Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

Implementation of Secure Voting System using Blockchain

Dipali Pawar, Pooja Sarode,
Shilpa Santpure, Poonam Thore
Department of Computer Engineering
JSPM's Imperial College of Engineering
and Research Pune, India

Prof. Pravin Nimbalkar
Department of Computer Engineering
JSPM's Imperial College of Engineering and Research
Pune, India

***Abstract*—It is very challenging to build a secure voting system that offers fairness and privacy of current voting schemes. In this implementation paper, we evaluate an application of blockchain as a service to implement distributed electronic voting systems. Our objective is to provide a decentralized architecture to run and support a voting scheme that is open, fair, and independently verifiable. Our proposed solution implements the protocol which achieves fundamental e-voting properties as well as offer a degree of decentralization and allow for the voter to change/update their vote and the experimental result shows that our proposed solution is beneficial for the existing and upcoming voting system.**

Keywords*— Blockchain; Cryptocurrency; SHA-3; E-Voting; Decentralized.

1. INTRODUCTION

A fair and Transparent election is need for today's society according to the today's social environment. The current ballot system does not offer transparency in counting of votes. There are several threats of voting frauds, like fake voters, frauds in the polling booths etc. So, this need for establishment of secure decentralized fraud less, voting system came into existence. Decentralized voting system using blockchain can overcome all the issues in traditional voting systems. Blockchain provides various properties due to its decentralized ledger technology. Blockchain is a decentralized computational and information sharing platform which enables multiple authority domain who do not trust on each other but they cooperate and collaborate in certain decision making process. Blockchain uses add and append only strategy. We cannot delete the existing data in blockchain. Blockchain uses peer to peer network systems. Blockchain is a chain of blocks and it include all the information of user through distributed ledger technology. The concept of block interconnection was evaluated from Merkle tree by Ralph Merkle. Every node is labeled with a cryptographic hash of a block data. Thereby a non-leaf node is labeled with a cryptographic hash of labels of child nodes.As all the blocks are connected to each other,any change in blockchain can be easily detected.

To carry out a national election certain e voting system should ensure many of the security requirements. They can be listed as voting system should not be traceable The voting system should ensure whether the voter's vote was counted & proof of vote should be provided.Voting system should not enable single entity to control systems. Only eligible individuals are allowed to participate in voting. The Election system should not be expensive. Depending on the role election system should provide limited access to participants.The use of blockchain Technology in E-Voting system can meet all the above needs as a blockchain is tamper proof and non-alterable.

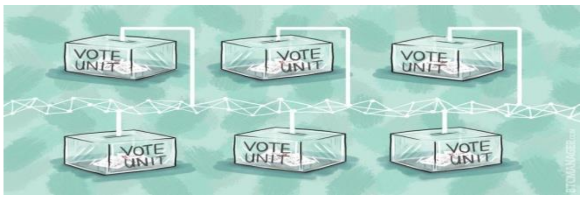


Fig 1: Blockchain

1.1 Key features of Blockchain :

- ❖ High Availability
- ❖ Verifiability
- ❖ Transparency
- ❖ Immutability
- ❖ Distributed Ledgers
- ❖ Decentralized
- ❖ Enhanced Security

1.2 Modules of Voting System

Typically it consist of two models :

1. The Administrator Module

The Administration module is made for the authorized person or admin of the organization. Admin has ability to handle the every function of the voter and the Candidate.The Admin can perform the functions such as Insertion of the name, Deletion of the name, updating the name and the authority to carry out the voting procedure.Admin will able to see if someone tampered the vote and he will take necessary action against it.

2. The User or Voter Module

In this module User or voter will able to see the names of all electing Candidates and vote the candidate.

2. SECURITY IN BLOCKCHAIN

In proposed blockchain system we used ECC cryptography to provide security in the system. ECC cryptography contains a key pairs of two parts: (i) public key and (ii) private key. The public key is shared among everyone where anyone can view all the public details in the network. It is strongly tied with the private key for security purposes. These keys are helpful for encryption and decryption process. A private key is similar to a password and is linked with a public key. Private key is not publicly available to everyone and is not shared with anyone in order to provide security to an account. It is kept secret and known only to the account holder. The private key is used to provide authenticity actions for accounts. Unlike with normal account, to access and know the account details, or to take any important action, one must use the private key at the receiver end which is known to receiver only so that security can be provided to an account using ECC algorithm. In the graphic below one can see how public key and private key pairs work, when sender is sending a message to receiver. Initially the sender encrypts the message with the public key of the receiver and then sends encrypted message to the receiver safely, on the other side when this encrypted message reaches to the receiver then the receiver receives this message and decrypts that using the private key of the sender which is known to receiver only. In this way security is provided to the message using ECC cryptography.

