Journal of
Advancements in Robotics

ISSN: 2455-1872
Volume 11, Issue 2, 2024
May–August
DOI (Journal): 10.37591/JoARB

https://journals.stmjournals.com/joarb

Review JoARB

A Secure and Transparent Voting System Leveraging Ubiquitous Computing and Blockchain Technology

Deekshith S.M.*

Abstract

Ubiquitous computing and blockchain technology are two pivotal innovations driving significant changes in the digital world. This article explores the intersection of these technologies, analyzing how their combination can unlock new opportunities and address existing challenges. Ubiquitous computing envisions seamlessly integrating computing capabilities into everyday objects and environments, aiming to enhance user experience and efficiency. Meanwhile, blockchain technology, known for its decentralized and secure nature, offers robust solutions for transparency, trust, and immutability. The integration of ubiquitous computing and blockchain technology has the potential to revolutionize numerous industries. For instance, in smart energy grids, IoT devices can monitor energy usage, while blockchain ensures transparent transactions between consumers and producers, facilitating peer-to-peer energy trading and promoting renewable energy. In supply chain management, integration enables real-time tracking and verification of goods, improving transparency and minimizing the risk of counterfeiting. Similarly, in health care, IoT devices collect patient data that blockchain can securely store, ensuring privacy and integrity while enabling seamless access to medical histories. The article also addresses the challenges of integrating these technologies, such as scalability, interoperability, and security issues. We examine the need for standardized protocols and the development of efficient consensus mechanisms to handle the vast amounts of data generated by IoT devices. By examining real-world case studies such as smart cities, decentralized autonomous organizations (DAOs), and secure voting systems, we demonstrate the transformative potential of combining ubiquitous computing with blockchain technology. These examples demonstrate how this integration can enhance transparency, security, and efficiency across various domains. Finally, this article highlights future research directions, stressing the necessity of creating robust frameworks to facilitate the seamless integration of these technologies. By addressing these challenges and leveraging their synergies, ubiquitous computing and blockchain can jointly contribute to a more secure, transparent, and efficient digital future.

Keywords: Ubiquitous computing, blockchain technology, secure voting system, internet of things, IoT, smart cities, decentralized autonomous organizations, DAOs, smart energy grids, supply chain management

***Author for Correspondence**
Deekshith S.M.
E-mail: deekshithsm.mca23@rvce.edu.in

Student, Department of MCA, RV College of Engineering, Bangalore, Karnataka, India

Received Date: May 03, 2024
Accepted Date: June 10, 2024
Published Date: July 09, 2024

Citation: Deekshith S.M. A Secure and Transparent Voting System Leveraging Ubiquitous Computing and Blockchain Technology. Journal of Advancements in Robotics. 2024; 11(2): 9–13p.

INTRODUCTION

Ubiquitous computing, characterized by the seamless integration of computing capabilities into everyday objects and environments, has led to the emergence of smart cities, smart homes, and intelligent wearable devices. Meanwhile, blockchain technology, renowned for its decentralized and immutable ledger, has revolutionized finance, supply chain management, and digital identity verification. The integration of these technologies offers a new paradigm for creating secure, efficient, and intelligent systems.

UBIQUITOUS COMPUTING AND BLOCKCHAIN: A SYNERGIC APPROACH

The integration of ubiquitous computing and blockchain presents a myriad of opportunities across diverse domains. In smart cities, for example, blockchain can facilitate secure and transparent management of data generated by IoT sensors, enabling efficient resource allocation and enhancing urban sustainability. Similarly, in health care, ubiquitous computing devices can collect patient data, which is securely stored and shared on a blockchain, ensuring data integrity and patient privacy [1].

LITERATURE SURVEY

The integration of ubiquitous computing and blockchain technology has gained traction in recent years, with research exploring its potential applications and challenges.

Weiser's seminal work introduced the concept of ubiquitous computing, envisioning a world where computing capabilities are seamlessly integrated into everyday objects and environments [2].

Nakamoto's Bitcoin whitepaper laid the foundation for blockchain technology, offering a decentralized solution for peer-to-peer electronic transactions [3].

Christidis and Devetsikiotis discussed the potential synergies between blockchain and IoT technologies, highlighting use cases such as supply chain traceability and decentralized energy management [4].

Alzahrani et al. reviewed the integration of blockchain and IoT, focusing on scalability, interoperability, security, and privacy considerations [5].

By synthesizing insights from these studies, we aim to contribute to the discourse on the integration of ubiquitous computing and blockchain, exploring its potential applications, challenges, and future directions.

EXISTING EXAMPLES

Smart Energy Grids

In smart energy grids, IoT devices monitor energy usage, while blockchain ensures transparent and auditable transactions between consumers and producers. This setup facilitates peer-to-peer energy trading and promotes renewable energy production.

Supply Chain Traceability

Blockchain-based supply chain platforms, combined with IoT sensors, enable real-time tracking of goods from origin to consumer. This integration enhances transparency, reduces counterfeiting, and improves supply chain efficiency [6].

