RESEARCH ARTICLE OPEN ACCESS

Vote Blocks: A Block Chain Based E – Voting System

Arya Raj, Gispriya T George, Praful Konnully, Sreelakshmi R Nair
Department of Computer Science and Engineering
Toc H Institute of Science and Technology, Arakkunnam
Kerala - India

ABSTRACT
By allowing digital information to be distributed but not copied, blockchain technology created the backbone of a new type of internet. Originally devised for the digital currency, Bitcoin, the tech community is now finding other potential uses for the technology. Building a secure electronic voting system that offers the fairness and privacy of current voting schemes, while providing the transparency and flexibility offered by electronic systems has been a challenge for a long time. In this project we evaluate an application of blockchain as a service to implement distributed electronic voting systems. The electronic voting system based on blockchain that addresses some of the limitations in existing systems and evaluates some of the popular blockchain frameworks for the purpose of constructing a blockchain-based e-voting system. Our system assures a tamperproof voting system. The voter can track their vote during the election so as to ensure that the vote is not tampered. The system uses a fingerprint based authentication to avoid fake votes. The system uses truffle framework to build the web based decentralized voting application. In particular, we evaluate the potential of distributed ledger technologies through this project, the process of an election, and the implementation of a blockchain based application, which improves the security and decreases the cost of hosting a nationwide election.
Keywords:- E-Vote, Block Chain

I. INTRODUCTION

With the rise of blockchain technology, the core concept of decentralization has gradually drawn attention. In this context, the main objective is to realize more convenient and secure applications through the use of blockchain technology. Blockchain technology is supported by a distributed network consisting of a large number of interconnected nodes. Each of these nodes have their own copy of the distributed ledger that contains the full history of all transactions the network has processed. There is no single authority that controls the network. If the majority of the nodes agree, they accept a transaction. This network allows users to remain anonymous. A basic analysis of the blockchain technology (including smart contracts) suggests that it is a suitable basis for e-voting and, moreover, it could have the potential to make e-voting more acceptable and reliable.

Blockchain technology is one solution that can be used to reduce the problems that occur in voting.

Blockchain has been used in Bitcoin transaction database systems. Blockchain consists of several blocks that are linked to each other and in sequence. The block is related because from the previous hash used in the next block making process, the attempt to change the information will be more difficult as it has to change the next blocks. The database was made public, acquired by many users. In the Bitcoin system, a mining process is required. In this research, a method that use turn rules for each node in blockchain creation, with the assured importance of each node joining the blockchain.

Blockchain is a distributed, immutable, incontrovertible, public ledger. This new technology has three main features:

i. Immutability: Any proposed “new block” to the ledger must reference the previous version of the ledger. This creates an immutable chain, which is where the blockchain gets its name from, and prevents tampering with the integrity of the previous entries.

ii. Verifiability: The ledger is decentralized, replicated and distributed over multiple locations. This ensures high availability (by eliminating a single point of failure) and provides third-party verifiability as all nodes maintain the consensus version of the ledger.

iii. Distributed Consensus: A distributed consensus protocol to determine who can append the next new transaction to the ledger. A majority of the network nodes must reach a consensus before any new proposed block of entries becomes a permanent part of the ledger.

These features are in part achieved through advanced cryptography, providing a security level greater than any previously known record-keeping system. Blockchain technology is therefore considered by many, including us, to have a substantial potential as a tool for implementing a new modern voting process.

II. LITERATURE REVIEW

There are several Blockchain based e-voting systems. "Agora" Agora stands out as the first blockchain voting solution that is architected to meet the performance needs of a mission critical election. This technology runs on a custom blockchain that our team has been developing since 2015.This technology strive to meet the evolving needs of modern voters. Not only do voters demand greater transparency in their elections, but they also demand more convenient methods of participating. It allows to enable any authorized voter to participate in an election through their own digital device, all while guaranteeing the security and transparency of the electoral procedure.

Each step of the election process can be easily understood and open to scrutiny by all stakeholders (voters, political parties, outside observers and others). All results should be independently verifiable and auditable. All eligible voters, regardless of location, group membership or disability, are having reasonable and equal opportunity to cast their ballot.

Agora's platform protects voter privacy through verifiable ballot encryption and anonymization. The cryptographic methods that we use to ensure privacy come from widely researched and accepted models, including threshold ElGamal for ballot encryption and Neff shuffling for ballot anonymization.

