Blockchain Based E-Voting

Ravindra Ghugare[1], Ashish Patil[2], Ritesh Gunjal[3], Shubham Shewale[4]
[1, 2, 3, 4] Dept of Computer Engineering
[1, 2] Bharati Vidyapeeth College of Engineering, Navi Mumbai, Maharashtra

Abstract- *In every democracy, the security of an election is a matter of national security. Replacing the traditional pen and paper or EVM scheme with a new election system is critical to limit fraud and having the voting process traceable and verifiable. Blockchain-enabled e-voting could reduce voter fraud and increase voter access. Eligible voters cast a ballot anonymously using smart phones or laptops over internet. To use a digital-currency analogy, BEV issues each voter a "digital wallet" containing a user credential. Each voter gets a single "coin" representing one opportunity to vote. Casting a vote transfers the coin to a candidate's wallet from voter's wallet. A voter can spend his or her coin/token only once. BEV employs an encrypted key and tamperproof personal IDs. Blockchain technology is supported by a distributed network and contains large number of interconnected nodes. Each of these nodes have replica of the distributed ledger that contains the full history of all transactions the network has processed. Advantages of e-voting using blockchains includes: i) greater transparency, ii) inherent anonymity, iii) security and reliability and iv)immutability.*

Keywords- BEV, coin, digital wallet, distributed ledger, EVM, immutability

I. INTRODUCTION

Voting, whether traditional ballet based or electronic voting machine based, is what modern democracies are built upon.E-Voting the key public sectors that can be Implemented by blockchain technology. The idea in blockchain-enabled e-voting (BEV) is simple. To use a digital-currency analogy, BEV issues each voter a "wallet" containing a user credential. Each voter gets a single "coin" representing one opportunity to vote. Casting a vote transfers the coin/token to a candidate's wallet from voter's wallet. For a robust e-voting scheme, a number of functional and security requirements are specified including accuracy, transparency, system and data integrity, auditability, secrecy, availability, and distribution of authority. Electronic voting machines have been viewed as flawed, by the security community, primarily based on physical security concerns. Anyone with physical access to such machine can sabotage the machine, thereby affecting all votes cast on the aforementioned machine.

Blockchain technology is supported by a distributed network and consists large number of interconnected nodes. Each of these nodes has their own copy of the distributed ledger that contains the full history of all transactions the network has processed. Each node controls the network. If the maximum nodes agree, they accept a transaction.

This new technology works through four main features:

i. The ledger exists in many different locations: No single point of failure in the maintenance of the distributed ledger.
ii. There is distributed control over who can append new transactions to the ledger.
iii. Any proposed "new block" to the ledger must reference the previous version of the ledger, creating an immutable chain from where the blockchain gets its name, and thus preventing tampering with the integrity of previous entries.
iv. 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 technological features operate through advanced cryptography (like SHA-256 hashing algorithm), providing a security level equal and/or greater than any previously known database. The blockchain technologies therefore considered by many, including us, to be the ideal tool, to be used to create the new modern democratic voting process.

What is Blockchain?

Blockchain was first introduced in Bitcoin(crypto currency) by Satoshi Nakamoto, who developed a peer-to-peer online payment system that allows online transactions through the Internet without relying on any third-party payment gateways. Blockchain is secure by design with a high byzantine failure tolerance.A blockchain stores each transaction in a block, the block eventually becomes completed as more transactions are carried out. Once complete it is then added in a chronological order to the blockchain.Blockchain was first implemented in Bitcoin application which is a currency that could be exchanged over the Internet relying only on cryptography to secure the transactions. Blockchain is an ordered data structure that contains transactionhistory. Each block in the

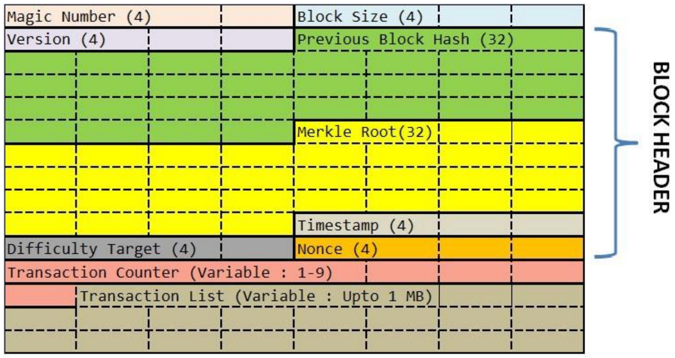


Fig. 1 Block Structure

chain is linked to the previous block in the chain using its hash value. The first block in the chain is referred as the foundation of the stack. Each new block created gets connected to the previous block to form a stack called a Blockchain.