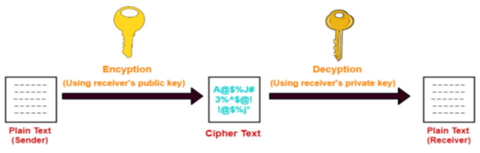


Fig 2: Public and Private key Encryption and Decryption process

3.METHODOLOGY

In this system we have used decentralize network in order to store voting data in the form of blocks. Blocks are interconnected with each other to creating the chain of voting records. In the proposed system the blockchain is used for security purpose and also we have created different levels of trusted contacts. If the higher authority allows the data to get stored in blocks then only it will be store in the blockchain database. Once the data gets stored it cannot be tamper as blockchain is so much securated. The blocks will contain the information as : username, previous hash value, timestamp.

The block is one transaction of blockchain, which will broadcast in the whole system when it gets verify. Whenever new block is authenticated by the system, block is added at end of the blockchain with help of hash value and this structure is looks like LinkedList. This sequence of blockchain goes on increasing as the blocks get added. The primary block in the blockchain is called as the Genesis Block. It has value as zero for previous block because genesis block does not have any previous block. The next block will have the hash value of the previous block and this way the process of adding blocks in the system take place.

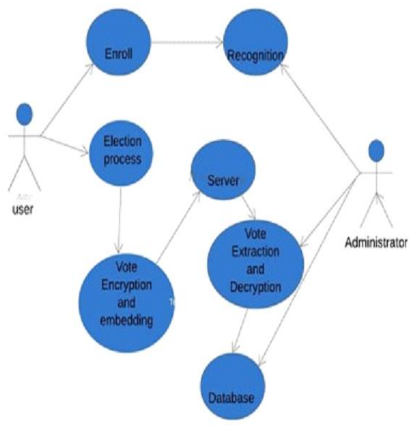


Fig 3 :Use Case Diagram

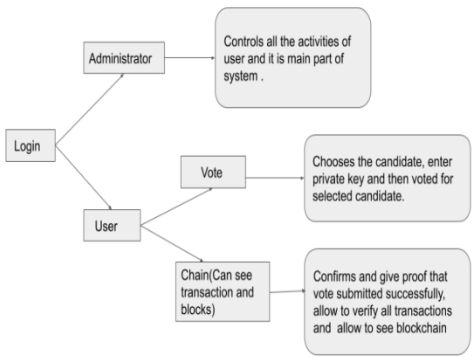

Administrator
Controls all the activities of user and it is main part of system .
Login
Vote
Chooses the candidate, enter private key and then voted for selected candidate.
User
Chain(Can see transaction and blocks)
Confirms and give proof that vote submitted successfully, allow to verify all transactions and allow to see blockchain

Fig 4: Data Flow Diagram

4.PROPOSED ALGORITHM

The algorithms for processing our proposed work are as follows.

4.1 ECC(Elliptic Curve Cryptography) Key Pair Generation:

```
from Crypto.PublicKey import ECC
key= ECC.generate(curve='P-256')
private_key=key.export_key(format='PEM')
print(private_key)
public_key=key.public_key().export_key(format="PEM")
print(public_key)
```

This will give 256 bit key pair which is of PEM(Privacy Enhanced Mail) format.

4.2 SHA3_256,DSS algorithm:

SHA(Secure Hash Algorithm) is used for generating hash value. It is better than MD5 algorithm because when hash value generated from data using SHA it is not possible to get original data from that. SO it is secured.

