Original Research Paper

Volume-10 | Issue-1 | January - 2020 | PRINT ISSN No. 2249 - 555X | DOI : 10.36106/ijar

Computer Science

BLOCKCHAIN BASED E-VOTING SYSTEM

Ashwathy Menon — Department Of Computer Engineering, Thadomal Shahani Engineering College (of Mumbai University) Mumbai, India

Vijayalakshmi Bhagat* — Department Of Computer Engineering, Thadomal Shahani Engineering College (of Mumbai University) Mumbai, India *Corresponding Author

ABSTRACT Blockchain is one of the new technologies that has emerged in the recent years and has found many applications. One such application of blockchain, owing to its immutability property is an e-voting system. The electoral process conducted these days are generally centralized where a single entity has complete control over the system. Blockchain being a decentralized and distributed public ledger is one of the potential solutions to address this issue. This paper presents an implementation of blockchain based e-voting system. It explains how to create a complete blockchain network along with other data structures required. All the necessary functionalities of e-voting from authentication of voter to displaying the live vote count have been mentioned here. The system proposed here has been developed using a test-driven development approach. The system was evaluated by conducting a trial voting process and it was found that no votes were lost or tampered with during the process. The voter remains anonymous throughout the process and blockchain being a decentralized network, all the nodes have equal computational power there by making the system more secure.

KEYWORDS : Blockchain, Cryptography, Digital signature, E-Voting, Wallet

I. INTRODUCTION

The fate of a country depends on its governing body and elections play a crucial role in the process. The main aspect of providing an e-voting system is to allow people to vote anytime from anywhere, encouraging more people to come forward and participate in the voting process. Considering digitalization also has security threats following it, easy access cannot be the only criteria for an electronic voting system to be acceptable, it has to gain trust of the voters by proving it to be reliable and secure.

Blockchains are new kind of replicated database which can be operated without control of any single party[6]. As a ledger blockchain serves the purpose of storing transactional data and is shared with everyone using the blockchain network. To avoid controversial elections, the process needs to be fair, transparent and verifiable. The immutability and transparency property of blockchain meets all the conditions making it one of the potential solutions.

Blockchain technology originates from the underlying architectural design of the cryptocurrency Bitcoin[1]. The blockchain is collaboratively maintained by anonymous peers on the network, so Bitcoin requires that each block prove a significant amount of work was invested in its creation to ensure that untrustworthy peers who want to modify past blocks have to work harder than honest peers who only want to add new blocks to the blockchain. Chaining blocks together makes it impossible to modify transactions included in any block without modifying all subsequent blocks[2].

Area where voting is to be carried out is divided into sub regions and one blockchain node is assigned for every region. Voters can access the node from website to cast their vote after getting their credentials verified. Every blockchain node has a digital wallet assigned to it.

A wallet is an application that serves as the primary user interface. The wallet controls access to its tokens, managing keys and addresses, tracking the balance, and creating and signing transactions[3]. All votes will be signed by the wallet's private key and can be verified only by its corresponding public key. This helps in tamper detection.

When a wallet makes a transaction, it is initially added to the transaction pool and during this period it is considered to be an unverified transaction. Each vote casted is considered to be one transaction. In order to add the votes in the transaction pool to the blockchain a process called mining is carried out. Miners validate new transactions and record them on the global ledger. Transactions that become part of a block and added to the blockchain are considered confirmed.

Consensus protocols are one of the most important and revolutionary aspects of blockchain technology [4].Consensus mechanisms are protocols that make sure all nodes (device on the blockchain that maintains the blockchain and (sometimes) processes transactions) are synchronized with each other and agree on which transactions are legitimate and are added to the blockchain.[5]

II. DESIGN

A blockchain is a distributed database holding a continuously growing list of records, controlled by multiple entities that may not trust each other. Records are appended to the blockchain in batches or blocks through a distributed protocol executed by the nodes powering the blockchain.[7]. Each block acts as a storage unit.

A. Block Structure

The block consists of meta-data like timestamp, last hash, hash, nonce and difficulty. The data stored in block includes a list of hash of voter ids and votes.

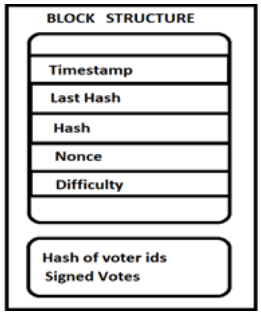

Figure 1: Block Structure

Timestamp: Indicates the time when the block was created.

Last Hash: Hash of the previous block in the blockchain. Last hash creates a link between subsequent blocks in the chain.

Difficulty: The number of leading zeroes that a block hash should have. It is adjusted dynamically according to the mine rate.

Nonce: A nonce is an arbitrary number used only once in a cryptographic communication. They are often random or pseudo-random numbers.[8]

Hash: Input for the block hash includes the data that it stores plus other meta data about the block. Block data combined with nonce produces the hash that satisfies the difficulty set.

