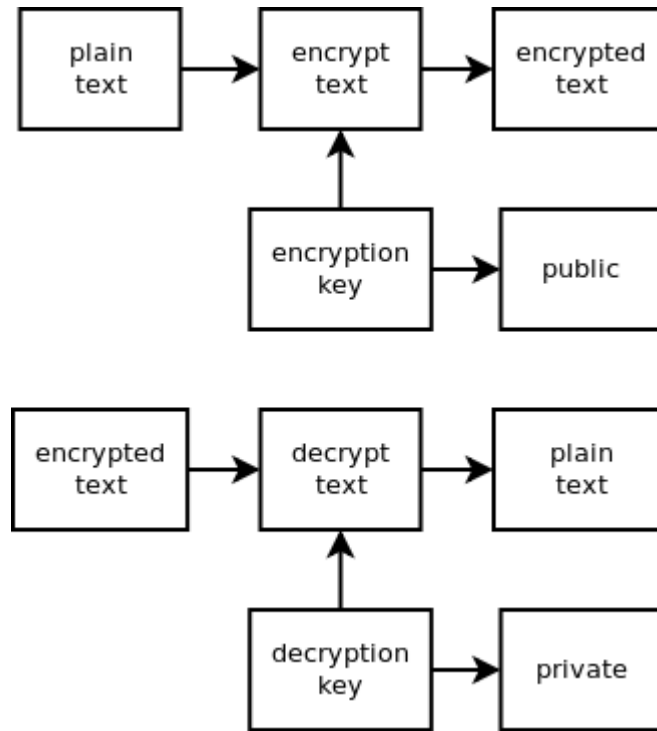
- a. Generate two large random primes, p and q , of approximately equal size such that their product $n=pq$ is of the required bit length, e.g. 1024 bits.
- b. Compute $n=pq$ and $\phi=(p-1)(q-1)$.
- c. Choose an integer e , $1 < e < \phi$, such that $\gcd(e, \phi) = 1$.
- d. Compute the secret exponent d , $1 < d < \phi$, such that $ed \equiv 1 \pmod{\phi}$.
- e. The public key is (n, e) and the private key (d, p, q) . Keep all the values d , p , q and ϕ secret. [Sometimes the private key is written as (n, d) because you need the value of n when using d . Other times we might write the key pair as $((N, e), d)$]

b. Encryption:

- a. Obtains the recipient B's public key (n, e) .
- b. Represents the plaintext message as a positive integer m with $1 < m < n$.
- c. Computes the ciphertext $c = m^e \pmod{n}$.
- d. Sends the ciphertext c to B.

c. Decryption:

- a. Uses his private key (n, d) to compute $m = c^d \pmod{n}$.
- b. Extracts the plaintext from the message representative m .



Encryption and Decryption Process in RSA

Functional and Security requirements of e-voting system:

For a strong and healthy e-voting scheme, several functional and security requirements are to be satisfied which includes:

- **Transparency:** Voters should be able to possess a general knowledge and understanding of the voting process.
- **Auditability:** It should be possible to verify that all votes have been properly accounted for the final election tally, and there should be reliable and demonstrably authentic election records, in terms of physical, permanent audit trail.

