p–ISSN: 2723 – 6609 e-ISSN: 2745-5254
Vol. 6, No. 5, May 2025 http://jist.publikasiindonesia.id/

APPLICATION OF BLOCKCHAIN TECHNOLOGY FOR E-VOTING SYSTEMS USING SMART CONTRACT

Denata Wijaya Aripin*
Universitas Widyatama, Indonesia
Email: denata.wijaya.aripin@gmail.com
*Correspondence

Keywords: Blockchain, E- Voting, Smart Contracts, System Security, Transparency, Ethereum

ABSTRACT

Blockchain technology has become a potential solution to improve security, transparency, and integrity in the e-voting system. This study examines the application of smart contracts in blockchain-based e-voting systems to reduce the risk of fraud and improve the efficiency of the voting process. The methods used include design and implementation prototype. The system uses the Ethereum platform, as well as security and performance analysis. Research results show that the use of smart contracts is able to guarantee automatic vote verification and ensure transparent and immutable election results. This study provides contribution in the development of a safe, transparent, and trustworthy e-voting system.

INTRODUCTION

General elections are an important foundation in a democratic system to determine people's representatives in a fair and transparent manner.

However, conventional voting systems are still vulnerable to manipulation, fraud, and a lack of transparency (Nugroho, 2021). To overcome these problems, blockchain technology is present as an innovative solution that is able to provide a secure, transparent, and immutable voice recording mechanism.

Blockchain is a distributed ledger technology that permanently records transactions in cryptographically connected blocks (Buterin, 2020). Smart contracts, as part of blockchain technology, allow the creation of digital contracts that automatically execute certain rules without human intermediaries (Sharma et al., 2021).

This research aims to apply blockchain technology and smart contracts in the e-voting system to improve the integrity and efficiency of the voting process. The main focus is on the development of Ethereum-based prototypes as well as their security analysis based on the latest literature.

Blockchain Technology

Blockchain is a distributed ledger technology that stores transaction data in interconnected blocks cryptographically and spread across many nodes. According to Zheng et al. (2020), blockchain ensures high security and transparency due to its immutable nature, where recorded data cannot be altered retroactively. Buterin (2020) introduced Ethereum as a blockchain platform that supports smart contracts — programs that run automatically according to set rules.

Several studies (Sharma et al., 2021) review the evolution of blockchain in various fields, including finance, logistics, to electronic voting systems (e-voting).

Smart Contract

Smart contracts are computer protocols that automatically execute, control, or document actions and agreements according to programmed rules. Smart contracts eliminate the need for third parties and reduce the risk of fraud.

The use of smart contracts in e-voting is able to guarantee that votes can only be cast once by verified voters, and the results can be published transparently (Sharma et al., 2021; Prasetyo & Putra, 2022).

Blockchain-Based E-Voting System

Several studies show that blockchain is a perfect fit for e-voting systems because:

- Transparency that allows for public audits of election results.
- High security with cryptography and decentralized network (Sari & Putri, 2020).
- Automation of vote validation and voting processes through smart contracts (Lestari et al., 2023).

Prasetyo and Putra (2022) implemented Hyperledger Fabric for e-voting that allows for strict access control and voter identity management. However, they noted challenges in terms of scalability and transaction processing time.

Blockchain-based e-voting systems must also consider voting privacy protections, such as the use of Zero-Knowledge Proof (ZKP) techniques to maintain voter anonymity (Nugroho & Rahayu, 2024).

Security and Privacy in the E-Voting System

The security of the e-voting system is the main focus due to the risk of vote manipulation and data breach (Sari & Putri, 2020). Asymmetric cryptography is used to encrypt voices so that only the authorities can decrypt the results.

Nugroho & Rahayu (2024) suggest the integration of Zero-Knowledge Proof to enable vote verification without revealing the identity of the voter. In addition, the system must also have a mechanism for detecting and preventing Distributed Denial of Service (DDoS) and double voting attacks (Kumar & Singh, 2021).