Decentralized Autonomous Organizations

DAOs utilize smart contracts on blockchain to automate governance and decision-making processes. IoT devices provide real-world data inputs, allowing DAOs to function autonomously without centralized control.

Agriculture and Food Safety

In agriculture, IoT devices monitor environmental conditions such as soil moisture and temperature. Blockchain records the supply chain from farm to table, ensuring food safety and traceability. IBM Food Trust and Walmart have implemented such solutions to enhance transparency and reduce foodborne illnesses [7].

Health care Data Management

IoT devices collect patient data from wearables and medical sensors. Blockchain ensures secure and immutable storage of health records, enabling patients and doctors to access accurate medical histories while maintaining privacy and compliance with regulations. Examples include MedRec and Guardtime.

Smart Cities

IoT sensors in smart cities manage traffic, waste, public safety, and environmental monitoring. Blockchain technology secures and ensures transparency in data transactions between city services, enhancing efficiency and trust. Initiatives like Dubai's Smart City and Barcelona's projects exemplify these applications [8].

Telecommunications and Network Management

IoT devices monitor network performance and manage infrastructure in real-time. Blockchain ensures secure data transactions and facilitates automated service agreements and payments. Nokia and Samsung use blockchain to enhance network management and security.

Insurance

IoT devices, such as telematics in vehicles or smart home devices, collect data on user behavior. Blockchain secures data sharing and automates claims processing through smart contracts, resulting in accurate risk assessments and faster, transparent claim settlements. Examples include AXA’s fizzy platform for flight delay insurance and State Farm’s blockchain-based auto insurance claims [9].

PROPOSED CASE STUDY

Secure Voting System

Introduction

Secure and transparent elections are fundamental to the democratic process. As observed in our democratic country, India, the traditional voting systems face challenges such as fraud, manipulation, and lack of transparency. Leveraging the convergence of ubiquitous computing and blockchain technology, I propose a secure voting system that aims to ensure the integrity, transparency, and verifiability of the election results as shown in Figure 1.

System Architecture

The proposed secure voting system consists of three main components: IoT devices deployed at polling stations, a blockchain network for recording votes, and a user interface for voters to cast their votes securely.

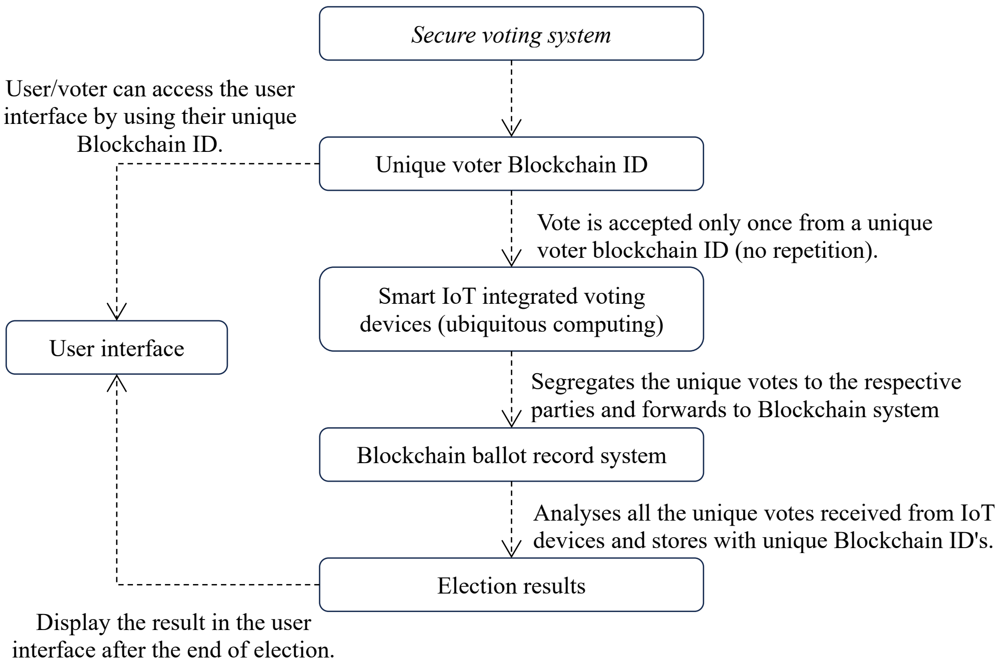

Figure 1. Architecture of secure voting system.

IoT Devices

At each polling station, IoT devices such as tablets or touch-screen kiosks will be deployed to facilitate the voting process [10]. These devices will be equipped with biometric authentication capabilities to ensure the identity of voters and prevent unauthorized access. Here, a voter can vote only if his blockchain ID and biometric data get verified. After the voting process, the vote will be encrypted so that it hides the voter's identity, which is useful to prevent knowing of the voter data from a political party member, which may lead to risk to the voter, so in order to maintain the voter's secrecy, the encryption of the votes is mandatory.

