International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-2, December 2019

E-Voting: Blockchain Based Voting For Secure Vote Casting

Vishal Baraiya, Seema B Joshi

Abstract: ***A blockchain is decentralized immutable ledger technology maintaining integrity. So to conduct tamperproof election it's one of the approach towards it. Smart contracts are Self executed code that is written on Ethereum platform in blockchain. An E-voting system should be completely secure and does not allow voting twice that is double spending in blockchain. So it should be completely transparent. In research work electronic voting application is implemented and tested using smart contract on Ethereum platform with the help of metamask wallet. The results of ballots and votes will be stored on Ethereum blockchain with the help of consensus algorithm proof of stake. This consensus is used in validating a transaction with concept of majority approval. Current electronic voting system requires a centralized authority to control the procedure from ballot input to result output and for monitoring of election. While blockchain technology provide decentralized system which is open across connected nodes. Blockchain assets provide increased level of system security from hacking and fraud. Every transaction in blockchain is time-stamped and signed digitally with the help of cryptographic algorithms, and it assigns unique hash value to every block so it can be trace easily. Blockchain technology is one of solutions because it embraces a decentralized system and the entire databases are owned by many users. The blockchain technology also has much vulnerability due to which many attacks like 51% attack, Double Spending attack, DDOS attack, Sybil attack, Eclipse attack and Routing attack can be performed on it.***

Keywords –blockchain, ethereum, smart-contracts-voting, metamask, distributed ledger, wallet, etc.

I. INTRODUCTION

In every democratic country election play most important role. So election must be transparent and secure. From the dawn the process of election is held on pen and paper. This traditional pen and paper method is replaced by blockchain technology to limit fraud and to have process traceable and verifiable. Electronic voting machine is under the supervision of security community. So anyone with physical access can sabotage. A blockchain is a distributed, immutable public ledger. It has 4 main features that consist of following:-

1) Because it has property of distributed ledger the record is stored at various locations so there is not a single point of failure.

2) There is a distributed control in adding a new block to ledger.

3) There is predefined structure of block, a new block is attached previous block creating immutable ledger and tamperproof.

4) As per the proof of authority algorithm in order to add block in blockchain a majority is needed which is to be done via consensus mechanism.

A. Blockchain

Blockchain is a distributed, public ledger and peer-to-peer (P2P) technology with its initial focus on crypto currencies like Bitcoin. For the first time in 2008, Satoshi Nakamoto introduced the concept of Blockchain as an emerging P2P technology for ledger computing and decentralized storage and sharing[1]. To avoid the threats of attacks which want to take control of whole system, this technology makes it unattainable due to its advance cryptographic techniques and working mechanism without centralized server. Blockchain is not only meant to be used in cryptocurrencies, but instead it is applied in several domains now-a-days due to its features like privacy, security, immutability, fault tolerance, authorization, integrity, etc. Some of the major domains are Monitor supply chains, digital IDs[2]. Data Sharing, Copyright and royalty protection, Digital Voting, Food Safety, immutable Data Backup, etc[3]. As shown in figure 1, the Blockchain structure is made up blocks that are interlinked to each other by previous hash so it is easy to trace. Block chain system compromises of user having a set of keys named public and private. As we know the mechanism, in asymmetric key cryptography, the private key is used for reading encrypted messages and public key is used for encrypting the plain text of message before sending. In case of blockchain, public key is used to provide authenticity for transaction. Initially user starts signing transaction with the help of private key and broadcast it to the peers. After validation, that particular transaction is spread across the other nodes of network by peers. Parties related with transaction mutually validate it to meet the consensus. On obtaining the consensus, special nodes called as miners, include this as valid transaction in hierarchy of blockchain. Report of block being included in sequence of blockchain is broadcasted back to network by miner. Broadcasted block has transaction and hash value matching it with previous block in blockchain. So, after validation new block is added to blockchain. Blockchain can be categorized in two types: Private Blockchain and Public Blockchain. Both types use decentralized approach and provide safety against malicious users of block chain network.

