VOL. 11. NO. 3 FEBRUARY 2026
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480 /jitk.v11i3.7622

JITK (JURNAL ILMU PENGETAHUAN DAN TEKNOLOGI KOMPUTER)

IMPLEMENTATION OF A SMART CONTRACT-BASED E-VOTING SYSTEM FOR COMPETITIONS

Tony Tan[1*]; Eric Valentino[1]; Fredian Simanjuntak[1]

Information Systems[1]
Universitas Internasional Batam, Indonesia[1]
www.uib.ac.id[1]
tony@uib.ac.id*, 2231029.eric@uib.edu, fredian.simanjuntak@uib.ac.id

(*) Corresponding Author
(Responsible for the Quality of Paper Content)

The creation is distributed under the Creative Commons Attribution-NonCommercial 4.0 International License.

Abstract— *Traditional voting methods in competitions often face challenges related to transparency and fraud, undermining fairness. This research presents the design and implementation of a hybrid e-voting system built on Ethereum blockchain technology to mitigate these issues. Specifically, this research integrates an off-chain HMAC-SHA256 privacy mechanism with Ethereum's Proof-of-Stake (PoS) consensus to ensure that voting records remain immutable and publicly auditable, while preserving voter anonymity. A prototype was developed using a decentralized architecture, leveraging smart contracts to automate the entire electoral process from registration to tallying. An evaluation involving 153 participants based on the Technology Acceptance Model (TAM) demonstrated high user acceptance, with scores of 76.6% for Perceived Usefulness, 73.4% for Perceived Ease of Use, and 72.8% for Acceptance of Technology. Although the system demonstrates effectiveness in competitive settings, current testing is limited to small- to medium-scale implementations. This research concludes that the proposed framework provides a secure, transparent, and efficient alternative for competitions, significantly enhancing trust in the election outcomes.*

Keywords: *Blockchain, E-Voting, Smart Contract, Transparency.*

Intisari— *Metode pemungutan suara tradisional dalam kompetisi sering terkendala oleh tantangan transparansi dan kecurangan yang dapat merusak keadilan. Penelitian ini menyajikan perancangan dan implementasi sistem e-voting hibrid yang dibangun di atas teknologi blockchain Ethereum untuk memitigasi isu-isu tersebut. Secara khusus, penelitian ini mengintegrasikan mekanisme privasi HMAC-SHA256 off-chain dengan konsensus Proof-of-Stake (PoS) Ethereum untuk memastikan bahwa catatan suara tidak dapat diubah (immutable) dan dapat diaudit secara publik tanpa mengorbankan anonimitas pemilih. Sebuah prototipe dikembangkan menggunakan arsitektur terdesentralisasi, memanfaatkan smart contract untuk mengotomatisasi keseluruhan proses pemilihan dari pendaftaran hingga penghitungan suara. Evaluasi yang melibatkan 153 partisipan berdasarkan Technology Acceptance Model (TAM) menunjukkan penerimaan pengguna yang tinggi, mencapai skor 76,6% untuk Perceived Usefulness, 73,4% untuk Perceived Ease of Use, dan 72,8% untuk Acceptance of Technology. Meskipun sistem terbukti efektif untuk konteks kompetisi, pengujian saat ini terbatas pada implementasi skala kecil hingga menengah. Penelitian ini menyimpulkan bahwa kerangka kerja yang diusulkan menyediakan alternatif yang aman, transparan, dan efisien untuk kompetisi, sehingga secara signifikan meningkatkan kepercayaan terhadap hasil pemilihan.*

Kata Kunci: *Blockchain, E-Voting, Smart Contract, Transparansi.*

INTRODUCTION

The rapid advancement of digital systems has led to a greater reliance on electronic tools to address societal challenges, necessitating the design of effective and user-centric systems [1]. In the context of voting, traditional methods often face significant issues such as fraud, inefficiency, and a lack of transparency, prompting the exploration of electronic voting (e-voting) as a viable alternative [2]. E-voting systems aim to streamline the electoral process and improve accessibility while addressing the risks of vote manipulation and result falsification [3].

