International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 6 June 2021, pp: 1068-1071 www.ijaem.net ISSN: 2395-5252

Blockchain-Based E-Voting System

Ms Vrushali S. Sakharkar, Mr.Prashant V.Jawale, Ms.Riya V.Mishra

PRMIT&R. BadneraPRMIT&R. Badnera
Department of Computer Science and Engg.
Department of Computer Science and Engg.
PRMIT&R. Badnera Department of Computer Science and Engg.

Submitted: 01-06-2021 Revised: 14-06-2021 Accepted: 16-06-2021

ABSTRACT

Democratic voting is a crucial and serious event in any country, the current voting scheme in any country is through ballot paper or by use of EVM. These processes have many drawbacks such as transparency, low voter turn-out, tampering of votes, distrust in the election body, forging of unique Id (voter id card), delay in giving out results and the most important is security issues. One way the security issues can be potentially solved is through the use of Blockchain Technology. Blockchain with smart contracts emerges as a promising candidate for building a safer, secure and transparent E-Voting Systems. Here we have tested and implemented a sample e-voting application using open-source, Blockchain-based, decentralized software platform through wallets and the Solidity language. Here we have also highlighted the pros and cons of using Blockchain Technology and also demonstrated a practical system by showcasing a web application for voting and its limitations.

Keywords : Blockchain Technology, E- Voting System, Decentralization, etc.

I. INTRODUCTION

Blockchain technology originates from the underlying architectural design of the cryptocurrency bitcoin. The software programs enforced by smart contracts are written into the smart contracts and are immutable. They can work properly, autonomously and transparently forever, without any external stimuli. Each block has a transaction data part, copies of each transaction are hashed, and then the hashes are paired and hashed again, this continues until a single hash remains.The block header is where the merkle root is stored. To ensure that a transaction cannot be modified each block also keeps a record of the previous blocks header. A blockchain is designed to be accessed across a peer-to-peer network, each node/peer then communicates with other nodes for block and transaction exchange

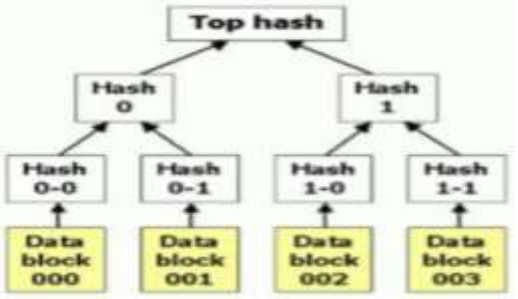


FIG 1.1 HASH TABLE

Once connected to the network, peers start sending messages about other peers on the network, this creates a Decentralized method of peer discovery. The initial block download makes the new node download and validate all blocks from block 1 to the most current Blockchain, once this is done the nodeis considered to be synchronised.

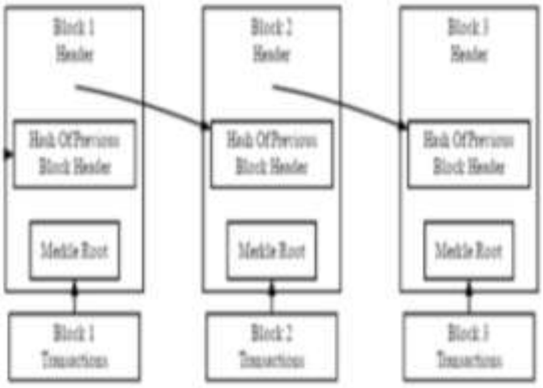


FIGURE-1.2 SIMPLIFIED BITCOIN BLOCKCHAIN

II. PRELIMINARIES OF E-VOTING AND BLOCKCHAIN

A Liquid Democracy Design Considerations. The main idea in a liquid democracy is that the voter has the power,

Here is thelist of our envisioned essential requirements that should fulfilled by an E- Voting

System in order for it to effectively be used in a National Elections :

- An election system should not enable coerced voting.
- An election system should not enable traceability of a vote to a voters identifying credentials.
- An election system should ensure and proof to a voter, that the voters vote, was counted, and counted correctly.
- An election system should not enable control to a third party to tamper with any vote. (v) An election system should not enable a single entity control over tallying votes anddetermining an elections result.

