International Journal of Scientific Research & Engineering Trends
Volume 6, Issue 2, Mar-Apr-2020, ISSN (Online): 2395-566X

Use of Blockchain for Secure E-voting

Er. Zainab Mirza Aalia Shaikh Sameena Shaikh Nagama Khalifa Yasirammar Khan
Department of Information Technology,
M. H. Saboo Siddik College of Engineering, Byculla, Mumbai-400008, India.
zainab.mirza@mhssce.ac.in,aaliashaikh3@gmail.com,sameenas482@gmail.com,nagamakhalifa@gmail.com,
yasirkhan2167@gmail.com

***Abstract* – Implementing a most secured technology based E-voting system which provides the high-level security and privacy to the voting system while still having the best features of current voting systems. In this paper, the technology suggested to be used for offering security is Blockchain. Blockchain is the driving force of the security and it will be used as a service to secure the and implement distributed E-voting systems. The paper addresses and talks about some of the limitations and drawbacks of current not-highly secured and easily tamperable voting systems. Like the case where pressing a button could sometimes send the vote to another unintentional party. The blockchain will help us improve security because of its immutable nature. Some of the various popular blockchain frameworks could be used like Etherium, Hyperledger, etc. In general, we use the blockchain to its full potential to maintain the integrity of the people rights and their votes and also thereby reducing the budget of conducting a voting nationwide.**

***Keywords* – E-voting, Blockchain, Security, Privacy, Immutable, Integrity.**

I. INTRODUCTION

A blockchain is a distributed database that provides secure transactions. A blockchain is a chain of digital "blocks" each block contains a record of transactions. Each block is connected to all the blocks before and after it.Therefore it is difficult to tamper with a single record of block.The records on a blockchain are secured through cryptography. Each network participant in the network has their own private keys that are assigned to the transactions.That key act as a personal digital signature. If a record is altered, the signature will become invalid. And once the key becomes invalid the peer network will know that something has happened.While the first proposals for cryptographic hash functions and distributed systems date from at least the 1970s, these powerful concepts were brought together in the anonymous whitepaper of Satoshi Nakamoto that detailed "Bitcoin: A peer-to-peer electronic cash system" in 2008. Bitcoin was not purely academic, but implemented in the wild: The open source code of Bitcoin made money transfers without a bank acting as a trusted third party possible for millions of users, and its distributed design gave Bitcoin the properties of a permissionless network with censorship-resistance. However, Bit-coin's design still struggles to ensure some measure of anonymity, despite the fact that most of its users believe it provides anonymous payments [3]. Research has been made even more difficult as the privacy and security properties of Bitcoin were never formally stated by Nakamoto in a provable manner, and so these properties have only recently begun to be formalized [1].Goldwasser and Micali's "Probabilistic Encryption" [2] formalized the notions of security in terms of a rigorous definition of semantic security.

II. SECURITY THREATS

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 [4]. An electronic voting portal should offer security and integrity along with the transparency of votes and privacy of voters [5].In the Traditional voting system voters choose their representatives and give their votes to them. then this election data gets stored in a database.but this database is vulnerable to modification.Traditionally, the database is maintained by a central authority or a single organization that has then complete control of the database. It has the ability to tamper with the database and manipulate the data. Usually the authority maintaining the database is the same that has created it and will be using it. In such cases the organization has no motive of manipulating or falsifying its own data. But in other cases involving financial matters or sensitive data like voting, it's not wise to give total control of the database to a single authority or organization[5]. There are many situations where data stored in databases gets exposed to some third party or hackers.Any database must follow ACID property:

- **Atomicity:** the entire transaction happens at once or doesn't happen at all.
- **Consistency:** the database must be consistent or remain the same before and after the transaction.
- **Isolation:** every task must be isolated or not occur independently without any interference.
- **Durability:** the changes of the system must be done even if the system fails. So existing system was vulnerable to the above properties.If any database

doesn't follow this property then the integrity of the database gets violated.

III. PROPOSED SYSTEM

1. Blockchain as a Service

- Blockchain, sometimes referred to as Distributed Ledger Technology (DLT), makes the history of any digital asset unalterable and transparent through the use of decentralization and cryptographic hashing.Three critical ideas of the technology:
- Digital assets are distributed instead of copied or transferred.
- The asset is decentralized, allowing full real-time access.
- A transparent ledger of changes preserves integrity of the document, which creates trust in the asset.
- Blockchain consists of three important concepts: blocks, nodes and miners.