The integration of blockchain technology has arisen as a viable means of addressing these challenges. As a decentralized database, blockchain ensures secure data storage across a distributed network [4]. Each block is cryptographically linked to the previous one, creating a tamper-resistant structure that maintains the integrity of stored data [5], [6]. This linkage, supported by cryptographic hash functions, ensures that any modification to data is easily detectable, thus preventing manipulation and unauthorized changes.

The decentralized nature of blockchain significantly enhances the security of e-voting systems. By distributing the voting process across multiple nodes, the system mitigates risks associated with centralized databases, which are often vulnerable to hacking and manipulation [7]. Research indicates that blockchain-based voting systems can achieve higher levels of security and reliability due to decentralization, majority-node validation, and cryptographic verification [8]. In addition, several studies highlight blockchain’s potential to strengthen privacy and voter confidence by ensuring anonymity while keeping every vote verifiable, traceable, and recorded immutably on the ledger [9].

This cryptographically secured process removes the need for centralized authorities, minimizing the risk of data tampering and unauthorized access. The transparency afforded by blockchain enables real-time monitoring, allowing stakeholders to verify election integrity without exposing voter identities [10]. Additionally, the flexibility of the Ethereum blockchain supports the creation of decentralized applications (dApps) that incorporate smart contracts to enforce election rules automatically, tally votes, and publish results, thereby producing verifiable and tamper-resistant outcomes suitable for various organizational or competitive contexts [7].

Challenges such as long waiting times, logistical constraints, and vulnerability to fraud in traditional voting can be mitigated through blockchain-based e-voting [11]. E-voting systems have also been shown to improve efficiency and accessibility through online participation [12]. Automation within the system reduces administrative effort and minimizes human error [13]. A systematic review of the field confirms that blockchain's primary benefits for e-voting are enhanced security, transparency, and decentralization, which are crucial for ensuring the legitimacy of election results [14]. Blockchain’s decentralized and transparent mechanisms generate permanent, unalterable records. Together with integrity, anonymity, and non-repudiation, these features make it ideal for secure voting applications [4], [15].

Smart contracts, a key component of blockchain-based e-voting, automate election rules and vote tallying, reducing human error and enhancing trust by providing a verifiable framework where voters can independently confirm their votes [4], [16]. While blockchain provides a robust security baseline through its decentralized and immutable properties, additional security layers such as encryption, secure authentication protocols, and privacy-preserving mechanisms like homomorphic encryption can further protect voter information while ensuring vote verifiability [13], [17].

Despite its recognized potential, implementing blockchain in e-voting faces several challenges. These include obstacles related to system design, deployment, and acceptance, the need to address existing vulnerabilities, and the requirement for more in-depth testing to ensure its effectiveness in other domains [18], [19] A significant and widely cited drawback of early blockchain systems, such as those using Proof-of-Work (PoW), is their high energy consumption and computational waste [20] The evolution of public blockchains, particularly with advancements like Ethereum's transition to the Proof-of-Stake (PoS) consensus algorithm, which markedly lowers energy usage relative to the Proof-of-Work (PoW) approach, has established a new baseline for developing secure and sustainable decentralized applications.

While most existing research focuses on e-voting in democratic elections, limited attention has been given to competitive environments, where fairness and transparency are critical yet often compromised. This research addresses that gap by designing and evaluating a blockchain-based e-voting system for competition events. 'Competitions' in this study refer to event-driven contests, including creative arts festivals, talent showcases, and academic awards, which are distinct from high-stakes political or organizational governance elections. Such events generally involve a limited

Accredited Rank 2 (Sinta 2) based on the Decree of the Dirjen Penguatan RisBang Kemenristekdikti No.225/E/KPT/2022, December 07, 2022. Published by LPPM Universitas Nusa Mandiri

group of voters, such as judges or attendees, for whom transparency is essential to maintain trust in the winner-selection process.

