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.
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.

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 secured. 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.

4. PROPOSED ALGORITHM

The algorithms for processing our proposed work are as follows.

4.1 ECC(Elliptic Curve Cryptography) Key Pair Generation:

```python
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.

```python
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 =
```


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_required
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, pcount = settings.PUZZLE, settings.PLENGTH
        nonce = 0
        block_transactions = Vote.objects.filter(id=vote_id).order_by('timestamp')
        root = MerkleTools()
        root.add_leaf([str(tx) for tx in block_transactions], True)
        root.make_tree()
        ballot_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(b'

            print('trial hash: {}' .format(block_hash))
            if block_hash[:pcount] == puzzle:
                stop_time = time.time()
                print('in block is sealed in {} seconds' .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=timestamp)
            block.save()
            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.

Fig 5: Admin Panel

Fig 6: Voter's Login Form
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. Aris Mednis, Girts Stazdins, Reinholds Zviedris, Georgijs Kanonis, Leo Selavo, “Real Time Pothole Detection using Android Smartphones with Accelerometers.”

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

[3] Ali Kaan Koc, Umut Cun abuk, Emre Yavuz, “Blockchain for E-Voting”, Anadolu University.

[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 (ICTSI) 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(12), 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/7908367/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 - ieexplore.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, 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-blockchain