INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 3)
Available online at: www.ijariit.com

Hyperledger based electronic voting system

K. H. Sudershan
sudershankh.15cs@saividya.ac.in
Sai Vidya Institute of Technology, Bengaluru, Karnataka

P. Eshwar Reddy
eshwarpr.15cs@saividya.ac.in
Sai Vidya Institute of Technology, Bengaluru, Karnataka

Kishore Nadiger
kishoren.15cs@saividya.ac.in
Sai Vidya Institute of Technology, Bengaluru, Karnataka

Sharat Kumar S.
sharatks.15cs@saividya.ac.in
Sai Vidya Institute of Technology, Bengaluru, Karnataka

ABSTRACT

In many countries, the elections are carried out by a single administration and have complete control over the database and system. The administration has to manage the entire election process which occurs for a long period of time. Generic elections still use a centralized system; some of the problems that can occur in conventional electoral systems are that it is possible to tamper with the database of considerable opportunities. The aspect of security and transparency is a threat from a still widespread election with the conventional system (offline). Unlike the electoral system, there are many conventional uses of paper in its implementation. The best way to overcome the difficulty faced is by decentralizing the system used for elections. This can be achieved by making use of Blockchain technology, the entire database is owned by many users in a blockchain. Blockchain itself has been used in the Bitcoin system known as the decentralized Bank system. By adopting blockchain in the distribution of databases on e-voting systems can reduce one of the cheating sources of database manipulation. Unlike Bitcoin with its Proof of Work, this paper proposes a method based on a hyper ledger to enable voting.

Keywords— *E-voting, Blockchain, Hyperledger*

1. INTRODUCTION

The security of an election in a democratic country is a matter of national interest. The voting system currently is working on pen and paper scheme. Replacing the conventional pen and paper system with a new election system is critical to limit fraud and having the voting process attributable and verifiable. The security fields of the modern era using the advanced technologies and cryptographic procedures are studying the possibilities of electronic voting schemes [1], which can minimize the cost of having a national election while assuring the security conditions of an election.

A blockchain is an immutable, distributed incontrovertible, public ledger. Some of the main features are:

(a) Ledger is present in numerous sites.
(b) There is distributed control over who can append new transactions to the ledger
(c) The anticipated "fresh block" to the ledger must refer the previous version of the ledger, thus forming an immutable chain from where the blockchain has its name and thus preventing altering with the integrity of previous entries.
(d) A majority of the network nodes must reach a consensus before a proposed new block of entries becomes a permanent part of the ledger.

These features function through advanced cryptography, which has a security level that is better than any database known to us. The blockchain technology is therefore considered by many [3], to be the perfect tool, used to create the upcoming contemporary democratic voting process. This paper evaluates the use of blockchain as a service to implement an Electronic Voting (e-voting) system. This paper makes use of permission blockchain to enable electronic voting.

2. USE CASES

In India, there are millions of military personals eligible to vote but are not able to make to it to the constituencies to cast their votes because of the difficulty in travelling to their respective constituencies. Non-Resident Indians (NRI) also face the same difficulty in casting their votes; they can make use of electronic voting technology to cast their votes. This resolves the problem of voters to travel a long distance to cast their votes.

3. PRELIMINARIES OF E-VOTING AND BLOCKCHAIN

This section explains the liquid democracy and its design consideration.

3.1 Democratic design reflections

In a fluid democracy at any given time the voter has the power, to assess the way his vote was cast in terms of a specific legislative proposal or a bill. This allows people with domain-specific knowledge to better influence the outcome of decisions, which results in better governance. The concept of fluid

© 2019, www.IJARIIT.com All Rights Reserved

democracy could be a possible answer to public requests, but there are certain social and technical barriers in the way. Below, we specify our envisioned essential requirements that need to be fulfilled by an electronic voting system in order for it to effectively be used in a national election:

(a) An election system should not enable traceability of a vote to a voter's identifying credentials.
(b) An election should not enable pressurized voting
(c) An election system should ensure and proof to a voter, that the voter's vote, was counted, and counted correctly.
(d) An election system should not enable control to a third party to tamper with any vote.
(e) An election system should not enable a single entity control over tallying votes and determining the result of an election.
(f) An election system should only allow eligible individuals to vote in an election.

3.2 Blockchain as a solution for electronic voting

In the year 2008, the blockchain technology was introduced by Satoshi Nakamoto, he created the first cryptocurrency called Bitcoin. The Bitcoin blockchain technology uses a decentralized public ledger combined with PoW (Proof-of-Work) based stochastic consensus protocol, with financial incentives to record a totally ordered sequence of blocks, the blockchain.

