IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue1, November 2023

Utilizing Blockchain Technology and Fingerprint Authentication for an Electronic Voting System.

Mr. Rohan Hivrale, Mr. Rushant Bendre, Mr. Rupesh Ahire, Mr. Parth Palange, Prof. Varsha Garad
Department of Computer Engineering
Shree Ramchandra College of Engineering, Pune, Maharashtra, India

Abstract: *The advent of digital technology has brought about a significant transformation in people's lives. However, unlike various aspects of modern life that have embraced digitalization, the electoral system continues to rely heavily on conventional paper-based methods. This reliance poses challenges to the fundamental principles of security and transparency, particularly in traditional offline elections. Presently, general elections employ a centralized system managed by a single organization, leading to potential vulnerabilities within the system. The concentration of control over the database presents opportunities for manipulation. Leveraging blockchain technology offers a viable solution by introducing a decentralized system where the database is collectively owned by multiple users. Blockchain's effectiveness in decentralized systems, as evidenced by its successful application in Bitcoin, presents an opportunity to address the vulnerabilities of the traditional electoral system. This project seeks to implement a blockchain-based algorithm for recording voting results across all polling locations. Unlike Bitcoin's Proof of Work mechanism, this approach will employ a predetermined rotation system for each node within the blockchain structure, ensuring enhanced security and integrity in the electoral process.*

Keywords: Security Measures, Safeguarding, Online Voting System, Voter Authentication, Visual Secret Sharing

I. INTRODUCTION

The era of digitization has ushered in electronic voting systems for general elections across several countries. Estonia pioneered nationwide public e-voting in 2005, followed by countries like Switzerland and Norway embracing similar systems. However, the transition from traditional ballot systems to e-voting encountered a significant challenge: ensuring voter privacy and vote integrity post-casting. The paramount concern was to prevent tampering or manipulation of votes under any external influence. Despite attempts to maintain anonymity, vulnerabilities remained, allowing certain agencies to detect and intercept votes cast. Blockchain technology presents a secure and reliable solution to fortify these systems. Since the inception of democratic elections, the voting process has relied on the conventional pen-and-paper paradigm. Introducing a new election system to replace this traditional approach is a burgeoning idea among researchers. An e-voting system demands robust security measures to ensure accessibility to voters while safeguarding against external manipulations that could alter cast votes or compromise the integrity of a voter's ballot. The recent adoption of electronic voting systems in various countries, starting with Estonia for its national elections [1], followed by Switzerland for statewide elections [2], and Norway for council elections [3], underscores the need for these systems to match the security and anonymity provided by traditional methods. Heightened security measures are imperative for an e-voting system to remain accessible to voters while shielding against external influences that might tamper with votes or compromise ballot integrity. Although many electronic voting systems rely on techniques to conceal voter identities [4], these measures fall short of ensuring complete anonymity or integrity, as numerous intelligence agencies worldwide possess control over segments of the Internet, potentially enabling identification or interception of votes.

1.1 Blockchain

Blockchain represents a type of distributed ledger technology (DLT) comprising a continuously growing list of records, referred to as blocks. These blocks are securely linked together using cryptography. Each block contains a

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue1, November 2023

cryptographic hash of the previous block, a timestamp, and transaction data, often depicted as a Merkle tree, where data nodes are visualized as leaves. The timestamp serves as proof that the transaction data existed at the time the block was created. As each block includes information about its predecessor, they form a sequential chain, akin to a linked list data structure, with each subsequent block linked to those that precede it. Consequently, once recorded, blockchain transactions become irreversible; the data within a specific block cannot be retroactively altered without modifying all subsequent blocks. Typically managed by a peer-to-peer (P2P) network, blockchains serve as public distributed ledgers. Nodes in this network adhere to an agreed-upon algorithmic protocol to validate and add new transaction blocks. While blockchain records are not entirely immutable due to the possibility of blockchain forks, they are often considered secure by design and represent a distributed system with high Byzantine fault tolerance.

1.2 Blockchain Features

A. Decentralization

The network operates in a decentralized manner, devoid of any central authority or singular oversight. Instead, a collective of nodes collectively maintains the network, ensuring its decentralized nature.

B. Immutability

Immutability signifies the inability to modify or alter something. This stands as one of the fundamental features of blockchain, ensuring that the technology remains constant—a permanent and unchangeable network.

C. Enhanced Security

By eliminating the necessity for a central authority, the system prevents unauthorized alterations to the network for personal gain. The utilization of cryptography adds an additional layer of security to fortify the system.

D. Distributed Ledgers

In most cases, a public ledger provides comprehensive information about transactions and participants, all openly available with no element concealed. While the scenario may differ slightly for private or consortium blockchains, many individuals still have visibility into the ledger's activities.