Hash of voter ids: The list of hash of voter ids is stored in the blockchain to check if a voter has already voted or not.

Signed Votes: The votes signed by the digital wallet.

A. Transaction Pool Map and Voter-Id Pool Map

Transaction Pool Map contains a recent list of transactions. When the voter casts a vote, it is initially added to the transaction pool map where it is considered to be unverified. Transaction Pool Map should support three main behaviours:

1) It should contain unique set of transactions.
2) Update existing stored transactions when change is submitted by the wallet. When a wallet makes a transaction for the first time a new transaction structure is created and added to the transaction pool. However, when the same wallet makes a transaction again, the transaction of the wallet already present in the pool is updated instead of creating a new one. So, every wallet has at the most one transaction in the pool at a time which eliminates duplicate entries.
3) Rewrite multiple transactions-replacing the transactions with an entire new set and replacing all or new transactions.

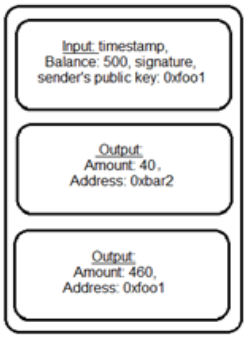

Figure 2: Transaction Structure

The transaction structure has an input map and output map. Input map includes timestamp, balance, signature and sender's public key. Output map has the token and the candidate address to whom the vote is sent. As shown in figure 2 output made by the wallet with an initial balance of 500 is such that if 40 tokens are sent to the address 0xbar2 it will make another transaction where it sends the remaining 460 tokens to itself. The summation of amounts in the output maps must always be equal to the balance in the input map for the transaction to be valid.

The hash of voter-id is added to the voter-id pool map. It is kept distant from the transaction pool map to maintain voter anonymity.

III. IMPLEMENTATION

Every region has a blockchain node assigned to it. Each node has a digital wallet which has a public-private key pair and some pre-defined number of tokens. Whenever a node mines a block its wallet will receive some tokens as mining reward which makes sure that wallet tokens will never be exhausted.

A. Credential Verification

The credentials of voter are checked against a registered voter's database. Before an OTP is sent to voter's registered email id it is important to ensure that he has not voted before. For this condition to be met, hash of the voter id must not be present in the voter-id pool and in the blockchain. After that, an OTP is sent to voter's email id for authentication purpose.

B. Voting Process

The wallet assigns one token for the authorized voter and a candidate list will be displayed. When the voter casts a vote, it will be signed by the wallet's private key. The hash of the voter id will be added to the voter id pool and the signed vote will be added as a transaction in the transaction pool map which is updated accordingly. The content of both the pools when updated are broadcasted to other nodes in the network which are accepted after they pass the validation tests.

The hashing algorithm used is SHA-256. SHA-256 is a member of the SHA-2 cryptographic hash functions designed by the National Security Agency[9]. Cryptographic hash functions are mathematical operations run on digital data; by comparing the computed "hash" to a known and expected hash value, a person can determine the data's integrity. A one-way hash can be generated from any piece of data, but the data cannot be generated from the hash [10].

The algorithm used for digital signature is Elliptic Curve Digital Signature Algorithm. Elliptic-curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC requires smaller keys compared to non-EC cryptography to provide equivalent security[11]. Elliptic curves are applicable for key agreement, digital signatures, pseudo-random generators and other tasks. Indirectly, they can be used for encryption by combining the key agreement with a symmetric encryption scheme[12]. They are also used in several integer factorization algorithms based on elliptic curves that have applications in cryptography. The primary benefit promised by elliptic curve cryptography is a smaller key size, reducing storage and transmission requirements, i.e. that an elliptic curve group could provide the same level of security afforded by an RSA-based system with a large modulus and correspondingly larger key.

C. Mining

Mining is the mechanism that underpins the decentralized clearinghouse, by which transactions are validated and cleared. Following actions have to be performed by the transaction miners:

1. Grab all the valid transactions in the pool
2. Generate a miner's reward
3. Do the CPU work to find a valid hash
4. Broadcast the updated blockchain
5. Clear the transaction pool

For a transaction to be valid it has to pass the following tests

1) Each Transaction must be correctly formatted.
2) Only one mining reward
3) Valid input amounts according balance in blockchain history
4) Block must not have identical transactions

The rate at which blocks are mined needs to be constant throughout hence a mine rate will be defined. Dynamic difficulty adjustment is carried out to achieve this. If miners take a while to mine the blocks then difficulty should be lowered and if blocks are mined too quickly then difficulty needs to be increased. The difference between the timestamp of new block and previous block is calculated.

If difference < MINE_RATE then difficulty=difficulty+1
If difference > MINE_RATE then difficulty=difficulty-1

Miners compete to solve a difficult mathematical problem based on a cryptographic hash algorithm. The solution found is called the Proof-Of-Work. This prevents attackers from rewriting the blockchain history and corrupt the entire data. When a node mines a block a miner reward of 50 tokens is sent to its public address.