Revised Manuscript Received on December 30, 2019.

* Correspondence Author

Vishal Baraiya, Master of Engineering Student Department of Computer Engineering, Graduate School of Engineering and Technology, Gandhinagar, State – Gujarat, India.

Seema B Joshi, Assistant Professor, Department of Computer Engineering, Graduate School of Engineering and Technology, Gandhinagar, State – Gujarat, India.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

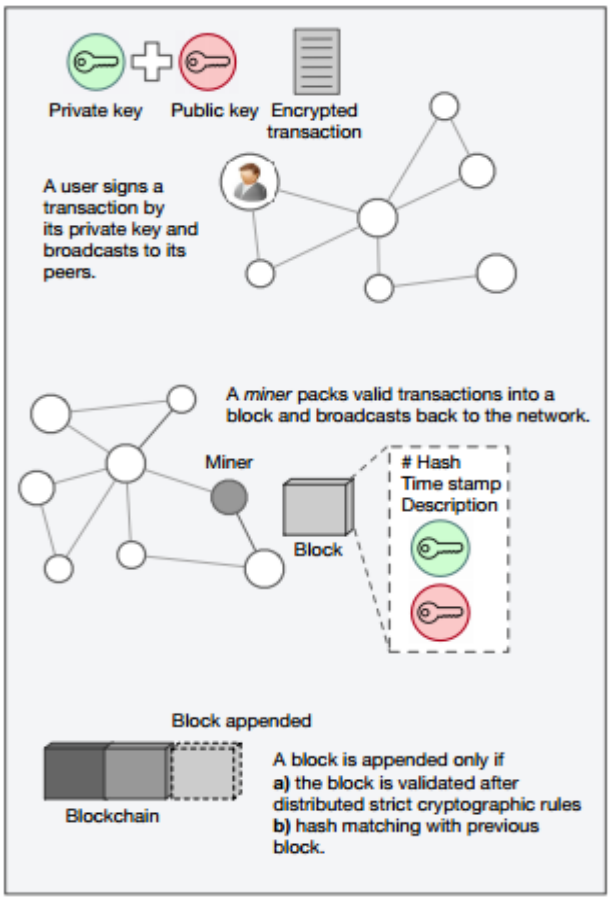

Figure 1: Working of Blockchain

The main differences between these two types are private blockchain requires permission to proceed as a user for doing transaction, while public blockchain is permission less, apart from that execution of general agreement, maintenance of distributed network and permission to join P2P network. In case of blockchain can be categorized based on two aspects: authorization and authentication. The central trustworthy authority takes care of authentication and authorization process for selecting miners in case of private blockchain. While in a public blockchain, no third party intrusion takes place for selecting the miners. The consensus protocols are main part of blockchain system. It is observed that vulnerability is around more than 50% for a new blockchain, which gets low as the blockchain grows in size and distribution[4].

B. Ethereum

Ethereum is an open source platform in blockchain which allows developer to make and test decentralized application. Ethereum was founded by vitalik buterin in late 2013. It's a next generation platform after the bitcoin. Unit of Ethereum is account. There are two types.

1) Contract account: A contract account has ether balance. It is programmed with logical code when executed it perform predefined operation.

When a contract account receives a transaction it will execute its code follow by input parameter which is sent as a part of transaction. The contract code gets executed in Ethereum Virtual Machine environment.

