Multimedia Tools and Applications
https://doi.org/10.1007/s11042-023-17837-x

A Blockchain Framework for E-Voting

Harikesh Singh[1] · Amit Sinha[2]

Received: 3 February 2022 / Revised: 17 November 2023 / Accepted: 8 December 2023

Abstract
An electronic democratic framework can also fulfill all the rules and regulations of any governing body. The election is one of the important events for a robust democratic system in a country, but still, many people are not thinking of it as major concern for democracy. There are several issues of vote fraud, hacking of EVM (Electronic Voting Machine), election manipulation, and booth capturing within the current electoral system. In this paper, we proposed a framework for E-voting (Electronic Voting) which might resolve these issues. This framework uses Blockchain technology as a service along with an E-Voting system that addresses all restrictions. Blockchain advancements proposed a wide scope of different applications to reduce the sharing of monetary economies. The proposed framework uses proof of voter's identity (PoVI) consensus algorithm that makes the proposed system more secure and differentiates this model from other models of E-voting systems. The objective of this paper is to clarify the utilization of Blockchain innovation as assistance for an authentic electronic democratic framework. The proposed framework evaluates the capability of distributed record advances with the assistance of illustrative contextual analysis, specifically the cycle of a political decision that improves security and minimizes the expense of facilitating a cross-country casting a ballot framework.

Keywords Blockchain · Voting · Framework · Blocks · Decentralized · EVM

1 Introduction

Voting plays an important role in our society and improving the election security is an important aspect of national security. In recent years, voting disregard has grown exponentially among the youngsters due to unawareness. E-Voting has the potential to attract younger voters. In the rigorous E-Voting system, a number of operational and security requirements have been specified including [1, 2]:

✉ Harikesh Singh
harikeshsingh@yahoo.co.in

Amit Sinha
amit.sinha@abes.ac.in

[1] JSS Academy of Technical Education, Noida, UP, India

[2] ABES Engineering College, Ghaziabad, UP, India

Published online: 27 December 2023

- **Openness**: We can see the first results before the end of the voting process; this guarantees that (the remaining) voters will not be affected by their vote.
- **Eligibility**: This power helps to ensure that only legitimate voters are allowed to vote and must do only once. The basis of this structure is verification because voters need to prove their identity before they can be considered eligible or not.
- **Privacy**: The way each person is voted that should not be disclosed to anyone. This unusual property by voting (non-electronic) is guaranteed to protect the voter from harmful eyes.
- **Verification**: This special power allows all parties that are part of the electoral process to have the power to determine whether their votes are registered or not. Usually two types of verification are defined, each verification and universal verification. Verification gives each voter the right to check whether his or her vote is registered. Public administration requires that everyone check to see if the election results are published.
- **Forced resuscitation**: A fraudulent person should not have the ability to distinguish whether a compulsory voter voted as instructed.
- **Forgiveness**: The power of the vote to change a vote after it has been cast. It will link to forcing contempt because it gives the unintentional voter a chance to change votes over time to express his or her true opinion.

1.1 Blockchain Technology

A simple definition is a 'chain' of blocks. Block is a fixed data set. Data blocks are stored, collected and processed for blocking by a special process called mining. Blocks in a ledger can be seen using block id or block number or merkle tree and using other cryptographic hash functions (also known as digital fingerprint). The created block will have the hash of the previous block created, so that the blocks can build a series from the first block ever (known as the Genesis Block) to the built block. In this way, all data can be linked via a linked list structure. Blockchain is split, distributed, static (add only), unchanged, public ledger. In a Blockchain-based system, there is no trusted medium link, each node involved in the Blockchain system holds a data block in place. Blockchain technology is maintained by a network of friends [3, 4].

The Blockchain based technology was first introduced to us in 2008 (Bitcoin White Paper) when a group of people or Satoshi Nakamoto (Anonymous) created the first crypto coin called Bitcoin.(Fig. 1).

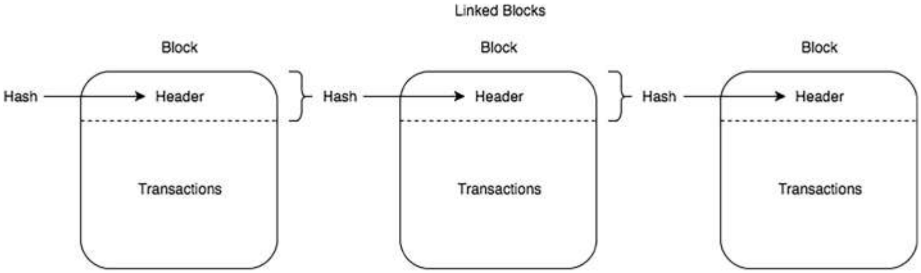


Fig. 1 A Block Structure

1.2 Features of Blockchain

1.2.1 Increased Power

This is the first and most important feature of Blockchain. The most important thing about this Blockchain technology is that it continues to increase power across the network. This is because there are so many computers (nodes) that work together that completely provide the power then a few devices where things can be shared.