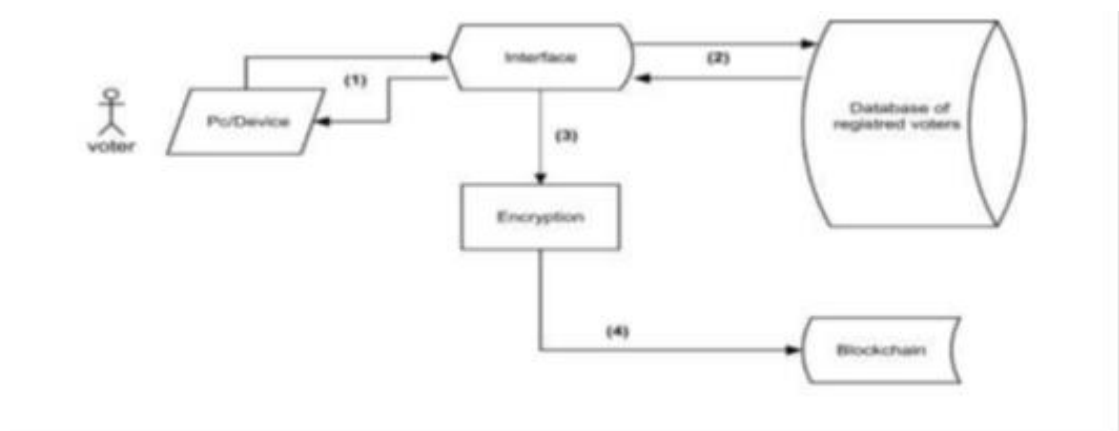
- **System and Data Integrity:** Ensure that the system cannot be re-configured during operation. Ensure that each vote is recorded as intended and cannot be tampered with in any manner, once recorded (i.e., votes should not be modified, forged or deleted without detection).
- **Secrecy/Privacy:** No one should be able to determine how any individual voted.
- **Availability:** the system must have high availability during an election campaign.
- **Distribution of authority:** The administrative authority shall not rest with a single entity. The authority shall be distributed among multiple administrators, who are known not to interact among themselves.

Motivation of the Work

- Vote at any time from anywhere.
- Boost participation: Since the people today are mostly inclined towards mobile technology, it will attract all those people who are lazy or have hurdles in coming to their hometown for voting, of the people who are ill at home etc.
- Less physical infrastructure: Since voting has to happen from the home itself through the network, there is no requirement of setting up schools, colleges etc for voting polls.
- Fast and easy votes tally: Since the tally in online voting is run by machines, you can assure that it will not have human counting errors and that it will in most cases run faster than a count carried out by persons, so the results of your election will be available sooner.
- More rich ballots: With the power of fast video, image and audio facility, online voting gives you the chance to add additional information to the ballots that would not be possible in the traditional system.

Working and Application of our Model

- The initial transaction added to the block is going to be a special transaction that represents the candidate.
- When this transaction is formed it'll include the candidate's name and can serve as the foundation block, with every vote for that specific candidate placed on top of it. In contrast to the other transactions, the foundation won't be counted as a vote, and it will only have the name of the candidate.
- Our e-Voting system will allow a NOTA vote, where the voter may return a blank vote to show his/her dissatisfaction with all candidates or a refusal of the current political system and/or election.
- Every time an individual votes, the transaction will be recorded and the blockchain will be updated.
- To ensure that the system is secure, the block is going to contain the previous voter's data. If any of the blocks were compromised, then it might become easy to find out since all blocks are connected to each other. The blockchain is decentralized and can't be corrupted, no single point of failure exists. The blockchain is where the actual voting takes place. The user's vote gets sent to one of the nodes on the system, and the node then adds the vote to the blockchain. The voting system will have a node in each district to ensure the system is decentralized.



Blockchain Based Electronic Voting System

Working of e-voting system using blockchain is:

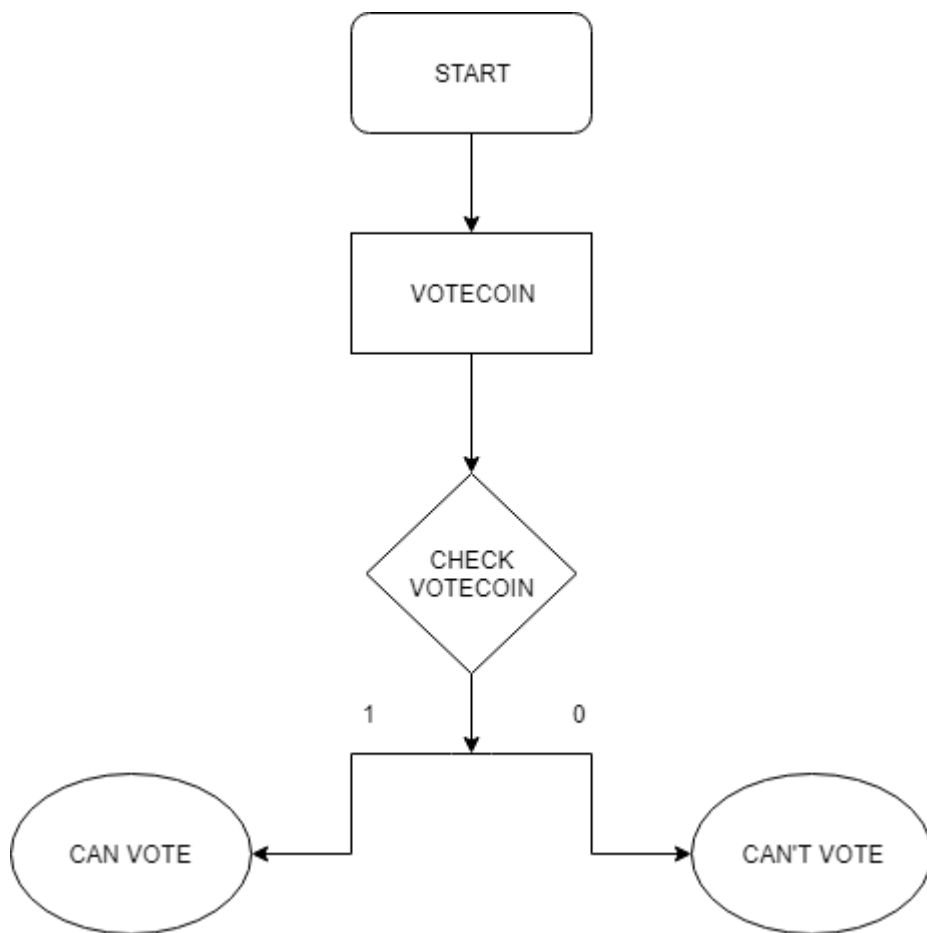
Requesting to vote:

- a. The user will have to register in the voting system. After successful registration, user will have a unique username and a password which he/she will use for logging in.
- b. The user will have to log in to the voting system using his credentials- in this case, the e-voting system will use his/her username which is created while registering and password. The system will check all information entered and, if matched with a valid voter, the user will be authorized to cast a vote.
- c. Our e-Voting system will not allow participants to generate their own identities and register to vote. Systems that allow identities to be arbitrarily generated are usually vulnerable to the Sybil attack where attackers claim many fake identities and stuff the ballot box with illegitimate votes.

Casting a vote:

- a. Voters will have to choose to either vote for one of the candidates or None of the above. Casting the vote will be done through a friendly user interface.
- b. For each voter a token is generated known as VoteCoin. When a new registration is done or when a new session of election starts the value for VoteCoin is marked as 1.
- c. Whenever a voter casts his/her vote the value for VoteCoin token becomes 0.
- d. A voter can cast a vote if and only if VoteCoin value is 1. In this way re-voting problem is resolved.

