Decentralized Digital Voting System Leveraging Blockchain for Electoral Integrity

Ranjani K[1], Jayasurya R [2], Saravanan R [3], Vishnu V [4], Madhesh SR [5]
[1] *Assistant Professor, Department of CSE (Internet of Things and Cyber Security including Blockchain Technology), SNS College of Engineering, Coimbatore-641107.*
[2], [3], [4], [5] *Student,Department of CSE (Internet of Things and Cyber Security including Blockchain Technology), SNS College of Engineering, Coimbatore-641107.*

Abstract: **A blockchain-enabled online voting system is proposed in the following paper. Blockchain technologies deliver an endless variety of applications that benefit from distributed economies. The proposed model is an Android application that has enhanced security features which include authentication. Authentication is incorporated by using a unique identification key. Elections have a great importance in determining who will rule a nation or an organization or it can be said as an event that decides the fate of our nation. In modern democracy, elections are very important but large sections of society around the world do not trust their election system which is a major concern for democracy. Even the world's largest democracies like India and the United States, still suffer from a flawed electoral system. Vote rigging, hacking of EVM (Electronic voting machine), election manipulation, and polling booth capturing are the major issues in the current voting system the blockchain is said an emerging, decentralized, and distributed technology that promises to enhance different aspects of many industries. Expanding e-voting into blockchain technology could be the solution to eliminate the present concerns in the e-voting system.**

***Keywords*—Blockchain, Ethereum, Decentralized, Digitalizing.**

I. INTRODUCTION

Extensive research has been done on electronic voting systems that enable voters vote at their convenience using a mobile phone, computer, or any other electronic device. Still, none of these technologies have been incorporated on a larger scale due to inherent security threats/concerns that these systems might pose to the integrity of the voting process. In this paper, we discuss an electronic voting system using blockchain, a secure and robust system that ensures anonymity of the voter, transparency, and robust functioning.

II. LITERATURE SURVEY

A. Online Voting System for India Based on AADHAR ID - Himanshu Agarwal, G. N. Pandey in the year 2013. A high-security password is checked in the main database before voting is allowed. The voter will be able to confirm if the vote is transferred to the correct candidate or party. A person from his or her allocated constituency may also vote. The tallying of the votes can be done manually, thus saving the data.

B. Biometric voting system using Aadhar card in India- S Chakraborty, S Mukherjee in the year 2016. The main goal of this venture is to build a safe electronic voting machine using a Fingerprinting technique that distinguishes evidence, so that we can use the Aadhar card database for specific marks. The online voting confirmation process should be possible during the race voting season using finger vein detection, which enables the electronic poll reset to allow voters to cast their votes.

C. Trustworthy Electronic Voting Using Adjusted Blockchain Technology - Basit Shahzad Raju, Jon Crowcroft in the year 2019 This paper suggests a system that makes use of appropriate hashing methods to ensure data security. This paper introduces the concept of block-creation and block sealing. The implementation of a block sealing principle helps to make the blockchain flexible to meet polling process requirements.

D. Security Analysis of India's Voting Machine - Hari K. Prasad, Arun Kankipati, Sai Krishna Sakhamuri in the year 2010. A Real Indian EVM Security Review is taken from an anonymous source. The paper states that EVM is vulnerable to extreme attacks that may alter the outcome and

breach the ballot's confidentiality. Using custom hardware, two attacks have been demonstrated.

III. PROPOSED SYSTEM

We are proposing a system that has greater accessibility as it is an Android application and possesses greater security as authentication. The system has been designed to support a voting application in the real- world environment considering specific requirements such as privacy, eligibility, convenience, receipt freeness and verifiability. The proposed system aims to achieve secure digital voting without compromising its usability. Within this context, the system is designed using a web-based interface to facilitate user engagement with measures such as mobile voting. With a clear need to administer the voters, constituencies, and candidates for constituencies, a user-friendly administrator interface is implemented to enable ease of access. Furthermore, the system allows all voters equal rights of participation and develops a fair and healthy competition among all the candidates while keeping the anonymity of the voters preserved. The cryptographic hash of the transaction (ID) is given to the voter as proof that the vote has been cast which may later on be tracked outside the premises of the constituency.