"Digital Voting" It is an integration of the blockchain technology to the current voting system in the UK in which the voters can vote at a voting district or on a web browser at home. In these blockchain containing information of who has registered to vote also allows our service to ensure each voter in unique. Once registered you are then allocated a vote after verification of your details has been completed. To ensure these registered voters are who they say they are when voting begins there is a 3 factor authentication method. Further to this we also need to ensure they are not forced to vote in a particular way so we have incorporated a double-check service where by users shall be prompted a second time to confirm their submission before the vote is sent; this also then allows us to almost eradicate accidental votes

"Netvote" At the current frequency of elections and the available pool of eligible voters, there should be at least 15 billion ballots cast every year. Everyone who wants to vote should. Every vote should count. Every count should be verified. Netvote is an open source voting protocol, available now for multiple blockchain platforms. Elections are executed according to smart contracts and every vote is stored on the blockchain. Netvote currently supports public and private Ethereum and in the future will support additional blockchain platforms including RChain, EOS, NEO and Hyperledger.

It is a decentralized blockchain-based voting network on the Ethereum blockchain. Netvote utilizes decentralized apps (dApps) for the user interface of the system. The Admin dApp allows election administrators to set election policies, create ballots, establish registration rules and open and close voting. The Voter dApp is used by individual voters for registration, voting and can be integrated with other devices (such as biometric readers)

III. OBJECTIVES

Building a secure electronic voting system that offers the fairness and privacy of current voting schemes, while providing the transparency and flexibility offered by electronic systems has been a challenge

for a long time. A blockchain framework for the purpose of constructing a blockchain-based e-voting system. Each step of the election process transparent (voters, political parties, outside observers and others). All results will be independently verifiable and auditable. The choices that each voter makes will remain private both during and after the election. Only eligible voters should be allowed to vote, and those votes must be protected from any alteration or

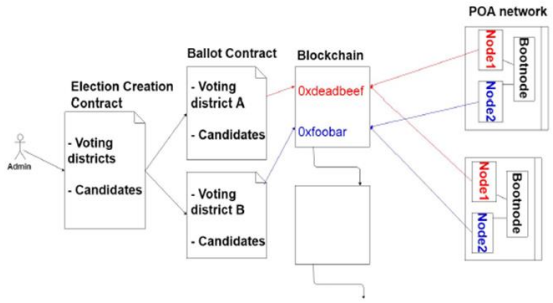


Figure 1

exclusion by using digital signature. The cost for election will be affordable. All eligible voters, regardless of location, group membership or disability, should have reasonable and equal opportunity to cast their ballot.

A. BLOCKCHAIN SETUP

In order to satisfy the privacy and security requirements for e-voting, and to ensure that the election system should not enable coerced voting, voters will have to vote in a supervised environment. In our work, we setup a Go-Ethereum permissioned Proof-of-Authority (POA) blockchain to achieve these goals. POA uses an algorithm that delivers comparatively fast transactions through a consensus mechanism based on identity as a stake. The structure of the blockchain is illustrated in Figure 1 and mainly consists of two types of nodes.

i. District node: Represent each voting district. Each district node has a software agent that autonomously interacts with the "bootnode" and manages the life cycle of the smart contract on that node.

ii. Bootnode: Each institution, with permissioned access to the network, host a bootnode. A bootnode is a discovery and coordination service that helps the district nodes to discover each other and communicate. After setting up a secure and private blockchain, the next step is to define and deploy a smart contract that represents the e-voting process on the blockchain infrastructure.

B. ELECTION AS A SMART CONTRACT

Defining a smart contract includes three parts:

1. Election roles: The roles in a smart contract include the parties that need to participate in the agreement. The election process has the following roles: “Election administrator” To manage the lifecycle of an election. Multiple trusted institutions and companies may be enrolled in this role. The election administrators create the election, register voters, decide the lifetime of the election and assign permissioned nodes. “Voter” An individual who is eligible to vote. Voters can authenticate themselves, load election ballots, cast their vote and verify their vote after an election is over.
2. Election process*:* Election process is represented, by a set of smart contracts, which are deployed on the blockchain by the election administrators as shown in Figure 1. A smart contract is defined for each of the voting districts. The main activities in the election process are: "Election creation" the administrators create election ballots using a smart contract. The smart contracts are then written onto the blockchain, where district nodes gain access to interact with their corresponding smart contract. "Voter registration" when an election is created the election administrators must define a deterministic list of eligible voters. This might require a component for a government identity verification service to securely authenticate and authorize eligible individuals. Using such a service is necessary to satisfy the requirement of secure authentication as this is not