There are several types of Blockchain [7] that are:

- Permissionless Blockchain or public blockchain, like Bitcoin or Ethereum, all can be a user or run a node, anyone can "write", and anyone can participate in a consensus in determining the state's validity.
- Permission Blockchain is inversely proportional to the previous type, operated by known entities such as consortium blockchains, where consortium members or stakeholders in a particular business context operate a Blockchain permission network. This Blockchain permission system has means to identify nodes that can control and update data together, and often has ways to control who can issue transactions.
- Private Blockchain is a special blockchain permitted by one entity, where there is only one domain trust.
- In Bitcoin, each contract is considered its hash value and entered into a database called Blockchain as defined in figure 1. To join between one block with another block, the hash value of the preceding block introduced into the next block then calculated its hash value. The hash value must meet a few necessities called difficulty in order to be considered a legitimate block. Looking through for hash values that match those requirements is called Proof of Work. Bitcoin eatables all transaction material in a database called blockchain in the internet network. Blockchain consists of numerous blocks associated with each other and in order as shown in figure 1 the blocks are related because the hash values of the preceding block are used in the subsequent block formation process. The effort to transform the information will be more challenging because it must change the subsequent blocks. The first block is called the genesis block.

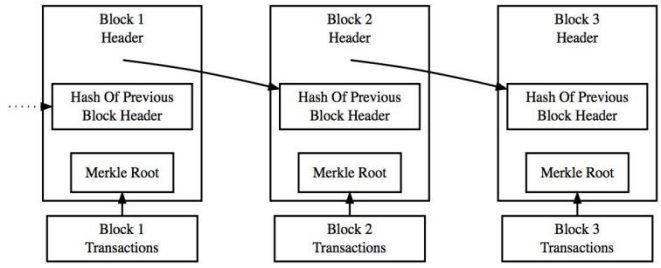

Fig. 1: Blockchain illustration

3.3 Hyperledger composer

In this, we have used a permission blockchain identified as Hyperledger composer. Hyperledger composer is a framework for mounting and deploying blockchain business networks. Composer is constructed on top of hyper ledger fabric blockchain Infrastructure.

Hyperledger fabric is ready for enabling consortium blockchains with different degrees of permissions. Fabric heavily depends on a smart contract system called Chaincode, which all peers of the network run in Docker containers. [xx] The fabric allows enterprises to make portions of the blockchain, if not all, permission. Participants who have authorization can join and issue transactions on a Fabric based blockchain. A most significant aspect of Fabric is the split-up between so-called "Endorsers" and "Consensus Nodes" unlike cryptocurrencies like Bitcoin you can't identify the split-up between miners and nodes. The Endorsers have the state and can form, validate and broadcast transactions or chaincode, while the Consensus Nodes orders the already validated transactions. This enables Fabric to implement a better division of labour so that not every peer of the network has to do every job.

The fabric allows the user to define assets from client side and use them with the Fabric Composer without any crypto-currencies involved in the transaction. Fabric's Chaincode Smart Contracts framework is similar to Ethereum.

Chaincode defines the business logic of assets, the rules for evaluation and altering the so-called state of the assets. Other than the public blockchains of cryptocurrencies Fabric allows participants to build a distinct channel for their assets and therefore insulate and segregate transactions and a ledger. With this system, the chaincode wanted to read and alter the state of an asset will only be installed on peers involved in this certain business case. Like in good chat programs Fabric's blockchains allow the user to take part in both open and private interactions.

4. DESIGN

The following are the key activities in the election process:

4.1 Election creation

Election superintendents will use an admin election decentralized application. This decentralized application interacts and initiates the chain-code to all peers in the network, the election administrator can add the list of candidates onto the block-chain when the election is formed, and each participant is given the authorization to interact with his corresponding ballot chain-code.

4.2 Voter registration

The recording of voter phase is conducted by the election administrators. When an election is formed the election administrators must outline a deterministic list of eligible voters. This requires a component for a government identity verification service to securely authenticate and approve eligible individuals. Using such verification services, each of the eligible voters should have a voter ID and email address.

4.3 Vote transaction

An individual votes using a decentralized application, the voter interacts with another peer who simulates and execute the chaincode and state is forwarded to Ordering node which verifies and appends the vote to the blockchain if consensus is reached.

© 2019, www.IJARIIT.com All Rights Reserved

Each vote is stored as a transaction on the blockchain whereas each individual voter receives the transaction ID for their vote for verifying purposes (see "Verifying vote" section). Each transaction on the blockchain holds information about which candidate was voted, Each vote is appended onto the blockchain by its corresponding chaincode, if and only if Ordering and peer node agree on the verification of the vote data. As can be seen in Table I, a single transaction on the public Ethereum blockchain includes the transaction ID, the block which the transaction is located, the age of the transaction, the wallet which sent the transaction and who received it, the total value which was sent and the transaction fee. A transaction in our proposed system doesn't require all of this information, a single transaction only has information of the transaction ID, and which candidate was selected. Finally, the value of the transaction is the data which was selected to cast, therefore a vote in our system reveals no information about the individual voter who casted this particular vote.

