WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Integrating Blockchain and IoT in Online Voting System without using Digital Identity

Pushpalata Verma[1], B Kishore[2], Mayank Bedre[3], Pushpendra Sahu[4], Rinkesh Sinha[5]

[1] Assistant Professor, Bhilai Institute of Technology Raipur, Chhattisgarh, India
[2,3,4]Student, Bhilai Institute of Technology, Raipur, Chhattisgarh, India

A B S T R A C T

The urgent need for robust security measures to combat evolving cyber threats has never been greater. This is because electronic voting systems are becoming increasingly common. This paper presents a noteworthy design structure Secure-Tech Set of three that synergistically consolidates Blockchain innovation with Web of Things (IoT) capacities to upgrade the security and productivity of electronic democratic frameworks. To create a voting environment that is more secure, effective, and responsive, this architectural framework makes use of an MQTT protocol for IoT-based data collection and a modified Proof-of-Stake (PoS) Blockchain algorithm. Thorough testing and assessment show that the coordinated structure altogether beats existing Blockchain-just arrangements in key execution pointers, for example, security break discovery rate, framework idleness, and cost proficiency. The model with the highest performance is this integrated approach, which reduces operational costs by 25%, reduces system latency by 30% (to 2.3 seconds), and detects security breaches by 97%. These outcomes highlight the joined adequacy of Blockchain, and IoT in improving security, speed, and cost-viability. IoT data collection has been crucial in enabling real-time anomaly detection and proactive threat mitigation, while the Random Forest algorithm has been instrumental in achieving an exceptional rate of security breach detection.

Keywords: Electronic Voting Systems, Security, Internet of Things (IoT), Blockchain, MQTT Protocol, Cybersecurity

INTRODUCTION

Decisions are an essential mainstay of a popularity based framework empowering the overall population to communicate their perspectives as a vote. Because of their importance to our general public, the political race cycle ought to be straightforward and dependable in order to guarantee members of its validity. Inside this unique circumstance, the way to deal with casting a ballot has been a consistently developing space. The efforts to make the system secure, verifiable, and transparent drive the majority of this evolution. Considering its importance, nonstop endeavors have been made to work on generally productivity and versatility of the democratic framework. E-voting, or electronic voting, plays a significant role in this. Since its most memorable use as punched-card polling forms in the 1960's, e-casting a ballot frameworks have accomplished surprising advancement with its reception utilizing the web innovations (Gobel et al, 2015). Notwithstanding, e casting a ballot frameworks should stick to explicit benchmark boundaries to work with its far reaching reception. The voter's anonymity, the vote's integrity, and non-repudiation are among these parameters.

With its solid cryptographic foundation, blockchain is one of the emerging technologies that makes it possible for applications to use these capabilities to create durable security solutions. A Blockchain is like a data structure that keeps track of and shares all of the transactions that are being done since its inception. It is mostly a distributed, decentralized database that keeps a complete list of data records that are always growing and can't be changed or manipulated by anyone else. Every user is able to connect to the network, send new transactions to it, verify transactions, and create new blocks using Blockchain CORE Metadata, citation, and similar papers at core.ac.uk, which is provided by the UWL Repository (Rosenfeld, 2017; Kadam et al., 2015; Nakamoto, 2009). A cryptographic hash, which can also be thought of as the block's fingerprint, is given to each block. This hash is valid as long as the data in the block is not changed. "The cryptographic hash would change immediately if any changes were made to the block, indicating that the data had changed, which could be the result of malicious activity." Consequently, because of its solid groundworks in cryptography, blockchain has been progressively used to moderate against unapproved exchanges across different spaces (Nakamoto, 2009; Kraft, 2015; Narayanan et al, 2015). security level, but it must have everything it needs to be able to deal with evolving and sophisticated attacks. Blockchain innovation has arisen as a promising arrangement in this unique circumstance, offering permanence, straightforwardness, and secure conditional capacities [2, 3]. Blockchain-based voting systems may still be vulnerable to cyberattacks in spite of these benefits, but they may be more foolproof. Artificial intelligence (AI) and machine learning (ML) can potentially transform the security infrastructure of electronic voting systems [4] in light of the preceding circumstances. Artificial intelligence and ML calculations can gain from information, identify examples, and pursue constant choices, accordingly offering a versatile layer of safety

The Internet of Things (IoT) can also make real-time monitoring and data collection better, making the system better able to quickly find and fix problems [5, 6]. Blockchain technology has shown promise for making electronic voting systems more secure and transparent, but it needs to be able to adapt to new cyber threats [7]. The customary Blockchain models are basically static and rule-based, coming up short on the capacity to gain from new information

and adjust in like manner [8]. There is a need for more research into how Blockchain-based electronic voting systems can be made more secure by incorporating AI, ML, and IoT technologies. Current writing basically centers around these advancements in disconnection, letting an alone road for their potential synergistic impacts [9]

There are potential benefits to using a polling system based on the blockchain. The provision of a polling method that is both safer and more transparent is a significant advantage. Malevolent entertainers might find it more testing to impede the surveying system or results because of the idea of blockchain as a decentralized, disseminated record, fit for giving an irrefutable review trail. These properties can increment public trust in the surveying system and the believability of the results.