FLOW CHART FOR CASTING A VOTE



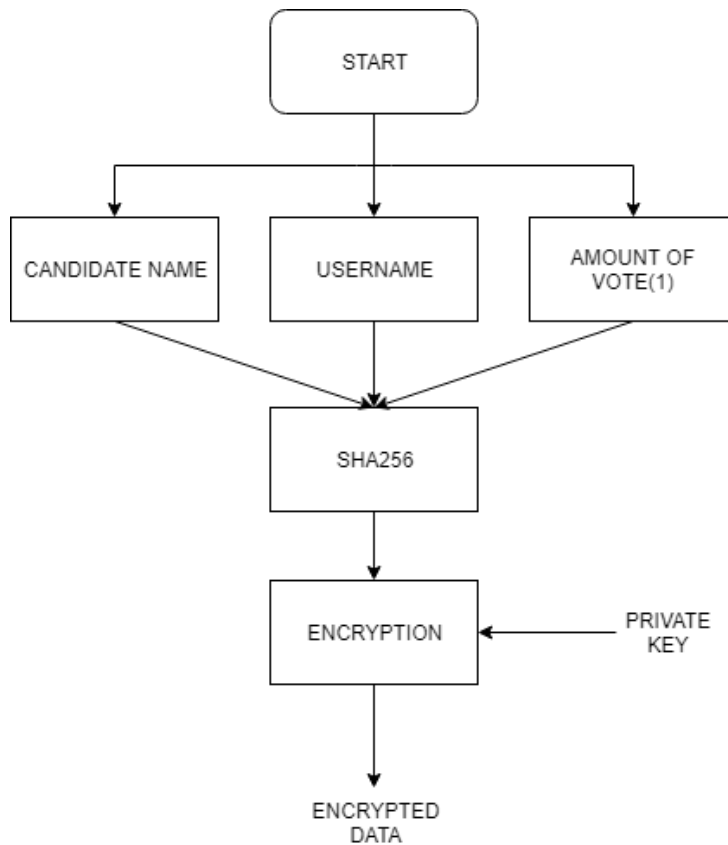
· **Encrypting votes:**

- a. When the user casts his vote, the system is going to generate an input that contains a distinct username or voter id of the voter, name of the candidate for whom he/she had voted for and the amount of vote available for the voter which is in our case will always be 1. This manner every input is distinctive and makes sure that the encrypted output is also distinctive.
- b. The information associated to each vote will be processed using SHA256 hash function that has no illustrious method reverse to it. The sole on paper potential way to reverse the hash would be to guess the seed data and the encryption method and then hash it to see if the results match.
- c. The result from hash function is now encrypted with the private key and an encrypted data is formed. This encrypted data is now added to the transaction and is ready to be stored in the blockchain.

- d. This manner of hashing votes makes it nearly impossible to reverse engineer, thus there would be no way voters' information could be retrieved. This makes the e-voting system secure.

· **Adding the vote to the Blockchain:**

- a. When a block is formed, verification of the vote is done in order to examine whether or not the vote is casted by the person himself or someone tampered it.
- b. For verification of the encrypted data is decrypted with the help of the public key.
- c. Decrypted data is then checked to confirm the integrity of the vote that whether or not it is tampered.
- d. After Successful verification, block gets linked to the previously cast vote.