- **Blocks :** Every chain consists of multiple blocks and each block has three basic elements:The data in the block , 32-bit whole number called nonce - which generates a block header hash ,256-bit number called hash wedded to the nonce.When the first block of a chain is created, a nonce generates the cryptographic hash. The data in the block is considered signed and forever tied to the nonce and hash.

- **Miners :** Miners create new blocks on the chain through a process called mining.In a blockchain every block has its own unique nonce and hash, but also references the hash of the previous block in the chain, so mining a block isn't easy, especially on large chains. Miners use special software to solve the incredibly complex math problem of finding a nonce that generates an accepted hash. Because the nonce is only 32 bits and the hash is 256, there are roughly four billion possible nonce-hash combinations that must be mined before the right one is found. When that happens miners are said to have found the «golden nonce» and their block is added to the chain.

- **Nodes:** One of the most important concepts in blockchain technology is decentralization. Nodes can be any kind of electronic device that maintains copies of the blockchain and keeps the network functioning. Every node has its own copy of the blockchain and the network must algorithmically approve any newly mined block for the chain to be updated, trusted and verified.

- **Smart Contract:** The Smart Contract is aimed to provide contracts between parties where both parties are given the priority and contracts are conducted upon establishing the conditions of both the parties. It is the executable code that runs on top of the blockchain to facilitate the terms required in an agreement of a contract between the two parties. The involvement of any third party is resolved as any medium between parties are not required, upon fulfilling conditions contracts are self-executed.

2. Blockchain Based E-Voting System

2.1 Voter Registration: In this phase, the voter will provide personal information including Aadhar card number (or voter identification number or any other relevant voter identification) and biometric information, fingerprint, to the authenticated officer. The Aadhar card issued by The Government of India contains the photograph of the card holder, name, date of birth, gender and the unique Aadhar card number. The Aadhar card database also stores the fingerprint of every Aadhar card holder. This can be used to register the voter without the hassle of any manual work. The information provided will be verified during the"Voter Authentication" phase of the election. Following steps are involved in the registration phase:

- The officer takes details of voter like unique Aadhar card number, voter identification number, name etc.
- Officer asks the voter to provide a fingerprint. Fingerprint scanner with fingerprint pulse at sensor is used to scan the fingerprint.
- A biometric based encryption algorithm with enhanced privacy and security [6] is used to the transform fingerprint image to feature based encrypted data. This encrypted biometric data along with voter identification number, name etc. are combined in the form and stored in a private blockchain.

2.2 Implementation in Blockchain

- Consider the structure of the blockchain:
- Org – the central voting authority (it is an organization in terms of Hyperledger Fabric, has one or more physical nodes).
- Dep – is a subdivision that is responsible for conducting voting in its district.
- CC – chaincode in terms of Hyperledger Fabric which is responsible for the logic of the voting.
- V – Voter, system user.

There are several client applications that can interact with Fabric network. Admin apps initialize voting, user apps cast vote and inspect the voting process.We aim to build a robust e-voting system where there will be a web-app in which the voter can register with their Aadhar card number, get a unique voterId which is used to login to the app, and cast the vote. The vote is tallied on the blockchain, and the web-app shows the current standings of the polls.[10]

As the voter approaches to vote providing his/her fingerprint, it is verified whether the voter is in the eligibility list and whether he/she has already voted. As the fingerprint is scanned, it is verified if the voter is inn

the database or not. As the voter has proved him/her as eligible , the voter is then to provide his/her Aadhar card number, district, first and last name as a need of verification that no other people except the voter is casting his/her vote . Then the certificate authority of the hyperledger network creates a public and private key for the voter and adds it to his/ her wallet.

After that, we use our Aadhar card number to submit our vote, during which the application checks if this Aadhar card number has voted before and tells the user they have already submitted a vote if so. This is a double measure to ensure that no duplicate vote is casted. If all goes well, the political party which the voter has chosen is given a vote, and the world state is updated. The application then updates our current standings of the election to show how many votes each political party currently has.Since each transaction that is submitted to the ordering service must have a signature from a valid public-private key pair, we can trace back each transaction to a registered voter of the application, in the case of an audit.Voting results are publicly auditable.However; blockchain systems are complex in nature which may hinder its wide acceptability. For e-voting systems continuous broadband access is another concern. Another issue can be the digital user skills. For large number of users' authentication and validation, blockchain requires much energy. So using blockchain based voting system for national e-voting require more research on its consensus.[7]

2.3 Benefits of Blockchain

Blockchain based e-voting system provides following benefits:

- We know that without transparency, people can become discouraged about the legitimacy of their votes and can lead to questions about tampering and falsified results.In turn, by allowing voters to see live records of the number of votes coming in, everyone will be able to see the legitimacy of the voting, making for a transparent and trustworthy voting system.
- Currently, voting systems are very open to hacks.Using blockchains,all votes could be verified as soon as voting is finished to ensure they are all counted correctly.
- Blockchain allows for anonymity when voting.Voters can use their private keys to keep them anonymous. They can then vote in the system without the worry of others knowing how they voted.
- Often when voting stations are in different areas and offices are not all together, it can be difficult to gather all the information quickly and efficiently.Using blockchain, results can be gathered and processed quickly and straight after the voting has finished.

