Blockchain Enabled Distributed Consensus for EVM (Electronic Voting Machine) with IoT Integration.

Vedant V. Gune
Electronics & ComputerEngg.
Amrutvahini College of Engineering,
Sangamner, India
vedantgune41@gmail.com

Pritesh B. More
*Electronics & Computer Engg.Amrutvahini College of Engineering,*Sangamner, India
priteshmore2003@gmail.com

Niranjan Vikas Sathe
Independent Researcher,
Thane, India
satheniranjan@gmail.co

***Abstract*— The fundamental premise of democracy is that representative of the people represents the complete and true opinions and votes of the users over any issue, this may not be obviously always true, In the ancient Greece, the voting was done by the citizens directly for any specific issue or bill. In the current democracy system over the world all the decisions such as operational or lawmaking decisions are finally taken by law makers which are representatives of people. Perfect representation of democracy would be the exact opinions collected and drafted into law, otherwise all the laws which are already drafted have to be voted and selected by all the citizens. This would be a perfect representation of democracy and can be seen as a consensus mechanism for every law. Some laws if not all, can be passed or developed via such consensus mechanism, Now the fundamental problem in the consensus mechanism is the scale, and the manipulation, the mechanism and other engineering issues in collecting, securing and aggregating the votes. And finally, the heavy cost associated with such a voting. This is the issue that we are trying to address in the given research paper.**

There are other issues like which bills or which laws have to be put for the consensus, need of the consensus, and the controversy handling and repercussions of the inclusion of the masses which might not be completely aware of the issues, are other problems which we are leaving to the future of the democracy, so, nationwide hundred crore capable system for consensus, for law making is our goal.

Keywords—Blockchain Enabled Electronic Voting Machine, IoT with Blockchain, Distributed Consensus, Trustworthy Democratic Voting System, Nationwide Consensus based Voting System, Blockchain based Consensus, Consensus over the Bill, etc.

I. INTRODUCTION

Nowadays, making a right decision is a very complicated process in environments such as parliament, lawmaking houses, general assembly's etc. The opinions and perspective of every individual is different and may create a bias in the decision-making process. To ensure that everyone's vote counts with that transparency, trust, and faultlessness, and a simple voting can be conducted on nationwide or unprecedented scale by everyone in the democracy, this paper presents a solution proposed as a 'Blockchain-Enabled Distributed Consensus for EVM (Electronic Voting Machine) using Blockchain with IoT (Internet of Things)'.

At present, the conventional EVMs cannot be properly taken to blockchain network in secret voting system adapted by India. What if, the consensus itself is distributed? This will ensure that everyone's vote counts, and every vote is submitted transparently and faultlessly. Hence, this paper aims on providing a solution that makes the process of consensus over the bill and decision-making process more secure, trustworthy, transparent, and immutable. The blockchain and IoT integration can work alongside, and can enhance the system by having transparency and trustworthiness of blockchain consensus and physical sensing and computing capabilities of IoT collectively.

The microcontroller (ESP32) based hardware system will work as our electronic voting system or voting unit itself will work as a node connected to the blockchain network. The voting unit will authenticate the user's identity, and it will allow the users to select their vote, and the blockchain will make sure to provide secure platform to store the data of consensus with transparency and immutability, which will make sure that no one has a

control over the voting process and no tampering can be done to the overall system.

Currently the traditional EVM systems are immutable and cannot be manipulated but for implementation of distributed consensus over the bill, and democratic voting where every individual has a right to vote for the nationwide decisions. As the technologies like blockchain are evolving with rapid pace, the adaptation of EVM with blockchain is an important curve in technology which essentially will provide in high security, transparency, trust-building activity, and decentralization. Hence, we propose this solution which can be implemented to enhance the current nationwide decision-making processes of passing the bills in law houses, parliaments, and general assembly's etc. by implementation of consensus, where each one of us can be a part of the decision-making process.

II. LITERATURE SURVEY

[1] Bitcoin Blockchain, the first ever proposed blockchain research paper, ensures that electronic transactions based on peer-to-peer connected nodes can be done from one party to another without any central authority and with high level of trust and with consensus. The system mainly aims on digital signatures to ensure the ownership of coins and transactions to prevent double spending. It also maintains a distributed public ledger copy in highly encrypted manner which makes sure that system is secure from attackers, The proof of work makes use of computational power to validate and verify the transactions of blockchain.

But, this may not be limited for commercial, or economic transactions only, the applications of blockchain extends beyond commercial or economic transactions as blockchain is a type of system where, the stored records can be of any type such as a database, documents, healthcare data, voting system data, and so on can be stored in public ledger format.

[2][3][4] E-voting is a term used for electronic voting system which is an advancement in the traditional paper-ballot based voting system which is highly manageable and organized form of voting system. E-voting makes sure to provide a safe, secure, and efficient system which keeps the votes of voters and their information safe.