FLOW CHART FOR ENCRYPTING VOTES

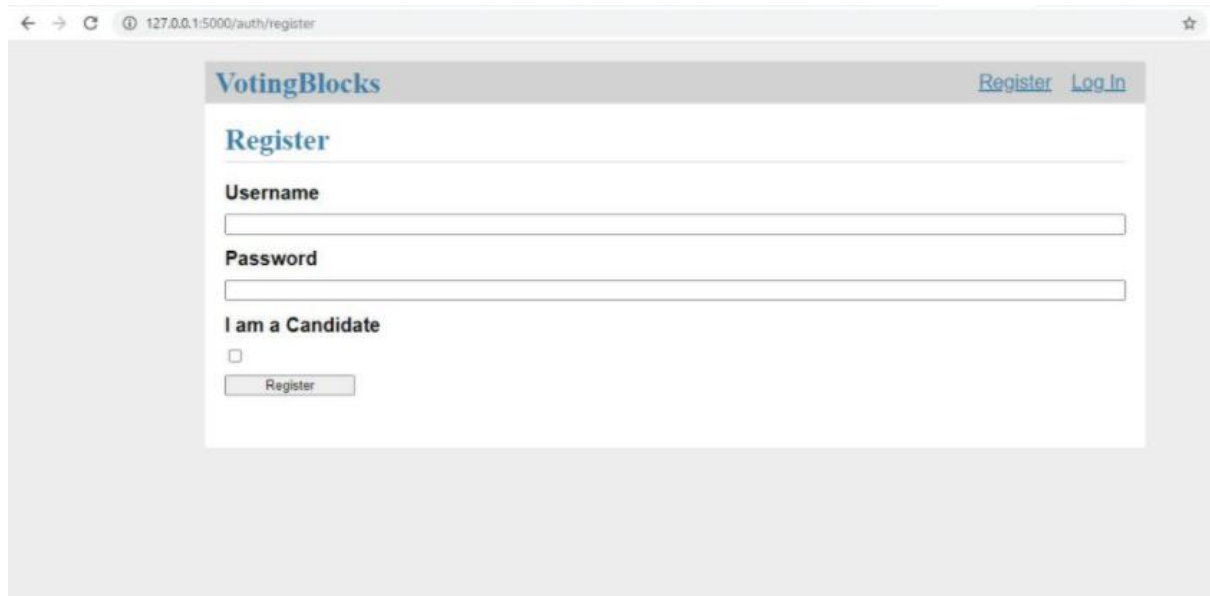
Experimental Results

In the end of this whole process we have the decentralised voting application which can be used to organise votes with no central authority in control. This application allows users to be on the network and all machines on the network run the server as peer to peer and all of them can act as a server and a client. Finally, we have an application which provides us with the following functionalities:

1. Adding a node in the network: We can add a machine to the network by exchanging addresses of the machines and refer to them as nodes, so we have a blockchain network set up.
2. Registering and logging in: We have the facility for users to register on the blockchain network as a candidate or simply a voter only. We create a public and private key pair for the users in this step. Then users can log into their account using these keys.
3. Casting vote: We get the ability to cast vote which in our case is transfer of the VoteCoin to the candidate. We can only cast vote when our account has a VoteCoin, when we cast our vote, we transfer our VoteCoin to the receiver candidate, and our VoteCoin balance is reduced to 0 and we can no longer vote anymore.
4. Live monitoring: We can view the vote stats of the candidates in real time on the home page.
5. Verifying and viewing the chain: We can check the correctness of the chain and we can view it any time to verify the stats of the candidates.

Thus, we have a full-fledged e-voting application that fulfils the properties:

- Transparency
- Auditability
- System and Data Integrity
- Secrecy/Privacy
- Availability
- Distribution of authority



A screenshot of a web browser displaying the registration page for 'VotingBlocks'. The browser's address bar shows '127.0.0.1:5000/auth/register'. The page has a grey header with the 'VotingBlocks' logo on the left and 'Register' and 'Log In' links on the right. The main content area is white and contains the title 'Register' followed by two input fields for 'Username' and 'Password'. Below these is a checkbox labeled 'I am a Candidate' and a 'Register' button.

VotingBlocks [Register](#) [Log In](#)