MATERIALS AND METHODS

This study was carried out through the design and development of a blockchain-based e-voting system prototype. The Agile Scrum methodology was adopted for the system development process because of its flexibility and ability to accommodate rapid, iterative improvements [21]. The development was structured into a series of sprints, with each sprint focused on building and testing a core feature of the e-voting system, including voter registration, the voting process, automated vote tallying, and the transparent announcement of results. The prototype was built on the Ethereum blockchain, with the core logic encapsulated in Solidity smart contracts.

System Architecture and Implementation

The developed e-voting system is architecturally composed of three main layers: the front-end client, the blockchain back-end (smart contract), and the system integration layer that connects users wallets to the Ethereum network.

A. Front-End (User Interface):
The client-facing web application was developed using Next.js, a popular React framework. The UI was designed to be intuitive, providing components for user authentication (wallet connection), viewing election candidates, casting a vote, and displaying the results transparently.

B. Blockchain Layer (Back-End Logic):
The core logic of the e-voting system was encapsulated in a smart contract. This contract was written in Solidity and deployed to the Ethereum blockchain. To ensure voter privacy and prevent duplicate voting, the system implements a sophisticated registration process. Each voter provides a unique ID (such as a national identity number), which is then immediately hashed using a cryptographic hash function. To protect sensitive information, this hashed ID is stored in a secure off-chain database and is never recorded on the blockchain. Security is enforced through strict server-side Role-Based Access Control (RBAC), ensuring that only authenticated API endpoints can query the registry. Furthermore, as the stored data consists solely of irreversible cryptographic hashes (generated using HMAC-SHA256), the system inherently mitigates the impact of potential data breaches, ensuring that no Personally Identifiable Information (PII) is exposed even if the off-chain storage is compromised. When an individual attempts to register, the system checks the off-chain database to determine whether the hash of a user's ID already exists. If it doesn't, the user's wallet address is added to the smart contract, and the hashed ID is stored. This mechanism ensures that each individual can register only once, preventing multiple registrations with different wallets. The smart contract also enforces the "one-person-one-vote" rule by permitting each allowed address to cast exactly one vote.

C. System Integration Layer:
This layer ensures seamless communication between the user interface and the Ethereum network via the Ethers.js library. The application connects to the Ethereum network via an RPC endpoint provided by Alchemy, ensuring reliable, scalable access to the blockchain. Users interact with the system through a web browser. Ethereum was chosen for its technological maturity, robust developer community, and compatibility with widely adopted wallet tools for signing and sending transactions.

Data Collection and Participants

Upon completion of the prototype, data were collected to evaluate user acceptance and perception. The primary data collection instrument was an online survey, administered through Google Forms, designed to capture user feedback on the system's functionality, transparency, and overall user experience. The survey was structured with Likert-scale questions intended to measure the core constructs of the Technology Acceptance Model (TAM). To gather feedback, participants were first familiarized with the system's features and workflow through a guided demonstration. Following this exposure to the system, they were asked to complete the survey. This study involved a small-to-medium-scale pilot implementation intended to replicate a typical competition environment. Data were obtained from 153 participants who evaluated the system. Although this sample size is adequate for assessing functional integrity and user acceptance in competition-based scenarios, it does not reflect the scale of a national election context.

Data Analysis

The collected survey data were analyzed using the Technology Acceptance Model (TAM) to assess user perceptions of the system. The analysis focused

Accredited Rank 2 (Sinta 2) based on the Decree of the Dirjen Penguatan RisBang Kemenristekdikti No.225/E/KPT/2022, December 07, 2022. Published by LPPM Universitas Nusa Mandiri

