# Electronic Voting System Based on Blockchain-II

**Limje Chinmay Anil[1], Pawar Naman Keshav[2], Chavan Hrushikesh Santosh[3], Adagale Somnath Bhagwan[4]**
[1, 2, 3, 4] Dept of Information Technology
[1, 2, 3, 4] Genba Sopanrao Moze College of Engineering, Balewadi, Pune,

***Abstract***- *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 work-in-progress paper, we evaluate an application of blockchain as a service to implement distributed electronic voting systems. The paper proposes a novel 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. In particular, we evaluate the potential of distributed ledger technologies through the description of a case study; namely, the process of an election, and the implementation of a blockchain based application, which improves the security and decreases the cost of hosting a nation wide election.*

## I. INTRODUCTION

Currently available blockchain-based voting systems have scalability issues. These systems can be used on a small scale. Still, their systems are not efficient for the national level to handle millions of transactions because they use current blockchain frameworks such as Bitcoin, Ethereum, Hyper ledger Fabric, etc. The scalability issue arises with blockchain value suggestions, therefore, altering blockchain settings cannot be easily increased. To scale a blockchain, it is insufficient to increase the block size or lower the block time by lowering the hash complexity. By each approach, the scaling capability hits a limit before it can achieve the transactions needed to compete with companies such as Visa, which manages an average of 150 million transactions per day.

## II. E-VOTING REQUIREMENTS AND COMPLIANCE BY THE

### *A. Eligibility*

All eligible users are required to register using unique identifiers such as government-issued documents to assert their eligibility. In addition to this, our system implements strong authentication mechanism using hashing technology to assert that only authorized voters can access the system. Furthermore, the use of biometrics also enables the system to protect against double voting.

### *B. Receipt Freeness*

The proposed system enables a voter to vote as per their choice and creates a cryptographic hash for each such event (transaction). This is important to achieve verifiability i.e. to verify if a certain vote was included in the count. However, possession of this hash does not allow to extract information about the way voter has voted.

### *C. Convenience*

The system has been implemented using a user friendly web based interface with the voting process requiring minimal input from the user. For instance, hashing is implemented for authentication mechanism to avoid the requirement to remember username/passwords. Furthermore, the overall process is integrated which enables the user to interact with it in a seamless manner.

### *D. Verifiability*

Upon casting their vote successfully, a user is provided with their unique transaction ID in the form of a cryptographic hash. A user can use this transaction ID to track if their vote was included in the tallying process. However, this process does not enable a user to view how they voted which has been adopted to mitigate threats when under duress.

## III. DETAILED DESCRIPTION OF THE LAYERED APPROACH

User Interaction and Front-end Security layer is responsible for interacting with a voter (to support vote casting functions) and the administrator (to support functions pertaining to administering the election process). It encapsulates two key functions i.e. authentication and authorization of the users (voters and administrators) to ensure that the access to the system is restricted to legitimate users in accordance with the predefined access control policies. A number of different methods can be applied to achieve this function ranging from basic username/password to more advanced such as fingerprinting or iris recognition. Therefore

these are rendered specific to individual implementation of the proposed architecture. Overall, this layer serves as the first point of contact with the users and is responsible for validating user credentials as governed by the system-specific policies.

.

*A. Access Control Management layer*

Access Control Management layer is envisaged to facilitate layer 1 and layer 3 by providing services required for these layers to achieve their expected functions. These services include roles definition, their respective access control policies and voting transaction definitions. The role definition and management provides core support for the access control functions implemented by layer 1 whereas the voting transaction definitions support the blockchain based transaction mapping and mining performed at the layer 3. Overall, this layer enables a coherent function of the proposed system by providing the foundations required by individual layers.

*B. E-Voting Transaction Management layer*

e-Voting Transaction Management layer is the core layer of the architecture where the transaction for evoting constructed at Role Management / Transactions layer is mapped onto the blockchain transaction to be mined. This mapped transaction also contains the credentials provided by a voter at layer 1 for authentication. An example of such data can be the ID of the voter. This data is then used to create the cryptographic hash and contributes towards creating the transaction ID. The verification of such credentials is envisioned to be achieved at User Interaction and Front-end Security layer (layer 1). A number of virtual instances of nodes are involved in the process of mining to get this transaction finally enter into the chain.

*C. Ledger Synchronization layer*

Ledger Synchronization layer synchronizes Multichain ledger with the local application specific database using one of the existing database technologies. Votes cast are recorded in the data tables at the backend of the database. Voters are able to track their votes using the unique identifier provided to them as soon as their vote is mined and added into the blockchain ledger. The security considerations of the votes are based on block-chain technology using cryptographic hashes to secure end-to-end communication. Voting results are also stored in the application's database with the view to facilitate auditing and any further operations at a later stage.

*D. The Voting Process*

Typically, a voter logs into the system by providing his/her Unique ID. If the match is found, the voter is then presented with a list of available candidates with the option to cast vote against them. On the contrary, if the match is unsuccessful, any further access would be denied. This function is achieved using appropriate implementation of the authentication mechanism (fingerprinting in this case) and predefined role based access control management. Furthermore, it is also envisioned that a voter is assigned to their specific constituency and this information is used to develop the list of candidates that a voter can vote for. The assignment of voter to a constituency is rendered an offline process and therefore out of scope of this research.

After a successful vote-cast, it is mined by multiple miners for validation following which valid and verified votes are added into public ledger. The security considerations of the votes are based on blockchain technology using cryptographic hashes to secure end-to-end verification. To this end, a successful vote cast is considered as a transaction within the blockchain of the voting application. Therefore, a vote cast is added as a new block (after successful mining) in the blockchain as well as being recorded in data tables at the backend of the database. The system ensures only one-person, one-vote (democracy) property of voting systems. This is achieved by using the voter's unique thumbprint, which is matched at the beginning of every voting attempt to prevent double voting. A transaction is generated as soon as the vote is mined by the miners which is unique for each vote. If the vote is found malicious it is rejected by miners.