II. BLOCKCHAIN AS A SERVICE FOR E-VOTING

In this paper, we consider existing electronic voting systems, blockchain-based and non-blockchain-based, and evaluate their respective feasibility for implementing a national e-voting system. Based on this, we devised a blockchain-based electronic voting system, optimizing for the requirements and considerations identified. In the following subsection, we start by identifying the roles and component for implementing an e-voting smart contract then, we evaluate different blockchain frameworks that can be used to realize and deploy the election smart contracts. In the last subsection, we will discuss the design and architecture of the proposed system.

Design Properties Security properties BEV system should hold:

• **Fairness:**Results should be available after completion of voting process. It ensures that the remaining voters are not influenced.
• **Eligibility:**Eligible voters are allowed to cast their votes only once. It is based on authentication. since voters need to prove their identity using user credentials.
• **Privacy:**Each vote is kept hidden from other voters. This property in non-electronic voting schemes is ensured by physically protecting the voter from prying eyes.
• **Verifiability:** This property guarantees that all parties involved have the ability to check whether their votes have been counted or not. Typically, two forms of verifiability are defined, individual and universal verifiability. Voter can track his vote whether it is considered or not.
• **Coercion-resistance:**Each voter should record vote as they are instructed to.

Election as a Smart Contract

Let’s first understand what does smart contract means. Smart contracts help you interchange money or property or shares, in a conflict freeway avoiding a middleman’s work.

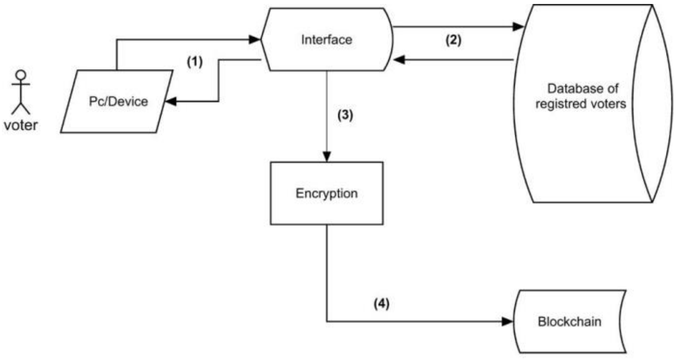


Fig. 2 The Voting Process

Says the best way to describe smart contracts is with the example, let’s consider that you have to transfer the money to another person you can’t send it to him directly because on later he can also deny that he didn’t receive money so there is a middleman required to approve the transaction and that transaction is approved by bank here bank acts as a middleman. But in the blockchain, there is no need of a middleman the smart contract and the nodes on the network do the work of a middleman.

1. *Election Roles:*

Elections in a proposal which enables individualsor an administrator to enrol themselves in the following role as per where multiple individuals (Voters) can be enrolled in the same role.

i. **Administrators:**Administrator plays an important role in an election who manages the whole lifecycle of an election. Multiple numbers of the institute can enrol as an administrator role and can specify the election type and create an election also configure ballot register voters and decide the lifecycle of an election (i.e. for how many hours the election window will be open).
ii. **Voters:**The voters should be authenticated first and then only allow for the election. After that, the voter's can say load election ballots, cast their vote and verify their vote after an election is over.
iii. **District nodes:** When the election administrators create an election, each ballot smart contracts, will

act as an individual voting district, which is deployed on the blockchain. When a ballot smart contracts are created, each of the equivalent district nodes is given the authorization to interact with their corresponding vote smart contract. When an individual voter casts his vote from his smart contract, the vote data gets verified by all of the corresponding district nodes and every vote they agree on are attachedto the blockchain.

iv. **Bootnodes:** Each association, with permission access to the network, will host a unique bootnode. A bootnode helps the district nodes to determine each other and communicate. The bootnodes do not keep any state of the blockchain and are ran on a static IP so that district nodes find its peers faster.