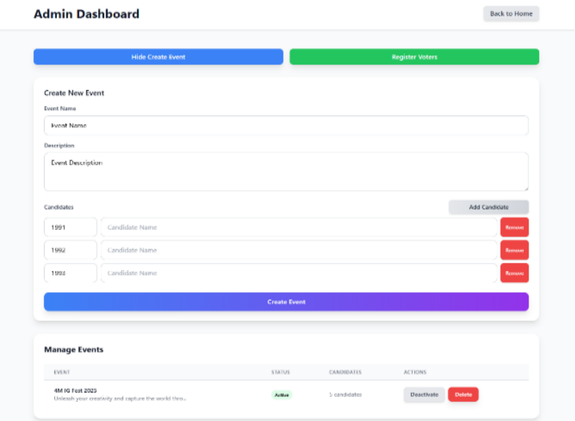
on two primary variables influencing adoption: Perceived Usefulness (PU), which measured how much users believed the system would improve the efficiency and security of voting, and Perceived Ease of Use (PEOU), which evaluated the system's user-friendliness. Mean scores for all questions related to PU, PEOU, and the overall Acceptance of Technology (AOT) were calculated. This quantitative analysis provided insight into the system’s potential adoption and suggested avenues for future refinement.

RESULTS AND DISCUSSION

The development process culminated in a functional e-voting prototype that successfully implements the core features of a transparent and secure voting system on the Ethereum blockchain. The system's performance, integrity, and user acceptance were evaluated through its on-chain activities, administrative interfaces, and user feedback.

Event Administration and Setup

The system includes an administrative dashboard that enables event organizers to create and manage voting events without directly interacting with the smart contract. As shown in Figure 1, administrators can define event parameters, including the name, description, and candidate list. From the same interface, they can also access the voter registration panel to allowlist eligible participants. This feature establishes a clear separation between the administrative and voter roles, ensuring a secure workflow for event management. It demonstrates that the prototype functions not only as a voting mechanism but also as a practical event management tool suitable for competition-based contexts.



Event Name: Event Name

Description: Event Description

Candidates

1991	Candidate Name
1992	Candidate Name
1993	Candidate Name

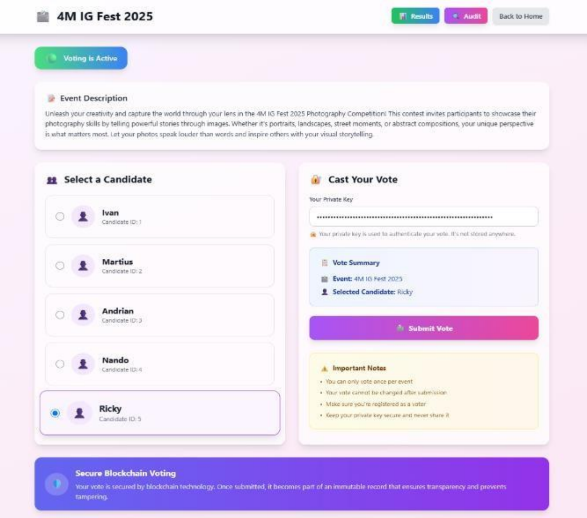
Manage Events

EVENT	STATUS	CANDIDATES	ACTIONS
4M IG Fest 2025 Unleash your creativity and capture the world thro...	Active	5 candidates	Deactivate Delete

Source: (Research Results, 2025)
Figure 1. Admin Dashboard for Event Creation

The Voting Process and On-Chain Integrity

The development resulted in a fully operational web application that allows users to participate in a voting event hosted on the blockchain. The primary voting interface, as shown in Figure 2, was designed for clarity and ease of use, presenting the event description, a clear list of candidates, and a straightforward voting process. The user interface was intentionally kept simple to lower the barrier to entry for users who may lack prior familiarity with blockchain technology. The design centralizes all necessary information on a single page to streamline the user journey. The interface also includes educational elements, such as the "Important Notes" section, which explains key blockchain properties, such as immutability. A known limitation in this prototype's UI is the private key input field; a production-ready application would instead interface with a secure wallet like MetaMask to handle transaction signing without exposing the key.



Event Description

Unleash your creativity and capture the world through your lens in the 4M IG Fest 2025 Photography Competition! This contest invites participants to showcase their photography skills by telling powerful stories through images. Whether it's portraits, landscapes, street moments, or abstract compositions, your unique perspective is what matters most. Let your photos speak louder than words and inspire others with your visual storytelling.

○ Ivan — Candidate ID: 1
○ Martius — Candidate ID: 2
○ Andrian — Candidate ID: 3
○ Nando — Candidate ID: 4
● Ricky — Candidate ID: 5

Your Private Key: ••

Your private key is used to authenticate your vote. It's not stored anywhere.

