

Secured Electronic Voting Transactions Integrated with Blockchain

Shubhangi Priya, Garima Srivastava, Sachin Kumar
Amity University, Lucknow Campus, Lucknow

Abstract: Elections forms the basis of functional proceedings of democratic nations, it is the process that decides the ruling party and hence the office bearers for the defined period. Format for voting has evolved over the years, from ballots to Electronic Voting Machines (EVMs), particularly to minimize the errors involved that might occur with manual counting process and the time frame required for counting process. Despite advancements still the process is prone to tampering and intentional frauds. Possibilities of error in EVM may range from playing memory chip or replacing with a wrong ones and chances of multiple voting. Work is an attempt to address to the problems by storing the vote data in a secured network by employing blockchain framework, with its features as decentralized, enhanced Security, distributed ledgers, consensus, and faster settlement. Proposed EVM with blockchain enabled security is more efficient and reliable, the work proposes a technique to incorporate concepts of blockchain, to secure the votes stored in an EVM, the system has been implemented in remix ide. Integrated EVM proposed will be tamperproof, and any unauthorized access to change the votes casted, will be identified and can then easily be replaced with correct ones. The technique has also been subjected to unit testing and integration testing; the proposed technique has been found to be more secured. As election is a sensitive issue the proposed technique can be employed for testing at small scale applications and then the same can be employed full scale to ensure easy yet extremely secured platform for voting.

IndexTerms – EVM, blockchain, smart contract, consensus, ballot.

I. INTRODUCTION

Ever since the lockdown has started everyday life has been disturbed because of COVID-19 and the world has come at a halt. Under these circumstances, the government has to work to keep the normalcy among people. One such work is to conduct election in democracies across the world. In all democracy, electoral security is a matter of national security and the cybersecurity industry has working hard to find a solution for electoral voting system for the past decade, with the aim of reducing the cost of national elections, while achieving and expanding electoral security conditions. In the very beginning, the democratic elections were held using voting system that was based on pen and paper system. Changing this paper and pen system with the new electoral voting system was very important to limit fraud. Even with the electronic voting machines, the security is still in question, especially in terms of physical security issues. Anyone who has physical access to the machine may damage the machine, thus affecting all votes cast on. Also, with the current situation where people are not free to roam around and are afraid for their safety and health to come out and cast votes. A new more secure and portable system is required. This is where E-voting system using blockchain comes into action. It will not only make the voting system more secure but also distributed so that the voter can access it from any place at any time and can vote securely.

A blockchain is a distributed, consistent, irrefutable, public ledger. Four main components of blockchain that is turning point for E-voting system are:

- i. The ledger can exist in many different places: There is not a single point of failure in maintaining the distributed ledger.
- ii. A distributed consensus protocol to determine who can append the next new transaction to the ledger.
- iii. Any “new block” proposed to the log must refer to the previous version of the log, form a fixed chain where the blockchain gets its name, and thus prevent it from disrupting the integrity of the previous login.
- iv. Most network nodes must reach an agreement before a new input block becomes part of the permanent document.

These technical features work with advanced encryption, which provides a level of security equal to and / or greater than any previously known database. Blockchain technology is therefore taken by many, including us, as the right tool, which will be used to build a new modern democratic voting 2 system. This paper examines the use of the blockchain as an e-voting service. [1-4]

