ISSN No:-2456-2165

E-Voting System Using Blockchain

Prof. Vishal Polara[1], Pranav Baraiya[2], Harsh Ajudia[3], Harshil Buha[4], Harsh Kadivar[5]
[12345]Information Technology Department
Birla Vishvakarma Mahavidyalaya
Anand, Gujarat, India

Abstract: Democratic voting is a crucial and serious event in any place, the current election scheme in any place, be it a school college, or even a country is done through ballot papers or using EVM. This process has many disadvantages such as transparency, low voter turnout, vote tampering, lack of trust in electoral authorities, delay in results, and above all security issues. So the growing digital technology has helped many people's lives nowadays. The concept of electronic voting is introduced to combat the disadvantages of the traditional voting system. Electronic voting is essentially an electronic means of casting and counting votes. It is an efficient and cost-effective way of conducting a voting procedure that is data-rich and real-time and requires high security. Nowadays, concerns about the security of networks and the privacy of communications for electronic voting have increased. Thus, the provision of electronic voting is very urgent and is becoming a popular topic in communication and networking. One way to solve security problems is blockchain. The paper proposes a new blockchain-based electronic voting system that addresses some of the limitations in existing systems and evaluates some of the popular blockchain frameworks to create a blockchain-based electronic voting system. Because the blockchain stores its data in a decentralized manner, the implementation result shows that it is a practical and secure electronic voting system that solves the problem of vote forgery in electronic voting.

Keywords: *Blockchain, Ethereum, Decentralized, Digitization, Secure Voting, Facial Recognition.*

I. INTRODUCTION

Blockchain technology is shining sort of a star these days when its entry and wide-spread adoption of Bitcoin, the terribly initial cryptocurrency that involves people's minds. Blockchain technology originates from the fundamental subject style of the bitcoin cryptocurrency, wherever it absolutely was initial introduced to the net world and previously became a promising technology thanks to the high degree of transparency within the system, turning into a vigorous space of analysis and study for its varied applications. alternative fields.

Blockchain, simply put, may be a shared, changeless ledger that facilitates the method of recording transactions and following assets in a very business network. Associate in Nursing quality are often tangible (house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding). during this era nearly we are able to track and trade something on a blockchain network, reducing prices and risk for everybody. Blockchain stores its knowledge in blocks. First, all the info to be keep within the blockchain is reborn into smaller components, that square measure allotted to totally different blocks within the suburbanized network. The initial block in a very blockchain is understood as a "Genesis Block" or "Block 0". "Block Gene-sis" or "Block 0". The genesis block is sometimes hard-coded into software; is peculiar therein it doesn't contain a link to the previous block. The genesis block is sometimes hard-coded into the software; it's special therein it doesn't contain a regard to the previous block (the Genesis block).

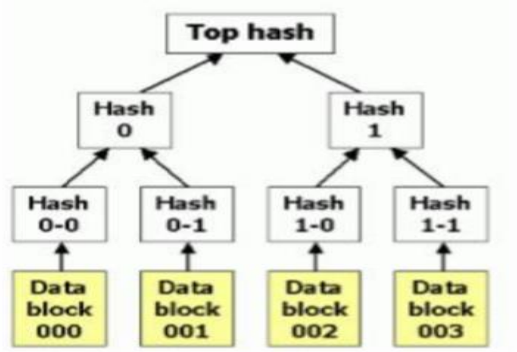

Fig 1: Hash Table Ref. [1]

Once the genesis block is initialized, "Block 1" is created and when completed is attached to the genesis block. Each block has a transaction data part, a copy of each of the transactions is hashed and then the hashes are matched and hash again, this continues until there is only one hash left; to known as the Merkle root (Figure 1). The block header is where the Merkle root is stored, which ensures that the transaction cannot be modified by third parties.

Before 2004 there was a paper-primarily based totally vote casting device referred to as ballot paper device in India. Ref. [2]So, to eliminate all the shortcomings of the traditional voting system, the blockchain fits as the best suitable solution for the e-voting platform. Electronic voting is extensively studied and many implementations are tested and even used for a while where we encountered some problems like user authentication, vote tempering, etc. Of course, there are many government websites like polls, networks to gain knowledge about new government schemes, questionnaires where common people raise their questions, etc. still we can't say the same for online elections because every vote matters here for a candidate so the system needs to be more secure, reliable and authentic. This is mainly because official elections are the basic elements of democracy and democratic governance which is the most preferred administrative methodology in the modern world. The electronic voting system will be a new change from the regular voting system, which is less complicated, and more open to the voters, and besides, security will come first. These tactics reduce the cost of many laws to some voters by creating more ways for them to cast a ballot. This gives it a chance to survive long queues at check stations and offers a better experience to those who are sick, serving in the military, people living abroad or gone abroad on holiday, etc. It has been found that many people did not vote due to laziness, so it can serve its purpose here in the electronic voting system. And all the things in today's world are digitized, then the electoral system falls behind, young people between the ages of 18 and 30 are special voters, and the web is a process to attract those citizens who seem to be the hardest to reach.