Table 1: Example of a public transaction (Ethereum)

TxHash	Block	Age	From	To	Value	[TxFee]
0xdead...	1337	33 sec ago	0xbeef...	Token	10 Ether	0.087
0xface...	1337	33 sec ago	0x4242...	0x1234...	1 Ether	0.056

Source: Blockchain based e-voting system by Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson [5].

Table 2: Example of a transaction in our system

Transaction ID	political party	Timestamp
2ad174a5b408c1dd1ad0e37 495bbb833dce7feac4ce5db b7105bd7223077d4d1	Nota	2019-04-28T22:34:57.975Z

4.3.1 Tallying results: The tallying of the election is done on the fly in the smart contracts. Each ballot chain code does their own tally for their corresponding location in its own storage. When an election is over, the final result for each chain code is published.

4.3.2 Verifying vote: As was mentioned earlier, each individual voter receives the transaction ID of his vote. The transaction ID can be used to verify His/her vote.

5. IMPLEMENTATION

5.1 Model file

A model file in Hyperledger Composer consists of data schema of the project. The model file defines participants, assets and transactions involved in the process.

```
namespace org.example.evoting

participant voter identified by voterID {
  o String voterID
  o String email
}

asset ifVoted identified by voterID {
  o String voterID
  o Boolean votedOrNot
}

asset candidateVote identified by politicalParty {
  o String politicalParty
  o Integer totalVote
}
transaction vote {
  --> candidateVote candidateVoteAsset
  --> ifVoted ifVotedAsset
}
```

Fig. 2: Model file

5.2 Chaincode

Chaincode is the transaction logic simulated and executed by each peer in the organization. In this paper, we have implemented a simple voting logic.

```
'use strict';

/*
  Voting transaction
  @param {org.example.evoting.vote} vote
  @transaction
 */
function vote(tx) {
    if (!tx.ifVotedAsset.votedOrNot) {
        tx.candidateVoteAsset.totalVote = tx.candidateVoteAsset.totalVote + 1;
        return getAssetRegistry('org.example.evoting.candidateVote')
            .then(function (assetRegistry) {
                return assetRegistry.update(tx.candidateVoteAsset);
            })
            .then(function () {
                return getAssetRegistry('org.example.evoting.ifVoted')
                    .then(function (assetRegistry) {
                        tx.ifVotedAsset.votedOrNot = true;
                        return assetRegistry.update(tx.ifVotedAsset);
                    })
            });
    } else {
        throw new Error('Vote already submitted!');
    }
}
```

Fig. 3: Chain code

This code takes vote asset which is defined in model file and checks whether the voter has voted or not. Voter chooses candidate total vote gets incremented by 1.

5.3 Transaction process

Every vote in this proposed model is a transaction.

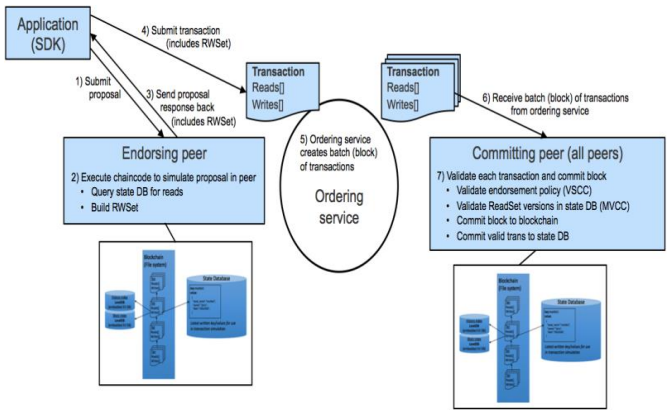

Fig. 4: Transaction process

Source: IBM Hyperledger Developers: Sharon Cocco and Gari Singh.

(a) Voter submits his vote transaction through application SDK.Application sends a proposal to append to the blockchain through endorsing peers in the network.

(b) Endorsing peers accept the proposal and simulate the request using docker engine and execute the chaincode, it also queries state DB for reads and builds Read-Write set for the transaction.

(c) Endorsing peer sends back the proposal to application SDK including RW head.

(d) Application SDK then sends the transaction to ordering node.

(e) Ordering node creates a batch of transactions, which transaction comes after which transaction. In this paper, there is no need for batching of transactions.

(f) Committing Peer does the following Tasks:

- Validate Endorsement policy.
- Validate read set in stateDB.
- Commit to the blockchain.
- Commit valid transaction in State DB.