Study Case and Latest Implementations

- Lestari et al. (2023) used a Proof of Stake (PoS) algorithm to reduce energy consumption in an e-voting blockchain network, compared to traditional Proof of Work (PoW).
- Prasetyo and Putra (2022) report that smart contracts can automatically validate voters and process votes without manual intervention, improving system efficiency.
- Sharma et al. (2021) describe a blockchain-based e-voting framework that has been tested in simulation environment with high accuracy and safety results.

METHOD

This research uses the **design and implementation method of a prototype of a blockchain-based e-voting system** with smart contracts on the Ethereum platform. The methodological stages include:

1. **System Needs Analysis** Identify Functional and non-functional needs of the e-voting system such as:
   - Voter authentication
   - Voting process
   - Secure, immutable sound storage
   - Transparency of voting results

2. **System Architecture Design**
   The system is designed with a distributed architecture using the Ethereum blockchain, it consists of the main components:
   - **User Interface (UI):** An interface for voters to vote.
   - **Smart Contract**: Contains voting logic, voter validation, and automatic recording of vote results (Sharma et al., 2021).
   - **Blockchain Network**: Ethereum testnet as a ledger network that records voice transactions (Buterin, 2020).
3. **Smart Contract Implementation** Smart contract is developed using Solidity with the main features:
   - The function **of voter registration** is to register identities and ensure one vote per voter (Prasetyo & Putra, 2022).
   - A voting **function** that records votes in an encrypted manner and ensures data integrity (Sari & Putri, 2020).
   - A result publication **function** that automatically counts votes and displays transparent results.
4. **System Testing**
   Done Testing to ensure:
   - There is no duplication of votes (double voting) (Kumar & Singh, 2021).
   - The system is capable of withstanding security attacks such as DDoS and data manipulation attempts.
   - Vote validation and the voting process run according to the rules (Nugroho & Rahayu, 2024).
5. **Analysis Result**
   Performance and safety analysis was carried out by comparing test results with literature studies (Lestari et al., 2023).

RESULTS AND DISCUSSION

1. Smart Contract Implementation

Smart contracts were successfully created with several main functions: voter registration, voting, and automatic result counting. The registration function ensures that only registered voters can cast their votes once (Sharma et al., 2021).

Contract codes are equipped with a voice encryption mechanism to maintain the confidentiality of voter data and prevent manipulation (Sari & Putri, 2020).

2. System Security

Testing shows that smart contracts are able to prevent **double voting** with the validation of voter unique IDs (Kumar & Singh, 2021). The system is also able to withstand simulated light DDoS attacks thanks to the decentralization of the Ethereum network.

The implementation of Zero-Knowledge Proof in smart contracts is tested to maintain voter privacy without compromising the ability to verify votes (Nugroho & Rahayu, 2024).

3. Efficiency and Scalability

The use of the Proof of Stake (PoS) algorithm on the Ethereum testnet network has been proven to reduce energy consumption and speed up voice transaction confirmation compared to Proof of Work (PoW) (Lestari et al., 2023).

However, the test also identified scalability limitations when the number of voters is very large, requiring advanced optimization of network protocols and infrastructure

(Prasetyo & Putra, 2022).

4. **Transparency and Accountability**
   The results of the votes recorded on the blockchain are publicly accessible in real-time, thereby increasing transparency and voter trust. Voice audits can also be performed by third parties without invading an individual's privacy.
5. **Comparison with Conventional Systems**
   Compared to traditional voting systems, these blockchain systems offer significant improvements in security and transparency, as well as efficiency in the vote counting process (Sharma et al., 2021; Prasetyo & Putra, 2022).

CONCLUSION

This research shows that the application of blockchain technology in the e-voting system through smart contracts offers significant improvements in terms of security, transparency, and efficiency of the election process. The Ethereum-based system allows each vote to be permanently recorded and cannot be manipulated, while still maintaining voter anonymity.

The smart contracts that have been built have succeeded in overcoming some of the main problems in the traditional election system such as the potential for fraud, double voting, and manipulation of results. The system trial also proves that this solution can be adopted on a larger scale with optimization on the blockchain infrastructure.

However, challenges such as transaction gas costs, adoption of technology by the community, and the need for supportive regulations, remain obstacles to the full implementation of this system nationwide. Further research is suggested to develop more efficient architectures as well as integrate technology like identity digital and biometric-based authentication systems.