Vote Summary
Event: 4M IG Fest 2025
Selected Candidate: Ricky

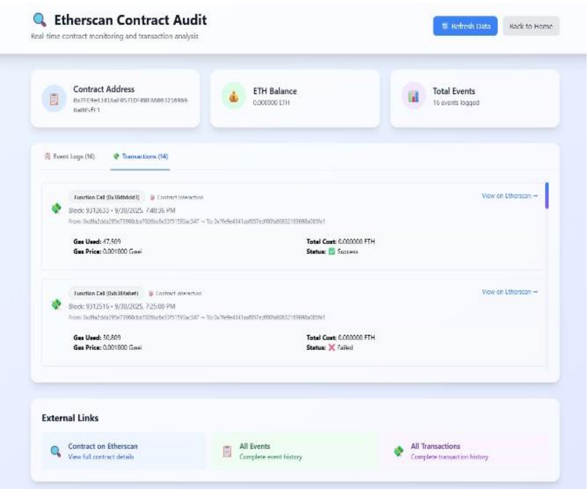
Important Notes
- You can only vote once per event
- Your vote cannot be changed after submission
- Make sure you're registered as a voter
- Keep your private key secure and never share it

Secure Blockchain Voting
Your vote is secured by blockchain technology. Once submitted, it becomes part of an immutable record that ensures transparency and prevents tampering.

Source: (Research Results, 2025)
Figure 2. Main Voting Interface

On-Chain Transaction Integrity and Rule Enforcement

The core objective of this research was to ensure that all voting activities are recorded immutably and that the election rules are automatically enforced. Figure 3 shows the transaction history on the Etherscan block explorer for the smart contract, confirming that actions such as Register Voter and Vote were successfully executed and stored on-chain. This result confirms the system's ability to create a permanent, tamper-resistant record of all electoral activities, a significant advantage over traditional, centralized databases.



Etherscan Contract Audit
Real-time contract monitoring and transaction analysis

Contract Address
0x7FE9e4341AaF057EDF00FA60632169698a085fE1

ETH Balance
0.000000 ETH

Total Events
16 events logged

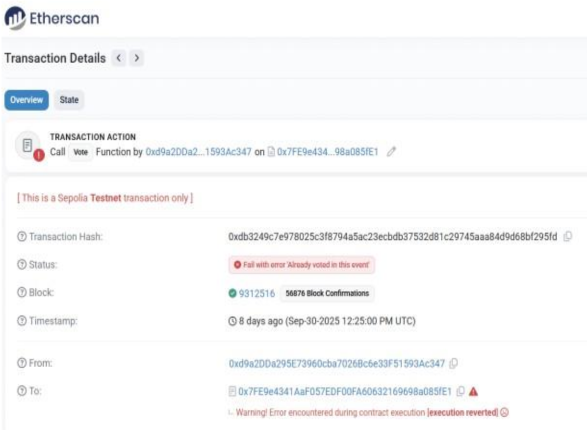
Function Call ([illegible]) Contract Interaction
Block: 9312633 • 9/30/2025, 7:40:36 PM
From: 0xd9a2dda295e73960cba7026bc6e33f51593ac347 → To: 0x7fe9e4341aaf057edf00fa60632169698a085fe1
Gas Used: 47,509
Gas Price: 0.001000 Gwei
Total Cost: 0.000000 ETH
Status: ✅ Success

Function Call ([illegible]) Contract Interaction
Block: 9312516 • 9/30/2025, 7:25:00 PM
From: 0xd9a2dda295e73960cba7026bc6e33f51593ac347 → To: 0x7fe9e4341aaf057edf00fa60632169698a085fe1
Gas Used: 30,809
Gas Price: 0.001000 Gwei
Total Cost: 0.000000 ETH
Status: ❌ Failed

External Links
Contract on Etherscan
View full contract details
All Events
Complete event history
All Transactions
Complete transaction history

Source: (Research Results, 2025)
Figure 3. Transaction Log for the Smart Contract

Furthermore, the system was tested to validate its ability to prevent double voting. As shown in Figure 4, when a registered user who has already voted attempts to submit a second transaction, the transaction fails with an "execution reverted" error. This is a crucial finding, as it demonstrates the smart contract's autonomous enforcement of the election rules. The contract's logic, which prevents an allowed address from voting more than once, operates without requiring a central administrator to check for duplicates. This directly mitigates fraud risk and aligns with research highlighting the integrity-enhancing capabilities of smart contracts in automated processes.