After validation process, a notification is immediately sent to the voter through message or an email providing the above defined transaction id by which user can track his/her vote into the ledger. Although this functions as a notification to the voter however it does not enable any user to extract the information about how a specific voter voted thereby achieving privacy of a voter. It is important here to note that cryptographic hash for a voter is the unique hash of voter by which voter is known in the blockchain. This property facilitates achieving verifiability of the overall voting process. Furthermore, this id is hidden and no one can view it even a system operator cannot view this hash therefore achieving privacy of individual voters.

## IV. ETHEREUM BLOCKCHAIN NETWORK

For implementing this proposed work an Ethereum block chain network is used. It is a decentralized open source blockchain network featuring smart contract functionality. In Ethereum platform, the crypto currency used here is Ether (ETH). It uses Proof of Work as the consensus algorithm

where the one who can quickly solve a problem using the computation power can add a new block to the network. The blockchain arrangement takes care of vote tampering problems. [14] used the Ethereum block chain network for online voting application. In blockchain, each and every block is chained with its next block and its previous block. Hence if the hackers tries to access the Block N then it will be notified to Block N+1, and the changes in Block N+1 also reflects in Block N+2 and so on. The hash value of Block N+1 is computer using (1)

**Algorithm 1** Electronic Voting System

**procedure** INPUT:(voter User Id, voter Password)
OUTPUT: Complete vote in the form of blockchain
**BEGIN**
The voter registered with the voting system.
Get the voter ID, choose the password and private key.
**if** (voter Id == registered_voter Id) and (voter is eligible) **then**
Enter your password.
**else**
voter is not registered or he is not eligible.
**if** (Password is correct) **then**
Open the candidate choosing page and choose the candidate.
**else**
Enter the correct password.
Encryption of voting data- $ENCRYPT_{pubkeyUEC}(vote)$
Signing the encrypted data - $SIGN_{Vprikey}(E_{pubkeyUEC}(vote))$
Generation of the block BLOCK(block header+encrypted block data).
Total no. of votes - $\sum_{i=1}^{n} zone_i = \sum_{i=1}^{n}\sum_{j=1}^{k} CL_{ij} = \sum_{i=1}^{n}\sum_{j=1}^{k}\sum_{p=1}^{v} BLOCK_{ijp}$, where n is the total number of zone, k is the total number of college in a particular zone, v is the total number of blocks in a particular college.
**END**

*A. Framework of digital voting system*

The proposed electronic voting system uses the blockchain technology, which is explain in the Algorithm 1. This system is made based on the two concepts: hashing and encryption. Encryption algorithm={AES,DES}, Hash algorithm={SHA-256}, voting server.

## V. ETHEREUM BLOCKCHAIN NETWORK

According to the proposed e-voting system, blockchain will be stored into the voting server.During the data transmission all the related information is stored in the block and this block is secure against different attacks and threats. Somehow, if any user gets the blocks, the attacker is not able to get any meaningful information because all the data will present in hashed and encrypted form.

*A. Voter confidentiality*

To provide the confidentiality of the voter identity, we have used the SHA-256 hash algorithm and encryption algorithm. The information related with the votes is kept in encrypted form. So, that if the block is tempered then also the attacker will not be able to know the vote. Thus, this protocol maintains the voter confidentiality.

*B. Duplication and forgery into the system*

We have created a blockchain to overcome the forgery and duplication cases during the voting. To ensure that no one will able to give two votes, we have used unique voter ID for unique identification. The blockchain contains the hash of the previous block, signature and Merkle root hash. The signature is used to prove the authenticity and integrity of the transaction data. The hash of the previous block is used to maintain the data integrity in the blockchain. The Merkle root hash tells the root (origin) of the voter data. Thus, our proposed e-voting system resist the duplication and forgery issue.

*C. System level threats and attacks*

As discussed before, the proposed e-voting system is based on the encryption and hashing. If an attacker performs any type of attacks into the system, the system will identify and block them. For instance, any attacker performs the data modification attack on one block. The hash of the modified block will change and it will reflect into the whole blockchain. The sybil attack is also not possible because the system will not allow to do duplicate registration or duplicate voting or multiple time voting.

## VI. CONCLUSION

We have mitigated all the possible threats and attacks into the electronic voting system. The proposed work is based on the blockchain technology, which remove all the threats from the communication link. It is a decentralized system, contain hashing and encryption concept for providing the security. Our proposed system ensures that only registered and eligible voter is able to give own votes. Once any voters completed her/his vote, the block will be created, which will be publicly verifiable and spread over the network. After completion of the blockchain no one will do any modification into the block. If an attacker wants to do any modification into the block, the hash value of the block will change and the effect of the modification will reflect into the whole blockchain. The voter has facility to register only once into the system. The voter ID is used for unique verification and checking the eligibility of the user. Thus, our model ensures that one voter gives only one vote, no one will allow to give two votes. The system security analysis shows that the system is more robust and secure against existing attacks.

## REFERENCES

[1] Douglas W Jones. Threats to voting systems. In NIST workshop on threats to voting systems, 2005.

[2] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE transactions on information theory, 31(4):469–472, 1985.
[3] Rifa Hanifatunnisa and Budi Rahardjo. Blockchain based e-voting recording system design. In Telecommunication 866 Systems Services and Applications (TSSA), 2017 11th International Conference on, pages 1–6. IEEE, 2017.