DSS(Digital Signature Standard) algorithm is used to create signature for security purpose.

```
from Crypto.Hash import SHA3_256
from Crypto.PublicKey import ECC
from Crypto.Signature import DSS
try:
  priv_key =ECC.import_key(private_key_input)
  hash_string=
  SHA3_256.new(ballot.encode('utf-8'))
  signature=
  DSS.new(priv_key,'fips-186-3').sign(hash_string)
  print('\n signature: ', signature.hex())
  public_key=
  ECC.import_key(request.user.user_public_key)
  verifier = DSS.new(public_key, 'fips-186-3')
  verifier.verify(hash_string, signature)
  status = 'The ballot is signed successfully.'
  error = False
except Exception as e:
  status = 'The key is not registered.'
  error = True
  print("not matched")
  print(e)
  messages.warning(request, str(e))
 return render(request, 'create_vote.html’)
```

5.3 Merkle Tree:

Merkle tree is a fundamental part of **blockchain** technology. It is a structure that allows for efficient and secure verification of content in large body of data. This structure helps to verify the consistency and content of the data.

```
import datetime
from uuid import uuid4
from Crypto.Hash import SHA3_256
from Crypto.Signature import DSS
from django.conf import settings
from django.contrib import messages
from django.contrib.auth.decorators import login_require
import time
from ballot.merkle.merkle_tool import MerkleTools
def seal(request):
   if request.method == 'POST':
     ballot = request.POST.get('ballot_input')
     vote_id = request.POST.get('vote-id')
     ballot_byte = ballot.encode('utf-8'
     ballot_hash= SHA3_256.new(ballot_byte).hexdigest()
     # Puzzle requirement: '0' * n (n leading zeros)
 puzzle, pcount = settings.PUZZLE, settings.PLENGTH
     nonce = 0
     block_transactions=
     Vote.objects.filter(id=vote_id).order_by('timestamp')
 # create Merkle hash
     root = MerkleTools()
  root.add_leaf([str(tx) for tx in block_transactions],
True)
      root.make_tree()
      merkle_hash = root.get_merkle_root()
     # Try to solve puzzle
       start_time = time.time()  # benchmark
      timestamp = _get_timestamp()
   # mark the start of mining effort
  # get prev hash from prev block
       prev_hash = get_prev_block_hash()
       while True:
          block_hash =
       SHA3_256.new(("{}{}{}".format(ballot,nonce,
timestamp).encode('utf-8'))).hexdigest()
          print('\ntrial hash: {}\n'.format(block_hash))
          if block_hash[:pcount] == puzzle:
             stop_time = time.time()
             print("\n block is sealed in
           {} seconds\n".format(stop_time - start_time))
             break
           nonce += 1
             block=
 Block(prev_h=prev_hash,block_hash=block_hash,
nonce=nonce,merkle_h=merkle_hash,timestamp=timestam
p)
              block.save()
             # create block object
             context = {
                   'prev_hash': prev_hash,
                   'transaction_hash': ballot_hash,
                   'nonce': nonce,
                   'block_hash': block_hash,
                   'timestamp': timestamp,
               }
            return render(request, 'seal.html', context)
  return redirect('/vote/')
```

5.EXPERIMENTAL OUTPUT

After implementing the project, the generated output is shown below.

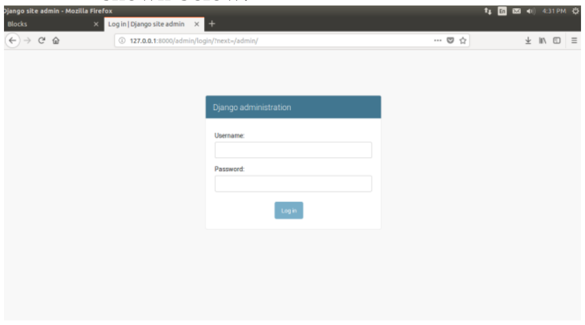

Django site admin - Mozilla Firefox
Blocks
Log in | Django site admin
127.0.0.1:8000/admin/login/?next=/admin/
Django administration
Username:
Password:
Log in

Fig 5 : Admin Panel

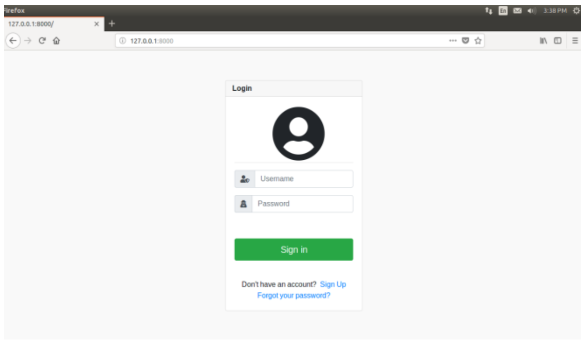
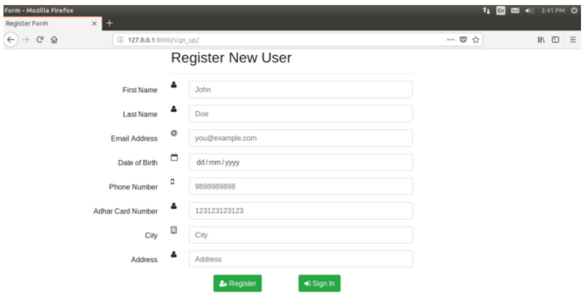