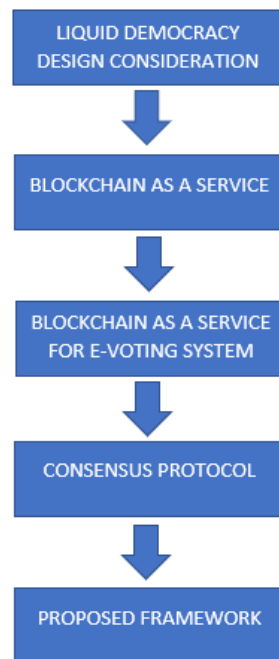
II. LIERATURE SURVEY

People have been working on modifications and improvements in voting systems [5-7] as a solution to the open issues and t challenges current voting system is having. Researcher have even integrated electronic voting systems and biometric authentication systems for ensuring security and accuracy [7]. With technological developments in wireless networks, it is now possible to encrypt the data like votes and then re-transmit them to the server for further processing. Presently data encryption algorithms like Rivest-Shamir-Adleman, Advanced Encryption Standard and Data Encryption Standard are being employed for the encryption technique. Keys employed for de-coding are usually stored in local servers, un-authorized software and viruses may access these keys and may sell them to criminals. Moreover, local server might not be so equipped to handle these issues. This opens the doors to cyber-attacks, DoS and code injection [2]. Leading loss of data integrity and security. These issues can be alleviated by employing decentralized networks. Security to the data stored in such systems, a technique that known as blockchain is utilized. Satoshi Nakamoto published a paper on blockchain [9], that had a public, permissionless framework is implemented for e-commerce. Proposed model, a permission model is used, where a set of already registered users are employed for voting. Blockchain assisted voting techniques have been proposed in number of articles [10, 11]. Ahmed Ben Ayed presented a work a blockchain architecture that used a separate blockchain implementation to each candidate contesting in election. Work employed common blockchain for all contestant and stored results with timestamp. [10] R. Hanifatunnisa et al presented a model to enhance the security performance

of asymmetric encryption using RSA on data before applying blockchain technique. [11] F. P. Hjálmarsson et al presented an E-Voting model based smart contracts. The model studies three blockchain techniques, Exonum, Quorum and Go-Ethereum, for evaluating suitability. Mobile App voting models with blockchain security were proposed in [12, 13]. D. Dwijesh Kumar et al presented a PIN based authentication scheme for voter identification and result verification after the voting process is over. [12] Sagar Shah et al presented a technique with authentication Server, a centralized system for verifying voters and a arbitration Server, decentralized system to securely store votes. Number of works have been presented for securing Voting mechanism, present work is an effort to improve the security feature further.[13]

III. PROPOSED METHODOLOGY

The work proposed presents a secured blockchain assisted Electronic voting machine, the architecture comprises of different elements of blockchain integrated with functional blocks of Electronic voting machine to ensure fair voting procedure and to check any tampering from unauthorized intrusion, figure 1 depicts the generalized flow of the methodology adopted.



1. Methodology Flow

The functional blocks of methodology may be summarized as:

3.1 LIQUID DEMOCRACY DESIGN CONSIDERATION

The main idea in a liquid democracy [6] is that the voter has the power, at any given moment, to review the way his vote was cast in terms of a specific legislative proposal or a bill. This permits individuals with area explicit information to more readily impact the result of choices, which should prompt to a large better administration and governance. The idea of liquid democracy could be a potential response to the public requests, however there are specialized and social hindrances in the manner. The answer for the specialized concerns related with the liquid democracy idea could be imperative for the advancement of democracy as we know it.

3.2 BLOCKCHAIN AS A SERVICE

Back in 2008, an individual or group of people under the name Satoshi Nakamoto published a white bitcoin paper called "Bitcoin: A Peer-to-Peer Financial System". It was the first time the technology named Blockchain was defined. Since its first release, Bitcoin has caught the public. Satoshi's white paper described a peer-to-peer network that solves the problem of double-digit digital spending without the need for intermediaries or a central authority. The transaction is confirmed by a group of nodes called miners, who continue to rush to solve a complex mathematical problem created by the system. The chain is replicated, cryptographically signed and publicly verifiable at every transaction so that no-one can tamper with the data that has been written onto the blockchain [1]. Work designed to solve a problem requires a lot of computer power, which is why it is proof of work in the authenticity of the transaction. The first miner to win the race gets the privilege of adding a new block to a public ledger called Blockchain and earning a bitcoin reward for the work being done. As long as the majority of the nodes are trusted, the attacker cannot irritate any record because it needs to control more than 50% of the total computer power.

3.2.1 Ethereum and smart contracts

Ethereum is a Blockchain platform that allows for the creation of official applications. Ethereum supports smart contracts that add a layer of business logic, encoding smart contract code first as encoding language like Solidity and then merging into a bytecode that can be used on a Blockchain network. Ethereum has two types of accounts: (1) an external managed account (EOA) operated by a user represented by a 20-byte (160-bit) address, and (2) a smart contractual account account managed by its code and is represented by a 20-byte address. Both types of accounts can store Ethereum cryptocurrency 'ether', and transactions have cost (gas) Ethers, which is money to encourage miners to enter transactions or coding in Blockchain. Gas is therefore a metric for

measuring the cost of a code within a network, the performance of each assembly (opcode) has a limited amount of gas based on its performance time.