IV. PROPOSED METHODOLOGY

A. BLOCKCHAIN

Blockchain is a decentralized, distributed, public ledger. Blockchain is of three different types, i.e. public, private, and consortium blockchain. Ethereum and Bitcoin are examples of a public blockchain. This is proven by the complex mathematical functions. This research uses a public blockchain (Ethereum). Blockchain consists of a chain of blocks where a block is the primary component of the blockchain. A block is the header and the body, the block body contains the transactions that are being written to the network. The block header contains the block information which includes the previous hash, nonce value and difficulty, block timestamp, and transactions. Each block also stores information about the person participating in the transaction. The block length is variable and is estimated to be about 1 and 8 MB in size. The block header uniquely defines the block which should be put.

Working of Blockchain:

Blockchain is a system that is built around peer to peer system that can be shared openly among the users to generate a record of transaction that is immutable. In order to generate a block, a transaction needs to occur, after that the legitimacy of transaction needs to be verified. The transaction will then be stored in the block and a hash value must be given to the block for sealing. Thus, a block is created and sealed (fig.1).

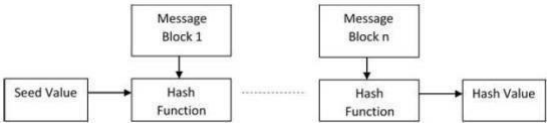

Fig. 1. Blockchain

B. ETHEREUM

Complex legal and financial applications such as Smart contracts can be built and deployed using Ethereum as an open platform. Ethereum can be imagined as a programmable Bitcoin in which the underlying blockchain can be used by developers to build markets, mutual ledgers, digital associations, and other endless possibilities involving unchanging data and agreements, all without the need for a middleman. Released in 2015, Ethereum is the brainchild of prodigious Vitalik Buterin who saw the possible applications of Bitcoins by Blockchain technologies as the next move in furthering the growth of the Blockchain culture. Ethereum is now the cryptocurrency with the second- highest coin market cap and is projected to overtake Bitcoin as both a valued investment and the most common cryptocurrency in the world.

C. HASHING

Hashing is the method of adjusting the arbitrary and variable input size to a fixed output size. Various functions perform different levels of hashing. We have implemented security by using SHA-256. SHA- 256 is one of the SHA-1 (collectively referred to as SHA-2) successor hash functions and is one of the strongest hash functions available. SHA-256 is not much more difficult to code than SHA-1 and is in no way corrupted yet. The 256-bit key makes AES a good partner feature which is a symmetrical key encryption cipher, meaning that the same key is used for encryption and decryption. Unlike its predecessors, the algorithm's versatility is that it embraces any input length and produces an arbitrary output length, whilst all other algorithms generate a set output length.

V. SOFTWARE REQUIREMENTS

A. EXPRESS JS:

Express.js is a lightweight and flexible web application framework for Node.js designed to build robust web applications and APIs efficiently. Known for its simplicity and performance, Express.js provides developers with essential tools to handle HTTP requests, manage routing, and integrate middleware for processing data. Its unopinionated nature allows developers to structure their applications freely while offering powerful features such as static file serving, template engine support, and seamless integration with databases like MongoDB and MySQL. Express.js is widely used for developing RESTful APIs, single-page applications, and server-side rendering. Its extensive ecosystem and compatibility with other Node.js modules make it an excellent choice for scalable and modern web development projects.

B. WEB3 JS:

Web3.js talks to The Ethereum Blockchain with JSON RPC, which stands for "Remote Procedure Call" protocol. Ethereum is a peer- to-peer network of nodes that stores a copy of all the data and code on the blockchain. Web3.js allows us to make requests to an individual.

Ethereum node with JSON RPC to read and write data to the network. It's kind of like using jQuery with a JSON API to read and write data with a web server. Mostly for convenience, you can use Infura to access an Ethereum node without having to run one yourself. Infura is a service that provides a remote Ethereum node for free. All you need to do is sign up and obtain an API key and the RPC URL for the network you want to connect to. The Ethereum Blockchain. It is a collection of libraries that allow you to perform actions like sending Ether from one account to another, reading and writing data from smart contracts, creating smart contracts, and so much more.

C. META MASK:

Fig 2. Meta Mask

Meta Mask is a free web and mobile crypto wallet that allows users to store and swap cryptocurrencies, interact with the Ethereum blockchain ecosystem, and host a growing array of decentralized applications (DApps),(fig.2).

It is one of the most widely used crypto applications in the world. Over ten million active monthly users logged into Meta Mask in August of 2020. In earlier versions, Meta Mask was only available as a desktop browser plugin for Firefox and Chrome, but in September 2020, Meta Mask Mobile was released for both Android- and iOS-powered devices. Meta Mask quickly established itself as the standard bearer for self-managed, non- custodial crypto wallets — in part thanks to its user experience (UX) and frequent updates. It has played an essential role in raising the standards of usability in blockchain and crypto technology, laying the foundation for the explosive growth of sectors like decentralized finance (DeFi) and non-fungible tokens (NFTs) by simplifying and streamlining the Ethereum user experience into one simple wallet interface.

