International Journal of Applied and
Natural Sciences (IJANS)
ISSN (P): 2319–4014; ISSN (E): 2319–4022
Vol. 9, Issue 4, Jun–Jul 2020; 11–20
© IASET

International Academy of Science,
Engineering and Technology
Connecting Researchers; Nurturing Innovations

DESIGN OF A SECURE BLOCK CHAIN BASED PRIVACY PRESERVING ELECTRONIC VOTING SYSTEM

Indushree. M[1], Sushmitha. N[2] & Shashidhara. R[3]

[1,2]Research Scholar, Department of Information Science and Engineering, RV College of Engineering, Mysore Road, Bengaluru, India

[3]Research Scholar, School of Engineering and Applied Sciences, Bennett University, Greater Noida, Uttar Pradesh, India

ABSTRACT

Block chain is an emerging technology, which offering numerous opportunities to develop decentralized and distributed digital services by ensuring privacy and transparency. It has mainly concentrating on the legal and technical issues rather developing advanced digitized services. In this article, we make use of the smart contracts with Blockchain to design the secure electronic voting system. The aspect of privacy, authenticity, transparency and security is a threat and challenging in the traditional voting systems. In general, mostly elections is based on the centralized infrastructure consists of central entity that maintains over all the voting process. The major pitfalls in the existing E-voting infrastructure are with an entity that has full influence over the system, it is feasible to modify with databases of considerable opportunities. In addition, the paper based voting systems are assisted by Electronic Voting Machines (EVMs) have multiple vulnerabilities, which can be caused to election rigging, fraudulent intent of the third party entities and government. The decentralized public Blockchain technology might offers a scalable solution to current voting systems by providing trust based and fraud proof digital voting.

KEYWORDS: *Blockchain, Ethereum, Smart Contracts, E-Voting, Transparency.*

Article History

Received: 02 Jul 2020 | Revised: 04 Jul 2020 | Accepted: 16 Jul 2020

INTRODUCTION

Voting is the foundation of any successful democracy and must therefore be accessible and secure for all eligible citizens in the country. Several Electoral systems take on to permit citizens to cast their precious vote, which includes electronic methods, ballot based voting and Electronic Voting Machine (EVM). However, we argue that existing techniques for voting, based on electronic voting machines, provides mistrust kind of transparency to voters. The issue commonly known as voter confidence. The Voting Systems have to heighten privacy and secrecy to provide electoral services available to the voters but secured against security vulnerabilities like keeping the voter ballot from being modified with the impact of changing casted votes by the voter. Several voting machines depends on Tor to provide anonymity of voters. Nevertheless, this mechanism doesn't achieve voter privacy and integrity services. Because, most of the intelligence authorities in the world is controlled by various parts of the Internet, which leads attackers to eavesdrop votes. As a result, as an alternative of move back to an inefficient and traditional

Mechanisms, the Modernization of state structure by the make use of emerging technology like Block chain [9].

Block chain is a digital public ledger that records online transactions. Block chain

Figure 1 shows Ensure security services like confidentiality, integrity, privacy by encrypting and validating the transactions. In the Block chain, when new block is added it will be connected to the last block using a cryptography hash produced from the in- formation of the previous block, which assure that the chain in the block chain is never broken and blocks are permanently stored. Further, it is highly impossible to modify previous transactions. Because, all the adjacent blocks must be modified first. This fundamental aspect of Block chain is what makes the technology tamper-proof and secure. The scenario of Block chain based E-Voting system is depicted in Figure 1.

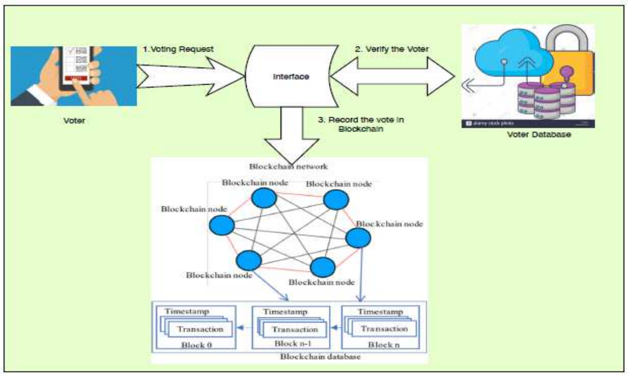


Figure 1: The Scenario of Block Chain Based E-Voting System.