Better Security This Blockchain technology provides high security and unbreakable security because the logger data is stored on multiple network nodes and all nodes are synced to other nodes so there is no chance of shutting down the entire system. Or there is a possibility that the top financial system could be hacked. Bitcoin on the other hand is ineffective. The main reason is that this Blockchain network is run on multiple nodes on behalf of all nodes connected to other nodes using the gossip protocol.

Consistency Making ledger (fixed) ledgers is one of the key principles of Blockchain Technology. Any unauthorized database is used for hacking and they ask for trust from another party to keep the database safe from hackers. Blockchain like Ethereum, Bitcoin keeps their ledgers in a constant state of continuous momentum.

Commercial Reduction Divided technology gives you the ability to store your assets on a network that continues to be accessible via the Internet, the asset can be like any other contract, document etc. The way the owner has direct access to all accounts with a private key attached to his accounts that gives the owner the ability to transfer his assets to anyone he wants.

Transparency Transparency makes the Blockchain available to the public for general use. Any peer-to-peer node in the Blockchain network can go through all the records created from the genesis block.

2 Literature Survey

Adida, B. and Helios (2008) propose to support an adequate safety model and methods of judging comprehension. It also describes the web voting theme, Durable Democracy, which shows that it satisfies a sufficient security model that is more understandable than the Good Smart Democracy, which is now the only body that satisfies beyond that a planned security model [5, 6].

Chaum, et al. (2008), describes scantegrity as having a small impact on selection processes and is the first independent method to validate E2E which maintains optical scan as a basic voting system and does not interfere with hand counting [7, 8].

Dalia, et al. (2012) proposes a cycle of cover-ups so that election results can be announced when voters have abortions and add a cycle of commitment to ensure justice. In addition, it also provided proof of computer security for the confidentiality of the vote [9, 10].

Bell, et al. (2013) describes the STAR-Vote design, which may be Travis County's next-generation electoral system and could be elsewhere [11, 12].

The latest technological challenges related to electronic voting systems are inclusive, yet they are not limited to protecting digital identity management. Any potential citizen must re-register in the pre-election process. Their data must be in a digital format. Alternatively, their identity data must be personal and not confidential to any information involved. The old E-voting system may face the following problems [13, 14]:

- Voting anonymously
- Individual voting procedures
- Confirmation of voting (and only) by voter
- Top initial setup costs
- Increasing security issues
- Confidentiality and trust
- Voting delays or efficiency related to remote /absent voting

As blockchain have certain advantages such as immutable, transparent and more secure as compare to other methods we have chosen blockchain based model for E-voting system. Below is the comparison with other methods [15, 16]:

1. **Traditional E-Voting Systems:**
2. **Security:** Blockchain offers enhanced security compared to some traditional e-voting systems.
3. **Transparency:** Blockchain provides a more transparent and auditable process.
4. **Cost:** Traditional systems might be less resource-intensive initially.
5. **Mobile/Internet Voting:**
6. **Security:** Blockchain offers a decentralized security model, potentially more resilient to cyber threats.
7. **Access:** Mobile/Internet voting may be more accessible but can pose security and privacy challenges.
8. **Paper-Based Voting:**
9. **Security:** Blockchain can enhance security and reduce the risk of tampering compared to traditional paper-based systems.
10. **Trust:** Some voters may still have more trust in the physicality of paper ballots.

As blockchain offers several advantages for e-voting, it is not a one-size-fits-all solution. Careful consideration of technical, social, and regulatory factors is essential in determining whether blockchain is the most suitable option for a particular e-voting system[17, 18].

3 Proposed Framework

According to our design we have tried to create a system that does not completely include the current vote but integrates within the current system. We have decided to do this to allow for as many different types of voting as possible, this is because voting can be achieved by the majority of the people. The proposed system of E-Voting facilitate to each person of any country from anywhere in the world through internet. It also ensures with maximum level of privacy and security that can be fixed according to election regularity committee defined for the entire process of voting. This framework is developed for the improvement of the current voting process with following steps:

Step-1: It gives voters the special power to vote from anywhere (poll site) in the country without the use of tickets.
Step-2: Reduce the no. of legitimate vote not counted by reducing the number of over-votes, and eliminating vote tampering.
Step-3: Increasing voter confidence and improving the voting experience.
Step-4: The main reason for adopting the digital voting systems is to make the voting system process useful for common people, cheaper, faster and easier, and easily adopted by modern society.
Step-5: Keeping the authenticity of our voters safe.
Step-6: The voting system is scalable and applicable.
Step-7: The voting system is platform-independent and provides comprehensive security assurances.

4 Need of Blockchain

A Blockchain instead of traditional web technology, if we somehow managed to lead our E-Vote casting a ballot framework on the Custom Web, we would experience various issues in one information base can be changed, it can be checked more than once for a specific client, or erased by and large. Source code on web worker can likewise be changed whenever. Hence, we should expand on the Blockchain where anybody associated with the system can take an interest in the political decision at once.