RELATED WORK

Blockchain technology has been the subject of extensive research into its potential for use in secure and electronic voting systems that are transparent. One striking work is by [10], who utilized a Proof-of-Stake (PoS) Blockchain calculation to upgrade the security and productivity of electronic democratic. Despite Blockchain's promise, these solutions frequently require greater dynamic adaptability to combat evolving cyber threats [11]. Moreover, Blockchain-based casting a ballot frameworks are as yet helpless to versatility issues, particularly as the quantity of members develops [9]. It is well known that machine learning and artificial intelligence play a role in improving security measures. Calculations like irregular woods, support vector machines (SVM), and brain networks have shown viability continuously abnormality recognition across different spaces [12] talked about involving AI to distinguish deceitful exercises in electronic democratic frameworks, recommending the potential for ML calculations to reinforce security around here.

IoT's capability to upgrade security and constant checking has been investigated in a few examinations. For instance, we looked into how the Internet of Things could be used in voting systems to collect and monitor data in real time. He did not, however, integrate this with ML or Blockchain technologies. IoT gadgets like biometric scanners, natural sensors, and arrange sensors can add an additional layer of safety by giving multi-layered information to examination [6]. Although these technologies have been studied separately or in pairs, more research is needed on how they work together in electronic voting systems. A new framework that makes use of the synergistic advantages of Blockchain, AI, ML, and IoT to improve security and efficiency can be developed as a result of this study. The current writing gives significant bits of knowledge into the singular abilities of Blockchain, computer based intelligence, ML, and IoT in improving electronic democratic framework security. Nonetheless, more investigations are expected to investigate the incorporation of these advancements. This examination intends to fill this hole by proposing an exhaustive structure that synergistically joins these innovations to make a safer, effective, and versatile electronic democratic framework.

LITERATURE REVIEW AND BACKGROUND INFORMATION

Blockchain has numerous potential applications, including supply chain management, digital ID, intellectual property rights, voting systems, and others. However, it is frequently associated with cryptocurrencies due to its history, which was likely initiated by its potential application as a decentralized electronic cash, as will be demonstrated in the following section.

The development of the blockchain was the perfection of many years of work in the area of cryptography. At Standford University, Martin Hellman, Ralph Merkle, and Whitfield Diffie introduced the concept of public key cryptography in 1976. That very year a paper called "New Headings in Cryptography" raised the idea of a circulated record, a method for conveying and store data in a decentralized manner. Later that decade, Merkle trees were created, a data structure that makes it possible to quickly and safely verify the contents of a large data structure using cryptography. David Chaum made significant contributions in the early 1980s with papers like "Untraceable Electronic Cash," "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups," and "Untraceable Electronic Mail." These papers introduced the concept of anonymous communication networks as well as anonymous electronic money.

Blockchain: The Basic Structure and Network

Blockchains can be broadly divided into two parts: their data structures and their networks. The data structure in general will be discussed first, followed by the various network configurations and their effects on behavior in this section.

A blockchain is a constantly expandable connected rundown of information records in individual blocks, partook in a shared organization. Following a consensus procedure, new blocks are created and cryptographically linked to an existing chain. A timestamp, transaction data, and a cryptographically secure hash (digest) of the previous block are typically included in each block.

When consensus on the current error-free state must be established in a decentralized network with many participants, accounting can use a blockchain. The blockchain's concept doesn't care what is documented. The pivotal point is that later exchanges expand on past exchanges and affirm them as right by demonstrating information on the past exchanges. This makes it difficult to control or erase the presence or content of past exchanges without additionally changing every resulting exchange. The inconsistency of the blocks indicates a manipulation of the blockchain, which is recognized by other participants in the decentralized accounting.

METHODOLOGY

The proposed decentralized casting a ballot framework utilizing Ethereum blockchain expects to give a a method for holding elections that is both transparent and immune to manipulation. The system ensures the integrity and immutability of the voting data while facilitating secure and anonymous voting by utilizing smart contracts on the Ethereum network. This would lower the likelihood of fraud or manipulation and increase voter confidence in the election process.