guaranteed, by default, when using a blockchain infrastructure. "Tallying results" tallying of the election is done on the fly in the smart contracts. Each ballot smart contract does their own tally for their corresponding location in its own storage. "Verifying votes" In the voting transaction, each voter receives the transaction ID of his vote. In our e-voting system, voters can use this transaction ID and go to an official election site (or authority) using a blockchain explorer and (after authenticating themselves using their electronic identification) locate the transaction with the corresponding transaction ID on the blockchain. Voters can see their votes on the blockchain, and verify that the votes were listed and counted correctly.

3. Voting transaction: Each voter interacts with a ballot smart contract for her corresponding voting district. This smart contract interacts with the blockchain via the corresponding district node, which appends the vote to the blockchain. Each individual voter receives the transaction ID for their vote for verification purposes. Every vote that is agreed upon, by the majority of the corresponding district nodes, is recorded as a transaction and then appended on the blockchain.. A transaction in our proposed system (see Table 1) has information on i) the transaction ID, ii) the block which the transaction is located at, iii) to which smart contract the transaction was sent, and iv) the value of the transaction, i.e. the vote, indicating which entity (party) the voter voted for. A voting transaction in our system, therefore, reveals no information about the individual voter who cast any particular vote.

TxHash	Block	To	Value
0xdeadbeef...	1337	N1SC	D
0xG1345edf...	1330	N2SC	P

Table 1

IV. DESIGN

In this Blockchain based voting system, a voting contract where you initialize a few candidates contesting in an election and anyone can vote for them. The votes will be recorded on the blockchain. To connect between one block with another block, the hash value of the previous block inserted into the next block then calculated its hash value. It's an end to end traversal of an Ethereum transaction starting from your browser/console to the Ethereum network and back to your browser/console.

Before the election process begins, each node generates a private key and a public key. Public key of each node sent to all nodes listed in the election process, so each node has a public key list of all nodes. When the election occurs, the candidate can login there account with through there voter ID and scanning fingerprint and each node gathers the election results from each voter. When the selection process is completed, the nodes will wait their turn to create the block. Upon arrival of the block on each node, then done verification to determine whether the block is valid. Once valid, then the database added with the data in the block. After the database update, the node will check whether the node ID that was brought as a token is his or not. If the node gets a turn, it will create and submit a block that has been filled in digital signature to broadcast to all nodes by using turn rules in blockchain creation to avoid collision and ensure that all nodes into blockchain. The submitted block contains the id node, the next id node as used as the token, timestamp, voting result, hash of the previous node, and the digital signature of the node.

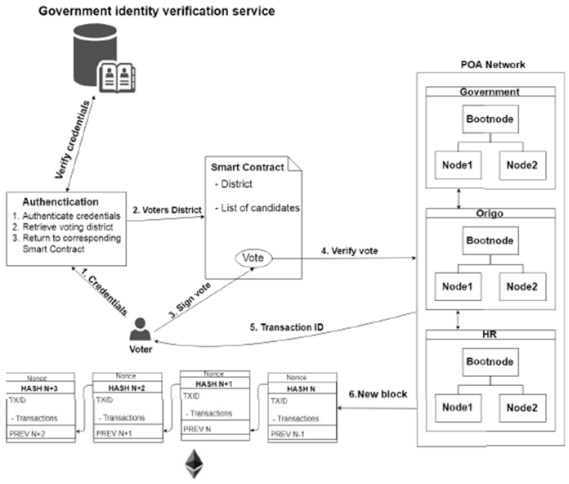
The verification is done by the Election Administrator. The election administrators create the election, register voters. The verification process starts from the acquisition of a block containing the voting result, the previous hash of the hash value originating from the previously valid block, and the digital signature. The electronic document is calculated its hash value. As for the digital signature is done by decryption process using the public key of the node that makes the electronic document. These two hash values are then compared, if the value is the same then the digital signature is valid and the

process continues, but if the value is not equal it is considered invalid and the system will refuse the block to continue the process.

After the digital signature verified and proven to be valid, further verification of the previous hash begins with the capture of the voting result, and the previous hash contained in the most recent in database, and searched hash values with the SHA-256 algorithm. Then compare it with the previous hash carried by the block being done verification.