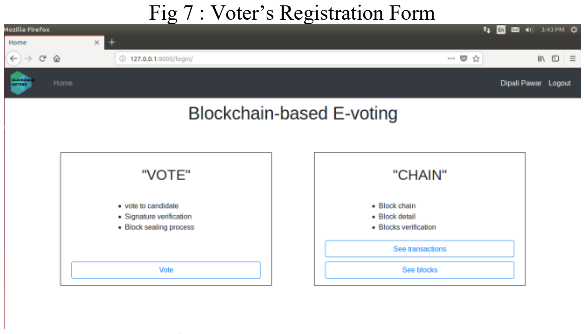
Fig 6 : Voter’s Login Form



Register New User

First Name	John
Last Name	Doe
Email Address	you@example.com
Date of Birth	dd / mm / yyyy
Phone Number	9898989898
Adhar Card Number	123123123123
City	City
Address	Address

Fig 7 : Voter's Registration Form

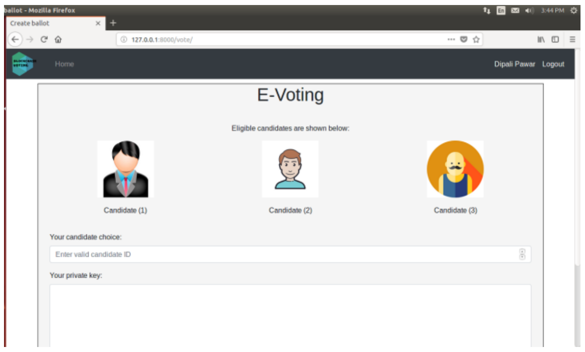


Blockchain-based E-voting

"VOTE"
- vote to candidate
- Signature verification
- Block sealing process

"CHAIN"
- Block chain
- Block detail
- Blocks verification

Fig 8: Voter's Home Page



E-Voting

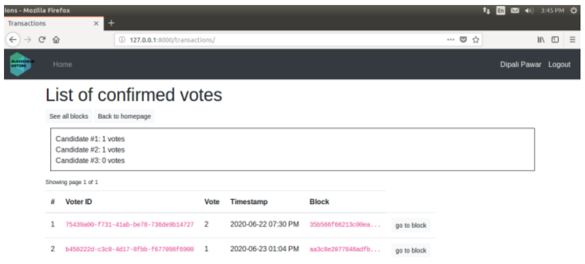
Eligible candidates are shown below:

Your candidate choice:

Enter valid candidate ID

Your private key:

Fig 9 : Ballot Creation Page



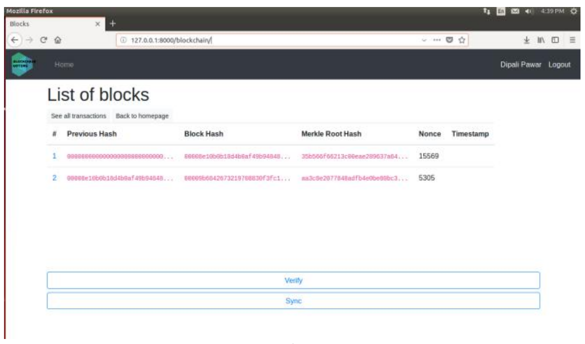
List of confirmed votes

Candidate #1: 1 votes
Candidate #2: 1 votes
Candidate #3: 0 votes

Showing page 1 of 1

#	Voter ID	Vote	Timestamp	Block	
1	75439a00-f731-41ab-be78-736de9b14727	2	2020-06-22 07:30 PM	35b566f66213c00ea...	go to block
2	b450222d-c3c8-4d17-8fbb-f677098f6900	1	2020-06-23 01:04 PM	aa3c8e2877848adfb...	go to block