3.2.2 Tokens

Cryptographic tokens are units of significant worth gave by an association dependent on Blockchain, they go about as options of digital currencies for errands that the later can't be utilized for. Ethereum empowers making tokens utilizing keen agreement. In our blockchain-casting a ballot framework, the democratic symbolic will permit citizens to partake in the organization, it will be given by the democratic authoritative board who are the main ones who can produce, move and destroy these tokens, our democratic token must be consumed when the elector cast their vote, the symbolic will give the holder the help to the activity of casting a ballot, it additionally limits elector in token deal or move between accounts.

3.2.3 Zero-Knowledge Proof

They make it possible to show that a statement is true about some secret data, without actually having to reveal any other information about the secret beyond that statement using cryptographic primitives. To just clarify it, we give the case of the riddle game Where's Wally? is a British series of children's puzzle books created by English illustrator Martin Handford. Children are tested to discover the Wally character. We can demonstrate that Wally is in the picture without really indicating his area by covering the picture with a paper with a little opening that lone shows Wally and no data about his area.

A ZKP needs to fulfil three standards:

- Completeness: the verifier must be completely persuaded with the assertion gave by the prover.
- Soundness: the likelihood of a verifier to accept a cheating prover must be exceptionally least.
- Zero information: the verifier adapts nothing about the assertion, aside from the way that it is valid.

3.3 BLOCKCHAIN AS A SERVICE FOR E-VOTING SYSTEM

In order to satisfy the privacy and security requirements for e-voting, and to ensure that the election system should not enable coerced voting, voters will have to vote in a supervised environment. In our work, we setup a Go-Ethereum permissioned Proof-of-Authority (POA) blockchain to achieve these goals. POA uses an algorithm that delivers comparatively fast transactions through a consensus mechanism based on identity as a stake.

3.3.1 Ballot Smart Contract

Characterizing a shrewd agreement incorporates recognizing the jobs that are engaged with the understanding (the political decision arrangement for our situation) and the various segments and exchanges in the arrangement cycle. We start by clarifying the political decision jobs followed by the political race measure. [14-17]

BALLOT	
1.	Struct Voter
2.	Struct Proposal
3.	Proposal [] proposals
4.	Mapping (address => Voter) public voters
5.	Address chairperson
Modifier onlyOwner	
1.	Ballot ()
2.	Register ()
3.	Vote ()
4.	winningProposal ()
5.	getCount ()

Figure 2 Architecture of Ballot Smart Contract

1. Election Roles: Election in our proposition empower investment of people or foundations in the accompanying jobs. Where various establishments and people can be selected to a similar job.
 - i. Election Chairperson: Manage the lifecycle of a political race. Various believed foundations and organizations are selected with this job. The political admin determines the political decision type and make previously mentioned political race, configurate polling forms, register citizens, choose the lifetime of the political decision and relegate permissioned hubs.
 - ii. Voters: For decisions to which they are qualified for, electors can validate themselves, load political race polling forms, made their choice and confirm their vote after a political decision is finished. Electors can be remunerated for casting a ballot with tokens when they cast their vote in a political race soon, which could be incorporated with a brilliant city venture.

2. Election Process: In our work, every political decision measure is spoken to by a bunch of keen agreements, which are launched on the blockchain by the political decision managers. A brilliant agreement is characterized for every one of the democratic regions of the political race so numerous keen agreements are associated with a political race.
 - i. Election creation: Election chairperson create election proposal using ballot smart contract in which the chairperson defines a list of candidates for each voting district. Then the smart contract that has been created is written into ethereum blockchain where district nodes gain access to interact with their corresponding smart contract.

- ii. Register voter: The registration of citizen stage is directed by the political race directors or chairperson. At the point when a political race is made the political decision directors must characterize a deterministic rundown of qualified citizens. This requires a segment for an administration character confirmation administration to safely validate and approve qualified people. Utilizing such confirmation benefits, every one of the qualified electors ought to have an electronic ID and PIN number and data on what casting a ballot area the citizen is situated in. For each qualified elector, a comparing wallet would be produced for the citizen.
- iii. Vote exchange: When a voter is registered, after that the voter can vote in the election using their validated wallet. According to the chairperson the voter has granted one vote each with equal value. After logging in their district nodes, the voter can vote for any of the candidate and only one vote is allowed to each voter. If a voter will try and cast another vote their vote will get rejected.
- iv. Verifying vote: As was referenced prior, every individual citizen gets the exchange ID of his vote. Every individual elector can go to his administration official and present their exchange ID subsequent to validating himself utilizing his electronic ID and its relating PIN. The public authority official, using region hub admittance to the blockchain, utilizes the blockchain adventurer to find the exchange with the relating exchange ID on the blockchain. The citizen can hence observe his decision on the blockchain, checking that it was tallied and checked accurately.
- v. Tallying results: After a block is created, and depending on the candidate selected, the information is recorded in the corresponding blockchain. Each block gets linked to the previously cast vote. At the point when an election is finished, the eventual outcome for each kept agreement is distributed.