Transaction Details

TRANSACTION ACTION
Call Vote Function by 0xd9a2DDa2...1593Ac347 on 0x7FE9e434...98a085fE1

[This is a Sepolia **Testnet** transaction only]

Transaction Hash: 0xdb3249c7e978025c3f8794a5ac23ecbdb37532d81c29745aaa84d9d68bf295fd
Status: Fail with error 'Already voted in this event'
Block: 9312516 56876 Block Confirmations
Timestamp: 8 days ago (Sep-30-2025 12:25:00 PM UTC)

From: 0xd9a2DDa295E73960cba7026Bc6e33F51593Ac347
To: 0x7FE9e4341AaF057EDF00FA60632169698a085fE1
Warning! Error encountered during contract execution **[execution reverted]**

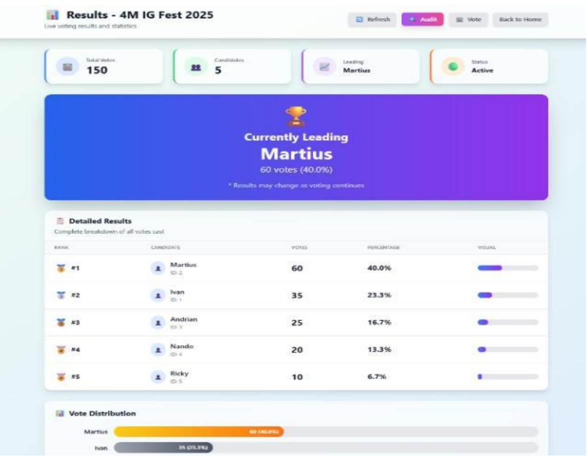
Source: (Etherscan, 2025)
Figure 4. Reverted Transaction on Attempted Double Vote

Role-Based Access Control and Modifiers

The contract integrates role-based access control to secure administrative operations. An admin address is set upon contract deployment. Critical administrative functions are protected by an onlyAdmin modifier that is implemented to ensure that only the designated administrator is permitted to perform sensitive actions such as creating new voting events (createEvent), managing candidates (addCandidate), registering voters (registerVoter), and starting or stopping an election (setEventStatus). This strict separation of roles prevents unauthorized manipulation of the election's parameters. While this grants the administrator significant control, every administrative action is itself a transaction that is permanently recorded on the blockchain. For instance, if an administrator were to reactivate an event after its official closing time maliciously, that action would create a public and time-stamped transaction log. The function also emits an EventStatusChanged event, ensuring that all administrative interventions are fully auditable and that the admin is held accountable for their actions.

Transparency of Results and Auditability

The system was designed to provide complete transparency for all stakeholders, featuring a real-time results dashboard (Figure 5) and a detailed audit trail (Figure 6). The results page displays a live tally of votes and their distribution, while the audit trail provides a complete, time-stamped log of every valid vote cast, linking each to a specific voter address and block number. This combination of a real-time dashboard and a public audit trail provides unprecedented transparency. Unlike traditional voting, where ballots are counted behind closed doors, this system allows any participant to independently verify the total vote count by cross-referencing the audit trail with the public records on the blockchain explorer. Such transparency enhances user trust and aligns with previous studies highlighting blockchain's role in ensuring audit data integrity [22].