MOTIVATIONS

Controversial E-Voting could have been avoided if the election and counting process is transparent, verifiable and secure. The existing voting system does offer voter privacy and even the vote counting by the officials is also not transparent. The voters are supposed to trust the result which is provided by the government body or Election Commission. There are also other electoral flaws like ballot stuffing, voter fraud and booth capturing. These issues makes difficult for election commission to differentiate between real votes and votes added without proper authentication and authorization. Some of the problems in current Electoral process are listed below:

- Designing a secure electronic voting system that offers the transparency, privacy and fairness has been a challenging.
- Current E-Voting protocols require a centralized authority to monitor and control the whole procedure from ballot to results.
- The centralized systems are vulnerable to security attacks like Distributed Denial-Of-Service (DDOS).
- Intelligence agencies have access to network and sufficient computing resources to analyze voting informative for the potential modification.

RESEARCH CONTRIBUTIONS

- Designing a secure and decentralized Blockchain based E-Voting system using smart contracts (Chain code).
- A user credential model will be proposed to ensure authentication, authorization and non-repudiation services.
- The voter can cast a vote using private key, after that transaction will be recorded in the decentralized Blockchain network.
- With help of voter Ethereum address, he/she can verify the casted vote in the later stages.

- Further, candidate count with details, Vote Count and winning proposal is implemented using smart contracts and deployed in Block chain network.

STRUCTURE OF THE ARTICLE

The rest of the article is structured as follows: Section 2, covers background, it includes challenges of the E-Voting and Blockchain. Section 3, defines the security requirements of E-Voting. Section 4, describes the proposed Blockchain based E-Voting protocol. Section 5, provides the implementation details with the experimental results and provides a performance analysis of the proposed work. Section 6, concludes the article.

BACKGROUND

Mistrust in the E-Voting process is a common circumstance even in the developed countries. To ensure the transparency and security that can be implemented in Blockchain based E-voting system. This could helps in solving most of the issues being faced in the voting process.

The concept of E-voting was initiated in 2001 at Estonia. They use digital smart cards for identification and authentication. for voters to attain the voting process by displaying contestants and start casting the votes through portal in the web as well as similar desktop application. In this regard, anyone having the smart device with Internet connection and ID card by the government can easily vote from anywhere [5].

The E-voting is based on centralized solution have a single point of failure, which leads to security attacks and vulnerabilities. In this context, Denial of Service, Man-In-The-Middle and insider attacks could crash the centralized databases and servers. The admins of the systems could act malicious and manipulate the information [2].

Brennan Center for Justice in 2015 identified the security vulnerabilities in America voting machines and published in the news. The study identified that, 43 out of 50 U S states used Electronic Voting Machines (EVM) that are old voting equipment's, exposed to crashes and failures. Further, the EVMs also easy to crack and modify with [8].

Zhao et al. presented an E-voting scheme, which proposes the reward and penalty based protocol for safe or unsafe conduct of voters. Notably, this is a first Blockchain based voting system [7]. Additionally, in 2016, Lee et al. introduced the voting scheme, which includes a trust third party using Blockchain to ensure choice of the voters. Although, the authors Bistarelli et al. presented an E-voting system, which partitions the voting process into two different parts called authentication and Distribution Server using token to safeguard privacy of the voters. Nevertheless, still there are some problems in this E-Voting scheme [1]. This system has been used in the countries like Ireland, Norway and Estonias [3]. Recently, there have been scenarios where it was faced several issues like transparency, fairness and not completely hygienic, which can be identified in countries like Brazil, Nigeria, India, Bangladesh and Pakistan [4, 6]. Notably, the issues causing the mistrust in the voting process are listed in Table 1.

SECURITY REQUIREMENTS FOR E-VOTING

The proposed Blockchain based E-voting protocol should satisfy the following security requirements:

- **Eligibility:** The authorized voters should be allowed to participate in voting process and cast their vote only once in the election. Further, the system must validate the voter identities.

- **Voter Privacy:** E-Voting protocol should not reveal the identities of the voter and not establish any links between identity information and ballots. Participants should remain anonymous and voting information is untraceable during and after the election.

