A Systematic Survey
on
E-VOTING SYSTEM USING BLOCKCHAIN TECHNOLOGY

1st Prof. Bhagyashree Kadam
Department of Information Technology Sinhgad Institute of Technology and Science,Narhe
Pune,India
bhagyashree.kadam.sits@sinhgad.edu

2nd Siddhi Phalle
Department of Information Technology Sinhgad Institute of Technology and Science,Narhe
Pune,India
siddhiphalle.sits.it@gmail.com

3rd Pranjali Khairnar
Department of Information Technology
Sinhgad Institute of Technology and Science,Narhe
Pune,India
pranjalikhairnar.sits.it@gmail.com

4th Apurva Mulik
Department of Information Technology
Sinhgad Institute of Technology and Science,Narhe
Pune,India
apurvamulik.sits.it@gmail.com

5th Tushar Gunjal
Department of Information Technology Sinhgad Institute of Technology and Science,Narhe
Pune,India
tushargunjal.sits.it@gmail.com

Abstract*–An electronic voting system based on blockchain technology, addressing the challenges of traditional paper ballots and digital voting methods. The system aims to provide security, integrity, transparency, and privacy for voters. It evaluates various blockchain frameworks and proposes a novel e-voting system that can be particularly useful for small-scale elections within corporate environments. The implementation relies on Ethereum's smart contracts, with development and testing facilitated by the Truffle framework and Ganache as the Ethereum client for testing. It also highlights the historical challenges in developing secure electronic voting systems that balance fairness and privacy with transparency and flexibility. The paper explores the application of blockchain technology in addressing these issues, emphasizing the potential of distributed ledger technology for hosting nationwide elections securely and cost-effectively. The paper also underscores the significance of blockchain technology in ensuring anonymity, privacy, verifiability, and fairness in the voting process.

Keywords- Blockchain, Decentralized, Ethereum, E-Voting, Smart Contracts.

I. Introduction

Democracy is defined as the ability of the people to elect their government. Voting is a crucial step that allows citizens to choose their government's head of state. A democratic, unbiased, and independent electoral system is required[1]. The most common method of expressing public opinion is through elections, which allow voters to choose their representative from a field of contenders. A fair election must be held in order for a nation to be considered democratic, giving voters a chance to endorse the democratic government's methods of operation. Only through holding fair elections will an authorized authority be able to maintain the public's faith in democracy. The election will be conducted using a variety of voting procedures worldwide. Many nations continue to use a traditional paper-based voting system in the age of digital information, which makes it difficult to hold an election that is free and fair[1], [9]. This traditional voting process has seen a number of problems, including booth capture, vote paper theft, and uneven counting. The introduction of an electronic voting machine (EVM) provides the ability for every vote to be recorded and counted accurately and fairly. In addition, EVMs make it simple to tabulate results, produce results that are more accurate and happen faster than traditional paper-based voting systems[3]. Blockchain is a decentralized network where users retain identical data replication while exchanging data with other node members. Blockchain technology offers features including data accuracy, privacy, and distribution. A trustworthy and secure electronic voting system can be created with the aid of blockchain technology. A dApp is a distributed web application that runs on the Ethereum blockchain. It has features that allow for the creation and operation of Smart Contracts and dApps without the usage, interference, or falsification of third parties. Smart contracts may be used by DApps to interact with the blockchain. It is accepted that a worldwide Ethereum virtual machine (EVM) device can be used to execute smart contracts.

When a smart contract is added to an EVM (Ethereum virtual machine), the code can no longer be changed or corrected and the EVM becomes static[1]. The number of decentralized and distributed apps has significantly increased because to Ethereum's specific-purpose virtual machine and specialized programming language. These characteristics have fostered a vibrant developer community, continuous improvement, and the introduction of novel technical possibilities.

This paper is organized as follows: Section 2 introduces necessary background study of Blockchain anf e-voting system. Section 3 describes the challenges that occurs in this process. Section 4 describes what technogies are required to implement this project. Section 5 concludes the paper.