4.1 Tools Used

These are the tools used for the Blockchain framework development used for E-Voting [19, 20]:

Hub Package Manager: The primary reliance we need is Node Package Manager or NPM [21].
Truffle Framework: The following reliance is the Truffle Framework which permits us to assemble decentralized applications on the Ethereum square Blockchain [22]**.**
Ganache: A local server [23].
Metamask: An ethereum wallet.
Solidity: A language specially used for smart contract development. It is a statically typed language. The best way to try out Solidity is with Remix (an online editor), the web-based IDE. Solidity supports various libraries, inheritance support, and complex types, abstraction and many more [24].
Smart Contracts: An account controlled byte code. This code instructs the smartcode how to behave in business based transactions [25].
Kovan: It is a public test network used where we deploy the contract for testing [26].
Web3.js: An Ethereum based JavaScript application platform interface used to get programmatic access to a deploy contract to a Blockchain which connects to the JSON RPC. A local or remote node must be run to use this library [24].

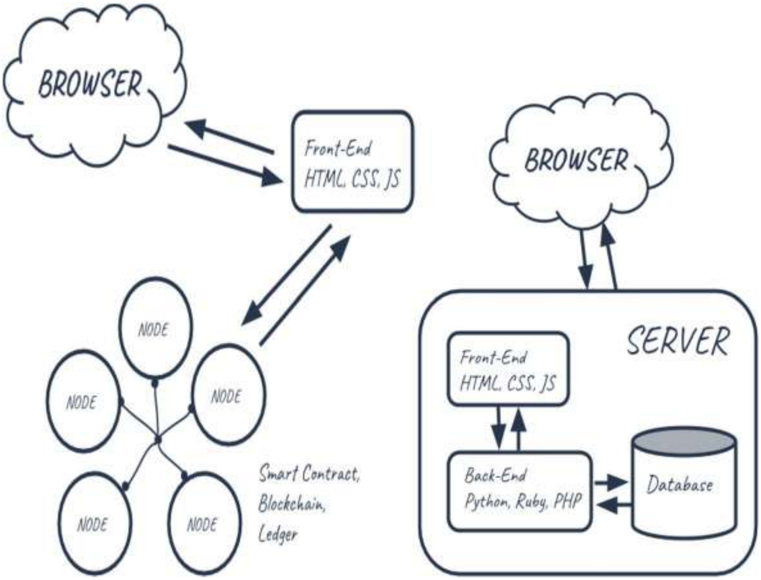


Fig. 2 **An Interface to Ethereum Blockchain** [25]

EtherScan: Etherscan, Ethplorer, and other Blockchain navigator websites are basically a read-only interface to the Ethereum Blockchain [27].(Fig. 2)

3.3 Despite the lack of a central authority to validate and verify the transactions, each and every transaction on the Blockchain is thought to be totally secure. Only the consensus mechanism, an essential component of every Blockchain network, makes this feasible. The process by which all of the peers in the Blockchain network come to a consensus over the current state of the distributed ledger is known as a consensus algorithm. Consensus algorithms accomplish this by building trust amongst strangers in a distributed computing environment and ensuring reliability in the Blockchain network. There are several types of consensus algorithms that can be used for consensus mechanisms. Ethereum blockchain uses a proof of work consensus algorithm.

5 Proof of Work:

The miner for the subsequent block generation is chosen using this consensus procedure. This PoW consensus algorithm is used by Bitcoin. This algorithm's main goal is to quickly and simply solve a challenging mathematical puzzle. The node that can answer this complex mathematical challenge the fastest gets to mine the next block because it demands a lot of processing power.

The given code represents a simplified PoVI consensus algorithm, where transactions are added to a blockchain if they are associated with registered voters and have valid signatures. Validator nodes play a role in block validation, and the algorithm includes basic transaction and block verification logic. Anonymity and privacy is maintained through cryptographic techniques, such as zero-knowledge proofs, are used to protect the anonymity of voters. Validators do not have access to the actual votes; they only verify the identity and uniqueness of voters.

6 Solidity code for Proof of work is as follows:

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract ProofOfWork {
    // Difficulty level for the PoW algorithm
    uint public difficulty = 3;

    // Target value for the PoW algorithm
    bytes32 public target;

    // Nonce (number used once) for the PoW algorithm
    uint public nonce;

    // Block hash to be mined
    bytes32 public blockHash;

    // Constructor sets the target value based on the difficulty
    constructor() {
        target = bytes32(2 ** (256 - difficulty) - 1);
    }
    // Function to mine a new block
    function mineBlock() public {
        // Increment the nonce until a valid hash is found
        while (blockHash >= target) {
            nonce++;
            blockHash = calculateHash(nonce);
        }
    }
// Function to calculate the hash of the block
    function calculateHash(uint nonce) public view returns (bytes32) {
// Example hash function (you should use a secure hash function in a
real implementation)
        return keccak256(abi.encodePacked(nonce));
    }