2) Externally Owned Account: An externally owned account (EOA) has ether in form of ether. It can send transactions this type of account is controlled by private keys and it does not contain any type of code. Some other terms related to Ethereum are as follow:

- **Transaction:** The term transaction is signed data package that stores the information which is to be send from externally owned accounts to another account in blockchain. Transaction has information of transaction with the timestamp.
- **Value Field:** The value field in transaction is the amount of token to transfer from sender to recipient.
- **Message:** A message is simple script that is written at the time of transaction.
- **Gas:** Gas is the price to be spent for the execution of smart contract.
- **Start Gas:** A start gas value represents the maximum numbers of computational steps that is allowed by transaction execution.
- **Gas Price:** A Gas Price is the amount of fee that client is willing to pay for Gas or it's also called transaction fees.
- **Ether:** Ether is crypto fuel in order to perform operation on Ethereum platform.
- **Metamask:** Metamask is Ethereum wallet which is used in web browser like Firefox, chrome and Brave browsers. It's also a browser extension. It works like a bridge between normal browsers and the ethereum blockchain.
- **Smart Contract:** Smart Contract is Self executing code that performs task automatically when executed and written in solidity language.

The remaining paper is organized as follow:

Section II discusses the existing challenges faced by E-voting systems.

Section III gives idea of proposed systems that will present the new way of online voting system using ethereum.

Section IV list down related of implementation and discusses it relevant aspects.

Section V result and discussion.

The final section VI concludes the discussion of the study.

II. MOTIVATION

Main agenda of this research is to have a secure voting environment with the help of blockchain technology. As blockchain technology is immutable so if someone tries to change the election result it won't allow because everything is in ledger. In order to organize complete election as online, we need to solve problems like transparency, authentication in the voting platform. We need to assure that people are real and legitimate user.

Estonia is very first city who implemented blockchain based voting system for their citizens. The concept of e – voting was in debate since 2001 and implemented in 2003 by the national authority. They are using smart digital Id card & personal card readers for authentication[5].

Switzerland is another amongst few countries that is involved in electronic voting. Switzerland is known widespread for its democracy. They have also started an official work on a voting system called remote voting[6].one more example of e-voting process is implemented

in website https://electionrunner.com/, they have mobile applications well as a web platform too.

III. PROPOSED SYSTEM

In Proposed system our system will include 4 main requirements that are listed as follows:

A. Authentication: The candidate who is already registered is able to caste vote. The system will not support registration in between because registration requires some document to be verified

B. Anonymity: The E-voting system should not allow any link between voter's identities and ballot. The voters have to remain anonymous till the end of election.

C. Accuracy: Every vote should be counted it can't be changed or removed.

D. Verifiability: The system should verify that each vote has been counted correctly.

The blockchain: When a transaction occurred it creates numbers of block and it is stored there like linked list structure and chains of block that is why it is called blockchain. Data added to blockchain cannot be deleted so it's immutable ledger.

The first transaction to blockchain is called genesis block and that will represent candidate information. Every time candidate votes get recorded and the Blockchain will be update it. It uses proof of stake algorithm for consensus.

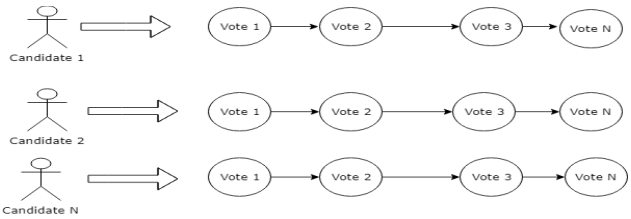

Figure 2: Voting Chain

In order to identify the security of system, each block will have previous voter's information in the form of hash value. If blocks get compromised, then it would be easily detected from missing hash. The system is decentralized and cannot be corrupted; and there is no single point of failure.