II. Related Work

Blockchain technology has emerged as a transformative force across a multitude of industries.These papers collectively highlight the blockchain's potential to reshape the modern landscape, offering innovative solutions and disrupting traditional paradigms.

In recent years, blockchain technology has emerged as a promising solution for enhancing the security and transparency of electronic voting systems. Several research papers have explored the diverse applications of blockchain in e-voting, addressing critical issues such as verifiability, fraud prevention, and trust in electoral processes.

A. *Application Background*

This research paper suggests the Byzantine Fault Tolerance (PBFT) consensus algorithm for the practical data security of blockchain digital currency in the transmission process, discussing the Bitcoin transaction process as an example, and thoroughly analyzing the application of searchable technology and the test results of encrypted key words. The experimental results demonstrate the viability and efficacy of this method.[10]

The proposed framework's two main goals are to first adopt blockchain technology for electronic health records and, second, to guarantee secure electronic record storage by outlining specific access guidelines for users. These technologies allow users total command and control over their personal data. Compared to any conventional system, it offers a much better ability to share and manage personal healthcare records.[11]

This study analyzes the use of private and public blockchains for insurance services through the trial and error use of smart contracts built on the Ethereum and Hyperledger Fabric platforms. The Ethereum Blockchain is the foundation for the suggested public insurance smart contract system. In comparison to the prior public approach, the proposed private solution using codechains on Hyperledger Fabric is more adaptable, more secure, quicker, and less expensive.[12]

The suggested work leverages the Ethereum smart contract for food supply chain management systems, which prevents information falsification, database corruption, and external threats. The challenges with centralized food supply chains have been described in the paper, along with how the blockchain implementation of the food supply chain has addressed them. The research also examined how several food-related companies used blockchain technology.[13]

By restructuring the system and applying blockchain technology without the use of tokens, the disadvantage of this centralized system can be lessened. Decentralized architecture is used by blockchain to store and access data across a database. One can lessen attacks on the system by using blockchain to distribute databases on banking systems. In order to create a system that is more dependable for banking to carry out transactions that must be protected at a very high level, blockchain without tokens is essential.[14]

B. *Technical Background*

In this research paper, three smart contracts that carry out various tasks related to the entire election process are discussed. As a result, the third party's engagement is lower than that of other existing systems. Up until the election's conclusion, the cast votes are kept secret. No one has been able to connect the vote to the voter.[1]

This study proposes a blockchain-based electronic voting system that guarantees voter anonymity while enabling safe and economical elections. Blockchain technology safeguards election security and integrity and paves the road for transparency by presenting a novel means to get over the limitations and adoption issues associated with electronic voting techniques.[2]

This research paper claims that our suggested digital voting systems have accomplished data integrity, anonymity, privacy, and security of the voters through the usage of markle tree and fingerprint hashes. enables voters to cast ballots via mobile devices from anywhere by creating the necessary conditions. This will assist in increasing the number of votes needed to establish democracy in any nation.[3]

This research paper discusses the difficulties that both traditional and electronic voting procedures encounter. the author guarantee a transparent, secure, and tamper-proof voting process by employing blockchain technology. Blockchain's decentralized structure avoids the dangers posed by centralized databases, offering a reliable framework for free elections.[4]

In order to develop a safe, open, and transparent voting system, the research paper suggests a cutting-edge mobile voting framework that incorporates blockchain technology with multi-factor authentication. in the use of mobile voting, there are difficulties in managing votes safely and preventing tampering. By doing away with traditional polling places, it enables voters to conveniently cast their ballots using mobile devices.[5]

III. Challenges

Blockchain technology presents a range of challenges when applied in real-world scenarios. One of the primary challenges is scalability, as blockchain networks face limitations in transaction throughput, making it difficult to handle large volumes of data efficiently. Privacy and data protection concerns are also significant, given that public blockchains inherently expose all transaction details, which is not always desirable in sensitive applications. Interoperability issues persist across various blockchain platforms, hindering seamless data and value exchange. Additionally, the security of smart contracts is a continual concern, as vulnerabilities in these self-executing contracts can lead to critical exploits. Regulatory uncertainty and compliance issues present legal challenges that vary from one jurisdiction to another. Addressing these multifaceted challenges is essential for realizing the potential of blockchain in diverse industries and use cases.
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.