Results - 4M IG Fest 2025
Live voting results and statistics

Total Votes 150
Candidates 5
Leading Martius
Status Active

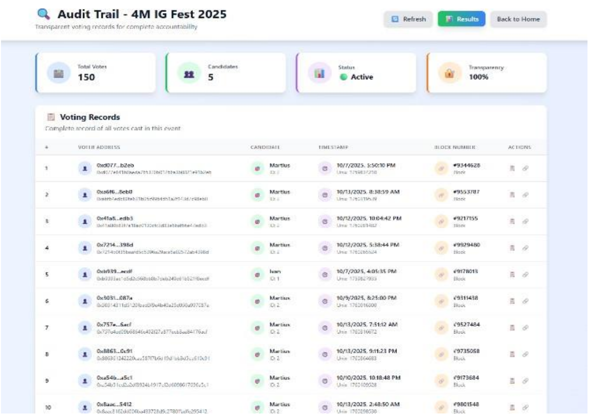
Currently Leading
Martius
60 votes (40.0%)
* Results may change as voting continues

Detailed Results
Complete breakdown of all votes cast

RANK	CANDIDATE	VOTES	PERCENTAGE	VISUAL
#1	Martius ID: 2	60	40.0%	
#2	Ivan ID: 1	35	23.3%	
#3	Andrian ID: 3	25	16.7%	
#4	Nando ID: 4	20	13.3%	
#5	Ricky ID: 5	10	6.7%	

Vote Distribution
Martius 60 (40.0%)
Ivan 35 (23.3%)

Source: (Research Results, 2025)
Figure 5. Real-Time Results Dashboard


Audit Trail - 4M IG Fest 2025
Transparent voting records for complete accountability
Refresh
Results
Back to Home
Total Votes
150
Candidates
5
Status
Active
Transparency
100%

Voting Records

Complete record of all votes cast in this event

#	VOTER ADDRESS	CANDIDATE	TIMESTAMP	BLOCK NUMBER	ACTIONS
1	0xd077...b2eb [illegible]	Martius ID: [illegible]	10/7/2025, 5:50:10 PM Unix: [illegible]	#9344628 Block	
2	0xa6f6...8eb0 [illegible]	Martius ID: [illegible]	10/13/2025, 8:38:59 AM Unix: [illegible]	#9553787 Block	
3	0x41a8...edb3 [illegible]	Martius ID: 2	10/12/2025, 10:04:42 PM Unix: [illegible]	#9217155 Block	
4	0x7214...398d [illegible]	Martius ID: 2	10/12/2025, 5:38:44 PM Unix: [illegible]	#9929480 Block	
5	0xb939...ecdf [illegible]	Ivan ID: 1	10/7/2025, 4:05:35 PM Unix: [illegible]	#9178013 Block	
6	0x3031...087a [illegible]	Martius ID: 2	10/9/2025, 8:25:00 PM Unix: [illegible]	#9311438 Block	
7	0x757e...6acf [illegible]	Martius ID: 2	10/13/2025, 7:51:12 AM Unix: [illegible]	#9527484 Block	
8	0x8863...0c91 [illegible]	Martius ID: 2	10/13/2025, 9:11:23 PM Unix: [illegible]	#9735058 Block	
9	0xa54b...a5c1 [illegible]	Martius ID: 2	10/10/2025, 10:18:48 PM Unix: [illegible]	#9173684 Block	
10	0x8aac...5412 [illegible]	Martius ID: 2	10/13/2025, 2:48:50 AM Unix: [illegible]	#9801548 Block	

Source: (Research Results, 2025)

Figure 6. Public Audit Trail of Voting Records

Comparative Analysis

To evaluate the system's efficiency and security, it was compared with Hassan et al. [20] on metrics such as transaction costs, confirmation latency, and security. Table 1 shows that the proposed Ethereum (PoS) system significantly outperforms the legacy PoW-based implementation in stability and cost-efficiency.