// Function to get the current block hash
    function getBlockHash() public view returns (bytes32) {
        return blockHash;
    }
// Function to get the current nonce
    function getNonce() public view returns (uint) {
        return nonce;
    }
// Function to check if the mined block meets the difficulty requirement
    function isValidBlock() public view returns (bool) {
        return blockHash < target;
    }
}
```

The above code uses a simple hash function (keccak256). Ethereum is transitioning to a PoS consensus mechanism for its Ethereum 2.0 upgrade.

7 Proposed E-Voting System

Our goal is to create a Dapp where voters can register with their unique ID, and then receive a unique token id used to sign in to Dapp and vote. The vote was recorded in a Blockchain register, and Dapp reflects the current voting for election representatives. Toward the start of the Assigned Location application, the voter registers to cast a ballot by giving the driver's permit number, recorder district, and name and surname and telephone number. In this step, you can check to see if their provided ID is active and not yet registered. If they are valid, we create a private and public key for the used voter and the cloud-operated CA and add those keys to the fund.

After that, voters use their unique ID to cast their ballots, during which Dapp checks whether the voter with this ID has voted before or not. If this particular ID is not previously used by anyone else, the vote experiences an agreement strategy, and the worldwide Blockchain is being evaluated. Dapp then refreshed the current political decision results to show which ideological group the voter decided in favor of whom. Since every exchange submitted to the request hub must have a mark from a substantial private and private key pair, we can follow every exchange in an enlisted Dapp voter, in case of a review.

Given that all exercises put away on the Blockchain have arrived at POW (Proof of Work) in the system and are unaltered (extra), utilizing Blockchain casting a ballot assembles trust between general society and the legislature. Likewise, by utilizing a chaincode to complete the democratic cycle, casting a ballot turns into a quicker and more secure cycle. Despite the fact that this is a standard application, this may be helpful. The following exercises utilized in the political decision measure as shown in Fig. 3:

(i) **Political race creation:** Election heads make voting forms utilizing Dapps. This decentralized application connects with a political race creation chaincode, in which the overseer characterizes a rundown of competitors (other candidates can also be added). The chaincode with smart contracts was created for multiple numbers of smart contracts and deploying them into the Blockchain based ledger, with a full number of candidates, for every constituency, where each constituency is a boundary in each keen agreement cum chaincode. At the point when the exchange was made, every single comparing locale hub has a privilege to speak with the relating savvy contract.

(ii) **Registration:** This registration process of the voters is started by the election commission of a particular district. When conducting txID for elections the district electoral

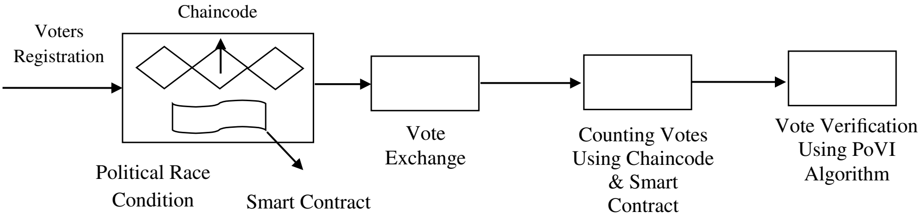

Chaincode
Voters Registration
Political Race Condition
Smart Contract
Vote Exchange
Counting Votes Using Chaincode & Smart Contract