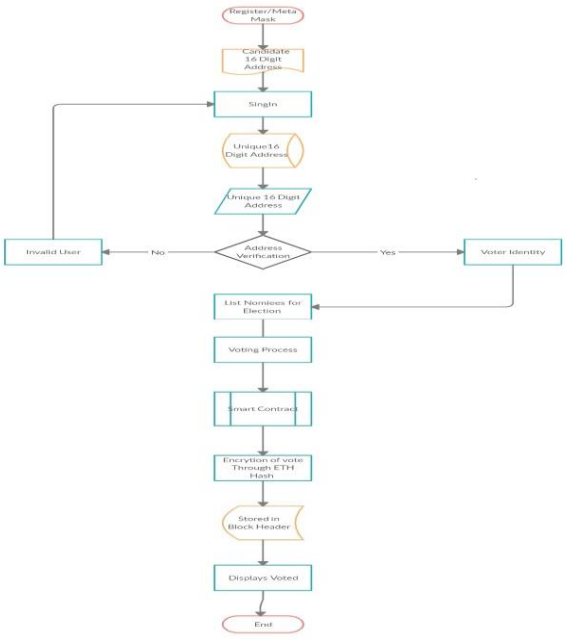

Figure 3 : Proposed System

Proposed Methodology:

1) First of all user will registered itself in order to get valid 16 digit wallet address.
2) Sign in with its unique wallet address.
3) After successfully signed in voter will be able to see his/her wallet address, private key and ether balance on main net network.
4) Voter will see a list of nominee.
5) Voter can vote a nominee of his/her choice through smart contract of blockchain.
6) As far Ethereum is platform it will be encrypted with eth-hash algorithm.
7) Its entry will create a new hash and that will stored in block and data is recorded in block and its immutable. At the end block will added to blockchain

IV. IMPLEMENTATION

Ethereum platform is used for development of blockchain network because it has a wide range of use cases within smart contracts which are written in solidity language while bitcoin was only meant to validate transaction. In the Ethereum network all operations are in real time environment. These are given as a price in form of ether to the miners, who execute this contract and validate the blocks.

This issue can be solved by blockchain which is decentralized and peer to peer. We define set of rules in a smart contract and contracts can start to execute. After the initialization of smart contract they cannot be removed nor modified from the blockchain and people can see the results of execution of smart contracts that is true or not. In Ethereum network there is no central authority to provide the proof of work. All peer nodes can perform calculations on their own. There are private Ethereum test networks available for the developers to test the code and allow them to test the code with fake ether for which we don't pay the actual money. One is kovan test network we have decided to use that in our work. For example, the kovan network forces it users to download all of the existing blocks in network. In order to use a test network, users should download a legitimate ethereum wallet from the ethereum website and change the connected network to the chosen test network, with the help of settings menu.

1) In Fig. 4 code shows the definitions of various variables. The "Voter" is defined as a struct in the Solidity language.

```
struct Voter {
    bool voted;
    uint voteIndex;
    uint weight;
}
address public owner;
string public name;
mapping (address=>Voter) public voters;
Candidate [] public candidates;
uint public auctionEnd;

event ElectionResult (string name, uint voteCount);
```

Figure 4 : Code That Defines Structure And Variable

The voter has properties like following:

- Voted: This keeps the track of candidate if already voted once or not.
- Vote Index: This keeps the record of the list of available party for election.
- Weight: This is special array this allowed to vote only if registered candidates have weight equal to 1 in their address.

2) Authorized function: In the code given in Fig. 5 shows the authorizes function. This function allows verified candidate and authorized them to the take a part in voting process.

```
function authorize(address voter) public  {
    require(msg.sender == owner);
    require(!voters[voter].voted);

    voters[voter].weight = 1;
}
```

Figure 5: Code That Defines Authorized Function

3) Winner function: In the code given in Fig. 6 shows the winner function that will decide the highest vote and declare that party as a winner.

```
function win() public  returns(string) {
   if(candidates[0].voteCount > candidates[1].voteCount) {
      return g0;
   }
```

Figure 6: Code That Declares Win Function

The person having ethereum wallet address, verified by the authorized function, has permission to vote within contract. Basically contracts are written in Solidity language that is a combination of C++ and JavaScript. Smart contracts are executed by the peer's network in every 15 seconds, and should be validated at least by 2 other users to be activated. After that, functions of contracts can be executed, and contracts can be shared with other candidates.