3. Consensus Protocol: Consensus convention is the main one in the blockchain innovation. The Blockchain consensus convention is the thing that which keeps the squares on all the hub to synchronize with one another. The term 'Consensus' implies that the hubs need to concur with a similar condition of the blockchain. For this Smart Contract Proof of Authority Consensus has been used.

Proof of Authority: Proof of Authority (PoA) is a standing based consensus calculation that presents a reasonable and productive answer for blockchain networks (particularly the private ones). The term was proposed in 2017 by Ethereum fellow benefactor and previous CTO Gavin Wood. The PoA consensus calculation use the estimation of characters, which implies that block validators are not marking coins yet their own standing all things considered. Hence, PoA blockchains are gotten by the approving hubs that are subjectively chosen as reliable elements. The Proof of Authority model depends on a predetermined number of square validators and this is the thing that makes it a profoundly versatile framework. Squares and exchanges are confirmed by pre-endorsed members, who go about as arbitrators of the framework. [17-20]

IV. PROPOSED FRAMEWORK

For a democratic framework to be viable, it needs to procure the accompanying models, below are the functional blocks involved in implementing secured voting mechanism integrated with blockchain:

- 1. Integrity: just qualified citizens can participate, and casts a ballot can't be adjusted or erased structure the framework.
- 2. Accessibility and accessibility: citizens can distantly get to the framework to partake in any case their actual area whenever during the whole discretionary period.
- 3. Privacy: the citizen decision ought to consistently stay mysterious during the political race and post-political decision period.
- 4. Transparency: the whole framework ought to be auditable by people in general, and citizens can check if their votes were casted and counted.
- 5. The implementation both admin and citizen applications were done through a truffle-suite to interface with Ethereum test-organization and remix for implementation of the smart contract.

```

ubuntu@ubuntu-vbox: ~/Minor/Ballot2
ubuntu@ubuntu-vbox:~/Minor/Ballot2$ truffle compile
ubuntu@ubuntu-vbox:~/Minor/Ballot2$ truffle migrate --reset
Using network 'development'.

Running migration: 1_initial_migration.js
Deploying Migrations...
... 0x16c0a37f652e72a356c4f13956d6717b4fbedfe7c87a13eb9f09655
Migrations: 0x8cdaf0cd259887258bc13a92c0a6da92698644c0
Saving artifacts...
Running migration: 2_deploy_contracts.js
Replacing Ballot...
... 0x8e97c91fd0909891085013b6765f966e054d575e73272c3cfa37c
Ballot: 0xf12b5dd4ead5f743c0baa640b0216200e89b60da
Saving artifacts...
ubuntu@ubuntu-vbox:~/Minor/Ballot2$ npm run dev

> Ballot@1.0.0 dev /home/ubuntu/Minor/Ballot2
> lite-server

** browser-sync config **
{ injectChanges: false,
  files: [ '/*/**/*.{html,htm,css,js}' ],
  watchOptions: { ignored: 'node_modules' },
  server:

ubuntu@ubuntu-vbox:~/Minor/Ballot2$ truffle develop
Truffle Develop started at http://localhost:9545/

Accounts:
(0) 0x627306090ab3a6e1400e9345bc60c78a8bef57
(1) 0xf17f52151bef6c7334fad080c5704d77216b732
(2) 0xc5fd4076b8f3a5357c5e395ab970b5b54098fef
(3) 0x821aea9a577a9b44299b9c15c88cf3087f3b5544
(4) 0x0d14e623d10f9fba5db95830f7d3839406c6af2
(5) 0x2932b7a2355d6fecc4b5c0b6bd44cc31df247a2e
(6) 0x2191ef87e392377ec08e7c08eb105ef5448eced5
(7) 0x0f4f2ac350a1b4e2280d04c21cea7ebd822934b5
(8) 0x6330a533fc93768f612722bb8c2ec78ac90b3bbc
(9) 0x5aeda56215b167893e80b4fe045ba0d5bab767de

Private Keys:
(0) c8750921c067bbde70beb793e6fa76530b6382a4c0241e54a9ec0a0f44dc0d3
(1) a6eae8cfcbbf04590405997ee2d52d2b330726137b875053c36d94e974d162f
(2) 0dbbe84ae425a6d2687f1a7e3ba17bc98c673636790f1b8ad91193c05875ef1
(3) c88b703fb08c8ea89b46aeff5544f92e78a18e19814cd85da83b71f772aa6c
(4) 388c684f0ba1ef5017716adb5d21a053ea8e90277d0868337519f97bede61418
(5) 659cbb0e2411a44db6377897b1e22153c086a95eb6b18bdf89de078917abc63
(6) 82d052c865f5763aad42ad438569276c00d3d88a2d062d36b2bae914d58b8c8
(7) aa3680d5d48a8283413f7a108367c7299ca73f553735860a87b08f39395618b7
    
```