III. BLOCKCHAIN AS A SERVICE FOR E-VOTING

We have considered an existing Electronic Voting Systems, a Non-BlockchainA. Election as a Smart Contract:

➢ **Election Roles :** Elections in our proposal enable participation of individuals or institutions in the following roles.

♦ **Election Administrators**: The election administrators specify the election type and create aforementioned election, configurate ballots, register voters, decide the lifetime of the election and assign permissioned nodes.

♦ **Voters:** For elections to which they are eligible for, voters can authenticate themselves, load election ballots, cast their vote and verify their vote after an election is over. Voters can be rewarded for voting with tokens when they cast their vote.

♦ **District Nodes:**When the election administrators create an election, each ballot smart contracts, representing each voting district, are deployed onto blockchain.

➢ **Election process:**In our work, each election process is represented by a set of smart contracts, which are instantiated on the blockchain by the election administrators.

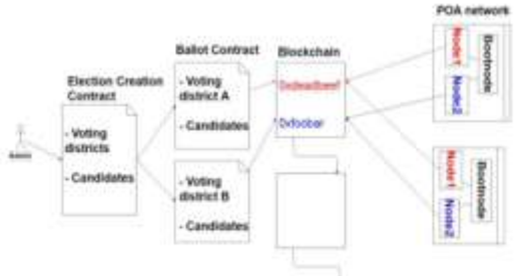


FIG.2.1 ELECTION AS A SMART CONTRACT

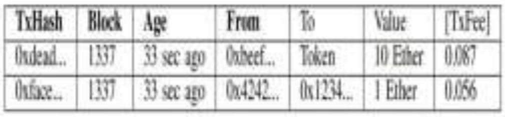
Smart Contract:A smart contract is defined for each of the voting districts of the election so multiple smart contracts are involved in an election.

♦ **Election creation:** Election administrators create election ballots using a decentralized app(dApp). This decentralized app interacts with an election creation smart contract, in which the administrator defines a list of candidates and voting districts.

♦ **Voter Registration**:Using such verification services, each of the eligible voter should have an electronic ID and PIN number and information

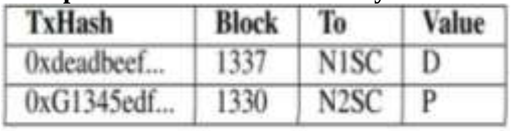
♦ **Vote transaction**: When an individual votes at a voting district, Each vote is stored as a transaction on the blockchain whereas each individual voter receives the transaction ID for their vote for verifying purposes. Each vote is appended onto the blockchain by its corresponding ballot smart contract, if and only if voter casts his vote, the weight of their wallet is decreased by 1, therefore not enabling them to vote more than once per election

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

Example of a transaction in our system



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

♦ **Tallying results:**Each ballot smart contract does their own tally for their corresponding location in its own storage. When an election is over, the final result for each smart contract is published.

♦ **Verifying vote:** Each individual voter can go to his government official and present their transaction ID after authenticating himself using his electronic ID and its corresponding PIN.

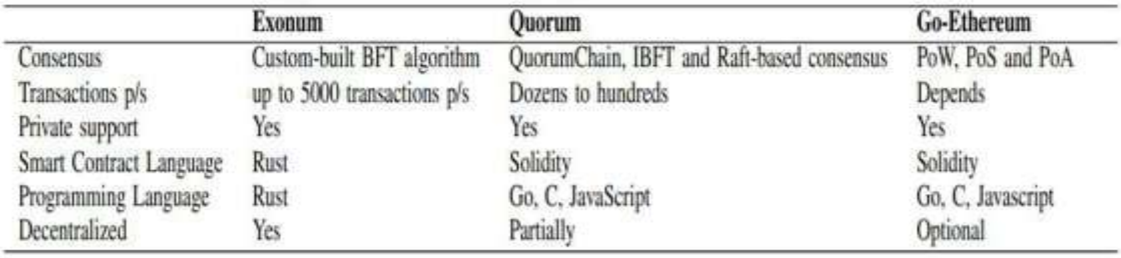
➢ **Evaluating Blockchain as a Service for E-Voting :**

There are three different blockchain frameworks that we consider for implementing and deploying our election smart contracts. Exonum, Quorum And Geth.