D. Broadcast

In blockchain it is necessary that all the nodes are in synchronization. To achieve this an entity called PubNub has been used. PubNub offers a real time infrastructure-as-a-service and provides enterprise grade security[13].

In this system, a publisher-subscriber module is made and three channels are created. All the blockchain nodes that are registered on these channels will be able to send and receive messages through this channel.

Three channels have been created:

1. Transaction: Transaction channel is used to keep the transaction pool map in sync. When the wallet makes a transaction, it will broadcast the transaction on this channel so all the nodes subscribed will receive it and perform all the validation checks before adding it to their pool.
2. Voter: Voter channel is used to keep the voter-id pool map in synchronization.
3. Blockchain: Blockchain channel is used so that all the nodes have same copy of the blockchain. When the node mines a block and adds it to its blockchain, it will broadcast the blockchain on this channel. All the nodes that receive this will perform the validation checks and replace their chains with the received blockchain if it is valid.

E. Chain Validation and Replacement

Chain Validation is a concept of inspecting the blockchain and checking that each block has been constructed correctly.

To check for correctness, following rules have to be followed:

1. Correct block fields present
2. Actual last Hash reference
3. Valid Hash

Chain Replacement: Unless the incoming chain is longer and it checks that the blocks are valid then only the current chain is replaced.

F. Live Vote Count

The system displays live vote count throughout the process in a graphical format.

IV. EXPERIMENT RESULT

In this research implementation is done using Node JS for server-side programming and React JS for the user-interface. The system has been developed using a Test-Driven Development approach. Three blockchain nodes have been created and hosted in the Heroku servers. A global data stream network called PubNub is used for creating publisher and subscriber channels. Three channels have been created for broadcasting blockchain, transactions and hash of voter id. All the blockchain nodes registered on these channels will be able to send and receive messages. A demo voting process was carried out to check the reliability of the system. It was found that only registered and authorized voters were allowed to cast a vote. Transaction Pool, Voter Id Pool and Blockchain across all the nodes were in synchronization. All the votes casted were added to pool successfully and eventually added to the blockchain. The live vote count displayed was accurate throughout the process and no votes were lost or manipulated. The system passes all the validation tests successfully.

V. CONCLUSION

Blockchain technology being a distributed public ledger has the potential to solve problems that occur in a general voting system. The digital signature generated for votes ensures that votes cannot be tampered or altered thereby creating trust among the users. The immutability property of blockchain further makes tampering impossible. Blockchain being decentralized all the nodes in the network have equal computational power. As the user interface is a website the voting portal is easily accessible. The dynamic difficulty adjustment factor improves the efficiency of the system. As all blocks in the chain are linked by last hash reference and any modification in the block will change its hash completely it becomes computationally expensive and impossible for the attacker to modify the blocks. The system achieves necessary level of transparency as the blockchain and live vote count are visible to the public throughout the process. All the nodes in the network carry out the necessary validation tests before accepting a transaction or a newly mined block. Thus, the system ensures that necessary tests have been carried at each step.

VI. REFERENCES

[1] A. Barnes, C. Brake, and T. Perry, “Digital Voting with the use of Blockchain Technology Team Plymouth Pioneers – Plymouth University,” 2016.
[2] https://bitcoin.org/en/developer-guide#proof-of-work [last accessed: 29 March 2019]
[3] Andas M. Antonopolus, ”Mastering Bitcoin: Unlocking Digital Cryptocurrencies”, pages 61-104,2014
[4] https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/consensus-protocols [last accessed: 26 February 2019]
[5] https://hackernoon.com/different-blockchain-consensus-mechanisms-d19ea6c3bcd6[last accessed : 2 April 2019]
[6] Patrik McCorry, Siamak F. Shahandashti and Feng Hao,” Contract for Boardroom Voting with Maximum Voter Privacy”
[7] Christian Cachin Marko Vukolic´,” Blockchain Consensus Protocols in the Wild”,2017
[8] Phillip Rogaway,” Nonce-Based Symmetric Encryption”
[9] "On the Secure Hash Algorithm family" (PDF). Archived from the original (PDF) on 2016-03-30.
[10] https://en.bitcoinwiki.org/wiki/SHA-256 [last accessed: 10 January 2019]
[11] T. Pornin,"Deterministic Usage of the Digital Signature Algorithm(DSA) and Elliptic Curve Digital Signature Algorithm(ECDSA)",Informational Category,pg 4
[12] Ms Shweta Lamba, Ms. Monika Sharma,"An Efficient Elliptic Curve Digital Signature Algorithm (ECDSA) ", IEEE paper, 2013 International Conference on Machine Intelligence Research and Advancement
[13] https://www.pubnub.com/company/[last accessed: 28 February 2019]