Figure 3 Deploying and developing smart contract in Truffle IDE.

To implement and check the result, we have deployed the smart contract in the remix IDE which is used to write, compile and debug Solidity code depicted in figure 3. Table 1 represents the addresses used during the run and their corresponding roles in the process.

Table 1. Addresses used during the run and their corresponding roles in the process.

Address	Role
0x5B38Da6a701c568545dCfcB03FcB875f56beddC4	Chairperson
0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2	Voter
0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db	Voter
0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB	Voter

Figure 4 depicts the process of creating ballot for secure transaction employing remix ide and figure 5 represents how a chairperson is defined for the election for voting using remix ide.

```
[vm] from: 0x5B3...eddC4 to: Ballot.(constructor) value: 0 wei data: 0x066...88029 logs: 0 hash: 0xf08...2ec36
status true Transaction mined and execution succeed
transaction hash 0xf075248f728c92f91808480815cc8480f2a5e5c9a775f2941f8a222a96
contract address 0x9145CC52D386f254917e481e844e9943f39138
from 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to Ballot.(constructor)
gas 3800000 gas
transaction cost 515968 gas
execution cost 351156 gas
hash 0xf075248f728c92f91808480815cc8480f2a5e5c9a775f2941f8a222a96
input 0x066...88029
decoded input {}
decoded output -
logs []
value 0 wei
```

Figure 4. Ballot Creation integrated with Blockchain via remix ide.

```
[call] from: 0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB to: Ballot.chairperson() data: 0x2e4...176cf
transaction hash 0x53442a5868027a45837333e9cf0e89f26491a69c8234ae7f9c1d9f159eb67a6c
from 0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB
to Ballot.chairperson() 0x9145CC52D386f254917e481e844e9943f39138
transaction cost 2325 gas (Cost only applies when called by a contract)
execution cost 1853 gas (Cost only applies when called by a contract)
hash 0x53442a5868027a45837333e9cf0e89f26491a69c8234ae7f9c1d9f159eb67a6c
input 0x2e4...176cf
decoded input {}
decoded output {"B": "address: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4"}
logs []
```

Figure 5. Ballot chairperson creation integrated with Blockchain via remix ide.

Figure 6 depicts the process of checking authentic voter wired with blockchain and figure 7 process of voting in secured environment employing remix ide for blockchain implementation.

```
[vm] from: 0x5B3...eddC4 to: Ballot.register(address) 0xd91...39138 value: 0 wei data: 0x442...cabab logs: 0 hash: 0x72b...f989d
status true Transaction mined and execution succeed
transaction hash 0x72b1236946294a7443274ef18c70f2f3c3332147987662752940f624af989d
from 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to Ballot.register(address) 0x9145CC52D386f254917e481e844e9943f39138
gas 3080000 gas
transaction cost 46565 gas
execution cost 23885 gas
hash 0x72b1236946294a7443274ef18c70f2f3c3332147987662752940f624af989d
input 0x442...cabab
decoded input {"address toVote": "0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB"}
decoded output {}
logs []
value 0 wei
```

Figure 6. Authentic voter verification wired with blockchain.