2.4 Benefits of using Hyperledger instead of Ethereum

Hyperledger based e-voting system provides the following benefits:

1. **Ledger Type**

- Hyperledger Fabric is a permissioned platform.It can offer the privacy that e-voting systems need.Hyperledger comes with membership arrangements for selecting who can get an entry into the system and who can't. More so, the Election Commission itself will decide who can enter the platform.So only eligible voters will be able to vote.
- On the other hand, Ethereum is a public platform. So, there is no form of privacy there. Users in the system won't have to pass any membership rules in order to get access to the network. Thus, it's not entirely suited.

2. **Throughput**

- Both technologies claim about being fast and offering a lot of transactions per second. However, Hyperledger Fabric is faster, it comes with > 2000 tps. So, you can expect it to process 2000+ transactions every second.More so, the Fabric can achieve this score because it offers parallel transactions, and it does limit the user are in the system, so it doesn't slow down.
- On the other hand, Ethereum, with a small number of nodes, can pull off a large number of transactions. But as it's a public domain, it slows down and can now offer something close to 20 tps.

1. **Cryptocurrency**

- Hyperledger Fabric doesn't have any native token or cryptocurrency is the system. So, cryptocurrency is not required to use the platform. However, if a company needs a token-based system, they can easily add it up. So, they won't be forced to use any native currencies.
- On the other hand, Ethereum comes with a native cryptocurrency called Ether. More so, there's another form of token called Gas in the system that one needs to perform the transactions in the system. The issue is the price of Gas keeps changing, and with more users, it can become a huge burden as well.

IV. CONCLUSION

In this paper, we have presented a e-voting system based on blockchain. This system runs on Hyperledger. The system stores the voter registration information and encrypted ballot on blockchain. Our system uses Hyperledger as a network as well as a database to store the above mentioned voter details.The system also makes use of smart contracts. This paper shows how blockchain implementation can overcome the limitations of traditional voting system. We have proposed a blockchain based system for voting for the country of India. However, the proposed e-voting system can also be applied to other countries as well. The system is adaptable to be implemented according to each country's own

election laws and regulations.

REFERENCES

[1]. Juan Garay, Aggelos Kiayias, and Nikos Leonardos. The bitcoin backbone protocol: Analysis and applications. In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pages 281–310. Springer, 2015.
[2]. Shafi Goldwasser and Silvio Micali. Probabilistic encryption. Journal of computer and system sciences, 28(2):270–299, 1984.
[3]. Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M Voelker, and Stefan Savage. A fistful of bitcoins: characterizing payments among men with no names. In Proceedings of the 2013 conference on Internet measurement conference, pages 127–140. ACM, 2013.
[4]. Hjálmarsson, Friðrik Þ., et al. "Blockchain-based e-voting system." 2018 IEEE 11th International Conference on Cloud Computing (CLOUD). IEEE, 2018.
[5]. Patidar, K., & Jain, S. (2019). Decentralized E-Voting Portal Using Blockchain. 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT).
[6]. N. K. Ratha, J. H. Connell and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," in IBM Systems Journal, vol. 40, no. 3, pp. 614-634, 2001.
[7]. R. Bulut, A. Kantarcı, S. Keskin and Ş. Bahtiyar, "Blockchain-Based Electronic Voting System for Elections in Turkey," 2019 4th International Conference on Computer Science and Engineering (UBMK), Samsun, Turkey, 2019, pp. 183-188.
[8]. Sadia, Kazi, et al. "Blockchain Based Secured E-voting by Using the Assistance of Smart Contract." arXiv preprint arXiv:1910.13635 (2019).
[9]. Kirillov, Denis, et al. "Implementation of an E-Voting Scheme Using Hyperledger Fabric Permissioned Blockchain." International Conference on Computational Science and Its Applications. Springer, Cham, 2019.
[10]. Horea Porutiu (IBM) ,A voting application that leverages Hyperledger Fabric and the IBM Blockchain Platform to record and tally ballots,(2019), GitHub repository, https://github.com/IBM/evote.git