D. ETHEREUM 2.0:

The launch of Ethereum 2.0 is especially significant compared to past upgrades because of the implementation of a Proof of Stake consensus mechanism, moving the network away from its existing Proof of Work architecture. Proof of Stake (PoS) is the most significant change in Ethereum 2.0 because it reforms the crypto economic incentive structure for validating the blockchain. Ethereum's current architecture is maintained by a Proof of Work (PoW) consensus mechanism. The components of Proof of Work are well-known to the blockchain community: it is the architecture used for the most utilized blockchains to date, including Bitcoin, Ethereum, Litecoin, and more. In Proof of Work, miners run nodes and expend computational energy to solve complex mathematical problems in a competition to mine the next block. The time and money that miners need to run hardware and expend electricity on PoW chains are validated by block rewards, which are distributed to miners who successfully mine a block into existence. PoW chains are extremely secure; the combined computational power required for an individual to compromise a well-established PoW blockchain like Bitcoin or Ethereum would cost an extraordinary amount of money, and may not even exist.

VI. WORKING

6.1. Meta Mask: A software cryptocurrency wallet, which is used to interact with the Ethereum blockchain. It allows users to access their Ethereum wallet through a browser extension or mobile app, which can then be used to interact with decentralized applications.

6.2. Truffle and Ganache: Truffle is a framework that was used throughout the process of developing the prototype. It was helpful by having the ability to act as a package manager, but also came with built-in functionality to compile Solidity code and deploy it to a blockchain. Truffle offered three different commands: truffle compile, truffle migrate, and truffle test which were used to compile the contracts, deploy them to a blockchain on the network, and perform tests on them. Ganache was used to simulate an Ethereum blockchain on a local machine. It came in two different representations, GUI and CLI. The below figure.3 is a Sequence diagram that demonstrates how the prototype starts and ends an election. It visualizes the steps before Alice votes, what happens when an election ends, and how Bob, as a consequence of ending the election, can access the results. The vertical lines represent a timeline that starts at the top of the diagram.

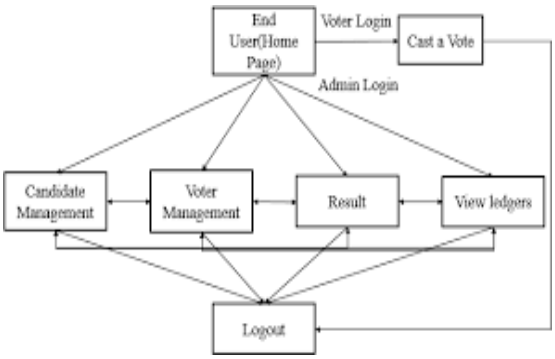

Fig 3. Blockchain-based voting system

6.3. Smart contracts: The purpose of the smart contracts is to act as a back-end for the system. They contain different variables, functions and provide rules for how the voting process works.

Due to the limitations of Ethereum, such as private variables that are not truly private and all transactions being public, solutions for keeping data inaccessible had to be made. Specialized tools were used to support the development of smart contracts Election administrators: Manage the lifecycle of an election. Multiple trusted institutions and companies are enrolled in this role. The election administrators specify the election type and create aforementioned election, configure ballots, register voters, decide the lifetime of the election, and assign permissioned nodes.

6.4. Voters: For elections to which they are eligible themselves, load election ballots, cast their vote, and verify their vote after an election is over. Voters can be rewarded for voting with tokens when they cast their vote in an election shortly, which could be integrated with a smart city project.

6.5. District nodes: When the election administrators create an election, each ballot smart contracts, representing each voting district, are deployed onto the blockchain. When the ballot smart contracts are created, each of the corresponding district nodes is permitted to interact with their corresponding ballot smart contract. When an individual voter casts his vote from his corresponding smart contract, the vote data is verified by all of the corresponding district nodes and every vote they agree on is appended onto the blockchain when block time has been reached.

6.6. Boot nodes: Each institution, with permissioned access to the network, hosts a boot node. A boot node helps the district nodes to discover each other and communicate. The boot nodes do not keep any state of the blockchain and are run on a static IP so that district nodes find their peers faster.