- **Fairness:** No election results should be leaked before completion of the election process. This ensures that the voters might not be affect by others in the voting process.

- **Verifiability:** This security service assure that all entities in E-Voting should have the facility to verify whether the vote casted have been counted or not. Here, an individual verifiability gives a voter to verify that one's vote has been counted.

- **Forgiveness:** The ability of the voter to modify ones vote after it has been cast.

Table 1: Nature of Problems Causing Mistrust in the E-Voting Process

Issues	Description
Casting duplicate votes	If there is no proper authentication and authorization, it is possible to cast again for the ones who have not voted.
Pre-poll rigging	In few places the polling stations are made too far and voters have no interest or refuse to vote.
Use of power to influence	The use of power to influence the voters or polling staff either by threats or by incentives based.
Lack of interest by public	Voters are not fully trusted and convinced with current voting system. These issues can be dealt with trustworthy E-Voting platforms like Blockchain.
Unsupervised vote counting	For the parties who do not have a strong representation in a region, it is likely their votes can be miscounted.
Lack of audit and appeals	The process of hearing and deciding the appeals on some issues is slow that can be finalized before the next elections.

PROPOSED SYSTEM

The motive beyond the proposed mechanism is to have the Blockchain based system that satisfies the mentioned security requirements and goals. The proposed system has been designed to achieve the high degree of decentralization to create the system which the voter reign as the network of nodes.

The first transaction added to the blockchain will represent the genesis block. When a voter cast his/her vote, the transaction is updated in the Blockchain network. The proposed e-Voting protocol permit for the protest vote, where an user might be return the blank vote to the refusal of the election system or like NOTA to dissatisfaction with all candidates. The Blockchain is decentralized Peer-to-Peer network and cannot be immutable. Even there is no central point of failure. In order to ensure the security and trust, the current block will uses the previous block hash like the previous voters data. If any of the blocks are corrupted, modified then it will be effortless to trace out. Because, all blocks in the blockchain are linked to each other with previous hash and serves as chain. During voting in the Blockchain, the vote gets transmitted to the nodes on Blockchain network. After that the node adds vote to the decentralized network.

The Proposed Protocol Consists of the Following Phases:

- **Setup:** This is an initialization phase to obtain the private key and public key pair using asymmetric cryptosystem.

- **Voter Authentication:** The user should logs to the system using the credentials. The protocol will authenticate the voter based on his/her identity information issued by the Election Commission. The E-voting system should verify and validate all information entered by the voter. If the verification is successful, the voter will be authenticated and authorized to cast the vote.

The Prototype for Voter Authentication is described Below:

(ID, PW): Enter the login details and link the node identity to the e-governance.

(Credentials, node id, user-Info): The system of E-governance authenticates voter credentials.

- **Casting a vote:** Voters should choose the candidates from list of contestants to cast their vote. The voter can cast the vote through a friendly user interface. The prototype for this phase is shown below:

V=vote (ID of the voter, candidate selected)

Add (V, Chain), the Vote V is added to the Blockchain network.

Next, the updated Block chain data is reacted in all the nodes.

Vote (ID, user List, true): Finally, Voter field will be switched to vote.

- **Formation of the Block:** Upon casting the vote by the voter will be recorded as a unconfirmed transaction in the Blockchain. The nodes in the Blockchain network will validate the casted vote based on consensus protocols.
- **Sealing of Blocks:** The transactions are stored in the Blockchain, by the end of polling time all blocks in the network needs to be sealed by cryptographic hash (SHA-256) using nonce and merkle root. Once the electoral process is complete and the results have been published, then there is no significance for the Blockchain mining.
- **Counting of votes:** We have implemented a mechanism to count the casted votes in a fair manner. Further, the proposed system supports the voter to check the casted vote is successfully counted during counting process or not. With help of the Ethereum address, a user can verify the status of the casted vote.

The prototype for counting process is given below:

Candidates=get Candidates (candidate List).

Receive the candidate details from E-Governance.

Results=count (chain, candidates)

Here, vote counting process will be completed and winner will be identified based on the maximum number of votes.