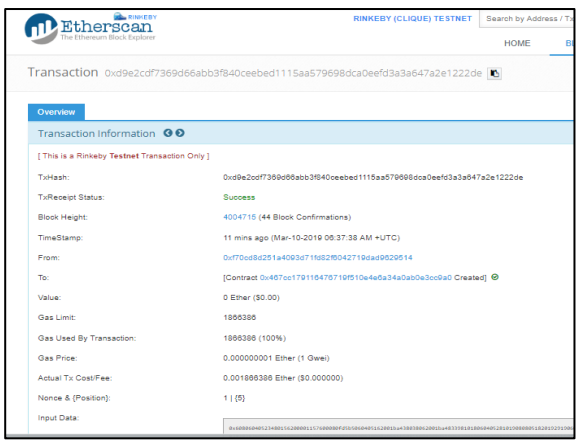

Figure 7: Trasnsaction History onEtherscan

In figure 7 transaction records is shown which is available to anyone by entering the transaction hash which is available worldwide on etherscan.io in ethereum blockchain.

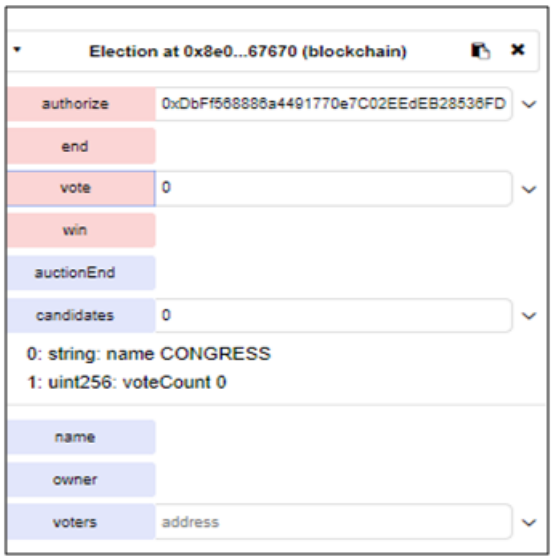

Figure 8: Deployed Contract

In figure 8 all the functions of deployed smart contract is shown. E.g. authorized function to authorized candidate for vote ,win function do declare winner, vote for casting a vote, election end, vote index etc.

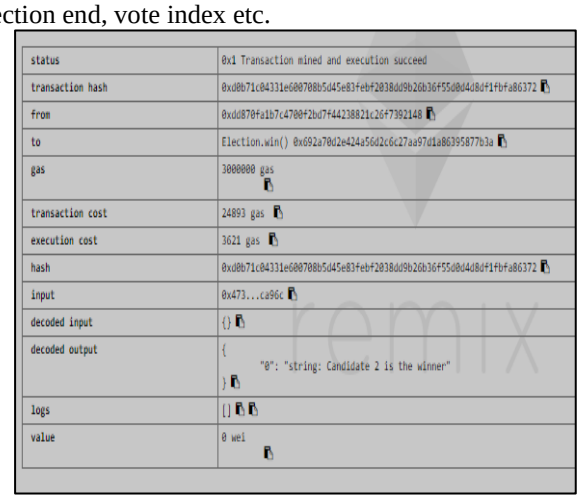

Figure 9: Proofof Stack

In figure 9 consensus algorithm proof of stack is shown which describe details like from sender wallet address to receiver, time, gas fees, nonce value, and hash.

V. RESULT AND DISCUSSION

Table 1 : Contract Creation and Voting Time in kovan

	Contract creation	Voter1 (transaction)	Voter2 (transaction)
Vote 1	17S	6.80S	6.80S
Vote 2	15S	6.50S	5.96S
Vote 3	12S	6.20S	5.50S

In above table 1 test net voters are present. We calculated time for each voter. Voter 1 is the candidates who created test net of the election and the one who grants the permission of other to be eligible for voting process. All the 3 transaction can run asynchronously.