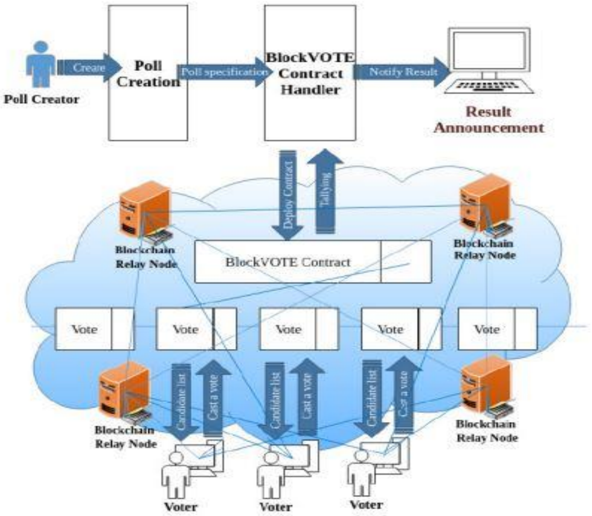

Fig 2: Architecture of E-Voting Ref. [3]

Our main motivation behind this project is to create a secure voting environment and show that a reliable e-voting scheme is possible using blockchain. Because when electronic voting is available to anyone with a computer or mobile phone, every single administrative decision can be made by people and members; or at least people's opinions will be more public and accessible to politicians and managers. This will eventually lead humanity to true direct democracy. This is important to us because elections can be easily corrupted or rigged, especially in small towns and even larger cities in corrupt countries. Moreover, large-scale traditional elections are very expensive in the long run, especially when there are hundreds of geographically distributed polling stations and millions of voters. Voter turnout at polling stations is also relatively low, as the person may not be staying at the address whose name is on the list, or maybe on vacation or other work. Electronic voting will be able to solve these problems if implemented carefully. The concept of electronic voting is significantly older than blockchain. So all known examples to date have used the means of centralized computing and storage models. By implementing blockchain, we can increase the security level of our system due to its way of storing data in a decentralized network. This project also has a facial recognition system to verify whether the user is valid or not. Some systems were found to have an OTP system to authenticate the user. But in this authentication model, the disadvantage is that if x person's phone is not with him, even though his phone is with his friend, his friend can vote twice because of the OTP system, one with the original chance and one because of his friend's login, and then x can't vote. So here comes the face recognition technique where the user has to verify his face before voting to maintain transparency.

Ref. [4] Estonia is a very good example as the Estonian government is one of the first to implement a fully online and comprehensive e-voting solution. The concept of electronic voting began to be discussed in the country in 2001 and was officially launched by the national authorities in the summer of 2003. Their system is still in use, with many improvements and modifications to the original scheme. As mentioned, it is currently very robust and reliable. They use smart digital ID cards and personal card readers (distributed by the government) for personal authentication. There is a dedicated web portal and an equivalent desktop application for citizens to participate in the elections by nominating candidates and casting their votes. So that anyone with a computer, an internet connection, and also an ID card can easily vote remotely.

II. LITERATURE SURVEY

Many research papers have been published writing different authentication systems to verify users, and different ways to create an electronic voting system such as without blockchain, with blockchain, or using Hyperledger to implement blockchain.

Ref. [6] research work was focused on different user authentication methods. There are different voter verification strategies. According to Kriti Patidar and Dr. Jain, voter authentication can be done using private key cryptography, which must be provided to voters before the election process. Voters should be registered by some authority, while voter registration must be generated and distributed to voters in hand.

Ref. [7] Friorik P. Hjalmarsson plans to use a 6-digit voter PIN that the voter can use for voter authentication. Each individual is identified and verified by the system by presenting an electronic ID from Auokenni and the corresponding 6-digit PIN at the polling station. Unsupervised, an individual could vote for multiple people if they knew the PIN for each matching electronic ID they had.

Ref. [8] Verifying voter identity from multiple angles is always a challenge; some work has tried biometric solutions such as fingerprint scanning, but this can be distorted and easily gamed or stolen. However, we believe that one way to protect stolen biometric data is to use complex algorithms that are difficult to crack. It can be hashed using any hashing algorithm instead of storing the biometric information as binary data and then stored as a reference string. The sample model should be hashed during the validation and identification process and then compared to the reference value.