IMPLEMENTATION AND EXPERIMENTAL EVALUATION

The proposed E-voting protocol is implemented using Ethereum platform called public Blockchain network. an Ethereum network provides a broader range of applications, with the power of smart contracts. Ethereum Blockchain consists of Ethereum nodes. The node is any device that is running the Ethereum protocol (blockchain). When we connect to the Ethereum protocol we are on the Ethereum Blockchain network. By running an Ethereum node we can connect to other nodes in the network, have direct access to the Blockchain, and even do things like mine blocks, send transactions, and deploy smart contracts. Many applications, that may normally require a web server, can be run through these smart contracts using Blockchain network. Hence, it is impossible to manipulate the transactions or smart contracts deployed in the Blockchain network.

After performing the transactions on Ethereum Blockchain network, the transaction fee is calculated in Gas, and paid for in Ether. The gas is the fuel of the Ethereum network, which is mainly used to conduct transactions, execute smart contracts and Launch Decentralized Applications (Dapps). The frequently used parameters in the Ethereum network are Gas, Gas price and Gas limit.

- **Ether (ETH):** is the Ethereum network's native crypto currency, the second largest by market cap on the crypto market.
- **Gas:** is the unit of calculation that indicates the fee for a particular action or transaction.
- **Gas Limit:** is the maximum amount of Gas that a user is willing to pay for performing this action or confirming a transaction (a minimum of 21,000).
- **Gas Price:** is the amount of Gwei that the user is willing to spend on each unit of Gas.

Additionally, we have set up a Meta Mask wallet in order to perform the transactions on Ethereum Block chain network. Meta Mask is just an Ethereum Browser and Ether wallet. It interacts with Ethereum Dapps and Smart Contracts without running a full Ethereum node. Furthermore, Meta Mask supports to connect different Ethereum based Blockchain networks and possible to import the accounts from other accounts through private keys.

We have defined the E-voting protocol through smart contracts, which consists of programming code and stored on a Blockchain network, then it execute when certain terms and conditions are met. It is called smart because of its ability to verify and execute a contract without any help from third parties. The contract exists in the decentralized Blockchain network and contains all the terms of a particular agreement. The smart contracts are meant to provide accuracy, transparency, autonomy, security and standardization.

Smart contracts defined in solidity programming language is executed by the Ethereum nodes in the blockchain network in every 10 seconds, and its validated by at least by two other nodes in the blockchain network. After that, functions of contracts can be triggered and executed.

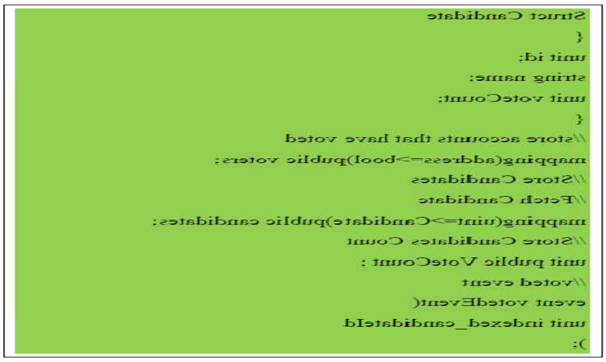
An E-Voting Smart Contract Implemented Using Solidity Code Given in Figure 2.

Figure 5 shows The Candidate is defined as a struct, the state variables are ID, Name and Vote Count. We used solidity mapping for storing and fetching the voter details. ID is the wallet address associated with the voter account in the Ethereum Block chain. The state variable Vote Count is used to count the number of votes received by the candidate. Figure 3 describes the code snippet of candidate details in the election contract. We have implemented the function “add candidate” to insert new candidate details into the election contract.

The vote () function, is demonstrated in Figure 4. This function will be executed by all the voters in the E-Voting. Voters will transfer identity of the associated proposal that they wanted to vote and their votes are recorded in the Blockchain network. Further, if a voters have a right to vote, and cast his/her vote, after that the voter is labeled as Voted already and the Vote-Count will be increased by one based on the voters weight. The E-voting contract is compiled using Remix IDE and deployed to the Ropsten Block chain test network using Ethereum Met Mask. The deployed smart contract address is “0x87F8a860e1F823D0a46f064D50eA5e75FB94e417”, which is shown in Figure 5. The contract deployment and smart interaction by the voter using E-voting smart contracts are depicted in Figure 6 and 7, respectively. The performance