Fig 10 : Transaction Page



List of blocks

#	Previous Hash	Block Hash	Merkle Root Hash	Nonce	Timestamp
1	0000000000000000000000000000...	00000e10b0b18d4b0af49b94848...	35b566f66213c00eae289637a84...	15569	
2	00000e10b0b18d4b0af49b94848...	00009b68426732197688830f3fc1...	aa3c8e2877848adfb4e0be08bc3...	5305	

Fig 11 : List Of Blocks

6.CONCLUSION

Nowadays,Blockchain technology is used in various fields.It is gaining more popularity day by day.As a result with the help of blockchain, voting system needs to be more secure,advanced and reliable.This application will provide transparency and cost-effective election by guaranteeing the privacy of voter.Encryption is used in the system.No votes are tampered in the system,it will detect the tampered votes and resolve it.This leads to achieve transparency.The main reason behind this system is to present an idea of implementation of blockchain in voting system.

REFERENCES

[1] Cosmas Krisna Adiputra, Rikard Hjort, and Hiroyuki Sato, " A Proposal of Blockchain-based Electronic Voting System ", Dept. of Electrical Engineering and Information Systems.Artis Mednis, Girts Strazdins, Reinholds Zviedris, Georgijs Kanonirs, Leo Selavo, "Real Time Pothole Detection using Android Smartphones with Accelerometers."

[2] Fridrik P. Hjálmarsson, Gunnlaugur K. Hreidarsson, Mohammad Hamdaqa, Gísli Hjálmtýsson,"Blockchain-Based E-Voting System ".Available: https://ieeexplore.ieee.org/document/8457919.

[3] Ali Kaan Koc,Umut Can abuk,Emre Yavuz ,Gokhan Dalkoloc,"Towards Secure E-Voting Using Ethereum Blockchain".Available at: ieeexplore.ieee.org/document/8355340/.

[4] Henry Rossi Andrian, Novianto Budi Kurniawan, Suhardi,"Blockchain Technology and Implementation : A Systematic Literature Review".2018 International Conference on Information Technology Systems and Innovation (ICITSI) October 22-25,2018.

[5] Ashish Singh,Kakali Chatterjee," Secure Electronic Voting System Using Blockchain Technology",2018 International Conference on Computing, Power and Communication Technologies (GUCON) Sep 28-29, 2018.

[6] Prakash K. Ukhalkar, Dr. Rajesh N. Phursule , Dr Devendra P Gadekar, Dr Nilesh P Sable. (2020). Business Intelligence and Analytics: Challenges and Opportunities. International Journal of Advanced Science and Technology, 29(12s), 2669-2676

[7] Nir Kshetri and Jeffrey Voas,"Blockchain-Enabled E-Voting",https://Blockchain%20Papers/kshetri2018.pdf.

[8]]Basit Shahzad and Jon Crowcraft,"Trustworthy Electronic Voting Using Adjusted Blockchain Technology."

[9] Tareq Ahram,Aman Sargotzaei,Saman Sargotzaei,Jeff Daniels,Ben Amaba,"Blockchain technology Innovations". https://ieeexplore.ieee.org/document/7998367/authors.

[10] Rishav Chatterjee,Rajdeep Chatterjee,"An Overview of the Emerging Technology:Blockchain".Available at:https://ieeexplore.ieee.org/document/8307344

[11] Christopher G.Harris,"The Risks and Challenges of Implementing Ethereum Smart Contracts".Available at:https://ieeexplore.ieee.org/document/8751493.

[12] H Halpin,M Piekarska,"Introduction to Security and Privacy on the Blockchain", 2017 IEEE European Symposium on 2017 - ieeexplore.ieee.org.

[13] Sable Nilesh Popat*, Y. P. Singh," Efficient Research on the Relationship Standard Mining Calculations in Data Mining" in Journal of Advances in Science and Technology | Science & Technology, Vol. 14, Issue No. 2, September-2017, ISSN 2230-9659

[14] Dipali Pawar, Pooja Sarode, Shilpa Santpure, Poonam Thore, Prof. Pravin Nimbalkar, "Secure Voting System Using Blockchain", Department of Computer Engineering, JSPMs Imperial College of Engineering and Research Pune,India.Available:https://www.ijert.org/secure-voting-system-using-blockchan