Vote Verification Using PoVI Algorithm

Fig. 3 Process flow diagram of proposed E-Voting system

officers must specify the full list of eligible voters. This requires part of the government's ID verification service to ensure the accreditation of eligible candidates. Utilizing such confirmation benefits, each qualified voter must have an electronic ID and token number and data of voter constituency. For each eligible and legitimate voting person, the corresponding fund will be produced for the voter. The token created for each voter must be different from each political race voter qualified for and NIZKP (Non Interactive Zero Knowledge Proof) can be consolidated to make such a token so that the framework itself doesn't realize which reserve is the equivalent for every voter.

(iii) **Vote exchange:** When a voter votes in a polling station, the voter experiences a brilliant ball cum chaincode voting form with a similar democratic stall as characterized for every voter. This brilliant temporary worker interfaces with the Blockchain blog with a relating local hub, adding a vote to the Blockchain record if an agreement is reached between the numerous regions related with the specialists.

(iv) **Counting votes**: Counting of the voting result is done by making use of chaincode cum smart contract. Every savvy contract checks their own decisions in favor of their relating voting public in their own record framework. When the political decision is finished, a definitive outcome for each and every candidate is announced.

(v) **Verification of vote:** Every individual user or voter gets his unique transaction ID of the vote. Every separate user goes to their election commission office and provide their unique transaction ID after checking themselves using their electronic unique ID and the accompanying unique PIN. The government official, making use of a district peer node can access the full Blockchain, uses the Blockchain explorer (etherscan or other tool) to find the hash of the transaction with the unique transaction ID on the Blockchain based ledger. The user can therefore see his vote on the Blockchain, verifying that it was counted and counted correctly.

8 Proof of Voter Identity (PoVI) Consensus Process

- A group of randomly selected validators (Voter Verifiers) is chosen from a pool of eligible voters.
- The validators, who are also registered voters, are responsible for verifying the legitimacy of the votes.
- To reach consensus, the validators validate each vote by checking that the voter's digital identity is unique and valid.
- Validators achieve consensus by signing the vote transactions.

In the given pseudocode, the functions are described as follows:

- The `ProofOfVoterIdentity` contract has an `electionAuthority` address that is set during deployment.
- The election authority can register voters using the `registerVoter` function.
- Voters can cast their votes using the `castVote` function, but only if they are registered and have not voted before.
- The contract emits events (`VoterRegistered` and `VoteCasted`) to log important actions on the blockchain.

In the algorithm, double-voting prevention is maintained as follows:

- The blockchain ensures that a voter can only vote once by checking the unique digital identity during the voting process.
- Validators prevent double voting at the consensus level.