[5][6][7]The voting is an essential part of democracy which can be either traditional paper ballot systems or new technologically advanced systems like internet, or electronic voting machines or can be based on both modern and traditional technologies collectively.

[8]The paper proposes a solution as, Public Key Encryption Cryptosystem protocol-based E-voting that uses RSA encryption and allows the voter to vote from connected PC, capable of replacing the existing unreliable internet or electronic voting systems as their votes will be counted with transparency.

III. PROPOSED SYSTEM ARCHITECTURE

SYSTEM ARCHITECTURE:

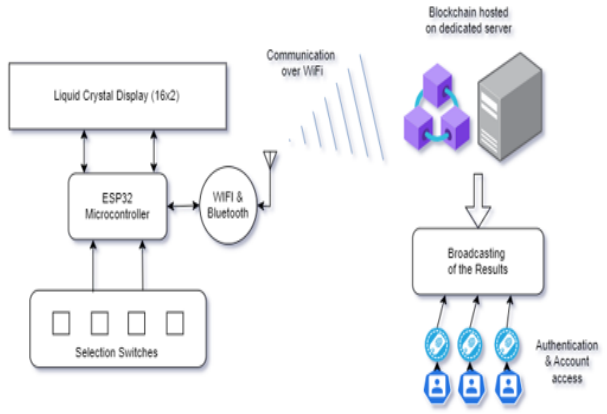

Fig 1: System Architectural Representation

Here, The systematic representational diagram, shows the flow of the system, ESP32 is used as a microcontroller node connected to blockchain network via WIFI module, user can vote using the selection switches and LCD display and the vote given will be sent over to the blockchain which is in the backend (on a dedicated server) which will store the votes and after a certain period will broadcast the results where each individual can login to their account after a layer of authentication, user can check their individual vote (democratically votes can be viewed), but here an individual can only view the details of own voting process and result but each user will be anonymous for and from one another.

The microcontroller, LCD, and, selection switches (buttons) are all the part of the electronic voting unit which will be connected to a private WIFI network with IPv6 protocol to ensure the security and encrypted data communication, at a specific location where people can go and vote their decision. The overall system will be packed inside a moderately secure casing as it is less likely to be attacked or damaged physically.

The voting unit or voting system which is basically a microcontroller/microprocessor-based hardware system connected as a node to blockchain, here an ESP32 microcontroller with inbuilt WIFI & Bluetooth capabilities. It will focus mainly on two main functionalities.

1) *Authentication.*
2) *Voting.*

Working & Flow of System:

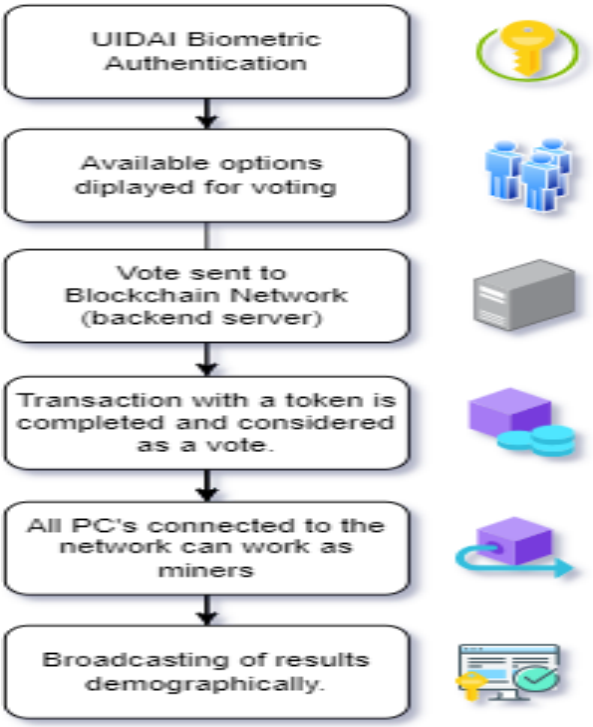

Fig 2: System Flow Diagram

A. *Biometric Authentication:*

The biometric scanner byUIDAI (Unique Identification Authority of India)can be used to authenticate the user uniquely by scanningboth the

i. Thumb Impression (fingerprint)

ii. Retina Scanner

Now, if an individual is authorized and verified, then canproceed for further steps.

B. Voting Process:

Once the authentication of an individual is completed, then all the available options (maximum of 16 options)are displayed to the user on LCD (Liquid Crystal Display), where the voters can select any option of their choice by pressing the respective buttons. Then the vote is sent over to the blockchain network at the backend server via inbuilt WIFI module in ESP32 and the blockchain makes sure to keep the votes safe and sound. The futher process repeats until voting is finished.