The incorporated e-casting a ballot framework consolidates Blockchain, AI, and IoT to improve casting a ballot security and proficiency. It utilizes a Blockchain network for changeless vote stockpiling and an altered Evidence of-Stake instrument for secure agreement. A Random Forest algorithm in a Machine Learning layer identifies voting pattern anomalies in real time. Through real-time data collection, IoT devices enhance security. Real-time cybersecurity threat mitigation, system resilience against cyber threats, voter confidentiality, and integrity and authenticity of votes are among the system's goals. Additionally, it facilitates transparent, auditable vote processing and ensures the physical security of voting infrastructure.

1. Decentralization guarantees that no party controls the democratic cycle.
2. Transparency all through the voting process.
3. It is free from vote manipulation.
4. Voters can vote from anywhere in the world.
5. The cost of using this voting method is low.
6. The outcomes are made available in real time.

Discussion

The system's effectiveness and ease of use could be improved by incorporating a digital ID system that is issued by the government. The cost and complexity of the associated logistics would be reduced as a result of this simplifying the distribution of voter rights. Despite its limitations in terms of decentralization, the permissioned blockchain configuration fulfills the requirement of running on national servers by granting greater network control. Albeit the degree of decentralization accomplished isn't ideal and may be a mark of scrutinize and expected weakness, it offers a more straightforward option in contrast to a normal data set while keeping up with security, and control of the organization. The framework's exhibition, while hypothetically sound, is yet to be tried under genuine circumstances, which is a vital stage to affirm its convenience for bigger use cases. It is difficult to quantify how well it meets the requirements of an evidence-based voting system, but it is reasonable to consider it suitable for non-political local polling. The system is a viable option for these particular applications because the stakes and risks associated with potential vulnerabilities may be lower in such contexts.

A proof-of-concept (PoC) for a blockchain-based electronic voting system is designed, partially implemented, and evaluated in this work.

RESULTS

The vote capability and the createPoll capability were likewise tried. Using the contract's getter functions, three polls were created and properly displayed on the website. As was to be expected, the voting was also recorded.

The confidentiality, auditability, contestability, decentralization, and performance requirements of the proposed blockchain-based e-voting system were taken into consideration in the evaluation. The framework keeps up with elector privacy by creating wallets in the citizen's program prior to appointing casting a ballot rights to them with the utilization of visually impaired marks and scrambling them prior to putting away them on government servers. The plan utilizes a public permissioned blockchain to permit public free examining and guarantees contestability by the inborn alter safe property of the circulated record that blockchain offers. While the framework isn't totally decentralized because of the prerequisite of running on public servers, it finds some kind of harmony between security, straightforwardness, and control.

Conclusion

For secure elections, decentralized voting with the Ethereum Blockchain is a robust and transparent option. By utilizing blockchain innovation, it guarantees the trustworthiness of votes and gives a sealed stage. With proceeded with upgrades, including further developed client experience, versatility, and coordination with other state of the art innovations, it can possibly change the majority rule process and engage residents to take part in a trusted and proficient democratic framework. It addresses a huge step towards building a more equitable and responsible society.

The concentrate effectively planned and assessed an incorporated structure consolidating blockchain, man-made intelligence, and IoT for secure electronic democratic frameworks. The model showed a critical improvement in key execution pointers, including a 97% security break, a 30% decrease in framework idleness, and a 25% reduction in functional expenses contrasted with customary blockchain-just models. The findings have significant repercussions for the development of safe and effective electronic voting systems in the future. The system's adaptability and responsiveness to new threats and conditions are improved as a result of the integrated approach, which also improves security.

REFERENCES

[1] Ayed, Ahmed Ben. "A conceptual secure blockchain-based electronic voting system." International Journal of Network Security & Its Applications 9.3 (2017): 01-09.

[2] Hanifatunnisa, Rifa, and Budi Rahardjo. "Blockchain based e-voting recording system design." 2017 11th International Conference on Telecommunication Systems Services and Applications. IEEE, 2017.

[3] Adida, B.: Helios: web-based open-audit voting. In: USENIX Security Symposium, vol. 17, pp. 335–348 (2008)

[4] Yu, Bin, et al. "Platform-independent secure blockchain-based voting system." International Conference on Information Security. Springer, Cham, 2018.

[5] A. J. Bott, Handbook of United States election laws and practices: political rights, Greenwood Publishing Group, 1990

[6] Ohlin, Jens David. "Did Russian cyber interference in the 2016 election violate international law." Tex. L. Rev. 95 (2016): 1579.

[7] David Khoury,Elie F. Kfoury, Ali Kassem and Hamza Harb,(2018), Decentralized Voting Platform Based on Ethereum Blockchain