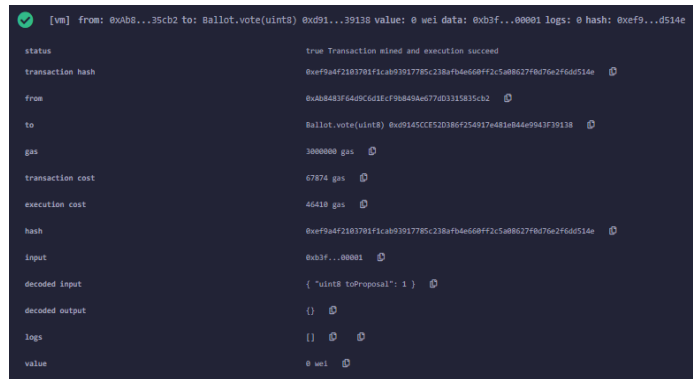


Figure 7. Voting process in Blockchain secured environment.

Remix IDE platform has been employed for implementation of secured voting environment integrated with blockchain, as a first step ballot was created followed by defining chairperson, then voter verification and finally voting process as depicted in figure 7. The outcome of the voting procedure and winning proposal is depicted in figure 8.

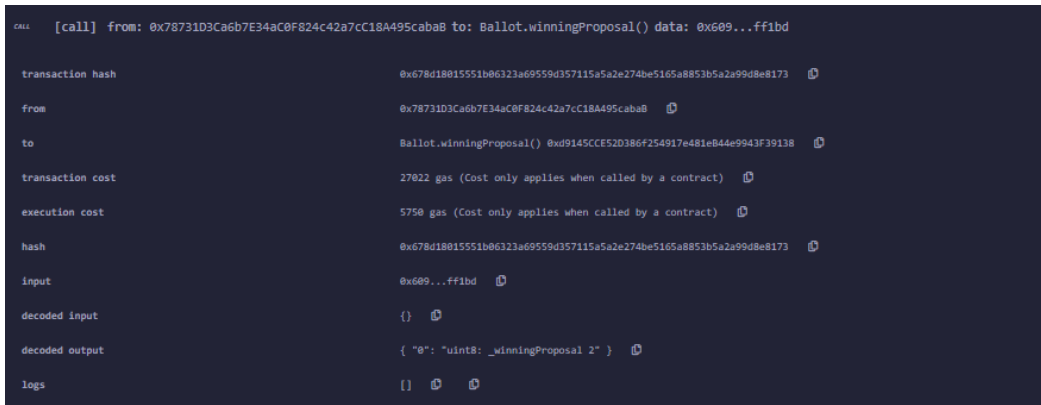


Figure 8. Outcome of voting and the winning proposal.

The last step would require the analysis of the performance for secure implementation of the smart contract, the process was evaluated via testing, that was conducted for every integrated module against the requirements of the Electronic voting machine as set by the conducting organization. Both unit testing and integration testing were performed. First and foremost, all modules were independently checked based on unit test as provided in the previous phase. Then, the complete contract was checked utilizing integration testing. Application was inspected for every requirement put forth conducting organization. Testing phase and results obtained were set in accordance. Figure 9 depicts the testing procedure for the model.



Figure 9: Testing process for the model

V. CONCLUSION

India is supposedly world's biggest democracy, basis of any democracy is voting and to ensure a fair election process, security and reliability must be guaranteed at every stage of the process. At first, elections in India were conducted using paper ballots, these ballots were manually counted leading to time consuming, further it lacked reliability and security, procedure for voting has evolved over the years, from ballots to Electronic Voting Machines (EVMs), particularly to minimize the errors. Despite advancements still the process is prone to tampering and intentional frauds. Possibilities of error in EVM may range from playing memory chip or replacing with a wrong ones and chances of multiple voting. Work is an attempt to address to the problems by storing the vote data in a secured network by employing blockchain framework, with its features as decentralized, enhanced Security, distributed ledgers, consensus, and faster settlement. Proposed EVM with blockchain enabled security is more efficient and reliable, the work proposes a technique to incorporate concepts of blockchain, to secure the votes stored in an EVM, the system has been implemented in remix ide. Integrated EVM proposed will be tamperproof, and any unauthorized access to change the votes casted, will be identified and can then easily be replaced with correct ones. The technique has also been subjected to unit testing and integration testing; the proposed technique has been found to be more secured. As election is a sensitive issue the proposed technique can be employed for testing at small scale applications and then the same can be employed full scale to ensure easy yet extremely secured platform for voting