The blockchain network remains secure through the use of a traditional consensus algorithm (e.g., PoS or PoA) to secure the overall ledger and prevent malicious activity.

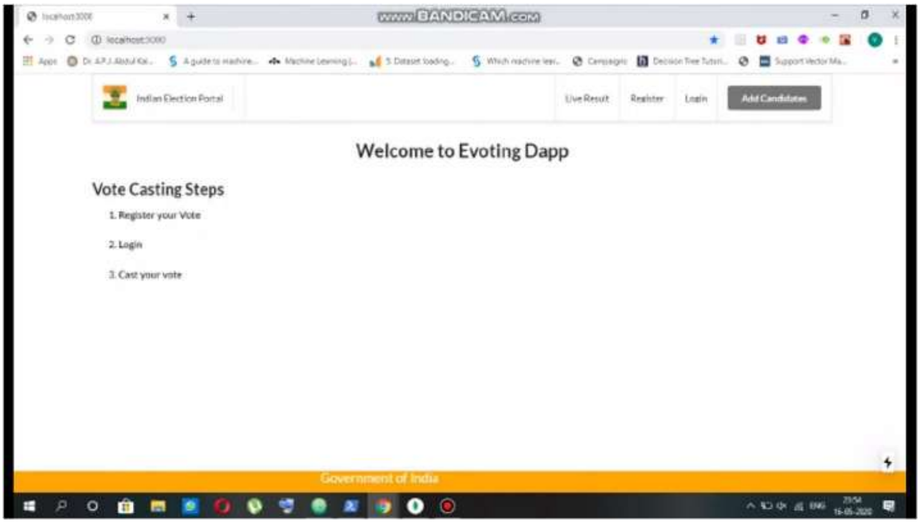
9 Post-Election Verification is done as follows:

- Voters receive a cryptographic receipt confirming their vote without revealing their choice, which they can use for personal verification.
- The overall blockchain can be audited to ensure the accuracy and integrity of the election.

10 Implementation Analysis

To introduce a secure authentication method, our proposed framework is intended to utilize electronic ID confirmation, which is an Icelandic help check specialist organization. It utilizes Nexus programming and RFID scanners. At the point when a client enrolls an electronic ID, the client chooses a PIN number for their relating ID number of 6. The client will in this way distinguish themselves at the voting booth by examining his ID and giving his comparing PIN number to confirm the framework.

1) Any PC in any democratic region might be utilized by any qualified voter, as the comparing voter's vote contains data on which body electorate a voter must cast a ballot. All together for the client to confirm effectively, a substantial ID and PIN number must be introduced in the democratic region utilizing a card per user and nexus programming.
2) If the affirmation is productive, a shrewd relating contract is told to continue with the political race. Casting a ballot in the previously mentioned political race is a smart agreement with a run-down of voters to browse.
3) Once a voter has chosen an up-and-corner and is casting a ballot, the voter keeps on marking their vote by returning the PIN comparing number into their electronic ID.
4) After a voter has marked their vote, the subtleties of the vote keep on being checked by the relating territorial hub, with which the voter manages a brilliant agreement. In the event that the previously mentioned provincial hub gets the democratic information, the subtleties of the vote must be settled upon by most of the relating territorial ward.
5) If most of local friend hubs concur on the quantity of votes cast, a particular vote was settled upon. The client at that point got an exchange ID with the relating exchange of their vote as a QR code and the choice to print the worker ID. When a vote has been projected and affirmed, a brilliant contracted representative can add one vote to the gathering decided in favor of. This keen agreement system is utilized to decide the



Welcome to Evoting Dapp

Vote Casting Steps

1. Register your Vote

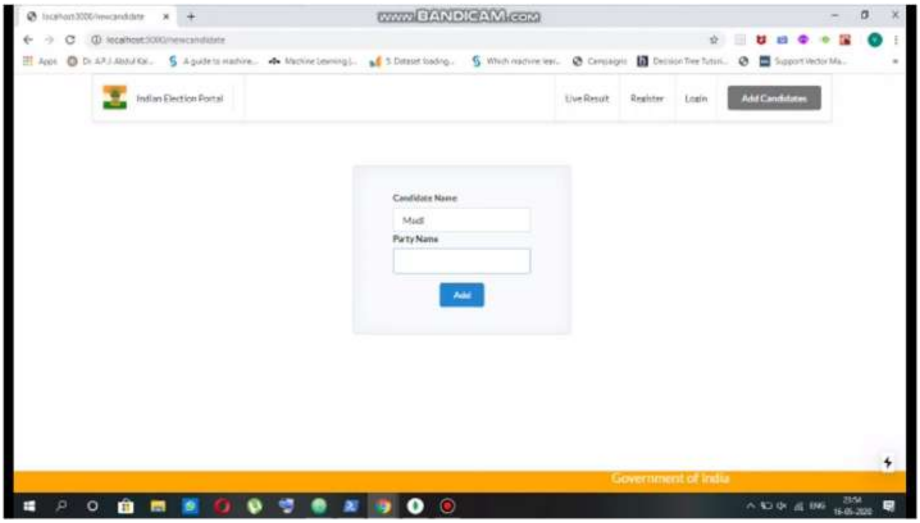
2. Login

3. Cast your vote

Fig. 4 Dashboard of E-Voting Blockchain Framework

political race results for every electorate. Figure 3 is a visual portrayal of the means we have quite recently depicted. (Figs. 4 and 5)

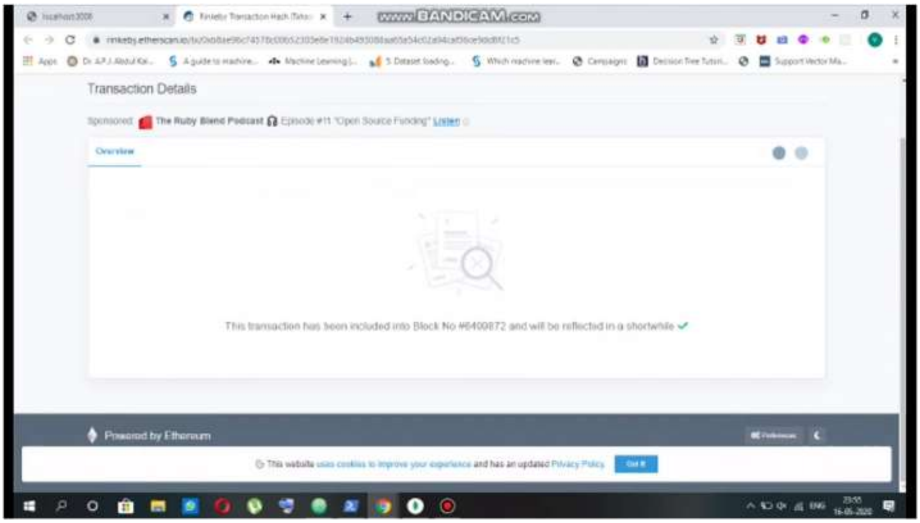
6) All exchanges got and checked during a persistent square are set on the Blockchain after the square time frame has arrived at its time limit (see Figs. 6 and 7). With each new square added to the Blockchain, each provincial site reestablishes its own record duplicate.(Figs. 8 and 9)



Candidate Name: Modi

Party Name:

Figure. 5 Login Screen of E-Voting Blockchain Framework



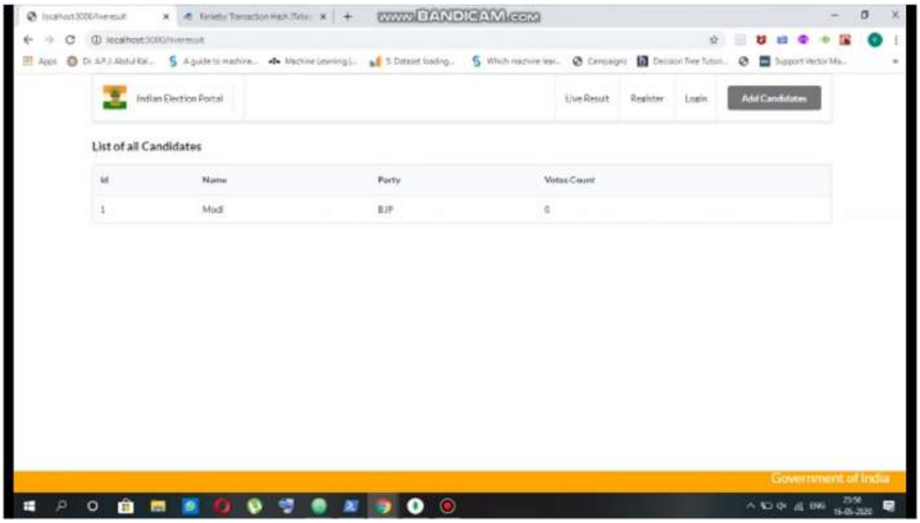
Transaction Details

Sponsored: The Ruby Blend Podcast Episode #11 "Open Source Funding" Listen