Ref. [9] The online voting system using the cloud. The paper proposes the development of a voting system where a voter can vote from anywhere over the Internet using a system based on SQL Server and Microsoft Azure cloud and C# as a programming language to implement functions such as voter reception, vote casting, and vote verification. and announcing the results after the election.

III. METHODOLOGY

In this section, we will show the design and functional phase of our application. The user accesses the web application where the platform is hosted and registers as well as votes securely and transparently. The methodology is given below.

1. Registration Stage: In this stage, the voter has to register with his unique aadhar number, email address, name, and phone number. They also need to add their clear photo here as this system uses facial recognition technology to log in.
2. Login: After registration, the voter tries to log in and cast his vote. At this stage, the voter first logs in using a password. After successful login, the voter must authenticate to vote. For real-time authentication, facial recognition technology is used to increase the level of security.
3. Blockchain Technology: Ref. [10]This technology is mainly used for its security features. Blockchain provides a secure and transparent environment. Blockchain encrypts the voter's message (Casted vote) using an asymmetric encryption algorithm. The public key is provided by the Blockchain and the private key is with the host. The public key is used for authentication purposes using the ledger.
4. Ethereum: The Ethereum network provides a framework for creating and storing the blockchain. Each block is created and its details are stored in an encrypted ledger. Ref. [11] These generated blocks are distributed among the nodes, providing the system with high fault tolerance. To cast a vote, a user must use Ethereum for their transactions. So Ganache is used for this. Ganache is a private Ethereum blockchain environment that allows you to emulate the Ethereum blockchain to interact with smart contracts on your private blockchain.
5. Database: All system data is stored in the MongoDB database. The data will be in the form of voter and candidate names, unique voter IDs, and voting details like time, time slot, region, etc.
6. Admin: Admin will control the entire environment. Verification of voters and candidates will be done by admin. Admin only arranges the voting schedule. All important notifications like results etc are also under admin control.
7. Results Phase: The processing and counting of votes take place in the results phase. The results are generated and displayed on the website. Users can verify their votes using their public key. This ensures the transparency of the voting system.
8. Meta Mask: Metamask allows blockchain users to manage their wallets. Using the browser extension, users can use the wallet and perform transactions through the browser. When a transaction is performed, a meta mask pops up and asks the user to confirm the transaction.
9. Truffle: Truffle offers an improved environment primarily based totally on the Ethereum blockchain. Truffle is capable of compiling the Ethereum contracts and migrating them. After migration contracts are deployed on ganache, any Ethereum takes a look at the net (e.g. Ropsten, Rinkeby, local network) or on an actual Ethereum network.

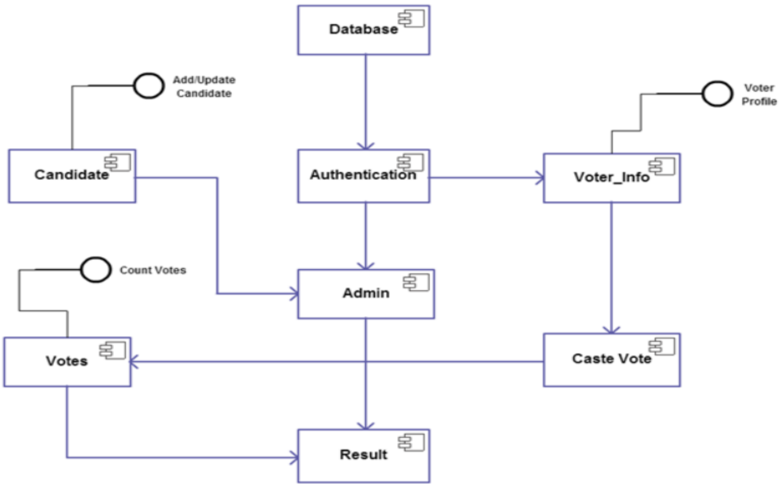

Fig 3: Overview of System

- *Voting Process:*

We now describe a typical user interaction with the proposed scheme based on our current system implementation. So basically, the voter logs into the system by scanning their face. After scanning the face, the facial recognition system authenticates the voter. If a match is found, the voter is presented with a list of available candidates with the option to vote against them. Conversely, if the match is unsuccessful, any further access would be denied. This functionality is achieved by using an appropriate implementation of an authentication mechanism (in this case a facial recognition system) and predefined role-based access control. Furthermore, it is also assumed that the voter is assigned to his particular electoral district and this information is used to create a list of candidates for which the voter can vote. Assigning a voter to a constituency is considered an offline process and is therefore beyond the scope of this research.