6. CONCLUSION

The idea of adapting digital voting systems to make the public electoral process cheaper, faster and easier, is a compelling one

© 2019, www.IJARIIT.com All Rights Reserved

in modern society. Making the electoral process cheap and quick normalizes it in the eyes of the voters, removes a certain power barrier between the voter and the elected official and puts a certain amount of pressure on the elected official. It also opens the door for a more direct form of democracy, allowing voters to express their will on individual bills and propositions.

In this paper, we introduced a unique, blockchain-based electronic voting system that utilizes chain code to enable secure and cost-efficient election while guaranteeing voters privacy. We have outlined the systems architecture and design. By comparison to previous work, we have shown that the blockchain technology offers a new possibility for democratic countries to advance from the pen and paper election scheme, to a more cost- and time-efficient election scheme, while increasing the security measures of the today scheme and offer new possibilities of transparency. Using a Hyperledger permissioned blockchain, it is possible to send thousands of transactions per second onto the blockchain, utilizing every aspect of the chain code to ease the load on the blockchain.

7. REFERENCES

[1] Sos.ca.gov.(2007).Top-to BottomReview|CaliforniaSecretaryofState. Availableat:http://www.sos.ca.gov/elections/voting-systems/oversight/ top-bottom-review/.

[2] Nicholas Weaver. (2016). Secure the Vote Today. Available at:https:// www.lawfareblog.com/secure-vote-today.

[3] TechCrunch, (2018). Liquid democracy uses blockchain to fix politics, and now you can vote for it [Online]. Available at: https://techcrunch. com/2018/02/24/liquid-democracy-uses-blockchain/

[4] Geth.ethereum.org. (2018). Go Ethereum. Available at: https://geth.ethereum.org/

[5] Vitalik Buterin. (2015). Ethereum White Paper. Available at: https:// github.com/ethereum/wiki/wiki/White-Paper.

[6] Nca.tandfonline.com. (2015). Pirates on the Liquid Shores ofLiberal Democracy: Movement Frames of European Pirate Par- ties. [Online]. Available at: https://nca.tandfonline.com/doi/abs/10.1080/13183222.2015.1017264#.Wr0zCnVl8YR

[7] Feng Hao, P.Y.A. Ryan and Piotr Zielinski. (2008). Anonymous voting by two-roundpublicdiscussion.

[8] Feng Hao and Piotr Zielinski. A 2-Round Anonymous VetoProtocol Available at http://homepages.cs.ncl.ac.uk/feng.hao/files/av_net.pdf.

[9] Blockchain-Based E-Voting System by Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson School of Computer Science Reykjavik University, Iceland {fridrik14, gunnlaugur15}@ru.is

[10] Patrick McCorry, Siamak F. Shahandashti and Feng Hao. (2017). A Smart Contract for Boardroom Voting with Maximum Voter PrivacyAvailable at:https://eprint.iacr.org/2017/110.pdf.

[11] Ronald Cramer, Rosario Gennaro and Berry Schoenmakers. A Secure and Optimally Efficient Multi-Authority Election Scheme Available at:http://www.win.tue.nl/~berry/papers/euro97.pdf

[12] Jonathan Alexander, Steven Landers and Ben Howerton (2018). Net vote: A Decentralized Voting Network Available at https://netvote.io/wp-content/uploads/2018/02/Netvote-White-Paper-v7.pdf.Agora(2017).Agora: Bringingourvotingsystemsintothe21stcentury

[13] Available at: https://agora.vote/Agora_Whitepaper_v0.1.pdf

[14] Kirill Nikitin, Kokoris-Kogias, Philipp Jovanovic, Linus Gasser, Nico- las Gailly, Ismail Khoffi, Justin Cappos and Bryan Ford (2017). CHAINIAC: Proactive Software-Update Transparency via CollectivelySigned Skip chains and Verified Builds Available at https://www.usenix. org/system/files/conference/usenixsecurity17/sec17-nikitin.pdf

[15] Alin Tomescu and Srinivas Deva das (2017). Catena: Efficient Non- equivocation via Bitcoin Available at https://people.csail.mit.edu/ alinush/papers/catena-sp2017.pdf

[16] Michael Del Castillo (2018). Sierra Leone secretly Holds First Blockchain-AuditedPresiden- trial Vote Available at: https://www.coindesk.com/ sierra-leone-secretly-holds-first-blockchain-powered-presidential-vote/

[17] Ethereum Blog. (2018). On Public and Private Blockchains-Ethereum Blog. Available at: https://blog.ethereum.org/2015/08/07/ on-public-and-private-blockchains/

[18] Bitfury.com. (2018). Digital Assets on Public Blockchains Available at http://bitfury.com/content/5-white-papers-research/bitfury-digital_ assets_on_public_blockchains-1.pdf

[19] Steve Ellis, Ari Juels and Sergey Nazarov. (2017). ChainLink: A Decentralized Oracle Network Available at https://link.smartcontract.com/ whitepaper.

© 2019, www.IJARIIT.com All Rights Reserved