This transaction has been included into Block No #6400872 and will be reflected in a shortwhile ✓

This website uses cookies to improve your experience and has an updated Privacy Policy. Got It

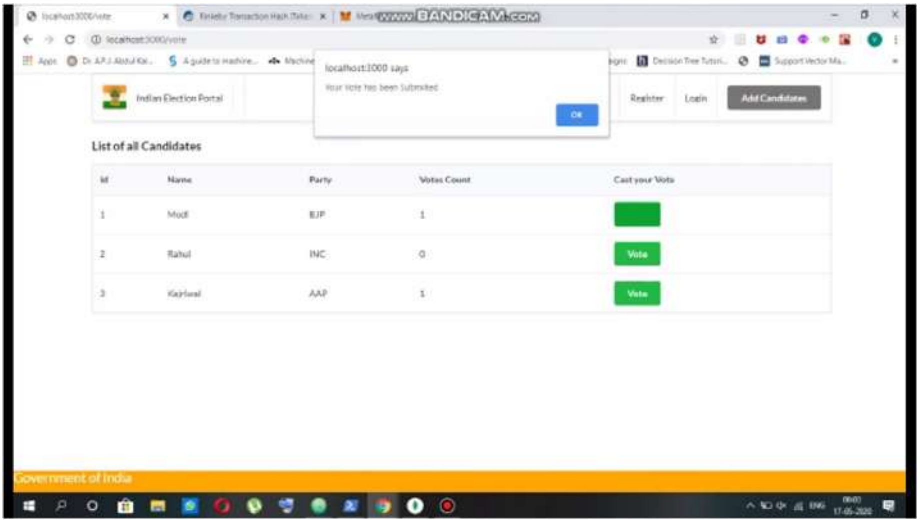
Fig. 6 Transaction details of E-Voting Blockchain Framework



List of all Candidates

Id	Name	Party	Votes Count
1	Modi	BJP	0

Fig. 7 Candidate details of E-Voting Blockchain Framework



localhost:3000 says

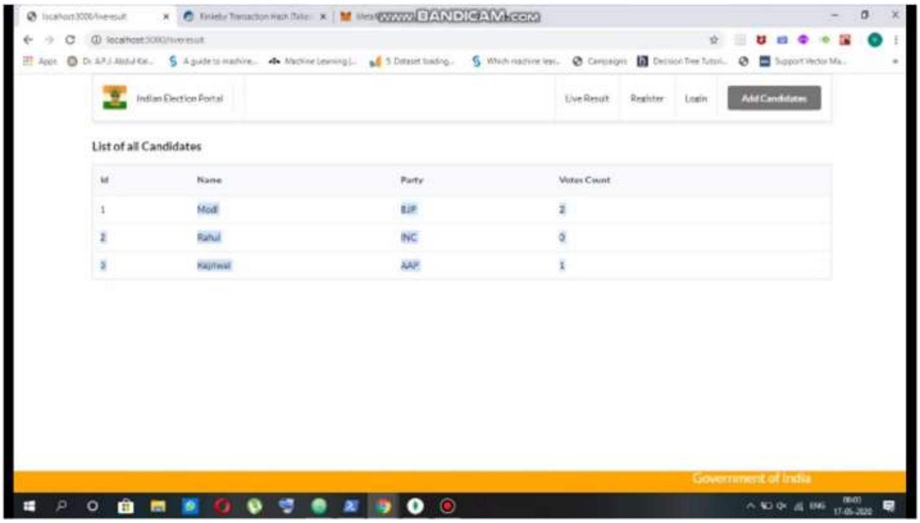
Your Vote has been Submitted

OK

List of all Candidates

Id	Name	Party	Votes Count	Cast your Vote
1	Modi	BJP	1	
2	Rahul	INC	0	Vote
3	Kajriwal	AAP	1	Vote

Fig. 8 Vote Casting details of E-Voting Blockchain Framework



List of all Candidates

Id	Name	Party	Votes Count
1	Modi	BJP	2
2	Rahul	INC	0
3	Kajriwal	AAP	1

Fig. 9 Vote Count details of E-Voting Blockchain Framework

11 Conclusion and Future Scope

The main reason for adopting the digital voting system is to make the voting system process useful for common people, cheaper, faster and easier, and easily adopted by modern society. It provides a faster electoral processing system that removes the hurdles faces between the voter and the elected official. E-Voting has a potential solution to the lack of interest in voting amongst the young generation. It also opens the door for a more direct form of democracy, allowing voters to express their will on individual bills and propositions. Build the good relationship between government and public.

A Blockchain that contains information on who is registered to vote and allows our service to ensure that each voter is different. Once you have registered you are given a vote after confirmation of your details. Ensuring the identity of these registered voters at the start of the voting process is a 3-factor verification process as described in Sect. 3. In addition, we also need to ensure that they are not forced to vote in a certain way and therefore include a double check service where users will be barred a second time to confirm their entry before a vote is cast, this also allows us to almost eliminate abnormal votes.

Funding This study was not funded.

Declarations

Conflict of Interest The author declares no conflict of interest.

References

1. Sekar S, Vigneshwar C, Thiyagarajan J, Soorya Narayanan VB, Vijay M (2020) Decentralized e-voting system using Blockchain. Int Res J Eng Technology (IRJET) 7(03):312–324
2. Chaithra S, Hima JK, Amaresh R (2020) Electronic voting system using Blockchain. Int Res J Eng Technol (IRJET) 7(07):323–338
3. Alvi ST, Uddin MN, Islam L (2020 August) Digital voting: A blockchain-based e-voting system using biohash and smart contract. In 2020 third international conference on smart systems and inventive technology (ICSSIT) IEEE. pp 228–233
4. Prasetyadi, GC, Mutiara AB, Refianti R (2020) Blockchain-based electronic voting system with special ballot and block structures that complies with Indonesian principle of voting. Int J Adv Comput Sci Appl 11(1)
5. Adida B (2008 July) Helios: Web-based Open-Audit Voting. In USENIX security symposium 17:335–348
6. Chaum D, Essex A, Carback R, Clark J, Popoveniuc S, Sherman A, Vora P (2008) Scantegrity: End-to-end voter-verifiable optical-scan voting. IEEE Security & Privacy 6(3):40–46
7. Chaum D, Ryan PY, Schneider S (2005) A practical voter-verifiable election scheme. In Computer Security–ESORICS 2005: 10th European symposium on research in computer security, Milan, Italy, September 12-14, 2005. Springer, Heidelberg, Proceedings 10:118–139