6.7. Vote transaction: When an individual vote at a voting district, the voter interacts with a ballot smart contract with the same voting district as is defined for any individual voter (fig.4). This smart contract interacts with the blockchain via the corresponding district node, which appends the vote to the blockchain if consensus is reached between the majority of the corresponding district nodes.

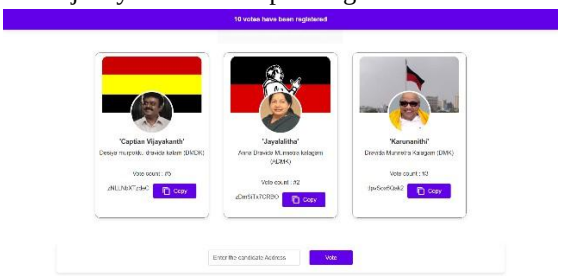

Fig.4: Final Output

VII. DISCUSSION AND FUTURE WORK

Many issues with electronic voting can be solved using blockchain technology, which makes electronic voting more cost-effective, pleasant, and safe than any other network. Over time, research has highlighted specific problems, such as the need for further work on blockchain-based electronic

voting and that blockchain-based electronic voting schemes have significant technical challenges.

7.1. Scalability and Processing Overheads

For a small number of users, blockchain works well. However, when the network is utilized for large-scale elections, the number of users increases, resulting in a higher cost and time consumption for consuming the transaction. Scalability problems are exacerbated by the growing number of nodes in the blockchain network. In the election situation, the system's scalability is already a significant issue.

An electronic voting integration will further impact the system's scalability based on blockchain elucidate different metrics or properties inherent to all blockchain frameworks and present a comparative analysis of some blockchain-based platforms such as Bitcoin, Ethereum, Hyperledger Fabric, Litecoin, Ripple, Dogecoin, Peercoin, etc.

One way to enhance blockchain scaling would be to parallelize them, which is called sharding. In a conventional blockchain network, transactions and blocks are verified by all the participating nodes. To enable high concurrency in data, the data should be horizontally partitioned into parts, each known as a shard.

7.2. User Identity

As a username, blockchain utilizes pseudonyms. This strategy does not provide complete privacy and secrecy. Because the transactions are public, the user's identity may be discovered by examining and analyzing them. The blockchain's functionality is not well suited to national elections.

7.3. Transactional Privacy

In blockchain technology, transactional anonymity and privacy are difficult to accomplish. However, transactional secrecy and anonymity are required in an election system due to the presence of the transactions involved. For this purpose, a third-party authority required but not centralized, this third-party authority should check and balance privacy.

7.4. Energy Efficiency

Blockchain incorporates energy-intensive processes such as protocols, consensus, peer- to-peer communication, and asymmetrical encryption. Appropriate energy-efficient consensus methods are needed for blockchain- based electronic voting. Researchers suggested modifications to current peer-to-peer protocols to make them more energy-efficient.

7.5. Immatureness

Blockchain is a revolutionary technology that symbolizes a complete shift to a decentralized network. It has the potential to revolutionize businesses in terms of strategy, structure, processes, and culture. The current implementation of blockchain is not without flaws. The technology is presently useless, and there is little public or professional understanding of it, making it impossible to evaluate its future potential. All present technical issues in blockchain adoption are usually caused by the technology's immaturity.

7.6. Acceptableness

While blockchain excels at delivering accuracy and security, people's confidence and trust are critical components of effective blockchain electronic voting. The intricacy of blockchain may make it difficult for people to accept blockchain-based electronic voting, and it can be a significant barrier to ultimately adopting blockchain-based electronic voting in general public acceptance. A big marketing campaign is needed for this purpose to provide awareness to people about the benefits of blockchain voting systems, so that it will be easy for them to accept this new technology.

7.7. Political Leaders' Resistance

Central authorities, such as election authorities and government agencies, will be shifted away from electronic voting based on blockchain. As a result, political leaders who have profited from the existing election process are likely to oppose the technology because blockchain will empower social resistance through decentralized autonomous organizations.

VIII. CONCLUSION

The goal of this research is to analyze and evaluate current research on blockchain- based electronic voting systems. The article discusses recent electronic voting research using blockchain technology. The blockchain concept and its uses are presented first, followed by existing electronic voting systems. Then, a set of deficiencies in existing electronic voting systems are identified and addressed. The blockchain's potential is fundamental to enhancing electronic voting, current

solutions for blockchain-based electronic voting, and possible research paths on blockchain-based electronic voting systems. Numerous experts believe that blockchain may be a good fit for a decentralized electronic voting system.