IV. Technologies Required

Blockchain technology is a decentralized and transparent digital ledger system that securely records and stores transactions across a network of interconnected computers. It ensures data integrity and tamper resistance through cryptographic techniques, making it virtually impossible to alter once a transaction is recorded. Originally designed for cryptocurrencies like Bitcoin, blockchain's applications have expanded to include smart contracts, supply chain management, healthcare, finance, and more. It relies on consensus mechanisms like Proof of Work and Proof of Stake to validate and add transactions, offering the potential for increased security, trust, and efficiency in various industries, though it also faces challenges related to scalability and regulation.

A. *Ethereum*

Ethereum, a leading blockchain platform, is distinguished by its incorporation of smart contract functionality, enabling the creation of decentralized applications (DApps) and au- tomated self-executing agreements. Its native cryptocurrency, Ether (ETH), is used for transaction fees and computational services within the network. Ethereum operates with a Proof of Work (PoW) consensus mechanism but is actively working on transitioning to a more energy-efficient Proof of Stake (PoS). The platform fosters innovation and interoperability through Ethereum Improvement Proposals (EIPs) and has played a pivotal role in the development of decentralized finance (DeFi) and the broader blockchain ecosystem, despite facing scalability challenges, which the community is working to address.[1]

B. Smart Contract

Smart contracts are self-executing, code-based agreements that run on blockchain technology, automating the execution of predefined actions when specific conditions are met. These contracts eliminate the need for intermediaries and facilitate trust in transactions by ensuring transparency and security. They can be utilized for a wide range of applications, from financial services like lending and trading to supply chain management and decentralized applications (DApps). Smart contracts are a fundamental innovation in blockchain, enabling programmable and trustless interactions, and they have the potential to revolutionize how agreements and transactions are conducted in a wide variety of industries.[2]

Truffle

Truffle is a popular development framework for Ethereum that simplifies the process of building and deploying smart con- tracts and decentralized applications (DApps) on the Ethereum blockchain. It provides a suite of tools and a development environment that streamlines the development and testing of Ethereum-based projects. Truffle is widely used by Ethereum developers and is known for its ease of use and robust features. Truffle greatly simplifies the development workflow for Ethereum projects, making it a valuable tool for both experienced and novice blockchain developers. It has become a standard in the Ethereum development ecosystem and is widely used for building and deploying decentralized applications and smart contracts. Truffle has a strong developer community and offers extensive documentation, tutorials, and resources to help developers get started and troubleshoot issues.[8]

C. Solidity

Solidity is a high-level programming language specifically designed for writing smart contracts on blockchain platforms. Smart contracts are self-executing contracts with the terms of the agreement directly written into code. Solidity is essential for developing decentralized applications (DApps) and other blockchain-based systems that require automation and trust. Developers use Solidity to create custom smart contracts that define the rules and logic for various decentralized applications, such as token contracts, decentralized finance (DeFi) appli- cations, and more. These contracts are then deployed on the Ethereum blockchain, where they execute autonomously and transparently, without relying on a central authority. Solidity is a crucial tool for building blockchain-based solutions and contributing to the growth of the decentralized ecosystem. Solidity code is compiled into bytecode that can be executed on the Ethereum Virtual Machine, the runtime environment for Ethereum smart contracts.[1]