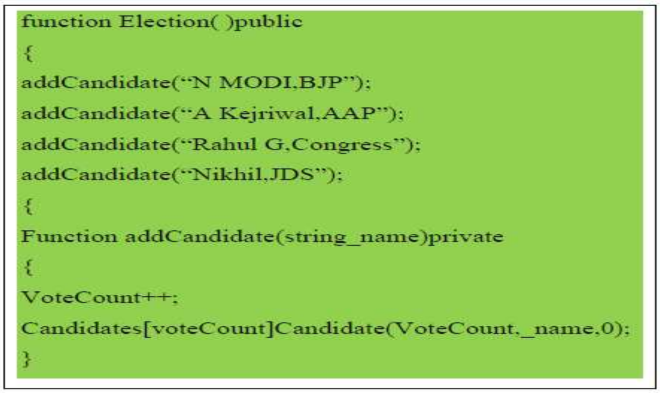
Figure 7 shows proposed protocol is evaluated by testing five ballots in the Ethereum Block chain network. We estimated the execution time required by the voter to cast their vote, which is presented in Table 2. Voter 1 creates the test-election smart contract using solidity, and have right to vote. Besides, other voters do not have the option called right to vote initially hence the system should offer them the voting permit. Initially, first voter node is faster than others nodes during electoral process. In the Block chain scenario, transactions will be running asynchronously, therefore voter does not require waiting for others to vote.

In this work, The E-Voting system scope is restricted for smaller elections and polls. The E-Voting with huge number of voters would require dynamic net- work structure and need to handle complex problems. The Block chain networks scalability is still unknown. In addition, the proposed smart contracts are implemented using solidity using Ethereum platform. The wallet is supported in windows, Linux and mac machines. Furthermore, a voter who willing to cast their vote should the Ethers in his/her wallet to complete the voting transaction.



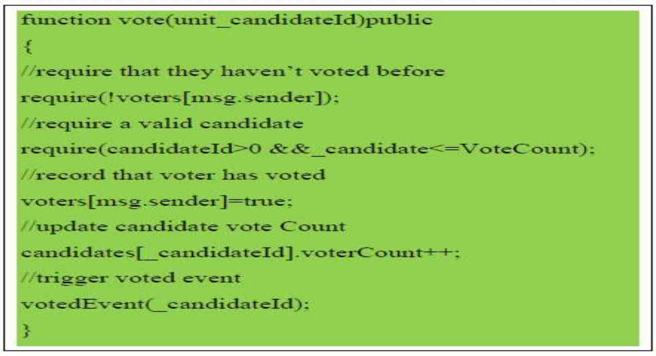
```
Struct Candidate
{
unit id;
string name;
unit voteCount;
{
//store accounts that have voted
mapping(address=>bool)public voters;
//Store Candidates
//Fetch Candidate
mapping(uint=>Candidate)public candidates;
//Store Candidates Count
unit public VoteCount ;
//voted event
event votedEvent(
unit indexed_candidateId
);
```

Figure 2: Solidity Code to Define the Structs and State Variables for E-Voting Contract.



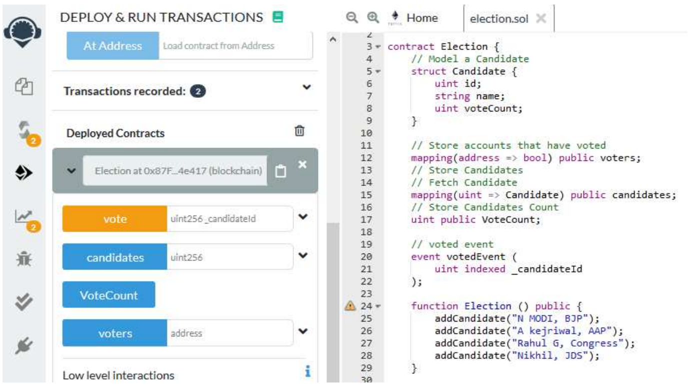
```
function Election( )public
{
addCandidate("N MODI,BJP");
addCandidate("A Kejriwal,AAP");
addCandidate("Rahul G,Congress");
addCandidate("Nikhil,JDS");
{
Function addCandidate(string_name)private
{
VoteCount++;
Candidates[voteCount]Candidate(VoteCount,_name,0);
}
```

Figure 3: Solidity Code to Add the Candidate for Election.



```
function vote(unit_candidateId)public
{
//require that they haven't voted before
require(!voters[msg.sender]);
//require a valid candidate
require(candidateId>0 &&_candidate<=VoteCount);
//record that voter has voted
voters[msg.sender]=true;
//update candidate vote Count
candidates[_candidateId].voterCount++;
//trigger voted event
votedEvent(_candidateId);
}
```

Figure 4: Solidity Code for E-Voting by the Voter.