Variation in experiment is due to creation of new block and we have deployed in kovan network. In above table comparison between two test networks is shown. In Rinkeby test network it takes more than 20 seconds to 1 min in creation of new block while in kovan it is 15-20 second only. Even though they both work with Proof of Authority. A table 2 shows the comparison between Rinkeby and Kovan test network. Contract creation time in voters respectively vote 1 17s, vote 2 15s, vote 3 12s in Kovan test network to that of Rinkeby are 38s, 32s, 42s.

Table 2 : Comparison Table Kovan Vs Rinkeby[5].

KOVAN VS RINKEBY	Contract Creation		Voter1 (transaction)		Voter2 (transaction)	
	PROPOSED USING KOVAN	EXISTING RINKEBY	PROPOSED USING KOVAN	EXISTING RINKEBY	PROPOSED USING KOVAN	EXISTING RINKEBY
Vote 1	17s	38s	33s	6.80s	47s	6.80s
Vote 2	15s	32s	32s	6.50s	45s	5.95s
Vote 3	12s	42s	39s	6.20s	56s	5.50s

Now moving towards transaction time in Kovan test network for voter1 are 33s, 32s, 39s to that of Rinkeby are 6.80s, 6.50s, 6.20s. Now moving towards transaction time in Kovan test network for voter2 are 47s, 45s, 56s to that of Rinkeby are 6.80s, 5.95s, 5.50s. In this research our scope is limited to small scale election may include universities elections, primary election, and special election. The scalability of Ethereum network is still not known perfectly and needs to research further so we cannot use this contract in our actual election. This contract runs in wallet of Ethereum blockchain so in any device that supports wallet we can use this system. A blockchain is fully transparent technology talking in context of voting any votes from wallet address A that goes to wallet address B is shown to anyone which has access to that blockchain and its uses eth-hash algorithm. In fact now Ethereum wallet metamask can be installed in mobile phone so if we want to organize election for small group of people it is possible.

VI. CONCLUSION

By implementing this proposed method of smart contract we are moving to secure layer with the help of blockchain technology and Ethereum as a platform. We also addressed a security issue that is integrity, security can be improved. As blockchain adds new layer to security by ensuring web 3.0 protocol that never save a information on server side
all the private key and password are at the user side. So it can't be manipulated. E-voting is still controversial within political and scientific circle. Blockchain based voting solution includes all security parameter like privacy of voters, integrity maintain, non-repudiation, and transparency.

REFERENCE

1 S. Nakamoto, "Bitcoin : A Peer-to-Peer Electronic Cash System," pp. 1–9.
2 D. W. B and G. Ateniese, "From Pretty Good to Great : Enhancing PGP Using Bitcoin and the Blockchain," vol. 1, pp. 368–375, 2015.
3 N. Kshetri, "Blockchain ' s roles in strengthening cybersecurity and protecting privacy," Telecomm. Policy, vol. 41, no. 10, pp. 1027–1038, 2017.
4 T. B. Attacks and C. Power, "1 Introduction 2 Preliminaries 3 The Block Discarding Attack," pp. 1–18.
5 A. K. Koç, "Towards Secure E-Voting Using Ethereum Blockchain," 2018.
6 I. Martinovic and L. Kello, "Blockchains for Governmental Services : Design Principles , Applications , and Case Studies," no. 7, 2017.

AUTHORS PROFILE

Mr. Vishal Baraiya is a Master of Engineering Student in department of Computer Engineering at Graduate School of Engineering and Technology, Gandhinagar, State – Gujarat, India. He has professional working experience in developing blockchain applications. His research interest includes data mining, Cyber Forensics, blockchain technology.

Ms. Seema B. Joshi is an Assistant Professor in department of Computer Engineering at Graduate School of Engineering and Technology, Gandhinagar, State – Gujarat, India. She is interested in cloud computing and security as well as blockchain technology she has worked in many Government projects.