D. Ganache

Ganache is a popular and widely used development tool in the Ethereum ecosystem. It is often used by blockchain developers for local testing, development, and debugging of Ethereum smart contracts and decentralized applications (DApps). It provides a local, private Ethereum blockchain environment that is fully configurable and runs on your own computer. Ganache creates a local, in-memory Ethereum blockchain on your development machine. This allows developers to test and interact with smart contracts and DApps in a controlled environment without interacting with the live Ethereum network. It is an invaluable tool for Ethereum developers, as it allows them to build, test, and debug their smart contracts and DApps in a controlled and efficient environment before deploying them to the live Ethereum network. It’s particularly useful for conducting local unit tests and for simulating different network conditions, ensuring that applications work as intended and are secure before they are released to the wider Ethereum ecosystem.[8]

CONCLUSION

In conclusion, the introduction of a blockchain-based elec- tronic voting system with smart contracts offers a transforma- tive solution to the challenges and limitations of traditional electronic voting systems. By ensuring security, privacy, and transparency, this innovative approach has the potential to

revolutionize elections. Through the use of Ethereum private blockchains, hundreds of transactions per second can be pro- cessed, though additional measures may be necessary for larger countries. The integration of smart contracts reduces third-party involvement, enhancing credibility. Encrypted votes and hashed voter information protect anonymity and reduce costs. Verifica- tion mechanisms further empower voters to participate remotely, potentially increasing voter turnout and advancing democracy. This system stands as a beacon of maximum security, including anonymity, integrity, privacy, fairness, verifiability and mobility, making it a promising choice for future elections.

REFERENCES

[1] Syada Tasmia Alvi , Mohammed Nasir Uddin , Linta Islam , Sajib Ahamed *”DVT Chain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system”*

[2] Fridrik p. Hjalmarsson , Gunnlaugur K. Hreidarsson , Mohammad Hamdaqa , Gisli Hjalmtysson *”Blockchain-Based E-Voting System”*

[3] Syada Tasmia Alvi, Mohammed Nasir Uddin , Linta Islam *”Digital Voting: A Blockchain-based E-Voting System using Bio hash and Smart Contract”*

[4] Rabeya Bosri, Abdur Razzak Uzzal, Abdullah Al Omar, ASM Touhidul Hasan *”Towards A Privacy-Preserving Voting System Through Blockchain Technologies”*

[5] T. P. Abayomi-Zannu 1, I. A. Odun-Ayo 1 and T. F. Barka *”A Proposed Mobile Voting Framework Utilizing Blockchain Technology and Multi-Factor Authentication”*

[6] R. Krishnamurthy , Geetanjali Rathee , Naveen Jaglan *”An enhanced security mechanism through blockchain for E-polling/counting process using IoT devices”*

[7] Alperen Kantarci, Serif Bahtiyar, Rumeysa Bulut, Safa Keskin *”Blockchain-Based Electronic Voting System for Elections in Turkey”*

[8] Patidar , Dr. Swapnil Jain *”Decentralized E-Voting Portal Using Blockchain”*

[9] Basit Shahzad , Jon Crowcroft *”Trustworthy Electronic Voting Using Adjusted Blockchain Technology”*

[10] Mengyi Xie, Zuobin Liao, Liting Huan *”Data Security Based on Blockchain Digital Currency”*

[11] Anurag Gharat, Pratik Aher, Punit Chaudhari and Bhavana Alte *”A Framework for Secure Storage and Sharing of Electronic Health Records using Blockchain Technology”*

[12] Veneta Aleksieva, Hristo Valchanov, Anton Huliyan *”Smart Contracts based on Private and Public Blockchains for the Purpose of Insurance Services”*

[13] D Sathya, S Nithyaroopa, D Jagadeesan, I Jeena Jacob *”Blockchain Technology for Food supply chains”*

[14] Niturkar Pallavi Pravin, Kulat Pratiksha Anil,Sukate Manasi Sunil, Mod- have Snehal Kundlik,Phalke Akshay Suhas *”Block chain technology for protecting the banking transaction without using tokens”*