8. Khader D, Smyth B, Ryan P, Hao F (2012) A fair and robust voting system by broadcast. Lecture Notes in Informatics, pp 285–299
9. Bell S, Benaloh J, Byrne MD, De Beauvoir D, Eakin B, Kortum P, Winn M (2013) {STAR-Vote}: A secure, transparent, auditable, and reliable voting system. In 2013 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 13)
10. Mehboob K, Arshad J, Khan MM (2018) Secure digital voting system based on Blockchain technology. Int J Electronic Government Res 14(1):53–62
11. Mohammedali N, Al-Sherbaz A (2019) Election system based on Blockchain technology. Int J Computer Sci Information Technol (IJCSIT) 11(5):13–31

12. Pandey A, Bhasi M, Chandrasekaran K (2019 October) VoteChain: A blockchain based e-voting system. In 2019 Global Conference for Advancement in Technology (GCAT). IEEE. pp 1–4
13. Wei CCZ, Wen CC (2018) Blockchain-based electronic voting protocol. Int J Informatics Visualization 2:336–341
14. Yi H (2019) Securing e-voting based on blockchain in P2P network. EURASIP J Wirel Commun Netw 1:1–9
15. Dagher GG, Marella PB, Milojkovic M, Mohler J (2018) Broncovote: Secure voting system using ethereum's blockchain
16. Hardwick FS, Gioulis A, Akram RN, Markantonakis K (2018 July. E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) IEEE. pp 1561 –1567
17. Li K, Li H, Wang H, An H, Lu P, Yi P, Zhu F (2020) PoV: An efficient voting-based consensus algorithm for consortium blockchains. Front Blockchain 3:11
18. Jafar U, Aziz MJA, Shukur Z (2021) Blockchain for electronic voting system review and open research challenges. Sensors 21(17):5874
19. Ge L, Wang J, Zhang G (2022) Survey of consensus algorithms for proof of stake in blockchain. Security Comm Net 2022:1–13
20. Li W, Deng X, Liu J, Yu Z, Lou X (2023) Delegated proof of stake consensus mechanism based on community discovery and credit incentive. Entropy 25(9):1320
21. Pathak S, Gupta V, Malsa N, Ghosh A, Shaw RN (2022) Smart contract for academic certificate verification using ethereum. In advanced computing and intelligent technologies: Proceedings of ICACIT 2022, Springer Nature, Singapore, pp 369–384
22. Rawat SS, Alotaibi Y, Malsa N, Gupta V (2023) Enhancement of UAV data security and privacy via ethereum blockchain technology. Computers, Materials & Continua, 76(2)
23. Sahni U, Garg S, Srivastava T, Sharma T, Malsa N, Ghosh A, Gupta V (2022 October) Framework for land registry system using ethereum blockchain. In international conference on advanced communication and intelligent systems. Springer Nature, Switzerland, pp 431–440
24. Malsa N, Srivastave T, Sahni U, Garg S, Ghosh A, Shaw RN (2022 October) SMART CITIES: P2P energy trading using blockchain. In international conference on advanced communication and intelligent systems. Springer Nature, Switzerland, pp 682–694
25. Liao X, Yin J, Chen M, Qin Z (2020) Adaptive payload distribution in multiple images steganography based on image texture features. IEEE Trans Dependable Secure Comput 19(2):897–911
26. Liao X, Yu Y, Li B, Li Z, Qin Z (2019) A new payload partition strategy in color image steganography. IEEE Trans Circuits Syst Video Technol 30(3):685–696
27. Tan J, Liao X, Liu J, Cao Y, Jiang H (2021) Channel attention image steganography with generative adversarial networks. IEEE Trans Netw Sci Eng 9(2):888–903

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.