Register

Username

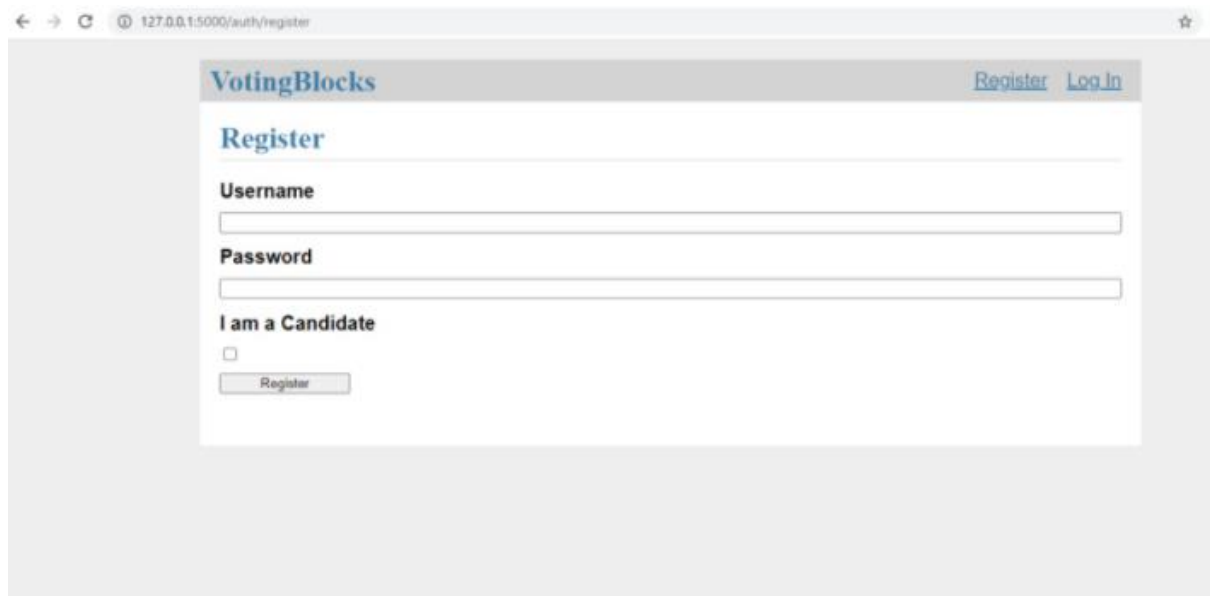
Password

I am a Candidate

☐

Register

Homepage of Application



A second screenshot of the same 'VotingBlocks' registration page, showing the same layout and elements as the first image. The browser address bar, header, and form fields are identical.

VotingBlocks [Register](#) [Log In](#)