II. LITERATURE REVIEW

The rise of digital technology has ushered in a new era for the millennial generation, transforming traditional paper-based electoral processes into technologically-driven methods. However, this shift towards digitalization raises concerns regarding the security and integrity of cast votes, particularly in offline systems. Blockchain technology emerges as a potential solution, offering a decentralized system where the entire database is collectively owned by multiple users, thereby ensuring data integrity within the system [1].

Among the tech-savvy younger generation, there exists a notable deficiency in voter participation. E-voting presents itself as a viable solution to address this issue. Implementing blockchain technology in e-voting endeavors to enhance transparency and openness in the process [2]. While blockchain technology holds promise across various sectors, its full potential remains untapped.

Electronic voting has been in use since the 1970s, offering advantages such as improved accuracy and reduced errors compared to paper-based systems. The emergence of blockchain technologies has prompted extensive exploration into its feasibility for e-voting. Initiatives employing approaches like Multi-chain and comprehensive evaluations aim to assess the viability of integrating blockchain into e-voting systems [3].

III. CURRENT ELECTORAL SYSTEM

India has adopted electronic voting as the primary method for conducting elections, employing Electronic Voting Machines (EVMs). Developed and tested in the 1990s by the state-owned Electronics Corporation of India and Bharat Electronics, these machines were gradually introduced in Indian elections between 1998 and 2001.

Before the implementation of electronic voting, India relied on paper ballots and manual counting. However, this method faced severe criticism due to instances of fraudulent voting and booth capturing, wherein party loyalists seized control of polling booths and inserted pre-filled fake ballots. Moreover, the paper-based system incurred significant expenses, requiring extensive resources for the manual counting of millions of individual ballots.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue1, November 2023

Embedded features within the EVMs, such as electronic limitations on the rate of casting votes, security measures like the "lock-close" feature, and an electronic database storing voting signatures and thumb impressions for voter identity verification, have significantly curbed electoral fraud, eliminated booth capturing, and fostered fairer and more competitive elections. Indian EVMs function as standalone machines, utilizing read-only memory that's written to only once.

The EVMs undergo secure manufacturing processes and are intentionally designed to be self-contained, battery-powered, and devoid of any networking capabilities. These machines lack both wireless and wired internet components or interfaces. The M3 version of the EVMs incorporates the Voter Verifiable Paper Audit Trail (VVPAT) system for added transparency and verification of votes.

IV. PROPOSED SOLUTION

From a distance, the risk of encountering counterfeit or fake products looms large for the general public. The repercussions of such fraudulent products extend beyond mere reputational damage, often resulting in substantial losses for consumers. Devising a definitive solution to this issue has proven elusive. Conventional barcodes, easily replicated, lack a foolproof system to distinguish counterfeit goods from authentic ones.

Blockchain emerges as a highly promising technology in recent years, offering a potential remedy to this predicament. Leveraging Blockchain Technology can facilitate the monitoring and tracking of shipped products, ensuring that consumers receive only genuine products. The primary aim of this project is to bring transparency to the product lifecycle, empowering consumers to easily verify the authenticity of the products they intend to purchase, thereby distinguishing between original and counterfeit items effortlessly.

4.1. System Objectives

- The genesis of this project stems from the escalating issue of counterfeit products. The primary objectives of this project include:
- Implementing biometrics for verification and identification purposes.
- Utilizing SHA256 for enhanced security measures.
- Streamlining processes to reduce dependency on manual labor.