Here, the mining of blocks on the blockchain is carried our by each individual connected to our system, each general user like us will have an account on the blockchain network, and after successfully voting the vote, the nodes connected to the blockchain as peer to peer connected nodes (our PCs), computers of individuals who are connected to the blockchain network will be responsible for mining the new blocks onto the blockchain.

The voting process here is vital and will be carried out as a transaction on the blockchain, each vote will be considered as a transaction, and a token whose value will remain constant over the network(independent of no. of users or market value), When a token is transferred to respective option, party, decision, it will count as a vote.

System Design:

Blockchain will be applied to the consensus system as follows:

- Each option in the consensus will be treated as an account.
- Every Aadhar holder citizen that can vote, will be treated as a token in the blockchain system.
- When citizen will get authenticated via Aadhar & select an option as a vote then, the encrypted Aadhar token will be generated and added to the account option.
- The system is then evaluated for results, just on the basis of account balances following are the unprecedented advantages of our system.

1. Unmatched security & Resilience for voting fraud, as every Aadhar is linked to an option & in the investigation scenario, can be back verified as a vote of a person to an option.
2. The voting, can be kept open for days or week along with political campaigns for the bill to be passed and at the same time, citizens can switch their vote from one option to another, and whole statistics can be online viewed by the world. This takes the democratic system to its next level.

C. Broadcasting Results:

Once the voting process is over,at a specific time the results will be broadcasted onto a web application where the user can log in and authenticate identity and can analyse each vote given by the individual, other people's votes will be hidden and encrypted and demographical

details like, total votes for each option, your votes, etc. will be accessible from own account.

For the same, blockchain also maintaines a copy of database containing everyones aadhar number and votes given by that specific user in encrypted format. This makes sure that user can log in and view personal data of account and the overall anonymity is maintained.

D. Blockchain Network

Here we are trying to propose an implementation of custom blockchain network using Python Programming, a class-based approach can be used to develop a whole blockchain. Due to the freedom, simplicity of code, readability, platform independence and availability of community support and vast number of libraries makes the blockchain implementation in python easier and reliable.

The blockchain is a very popular, secure, and strong way of storing transactions that are open to everyone, such as the voting process. Where the integrity of data is very important, the data is vital, in such cases, the blockchain provide a secure, tamperproof way and the most important thing is decentralization. The decentralization makes the blockchain independent of any central controlling authorities, hence the change of tampering and manipulation is reduced significantly.

But, to understand the blockchain, there are simple words like, Decentralized, Distributed, Highly Secure, Immutable, Tamperproof, Trustworthy system.

1. *Decentralization :*

   Decentralization, is achieved via connecting the nodes in peer-to-peer network, where all the nodes are connected to all of the otherswhich results in no central controlling authority and no authority which governs the blockchain. The blockchian hence becomes totally independent system where nobody has any authority to interfare between the ongoing processes, and transactions.

2. *Distributed :*

   Blockchain stores its data mainly in the format of ledger, which is distributed amongs all the nodes connected to the network, but meanwhile, it also makes sure that no one has access to the distributed ledger and the data on it by the means of encryption via hashing techniques. Basically, when the data in form of ledger is distributed onto the network, it adds the redundancy of data, and reduces the chances of loss of data.

3. *Immutable :*

   In blockchain, each block is encrypted with a secure hashing algorithm and cryptographic techniques. Whenever a block is created, it is hashed and linked with previous block hash, and whenever there is a requirement of change in the network, it must be done by voting process, where each node votes for accepting or rejecting the change. Hence it makes the blockchain system highly immutable, secure and trustworthy.

4. *Secure System :*

   Blockchain is highly secure and immutable due to the implementation of complex hashing techniques such as SHA-256, in our implementation we have utilized two rounds of SHA-256 hashing to improve security by two-layer-hashing. A merkel tree is maintained and established which enhances the security as it depends on previous hashes in the system, even if a single hash is modified, or changed, the whole merkel tree changes.

5. *Blockchain Mining :*

   In the diverse field of blockchain, transactions are stored in the form of blocks, each block holds several fields like transaction list, block header, Merkel tree, previous block hash, etc. Hence, whenever a new transaction is completed it is broadcasted to all the nodes connected to the blockchain network, where all the nodes validate the transaction and after the validation and verification of the transaction, a puzzle is given for the miners to solve and add block to the blockchain network.

   Miners are no different than that of nodes connected to peer-to-peer blockchain network, but are a part of the process of adding newly generated blocks to the blockchain. The mining process consists of solving a

puzzle with a specific difficulty which takes enumerous computations and when a specific puzzle is solved, the miner gets authority to add the new block to the blockchain network and miners receive rewards for mining and adding a new block to the network.