REFERENCES

- [1] Wolchok, et al. ,“Security Analysis of India’s Electronic Voting Machines”, Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS 2010, Chicago, Illinois, USA, October 4-8, 2010.
- [2] D. Ashok Kumar and T. UmmalSariba Begum. “A Novel design of Electronic Voting System Using Fingerprint”. International Journal of Innovative Technology & Creative Engineering 1. 2045-8711.
- [3] Mahdi H. Miraz and Maaruf Ali, “Applications of Blockchain Technology beyond Cryptocurrency”, Annals of Emerging Technologies in Computing (AETiC) Vol. 2, No. 1, 2018.
- [4] Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten, “Security Analysis of the Diebold AccuVote-TS Voting Machine”, EVT’07 Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology (2007), Boston, MA.
- [5] P. Vamsikrishna, S., D. Kumar, D. Bommesetty and A. Tyagi, "Raspberry Pi voting system, a reliable technology for transparency in democracy", 2016 IEEE International Conference on Advances in Electronics, Communication and Computer Technology (ICAECCT), Pune, 2016, pp. 443-449.
- [6] H. Agarwal and G. N. Pandey, "Online voting system for India based on AADHAAR ID", 2013 Eleventh International Conference on ICT and Knowledge Engineering, Bangkok, 2013, pp. 1-4.
- [7] Ankit Anand and PallaviDivya, “An efficient Online Voting System”, International Journal of Modern Engineering Research (IJMER), Vol.2, Issue.4, July-Aug. 2012 pp-2631-2634 ISSN: 2249-6645.
- [8] F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaq and G. Hjálmtýsson, "Blockchain-Based E-Voting System", 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, 2018, pp. 983-986.
- [9] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” (2008) [Online], Available: <https://bitcoin.org/en/bitcoin-paper>. [Accessed: September 23, 2019].
- [10] Ahmed Ben Ayed, “A Conceptual Secure Blockchain- Based Electronic Voting System”, International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3, May 2017.
- [11] R. Hanifatunnisa and B. Rahardjo, "Blockchain based e-voting recording system design," 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), Lombok, 2017, pp. 1-6.
- [12] D. Dwijesh Kumar, D. V. Chandini, B. Dinesh Reddy, Debnath Bhattacharyya and Tai-hoon Kim, “Secure Electronic Voting System using Blockchain Technology”, International Journal of Advanced Science and Technology Vol.118 (2018), pp.13-22.
- [13] Sagar Shah, Qaish Kanchwala and Huaqian Mi, “Block Chain Voting System”, Northeastern University, 2016.
- [14] Aung, Yu Nandar, and Thitinan Tantidham. ”Review of Ethereum: Smart home case study.” In 2017 2nd International Conference on Information Technology (INCIT), pp. 1-4. IEEE, 2017.
- [15] Haijun Pan, Edwin Hou, Senior Member, and Nirwan Ansari, Fellow, ”M-NOTE: A Multi-part Ballot based E-voting System with Clash Attack Protection”, IEEE ICC 2015 - Communication and Information Systems Security Symposium
- [16] Yirendra Kumar Yadav, Saumya Batham, Mradul Jain, Shivani Sharma, ”An Approach to Electronic Voting System using UIDAI”, 2014 International Conference on Electronics and Communication Systems (ICECS -2014), Feb. 13 -14, 2014, Coimbatore, INDIA
- [17] Kaushik, Akanksha, Archana Choudhary, Chinmay Ektare, Deepti Thomas, and Syed Akram. ”Blockchain Literature survey.” In Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2017 2nd IEEE International Conference on, pp. 2145-2148. IEEE, 2017.
- [18] Vincent Gramoli, Alex Ponomarev, Mark Staples, Ralph Holz, An Binh Tran, and Paul Rimba. ”On availability for blockchain based systems.” In Reliable Distributed Systems (SRDS), 2017 IEEE 36th Symposium on, pp. 64-73. IEEE, 2017.
- [19] Bozic, Nikola, Guy Pujolle, and Stefano Secci. ”A tutorial on blockchain and applications to secure network control-planes.” In Smart Cloud Networks & Systems (SCNS), pp. 1-8. IEEE, 2016.
- [20] Aste, Tomaso, Paolo Tasca, and Tiziana Di Matteo. ”Blockchain technologies: The foreseeable impact on society and industry.” computer 50, no. 9 (2017): 18-28.