V. SYSTEM ARCHITECTURE

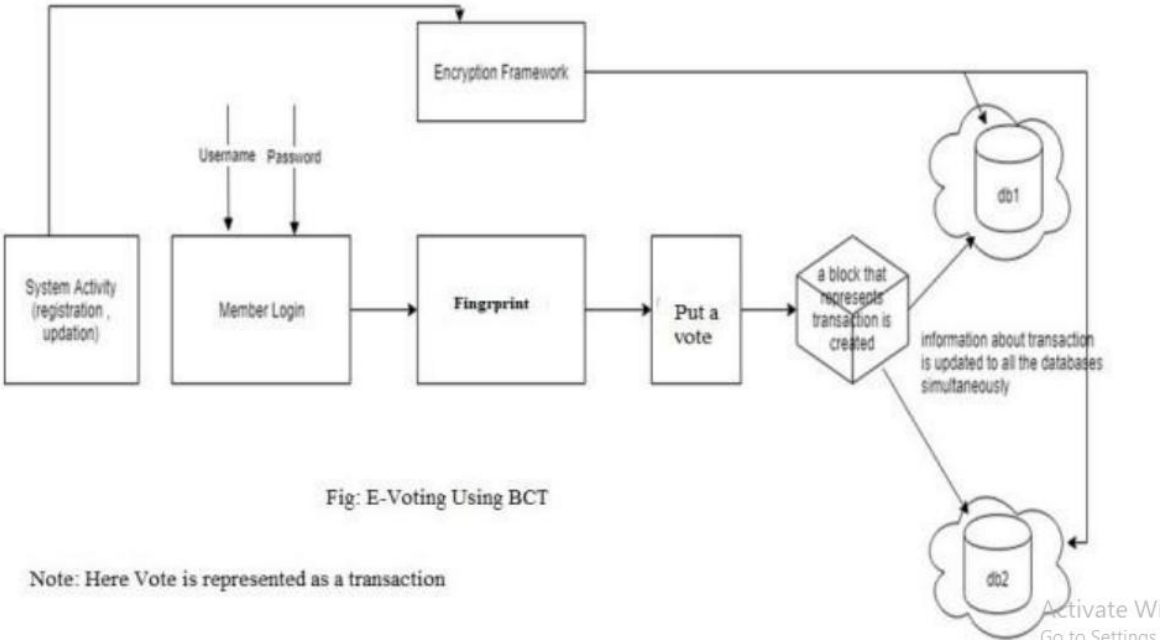

Figure 3: Proposed System Architecture

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue1, November 2023

Whenever a transaction takes place within the system, its record is preserved as a hash value in a block. Subsequent blocks are linked to preceding ones, creating a virtual chain of blocks. The hash value of a current block is derived from the data within that block and the hash of the preceding block. This interconnected structure ensures that if any block is tampered with, it necessitates the alteration of hashes in all subsequent blocks. Multiple copies of this chain are stored across various servers, ensuring data security and confidentiality. By conducting all operations through an application interface, the voting system maintains transparency in its processes.

5.1. Project Modules

Admin: The admin possesses the authority to add candidates, voters, wards, and elections. They can execute operations like updating, deleting, and announcing results.

Fingerprint: The Election Officer sends "share 1" to the voter's email before the election, while "share 2" becomes available in the voting system for the voter's login during the election. The voter receives a secret password to cast their vote by merging share 1 and share 2 using a Fingerprint scheme.

User: Voters can cast their votes only after logging into the system with the correct password, generated by combining two shares (Black & White dotted Images) using the Fingerprint scheme.

Blockchain: A blockchain serves as a distributed database storing data records that continuously expand, controlled by multiple entities. It operates as a reliable service system for a group of nodes or entities, essentially acting as a trusted third party to maintain coherence, facilitate transactions, and provide secure computational infrastructure.

5.2. Algorithms Used

SHA-256: The SHA-256 algorithm is a variant of SHA-2 (Secure Hash Algorithm 2), developed by the National Security Agency in 2001 as a replacement for SHA-1. SHA-256 is a cryptographic hash function that generates a 256-bit output.

1. The SHA-256 algorithm is employed within the blockchain to generate a consistent 256-bit hash each time. This algorithm is also integral to encryption technology. Let's delve into how this algorithm operates:
2. The illustration displays the algorithm's process. It starts with an initial value (IV) of 256 bits. The input data is typically large, so it's divided into segments of 512 bits.
3. As the input may not always be an exact multiple of 512 bits, there might be some remaining data.
4. To account for this, padding is applied by concatenating the input with additional bits to make it an ideal multiple of 512 bits.
5. The resulting 256-bit output is then combined with the 512-bit input from the subsequent block (B2).
6. The hashing process continues, ultimately yielding a final 256-bit output, which serves as the hash of the input file.

VI. CONCLUSION

The survey has explored various applications of Blockchain technology, ranging from its use in online transactions and the management of smart contracts to its role in machine-to-machine communication through M2M-REP systems. Considering the robust security measures inherent in blockchain, adopting this technology for the voting system emerges as a promising approach. Integrating blockchain into Internet-based voting systems ensures enhanced reliability and encourages greater participation. This solution is achieved cost-effectively while guaranteeing the integrity of each vote cast. The proposed system leverages visual cryptography to establish mutual authentication between voters and election servers. Furthermore, Blockchain technology plays a pivotal role in upholding data integrity and bolstering security measures within the system.

REFERENCES

[1]. Ahmed Ben Ayed, “A Conceptual Secure Block Chain-Based Electronic Voting System”,2017 IEEE International Journal of network &Its Applications(IJNSA),03 May 2017.

[2]. RifaHanifatunnisa, Budi Rahardjo, “Block-chain Based E-Voting Recording System Design”,IEEE 2017.

[3]. Kejiao Li, HuiLi,HanxuHou, KedanLi,Yongle Chen, “Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism & Consortium Block-chain”, 2017 IEEE 19th International Conference on High

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
onal Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue1, November 2023

Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems

[4]. Ali KaanKoç, EmreYavuz, Umut Can Cabuk, GokhanDalkilic, "Towards Secure E-Voting Using EthereumBlockchain",2018 IEEE