After successfully casting votes, it is mined by multiple miners for verification, after which valid and verified votes are added to the public ledger. The security aspects of voting are based on blockchain technology using cryptographic hashes to secure end-to-end verification. For this purpose, a successfully cast vote is considered a transaction within the voting application's blockchain. Therefore, the casting vote is added as a new block (after successful mining) in the blockchain and is also recorded in the data tables at the end of the database. The system ensures ownership of voting systems for only one person and one vote. This is achieved by using a unique voter face that matches at the start of each voting attempt to prevent double voting. Once miners mine a vote, a transaction is generated that is unique to each vote. If the vote is found to be malicious, the miner is rejected.

After the validation process, a notification is immediately sent to the voter via message or email with the transaction ID defined above, through which the user can track their vote to the ledger. While this works as a voter notification, it does not allow any user to extract information about how a particular voter voted, thereby achieving voter privacy. It is important to note here that the cryptographic hash for the voter is the unique hash of the voter by which the voter is known in the blockchain. This feature makes it easier to achieve verifiability of the entire voting process. In addition, this id is hidden and no one can view it, not even the system operator or administrator can view this hash, thereby achieving the privacy of individual voters.

IV. RESULT AND DISCUSSION

Finally, our service design features a distributed network comprising machines from both government and public infrastructure; this infrastructure contains two distinctly separate blockchains, one for voter information, such as who voted, and another for voting information, such as what was voted. These blockchains are kept completely separate to remove any threat of linking votes for certain parties back to individual voters while maintaining the ability to track who voted and how many votes are present. The blockchain containing information about who has registered to vote also allows our service to ensure that each voter is unique. Various other concerns related to transparency, confidentiality, and reliability were also considered and the proposed solution largely preserves every aspect of a secure voting system by overcoming various such challenges.

Once you register, you are assigned a vote after your details are verified. To ensure that these registered voters are whom they say they are when they start voting, there is a method of verification, i.e. facial recognition. In addition, we also need to ensure that the user does not accidentally vote for any other candidate, so we have incorporated a double-check service where users will be asked a second time to confirm their contribution before submitting their vote; this also allows us to almost eradicate random voices

To further advance the implementation with the appropriate infrastructure and resources, it is possible to implement the database on a distributed architecture to have no central authority for elections and decentralize the entire process.

V. CONCLUSION

The current voting system can be improvised and secured by applying a web-based voting solution and also improving the accuracy of the face detection model. The goal is that voters wouldn’t be able to cast invalid votes so, this system uses face-recognition for voter identification which makes it more secure and reliable. Blockchain technology has the potential to be implemented in a far more secure and accessible voting system. The proposed blockchain-based e-voting system manages the election process, which makes the voting process simpler, voters can just simply log in and exercise their right to vote. We believe that blockchain-based voting systems can replace the traditional voting system in the future.

REFERENCES

[1]. Fig 01: https://stackoverflow.com/questions/8411144/in-a-hash-tree-are-non-leaf-nodes-direct-hashes-of-data-or-are-they-hashes-of
[2]. Jayesh solanki, divykant meva, “Comparative Study Indian Electoral Reforms in Indian Context”, September 2019, IEEE
[3]. Fig 02: https://ph01.tci-thaijo.org/index.php/ecticit/article/view/227455
[4]. https://en.wikipedia.org/wiki/Electronic_voting_in_Estonia
[5]. https://techcrunch.com/2018/03/14/sierra-leone-just-ran-the-first-blockchain-based-election/
[6]. Raghav Chhabra, Uday Vohra, Vishrant Khanna, Aditya Verman, Poonam Tanwar, Brijesh Kumar, " The Next Gen Election: Design and Development of E-Voting Web Application" 10-12 June 2020, IEEE
[7]. Ramya Govindaraj, P Kumaresan, K. Sree harshitha, " Online Voting System using Cloud," 24-25 Feb. 2020, IEEE
[8]. Bhushan M. Pawar, Sachin H. Patode, Yamini R. Potbhare, Nilesh A. Mohota, " An Ef-ficient and Secure Students Online Voting Application," 8-10 Jan. 2020, IEEE
[9]. Mrunal Annadate, " Online Voting System Using Biometric Verification," April 2017, ResearchGate
[10]. https://www.blockchain-council.org/blockchain/how-does-blockchain-use-public-key-cryptography/
[11]. https://www.blockchain.com/explorer/assets/eth