Furthermore, all voters and impartial observers may see the voting records kept in these suggested systems. On the other hand, researchers discovered that most publications on blockchain-based electronic voting identified and addressed similar issues. There have been many study gaps in electronic voting that need to be addressed in future studies. Scalability attacks, lack of transparency, reliance on untrustworthy systems, and resistance to compulsion are all potential drawbacks that must be addressed. As further research is required, we are not entirely aware of all the risks connected with the security and scalability of blockchain- based electronic voting systems.

IX. REFERENCE

[1] R. Hanifatunnisa and B. Rahardjo, "Blockchain- based e-voting recording system design," 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), Lombok, 2017, pp. 1-○

[2] R. Krimmer, A. Ehringfeld, and M. Traxl, "The Use of E-Voting in the Austrian Federation of Students Elections 2009," Internet: https://pdfs.semanticscholar.org/6b8f/34a5bd 3e7eabc7e3a9a3f00818 7e4415e26a.pdf [Nov. 26, 2018]

[3] "The Geneva Internet Voting System" Internet: F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa and G. Hjálmtýsson, "Blockchain-Based E-Voting System," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, 2018, pp. 983-986.

[4] S. Ølnes, J. Ubacht and M. Janssen, "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing", Government Information Quarterly, vol. 34, no. 3, pp. 355-364,2017. https://www.coe.int/t/dgap/goodgovernance/ Activities/Evoting/EVoting_Documentation/pas sport_e voting2010.pdf [Nov. 25, 2018]

[5] A. Barnes, C. Brake, and T. Perry, "Digital Voting with the use of Blockchain Technology,"Available: https://www.economist.com/sites/default/file s/plymouth.pdf [Nov. 20, 2018] ○ A. Barnes, C. Brake, and T. Perry, "Digital Voting with the use of Blockchain Technology," Available: https://www.economist.com/sites/default/file s/plymouth.pdf [Nov. 20, 2018] ○ M. Pawlak, Poniszewska-Marańda and N. Kryvinska, "Towards the intelligent agents for blockchain e-voting system," Procedia Computer Science, vol. 141, pp. 239-246, 2018.

[6] P. Tarasov and H. Tewari, "The Future of E-voting," IADIS International Journal on Computer Science and Information Systems, vol. 12, no. 2, pp. 148-165. ○ Bartolucci, S., Bernat, P., & Joseph, D. (2018). SHARVOT: Secret SHARe-Based VOTing on the Blockchain. 2018 IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), 30-34.

[7] Reyna, C. Martín, J. Chen, E. Soler and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities", FutureGeneration Computer Systems, vol. 88, pp. 173-190, 2018. 22

[8] Wang, J. Sun, Y. He, D. Pang and N. Lu, "Large-scale Election Based On Blockchain", Procedia Computer Science, vol. 129, pp. 234-237, 2018.Internet: https://lisk.io/academy/blockchain- basics/how- does-blockchainwork/delegated-proof of stake [Nov.25, 2018]○Internet: https://www.turkiye.gov.tr/ [Nov. 25, 2018].

[9] Sos.ca.gov. (2007). Top-to-Bottom Review | California Secretary of State. Available at: http://www.sos.ca.gov/elections/voting-systems/ oversight/ top-bottom-review/.

[10] Nicholas Weaver. (2016). Secure the Vote Today. Available at:https:// www.lawfareblog.com/ secure-vote-today.

[11] TechCrunch, (2018). Liquid democracy uses blockchain to fix politics, and now you can vote for it [Online]. Available at: https://techcrunch. com/2018/02/24/liquid-democracyuses- blockchain/ Geth.ethereum.org. (2018). Go Ethereum. Available at: https://geth. ethereum.org/

[12] Vitalik Buterin. (2015). Ethereum White Paper. Available at: https:// github.com/ethereum/wiki/wiki/White-Paper. Nca.tandfonline.com. (2015). Pirates on the Liquid Shores of Liberal Democracy: Movement Frames of European Pirate Parties. [Online]. Available at: https://nca.tandfonline.com/doi/abs/10.1080/ 13183222.2015.1017264#.Wr0zCnVl8YR

[13] Feng Hao, P.Y.A. Ryan and Piotr Zielinski. (2008). Anonymous voting by two-round public discussion. Available at: http://homepages.cs.ncl.ac. uk/feng.hao/files/OpenVote_IET.pdf Feng Hao and Piotr Zielinski. A 2-Roun Anonymous Veto Protocol Available at:. The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability. Available at: https://users.ece.cmu.edu/~{}adrian/ 731-sp04/readings/dcnets.html