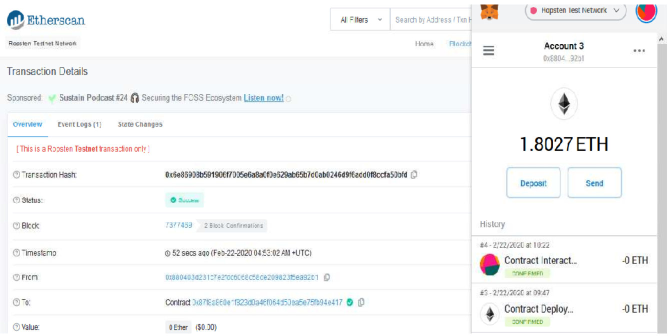
```
contract Election {
    // Model a Candidate
    struct Candidate {
        uint id;
        string name;
        uint voteCount;
    }

    // Store accounts that have voted
    mapping(address => bool) public voters;
    // Store Candidates
    // Fetch Candidate
    mapping(uint => Candidate) public candidates;
    // Store Candidates Count
    uint public VoteCount;

    // voted event
    event votedEvent (
        uint indexed _candidateId
    );

    function Election () public {
        addCandidate("N MODI, BJP");
        addCandidate("A kejriwal, AAP");
        addCandidate("Rahul G, Congress");
        addCandidate("Nikhil, JDS");
    }
```

Figure 5: Smart Contract Deployment Using Remix IDE.



Transaction Details

Sponsored: Sustain Podcast #24 Securing the FOSS Ecosystem Listen now!

[This is a Ropsten Testnet transaction only]

Transaction Hash: 0x6e85908b591906f7005e6a8a0f0e529ab65b7d0ab0246d9f6add0f8ccfa50bfd

Status: Success

Block: 7377459 2 Block Confirmations

Timestamp: 52 secs ago (Feb-22-2020 04:53:02 AM +UTC)

From: 0x880403d23157e2fdc6068c58de209823f5ea9261

To: Contract 0x87f8e8e0e1f323d0a46f064d50ea5e75fb94e417

Value: 0 Ether ($0.00)

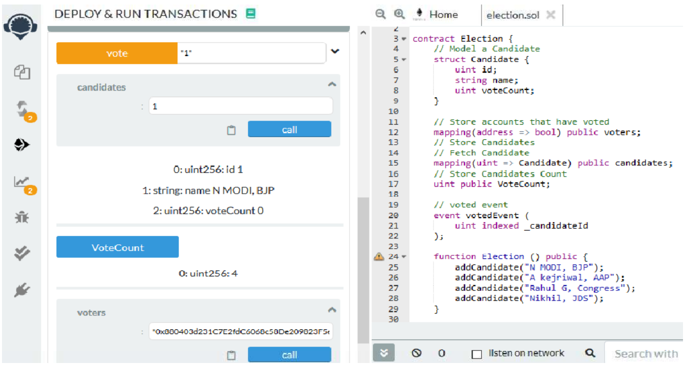
Account 3
0x8804...92b1

1.8027 ETH

#4 - 2/22/2020 at 10:22
Contract Interact... -0 ETH
CONFIRMED

#3 - 2/22/2020 at 09:47
Contract Deploy... -0 ETH
CONFIRMED

Figure 6: Contract Interaction with the Block Chain Network.



vote: "1"

candidates: 1

0: uint256: id 1

1: string: name N MODI, BJP

2: uint256: voteCount 0

VoteCount

0: uint256: 4

voters: "0x880403d231C7E2fdC6068c58De209823F5

```
contract Election {
    // Model a Candidate
    struct Candidate {
        uint id;
        string name;
        uint voteCount;
    }

    // Store accounts that have voted
    mapping(address => bool) public voters;
    // Store Candidates
    // Fetch Candidate
    mapping(uint => Candidate) public candidates;
    // Store Candidates Count
    uint public VoteCount;

    // voted event
    event votedEvent (
        uint indexed _candidateId
    );

    function Election () public {
        addCandidate("N MODI, BJP");
        addCandidate("A kejriwal, AAP");
        addCandidate("Rahul G, Congress");
        addCandidate("Nikhil, JDS");
    }
```

Figure 7: Smart Contract Call and Execution during E-Voting.