REFERENCE

Aziz, M. (2023). Utilization of Blockchain in Decentralized Government Systems. *Journal of E-Gov, 11*(1), 88–95.

Astuti, V. (2022). Challenges of Blockchain Voting Regulation in Indonesia. *Journal of Law and Technology, 5*(2), 60–68.

Bhargava, A., et al. (2022). Blockchain Smart Contracts: Applications and Limitations in Voting Systems. *Journal of Network Technology*.

Buterin, V. (2020). Ethereum White Paper. Ethereum Foundation.

Fauzi, T. (2023). Application of Digital Identity on Blockchain Voting System. *Journal of Digital Identity, 3*(2), 25–33.

Gunawan, I., et al. (2023). Scalability Issues in Blockchain-based Voting. *IT Infrastructure Review, 7*(2), 75–83.

Hartono, R. (2022). The architecture of the voting system uses blockchain technology. *Indonesian Journal of Computer Science, 10*(3), 201–209.

Johar, S., & Hanafi, A. (2021). Decentralized Election Architecture for Online Voting. *Journal of Emerging Tech, 3*(1), 34–42.

Kumar, A., & Singh, R. (2021). Secure Voting System Using Solidity on Ethereum Blockchain. *International Journal of Computer Applications, 182*(8), 35–42.

Kurniawan, B. (2021). Design of an Ethereum-based digital voting protocol. *Journal of Digital Technology, 6*(2), 110–117.

Lestari, H., et al. (2023). The Effect of Proof of Stake on Performance Blockchain Voting Network. *Journal of Applied Technology, 7*(2), 89–96.

Lin, H., & Liao, C. (2023). Smart Contracts for E-Governance: A Review. *Government Tech Review, 8*(3), 119–128.
Nugroho, T., & Rahayu, L. (2024). Zero-Knowledge Proof Implementation on E-Voting Smart Contracts. *Journal of Digital Cryptography, 9*(1), 12–20.
Prasetyo, D., & Putra, R. (2022). Implementation of Smart Contracts in Ethereum-Based E-Voting System. *Journal of Information Technology, 12*(1), 45–54.
Puspita, L. (2023). Efficiency of vote counting using smart contracts. *Journal of Applied Technology, 5*(1), 19–27.
Rahman, M., et al. (2022). A survey on smart contract testing and verification. *ACM Computing Surveys*.
Rinaldi, A., & Fauzan, R. (2020). Blockchain Voting: Opportunities and Challenges in Indonesia. *Journal of Technological Law, 2*(1), 55–64.
Rudianto, J. (2021). Security on Digital Voting Using Hybrid Blockchain. *Journal of Information Systems, 9*(4), 223–231.
Safitri, D., & Hidayat, S. (2023). Smart Contract Security Analysis for Electronic Elections. *Journal of Cybersecurity, 3*(1), 66–74.
Sari, M., & Putri, N. (2020). Digital Vote Security with Blockchain Voting. *Journal of Systems Engineering, 5*(4), 217–225.
Setiawan, D., et al. (2020). Blockchain Voting Simulation on School General Elections. *Journal of EduTech, 8*(1), 90–98.
Siregar, M., et al. (2021). Organizational Voting App with Open Source Blockchain. *Journal of IT Research, 4*(2), 44–51.
Wahono, S. (2024). UI/UX Design for Decentralized E-Voting Applications. *Journal of Digital Interaction, 6*(3), 70–78.
Wahyuni, S. (2020). Simulation of Voting for the Election of the Chairman with the Ethereum Blockchain. *National Seminar on Information and Communication Technology*.
Widodo, A. (2021). Comparison of Gas Fees between Ethereum and Binance Smart Chain Platforms on Online Voting. *Nusantara Blockchain Journal, 4*(1), 51–60.
Wijaya, F., et al. (2022). Implementation of Smart Contract Voting Using Remix IDE and Metamask. *Journal of Programming, 5*(3), 99–107.
Zhao, Y., et al. (2023). Efficient E-voting using zk-SNARKs and Blockchain. *Cryptography and Security Journal, 6*(2), 78–86.
Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2020). An overview of blockchain technology: Architecture, consensus, and future trends. *Proceedings of the IEEE, 108*(10), 1804–1830.