♦ **Exonum:**Looking at the Exonum blockchain, it is robust end to end with its full implementation done with the programming language Rust. It is built for private Blockchains.

- **Quorum:**Is an Ethereum-based distributed ledger protocol with transaction/contract privacy and new consensus mechanisms. It's a Geth fork and is updated in line with Geth releases. Quorum changed up the consensus mechanism and aimed more towards consortium chain based consensus algorithms.
- **Geth:** Go-Ethereum or Geth is one of three orginal implementations of the Ethereum protocol and it runs smart contract applications exactly as programmed without possibility of downtime, censorship, fraud or third party interference.

FIG : Framework Evaluation



	Exonum	Quorum	Go-Ethereum
Consensus	Custom-built BFT algorithm	QuorumChain, IBFT and Raft-based consensus	PoW, PoS and PoA
Transactions p/s	up to 5000 transactions p/s	Dozens to hundreds	Depends
Private support	Yes	Yes	Yes
Smart Contract Language	Rust	Solidity	Solidity
Programming Language	Rust	Go, C, JavaScript	Go, C, Javascript
Decentralized	Yes	Partially	Optional

IV. DESIGN AND IMPLIMENTATION

Implementation (Implementation include various phase such as):

1. Registration : The voter has register using voted id and moblie number
2. Login : The voter can login using authontication OTP
3. Database: User data is stored in database. Details like name, gender, Unique Id
4. Result phase: The processing and tallying of votes is done in results phase. Results are generated and displayed on website. Users can verify their votes using their own public key.

V. SECURITY ANALYSIS AND LEGAL ISSUES

➢ **SECURITY ANALYSIS:**

- **DDoS:** TosuccessfullyDDosadistributedsystemtheattackermustDDoS every singlebootnode in the private network. Each node is implemented with a Byzantine fault tolerance algorithm, which helps locating failed nodesinthe system
- **Authentication Vulnerability:**Eachindividual isidentified and authenticated by the systembypresenting an electronic ID and the corresponding 6-digit PIN in the voting booth.

➢ **LEGAL ISSUES:**

- **Remote Voting:**Remote elections provide no coercion resistance because of the non supervised factor in a remote election. Remote elections can therefore not guarantee the privacy that people have when they cast their vote in a voting booth.
- **Transparency**: In the today's election scheme, no method of transparency. there is no guarantee from the scheme that his vote was counted and counted correctly. Any individual vote can be misplaced, counted incorrectly because ofhuman error.
- **Voter Privacy:** In every pen and paper election scheme, voters privacy is a key element. The law forbids any individual or entity to be able to know from a single vote, who gave aforementioned vote.

VI. CONCLUSION

The idea of adapting digital voting systems to make the public electoral process cheaper, faster and easier, is a compelling one 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. A unique, Blockchain-Based Electronic Voting System that utilizes smart contracts to enable secure and cost efficient election while guaranteeing voters privacy. 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.

REFERENCES

[1]. Nir Kshetri, Jeffrey Voas, “Blockchain-Enabled E-Voting”.

[2]. G. Wood, "Ethereum: a secure decentralised generalised transaction ledger", Ethereum Project Yellow Paper, vol. 151, pp. 1-32, 2014.

[3]. C.D. Clack, V.A. Bakshi, and L. Braine, “Smart contract templates: foundations, design landscape and research directions”, Mar 2017, arXiv:1608.00771.

[4]. U.C. Çabuk, A. Çavdar, and E. Demir, "E-Demokrasi: Yeni Nesil Doğrudan Demokrasi ve Türkiye’deki Uygulanabilirliği", [Online]

[5]. "Final report: study on eGovernment and the reduction of administrative burden (SMART 2012/0061)",2014.

[6]. F. Hao and P.Y.A. Ryan, Real-World Electronic Voting: Design, Analysis and Deployment, CRC Press, pp. 143-170, 2017.

[7]. N. Braun, S. F. Chancellery, and B. West. "E-Voting: Switzerland's projects and their legalframework–In a European context", Electronic Voting in Europe: Technology, Law, Politics and Society. Gesellschaft für Informatik, Bonn, pp.43-52, 2004.