Table 2: Time Required for Smart Contract Creation and Interaction During E-Voting

	Chain Code Creation	1st Voter	2nd Voter	3rd Voter
Voting-process-1	35s	28s	37s	49s
Voting-process-2	32s	30s	40s	39s
Voting-process-3	35s	39s	42s	46s
Voting-process-4	40s	31s	36s	43s
Voting-process-5	49s	29s	28s	38s

CONCLUSIONS

In this article, a Blockchain based decentralized and peer-to-peer electronic voting protocol is proposed. The legitimate voters could have the power to vote through Internet by using smart devices like Mobiles, PCs, etc. The transaction will be recorded in the Blockchain network, which is verifiable, anonymous and adversaries are unable to modify the records in the network. The solidity smart contract is used to accomplish recording, managing, validating the voters during the electoral process. In order to provide the privacy and transparency of E-Voting protocol, secure cryptographic functions have been employed to ensure that the registration and voting is anonymous. The digital signatures using public key infrastructure makes the voting process more secure and reliable.

Further, the proposed protocol does not require mining like Bit coin network since the voters information is registered and authentic. Notably, the proposed approach addresses some of the security pitfalls that conventional E-voting protocols have. As a result of the proposed work, the concept of Blockchain technology, security algorithms and cryptographic primitives like hash functions, nonce and digital signatures, has become adaptable to elections and polls to secure the E-Voting environment.

REFERENCES

1. *Akbari, E., Wu, Q., Zhao, W., Arabnia, H.R., Yang, M.Q.: From blockchain to internet based voting. In: 2017 International Conference on Computational Science and Computational Intelligence (CSCI). pp. 218{221. IEEE (2017)*

2. *Ayed, A.B.: A conceptual secure blockchain-based electronic voting system. International Journal of Network Security & Its Applications 9(3), 01-09 (2017).*

3. *Batubara, F.R., Ubacht, J., Janssen, M.: Challenges of blockchain technology adoption for e-government: a systematic literature review. In: Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age. pp. 1-9 (2018).*

4. *Casino, F., Dasaklis, T.K., Patsakis, C.: A systematic literature review of blockchain-based applications: current status, classi_cation and open issues. Telematics and Informatics 36, 55-81 (2019).*

5. *Hanifatunnisa, R., Rahardjo, B.: Blockchain based e-voting recording system de- sign. In: 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA). pp. 1-6. IEEE (2017).*

6. *Hsiao, J.H., Tso, R., Chen, C.M., Wu, M.E.: Decentralized e-voting systems based on the blockchain technology. In: Advances in Computer Science and Ubiquitous Computing, pp. 305-309. Springer (2017).*

7. *JOHNSON, D.: Blockchain-based voting in the us and eu constitutional orders: A digital technology to secure democratic values? European Journal of Risk Regulation 10(2), 330-358 (2019).*

8. *Li, J., Wang, X., Huang, Z., Wang, L., Xiang, Y.: Multi-level multi-secret sharing scheme for decentralized e-voting in cloud computing. Journal of Parallel and Distributed Computing 130, 91-97 (2019).*

9. *Moura, T., Gomes, A.: Blockchain voting and its effects on election transparency and voter confidence. In: Proceedings of the 18th annual international conference on digital government research. pp. 574-575 (2017).*

10. *Shahzad, B., Crowcroft, J.: Trustworthy electronic voting using adjusted blockchain technology. IEEE Access 7, 24477-24488 (2019).*

11. *Yavuz, E., Koc, A.K., Cabuk, U.C., Dalkilic, G.: Towards secure e-voting using ethereum blockchain. In: 2018 6th International Symposium on Digital Forensic and Security (ISDFS). pp. 17. IEEE (2018).*