Blockchain Network

A secure and unique blockchain ID will be integrated with the voter ID, or we can say that every single voter will have his or her own blockchain ID for voting, so that there will be no fake votes and a permissioned blockchain network will be used to record and store the votes securely. Each voter's ballot will be encrypted and stored as a transaction on the blockchain, ensuring immutability and transparency. Smart contracts will be employed to enforce voting rules and automate the tallying process. If this is implemented, then all the loopholes of the current voting system, such as "fake votes, manipulation, and lack of transparency," will be washed out. Because once the voter has voted by using his or her blockchain ID, then his or her blockchain ID will be marked as "voted" by the integration of algorithms so that the person who has already voted cannot vote again using the same blockchain ID, and for clarification of readers, "the blockchain ID of an individual is only given by taking his or her fingerprint and Aadhar card or any government provided ID card," so there is no chance of fraud.

User Interface

Voters will interact with the secure voting system through a user-friendly interface on the IoT devices. They will authenticate themselves using their blockchain ID and cast their votes securely. The interface will provide real-time feedback and confirmation of the vote submission. The user interface is not only used for the process of voting, but this interface will also contain the voter's historical vote record (this will be achieved through the blockchain ID given to the user and giving them the feature to login and view their vote data based on the blockchain ID assigned to them) so that user will be have all the records. And the user can take a look at the number of votes in front of each political party name and symbol after the completion of the elections so that there is transparency provided to the voters. Here we are displaying the number of votes after the end of the election because if the current numbers are displayed, then there can be a possibility of manipulation by the political party members to the voters.

Proposed Test Deployment

To validate the efficiency of the secure voting system, a test deployment is proposed in a controlled environment. Several polling stations will be equipped with IoT devices connected to a private blockchain network. Participants will be invited to simulate the voting process, and their ballots will be recorded on the blockchain. Then, using algorithms, the ballots will be segregated to the respective political parties, and then the majority ballots owning party in the blockchain, and the winner's party name will be announced through the user interface. And then provide all the information (i.e., the number of votes of each political party) required to the voter after the completion of the election, and then collect the feedback from the voters.

Expected Results

It is anticipated that the proposed test deployment will demonstrate the feasibility and effectiveness of the Secure Voting System in ensuring secure and transparent elections. Participant's feedback and observations will be collected to evaluate the usability, security, and integrity of the voting process.

Conclusion

The proposed secure voting system represents a promising solution to address longstanding challenges in traditional voting systems. By leveraging ubiquitous computing and blockchain technology, it aims to enhance the integrity, transparency, and verifiability of election results, thereby strengthening democracy and fostering trust in the electoral process.

CONCLUSION

The integration of ubiquitous computing and blockchain holds immense promise for creating secure, efficient, and intelligent systems across various domains. By addressing the challenges and leveraging the synergies between these technologies, we can unlock new possibilities for digital innovation and societal transformation.

Acknowledgements

This article is completely proposed by Mr. Deekshith S M, all the research work and the proposed concept in this article is of his own views and research.

REFERENCES

1. Wang S, Zhang D, Zhang Y. Blockchain-based personal health records sharing scheme with data integrity verifiable. IEEE Access. 2019; 7: 102887–102901.
2. Weiser M. The computer for the 21st century. Sci Am. 1991; 265 (3): 94–105.
3. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. Bitcoin [Internet]. 2008; 4(2):15. [Online] Available at https://bitcoin.org/bitcoin.pdf
4. Christidis K, Sikeridis D, Wang Y, Devetsikiotis M. A framework for designing and evaluating realistic blockchain-based local energy markets. Appl Energy. 2021; 281: 115963.
5. Alshareef R, Al Zahrani A, Alzahrani A, Ghandoura L. Impact of the COVID-19 lockdown on diabetes patients in Jeddah, Saudi Arabia. Diabetes Metab Syndr. 2020; 14 (5): 1583–1587.
6. Cagnano A, De Tuglie E, Marcone F, Porro G, Rasolomampionona DD, Klos M, et al. Experimental results on the economic management of a smart microgrid. In: 2020 IEEE 20th Mediterranean Electrotechnical Conference (MELECON); 2020 Jun 16–18; Palermo, Italy: IEEE. 459–463 p.
7. Ding C. Risk assessment of physical and chemical analysis laboratory based on the laboratory risk assessment model. In: 2021 2nd International Conference on Urban Engineering and Management Science (ICUEMS); 2021 Jan 29–31; Sanya, China: IEEE. 293–296 p.
8. Sami MA, Wagner K, Parikh P, Hassan U. Smartphone based microfluidic biosensor for leukocyte quantification at the point-of-care. In: 2019 IEEE Healthcare Innovations and Point of Care Technologies (HI-POCT); 2019 Nov 20–22; Bethesda, MD, USA: IEEE. 119–122 p.
9. Kulkarni MG, Cheeran AN, Ray KP, Kakatkar SS. Design and implementation of CPW low pass filter with good filter selectivity and sharpness factor. In: 2018 3rd International Conference on Microwave and Photonics (ICMAP); 2018 Feb 9–11; Dhanbad, India: IEEE. 1–2 p.
10. Korobeynikov SM, Krivosheev SI, Magazinov SG, Loman VA, Ya N. Suppression of incoming high-frequency overvoltage in transformer coils. IEEE Trans Power Delivery. 2020; 36 (5): 2988–2994.