Voting is done using Smart contract which is a self-running program. Votes created and recorded using smart contract. The tallying of the election is done on the fly in the smart contracts. Each ballot smart contract does their own tally for their corresponding location in its own storage. Users are added into the smart contract when the verifying authority verifies the user. Smart contract will include options for Creating a vote, Voting and for Building.

The basic diagram of the Election Process in given below:



V. RESULT AND DISCUSSION

Each voter will be having a login id that is his/her voter's id and password. His/her account is authenticated using their fingerprint. Out voting system provides the facility to caste there. And also the admin login which is handled by election commission. The login can be used for adding candidates, starting candidates and Stopping candidates. The voters can caste their vote through their login. The votes get counted to the corresponding candidates vote count. After the specification time limit the admin stops the election. Afterwards no further voting is possible. Election candidate is declared as the winner to that specific position. Once the vote is done by the candidate it is stored in the blockchain, and no more modification is possible. Thus our E-voting system is much secured.

VI. FUTURE WORKS

The blockchain bears all kinds of potential for improving human systems. Most often we hear of that potential in reference to financial services and banking systems. But the human arena that could perhaps be most improved by the blockchain is voting. Our existing mechanisms did prove susceptible to outside infection. It became clear to everyone that something needs to change. And that's where the blockchain comes in: by moving our voting systems to the blockchain. Something several countries and states have experimented with already. The chief benefit of switching our voting systems over to the blockchain is the enhanced level of transparency the blockchain allows for. The blockchain would definitivelypreclude bad actors from cheating the system. It would make sure people do not vote twice, since we'd have an immutable record of their vote and their identity. And no one would ever be able to delete votes, because, again, the blockchain is immutable. Those charged with counting votes would have a final record of every vote counted that could be checked by regulators or auditors at any time.

VII. CONCLUSION

Through our project, we introduced a blockchain based electronic voting system that utilizes smart contracts to enable secure and cost-efficient election while guaranteeing voters privacy. Making the electoral process cheap and quick, normalizes it in the eyes of the voters, removes a certain barrier between the voter and the elected official and puts a certain amount of pressure on the elected official. We

have shown that the blockchain technology offers a new possibility to overcome the limitations and adoption barriers of electronic voting systems which ensures the election security and integrity and lays the ground for transparency.

Our approach is based private blockchain implementation and use district-based voting. Using an Ethereum private blockchain, it is possible to send hundreds of transactions per second onto the blockchain, utilizing every aspect of the smart contract to ease the load on the blockchain. Blockchain based electronic voting system that utilizes smart contract to enable secure and cost efficient election while guaranteeing voters privacy. The blockchain technology offers a new possibility for democratic countries to advance from pen and paper election scheme, to a more cost and time-efficient scheme, while increasing the security measures of the todays scheme and offer new possibilities of transparency. Our election scheme allows individual voters to vote at a voting district of their choosing while guaranteeing that each individual voters vote is counted from the correct district, which could potentially increase voter turnout.

REFERENCES

[1] Ahmed Ben Ayed(2017);A Conceptual Secure Blockchain –Based Electronic Voting System; International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3,

[2] Pavel Tarasov and Hitesh Tewari(2017);The Future of E-Voting; IADIS International Journal on Computer Science and Information Systems Vol. 12, No. 2, pp. 148-165 I

[3] Zibin Zheng1, Shaoan Xie1, Hongning Dai2, Xiangping Chen4, and Huaimin Wang3(2017);An Overview of Blockchain Technology : Architecture,Consensus, and Future Trends; IEEE 6th International Congress on Big Data.

[4] Jesse Yli-Huumo1, Deokyoon Ko2, Sujin Choi4*, Sooyong Park2, Kari Smolander3(2016); Where Is Current Research on Blockchain Technology?—A Systematic Review;PLOS-ONE.

[5] Mahdi H. Miraz1, Maaruf Ali2(2018); Applications of Blockchain Technology beyond Cryptocurrency; Annals of Emerging Technologies in Computing (AETiC) Vol. 2, No. 1, 2018

[6] Michael Crosby, Google,Nachiappan, Yahoo,Pradhan Pattanayak, Yahoo,Sanjeev Verma, Samsung Research America,Vignesh Kalyanaraman, Fairchild Semiconductor (2015);Blockchain Technology Beyond Bitcoin.

[7] Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis (2018); E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy; arXiv:1805.10258v2 [cs.CR]