Register

Username

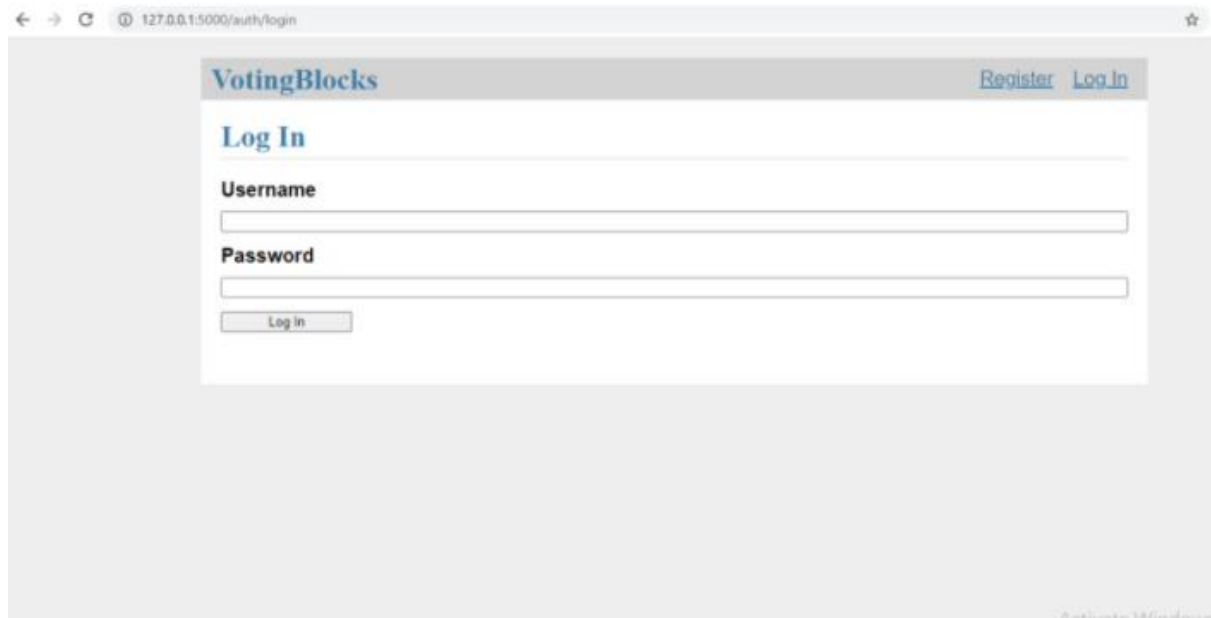
Password

I am a Candidate

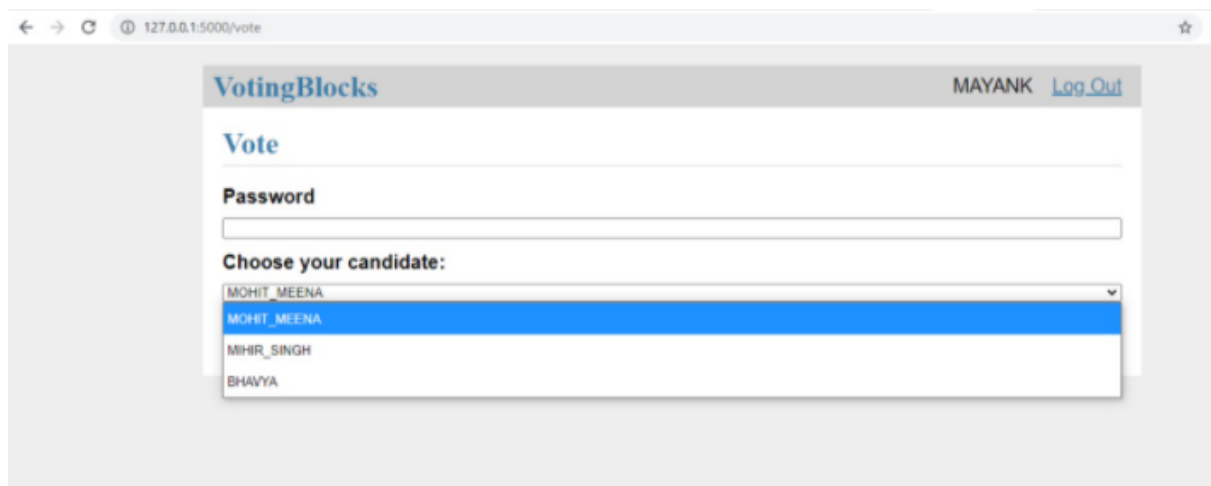
☐

Register

Registration Page



Login Page



Voting page after Successful login

References

- [1] Mrs. Harsha V. Patil, Mrs. Kanchan G. Rathi and Mrs. Malati V. Tribhuwan, “A Study on Decentralized E-Voting System using Blockchain Technology” in *International Research Journal of Engineering and Technology (IRJET)*.
- [2] Zibin Zheng¹, Shaoan Xie¹, Hongning Dai², Xiangping Chen⁴ and Huaimin Wang³ “An Overview of Blockchain Technology: Architecture, Consensus and Future Trends” in *IEEE 6th International Congress on Big Data*, 2017.
- [3] Mahdi H. Miraz¹, Maaruf Ali, “Applications of Blockchain Technology beyond Cryptocurrency” in *Annals of Emerging Technologies in Computing (AETiC)*, 2018.
- [4] Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis; “E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy”.
- [5] Zibin Zheng¹, Shaoan Xie¹, Hongning Dai², Xiangping Chen⁴, and Huaimin Wang³; “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends”; *IEEE 6th International Congress on Big Data*.
- [6] Ahmed Ben Ayed; “A Conceptual Secure Blockchain –Based Electronic Voting System”; *International Journal of Network Security & Its Applications*
- [7] Pavel Tarasov and Hitesh Tewari; “The Future of E-Voting”; *IADIS International Journal on Computer Science and Information Systems Vol. 12, No. 2, pp. 148-165*
- [8] Kibin Lee, Joshua I. James, Tekachew Gobena Ejeta, Hyoung Joong Kim; “Electronic Voting Service Using Block-Chain”; *Journal of Digital Forensics, Security and Law*.
- [9] Gautam Srivastava¹, Ashutosh Dhar Dwivedi² and Rajani Singh²; “Crypto democracy: A Decentralized Voting Scheme using Blockchain Technology”
- [10] Arul Lawrence Selvakumar, C. Suresh Ganadhas; “The Evaluation Report of SHA-256 Crypt Analysis Hash Function”; *2009 International Conference on Communication Software and Networks*.

Xin Zhou, Xiaofei Tang; “Research and Implementation of RSA algorithm for encryption and decryption”, *6th International Forum on Strategic Technology*, 2011.