2. ***Election Process:*** In our survey, the election process has been represented using smart contracts, which are characterized on the blockchain by the administrators. As there is a number of the district in an election and each has their respective smart contract. For each voter with its equivalent district location, defined in the voter'sregistration phase, the smart contract with the equivalent location will be prompted to the voter after the user validates himself when voting. There are some main activities in an election process they are as follows:

i. **Election formation:** Administrators creates an election ballot using a decentralized app. This decentralized app will interact with a smart contract, in which the administrator can define a number of candidates and voting districts.This smart contract creates a set of ballot smart contracts and deploys them onto the blockchain, with a list of the candidates, for each voting district, where each voting district is a factor in each ballot smart contract. When the election is created, each equivalent district node is given the authorization to interact with his equivalent ballot smart contract.

ii. **Voter registration:**The registration of a voter is directed by the administrators. When an election is formed the administrators must define a list of eligible voters. This requires a component for a government identity verification service or a biometric scan of a voter to securely authenticate and authorize eligible voter.With such verification services, each of the eligible voters should have an electronic ID and PIN and information on what voting district the voter is located in. For each eligible voter, an equivalent wallet should be generated for the voter.The wallet generated for each individual voter should be inimitable for each election the voter is eligible for and a non-interactive zero-knowledge proof could be integrated to generate such wallet so that the system itself does not know which wallet matches an individual voter.

iii. **Vote transaction:** When a discrete voter votes at a voting district, the voter interacts with a ballot smart contract with the same voting district where a respected voter has been registered. This smart contract will interact with the blockchain his equivalent district node, which attaches the vote to the blockchain if an agreement is reached between the majorities of the parallel district nodes. 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 transaction on the blockchain holds information about whom was voted for, and the location of the above-mentioned vote. Each vote is attached to the blockchain by its equivalent ballot smart contract, if and only if all corresponding district nodes agree on the verification of the vote data. When a voter casts his vote, the weight of their wallet is decreased by 1, therefore not enabling them to vote more than once per election. The age of a single transaction is omitted to protect individual voters from a timing attack.

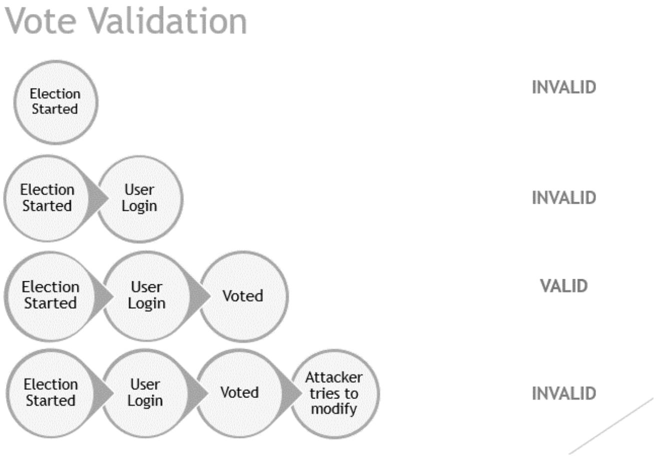


Fig.3 Vote Validation

iv. **Vote Validation:**After the whole process is completed the voting commission start the vote validation process. In vote validation, we check for the number of blocks in each chain. If number of blocks in chain is less than 3 then it is considered as the user didn’t voted and the chain is incomplete. If the number of blocks in the chain is greater than 3 then it is considered as someone tries to manipulate the vote that’s why new blocks are introduced in the chain. If number of blocks in the chain is equals to 3 then it is considered as the correct vote.

Algorithm:

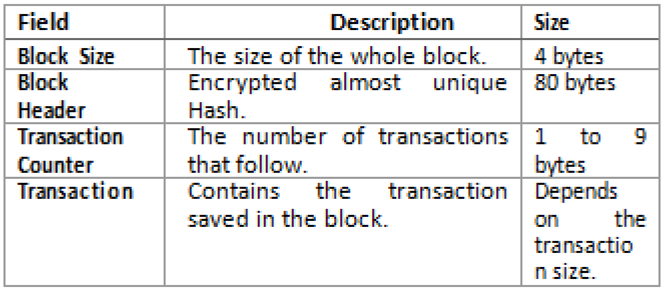
The main aim of blockchain enabled e-voting is to generate blocks, only one block per user and assign that block to the respected user. Each block should be unique and that uniqueness can be implemented by using the token. Token will have unique value, and that unique value will be generated by using the user id and timestamp. Token will be the id to identify each block separately. Here block is used to transfer the votes so by default value of each block will be one. So, the value field will not be there, as it is present in bitcoins.

Structure of Block:

Block will contain 4 fields/values:

1. Token: Token is the unique value
2. Date and time: Timestamp on each block when transaction happened
3. Current Hash: This hash value will indicate current block, it can be considered as location to indicate current block.
4. Previous Hash: It is the hash value which will indicate previous block of the chain.