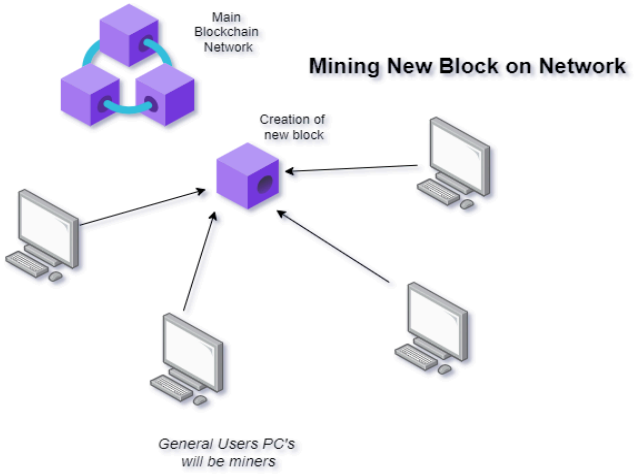

Fig 3: Block Mining

There are several consensus protocols and algorithms like,

i) Proof of Work(PoW)
ii) Proof of Stake(PoS)
iii) Proof of Capacity(PoC)
iv) Proof of Elapsed-Time(PoET)
v) Proof of Burn (PoB)

1) Proof of Work(PoW) :
An algorithm where a complex puzzle is given with a specific difficulty to the miners, the computer with high computational power can solve quickly and can get a chance to add the new block to blockchain.

2) Proof of Stake (PoS):
An algorithm where the selection of miner is based on how much crypto currency they own and can put as a stake, the more the currency the more are the chances to get selected.

3) Proof of Capacity (PoC):
An algorithm, where the hard drive space of computer is used instead of the computational (CPU) power, the more memory you have, the more are the chances of getting selected.

4) Proof of Elapsed-Time (PoET):
An algorithm, where the miners are selected randomly to add new blocks to the blockchain, like a digital lottery system.

5) Proof of Burn (PoB):
An algorithm, where the existing crypto currency is burnt (destroyed) by sending it to a specific address and in return they get new crypto currency / tokens from different blockchain.

Here, in our custom blockchain a simple mechanism is maintained to mine newly created blocks using a Proof of Work(PoW) consensus algorithm, by providing a difficulty such that the hex pattern (hash) being generated has four contiguous zeros at the start of encrypted hash, if not so, we will retry with incrementing the existing nonce and the process of generation of hash will repeat until the specific hash which meets our requirements is not matched.

These algorithms will be executed by the blockchain client software running on all of the connected voter's PCs to hence a simple algorithm is used which should need less CPU resources and less computational power.

II. FINDING & OBSERVATIONS

Electronic voting is becoming the need of era, although currently every system is focusing on adaption of voting onto the blockchain but, here we have discussed a simple yet worldwide applicable solution to conduct nationwide democratic consensus for passing the bill, where each one of us will have right to vote for any decision for our country.

Here the proposed system makes sure to keep the votes and voter's information safe, trustworthy, and transparent. And also gives the voters a way to verify and validate that their votes count. The perfect representation of democracy is the voting where each and everyone in the nation has equal right to be a part of the process of making a decision, which can be applied and executed with minimum cost, high reliability and easier access to all with the help of Blockchain Enabled Distributed Consensus for EVM with IoT Integration.

III. CONCLUSION

The adaptation of blockchain over the traditional EVM for consensus over the bills with IoT and Blockchain can be implemented to develop a cost-effective, efficient, reliable, and trustworthy system for distributed democratic consensus building process for decision-making. Hence, This system can be implemented for giving each individual

nantionwide, right to vote and make decision related to any issue in the country.

IV. REFERENCES

1. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

2. Xuechao Yang, Xun Yi, SuryaNepal, Andrei Kelarev,andFenglingHan:ASecureVerifiableRanked Choice Online Voting System Based on Homomorphic Encryption.

3. Rifa Hanifatunnisa and Budi Rahardjo:Blockchain Based E-Voting Recording System Design

4. Mohammad Hosam Sedky and Essam M. Ramzy Hamed: A Secure e-Government's e-Voting System

5. Himanshu Agarwal and G.N.Pandey: A Secure eGovernment's e-Voting System.

6. Khan K.M., Arshad J., Khan M.M. Investigating performance constraints for blockchain based secure e-voting system. *Futur. Gener. Comput.*

7. Gritzalis D.A. *Secure Electronic Voting*. Springer Science & Business Media; Berlin/Heidelberg, Germany: 2012.

8. Ashish Singh, Kakali Chatterjee, SecEVS: Secure Electronic Voting System Using Blockchain Technology, International Conference on Computing, Power and Communication Technologies (GUCON) Galgotias University, Greater Noida, UP, India. Sep 28-29, 2018.