Once blocks are created all these values are assigned to the block. All these values are constant means once they are assigned no one change them i.e. they are immutable.



Field	Description	Size
Block Size	The size of the whole block.	4 bytes
Block Header	Encrypted almost unique Hash.	80 bytes
Transaction Counter	The number of transactions that follow.	1 to 9 bytes
Transaction	Contains the transaction saved in the block.	Depends on the transactio n size.

Each block in the stack is identified by a current hash value. This hash is generated using the Secure Hash Algorithm(SHA-256)to generate an almost idiosyncratic fixed-size 256-bit hash. The mostly used algorithm was designed by the National Security Agency (NSA) that is SHA-256. It was used as the protocol to secure all federal communications. The SHA-256 will take any size plaintext as an input, and encrypt it to a 256-byte binary value. The SHA-256 is always a 256-bit binary value, and it is a strictly one-way function. The figure 4 below shows the basic logic of the SHA-256 encryption.

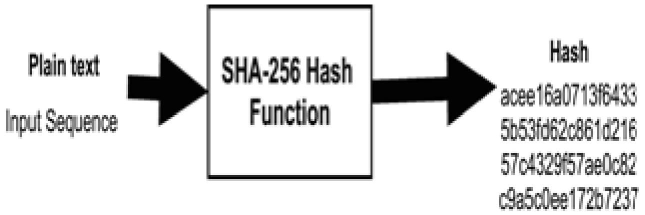


Fig.4 Basic Function of the SHA-256 Hash

Each block header contains hash value that links a block to its previous block in the chain, which creates a chain linked to the very first block ever created and it is referred to as the foundation. Each block is primarily identified by the encrypted hash present in its header. A digital fingerprint that was made combining the both the information concerning the new block created and the previous block in the chain.

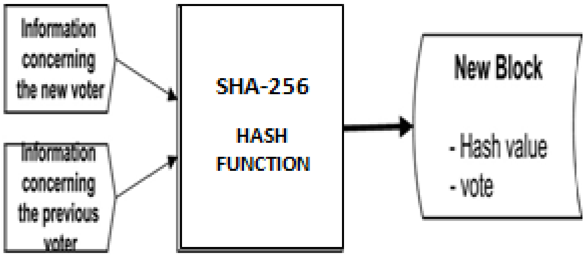

Information concerning the new voter
Information concerning the previous voter
SHA-256
HASH FUNCTION
New Block
- Hash value
- vote

Fig.5 Creation of new Block containing a Hash Value and a Vote

Newly created block is sent over to the Blockchain. The system continuously checks for new incoming blocks and updates the chain when new blocks arrive.

III. CONCLUSION

The main goalto adapt blockchain based 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. In this paper, we introduced a unique, blockchain-based electronic voting system that utilizes smart contracts to enable secure and cost efficient election while guaranteeing voters privacy. We have outlined the systems architecture, the design, and a security analysis of the system. 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 securitymeasures of the todays scheme and offer new possibilities of transparency.

REFERENCES

[1] Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson School of Computer Science Blockchain-Based E-Voting System. Available at: https://skemman.is/bitstream /1946/31161/1/Research-Paper-BBEVS.pdf

[2] Smart Contracts: The Blockchain Technology That Will Replace Lawyers Available at: https://blockgeeks.com/guides/smart-contracts/.

[3] Salanfe, "Setup your own private Proof-of-Authority Ethereum network with Geth", Hacker Noon, 2018. Available at: https://tinyurl.com/ y7g362kd

[4] Bitcoin.org (2009) Bitcoin Developer Guide. Available at: https://bitcoin.org/en/developerguide#block-chain-overview (Accessed: 27 September 2016)

[5] Estonian Ministry of Foreign Affairs (2015) Estonian Internet Voting System. Available at: http://mfa.ee/sites/default/files/contenteditors/2015%20Parliamentary%20elections%20Internet%20voting%20system.pdf (Accessed: 25 September 2016)

[6] E. Kuebler, “Making Voting, Elections Both Secure and Accessible with Blockchain Technology,” Bitcoin Magazine, 11 Jan. 2018; https: //bitcoinmagazine.com/articles/making -voting-elections-both-secure-and -accessible-blockchain-technology

[7] Don Tapscott and Alex Tapscott, Blockchain Revolution published in 2016

[8] William Mougayar, The Business Blockchain: Promise, Practice and Application of the next internet technology, published in 2016