Table 1. Comparative Analysis of the System

Evaluation Indicator	Previous Study [20] (Hassan et al.)	Proposed System (This Study)
Consensus Mechanism	Proof-of-Work (PoW)	Proof-of-Stake (PoS)
Avg. Transaction Fee	0.0071 Ether ($8.899)	~0.000036 ETH (~$0.11)
TPS	14 TPS	14 TPS
Block Time	Avg: 16 sec	Avg: 12 sec
Gas Used Average	~581,885	~183,223
Average Gas Fee	12.20173 Gwei (2023)	0.201 Gwei (2025)
Key Security Features	Double-Voting Prevention	Enhanced Double-Voting Prevention, Immutable Data, & Decentralized RBAC

Source: (Research Results, 2025)

The results demonstrate that the proposed system achieves a significant cost reduction by leveraging the Ethereum Proof-of-Stake (PoS) consensus mechanism, optimized smart contract design, and the reduced base fee environment introduced after the Dencun upgrade (EIP-4844). Specifically, the average transaction cost decreased from approximately $8.89 in the legacy Ethereum system used by Hassan et al. [20] to around $0.11 per voting transaction in the proposed implementation. While both systems exhibit a similar throughput of 14 transactions per second (TPS), the proposed system benefits from a more predictable block production time of approximately 12 seconds, resulting in lower latency and improved transaction confirmation stability. These improvements collectively enhance the system's cost efficiency, operational reliability, and suitability for real-world competitive voting scenarios.

Beyond performance, a fundamental architectural difference exists in data integrity. The previous study [20] implements a Mutable model where the administrator retains the authority to delete candidates even after deployment, which violates the core blockchain principle of immutability. The proposed system enforces immutability by cryptographically locking the candidate list at election start and upgrades identity management from centralized key assignment to a decentralized RBAC model, ensuring that only voters can cast their vote and preventing administrative manipulation.

User Acceptance Evaluation

Finally, the prototype's usability and user perception were quantitatively evaluated using the Technology Acceptance Model (TAM) to measure the key drivers of user adoption. The analysis focused on three primary constructs: Perceived Ease of Use (PEOU), Perceived Usefulness (PU), and Acceptance of Technology (AOT).

The descriptive statistics, summarized in Table 2, show the average user ratings for each construct, represented as a percentage of the maximum possible score. All constructs received highly positive scores, indicating a very favorable user reception. Notably, Perceived Usefulness (PU) achieved the highest score at 76.6%, strongly suggesting that users highly valued the system's core benefits, namely enhanced transparency and integrity in the competition. The strong scores for Perceived Ease of Use (PEOU) at 73.4% and Acceptance of Technology (AOT) at 72.8% further confirm the overall positive evaluation.

Table 2. Descriptive Statistics of User Evaluation

Construct	Items (n)	Mean Score	Maximum possible score	Score Obtained	Percentage (%)
PEOU	7	3.67	5355	3932	73.4%
PU	7	3.83	5355	4106	76.6%
AOT	7	3.64	5355	3899	72.8%

Source: (Research Results, 2025)

To understand the relationships between these constructs, a path analysis was conducted, with the results shown in Table 3. The study revealed that all hypothesized relationships were positive and statistically significant (p < .001), confirming the TAM's validity in this context.

Table 3. Correlations Among Latent Constructs

Relation ship	Correlation	SE	B	z-value	p-value
PEOU → PU	0.38	0.114	0.294	3.33	< .001
PEOU → AOT	0.47	0.123	0.347	3.87	< .001
PU → AOT	0.85	0.128	0.728	6.67	< .001

Source: (Research Results, 2025)

The most critical finding from this analysis is the robust positive correlation between Perceived Usefulness (PU) and Acceptance of Technology (AOT), with a path coefficient of 0.85. This indicates that the system's usefulness was the most dominant factor influencing user acceptance. In other words, users were willing to adopt the technology primarily because they believed it could deliver fair and trustworthy results. The combination of PU having the highest percentage score (76.6%) and the most decisive influence on acceptance (0.85) provides robust evidence that the system's core value proposition was successfully delivered. This suggests that usefulness is the primary determinant of adoption within blockchain-based voting systems.

However, the slightly lower Perceived Ease of Use (PEOU) score compared to PU suggests that, although users initially found the system somewhat less intuitive, they eventually recognized its clear advantages once they became familiar with the blockchain mechanism. This perception may stem from the underlying blockchain integration, which, while enhancing transparency, introduces a layer of complexity not all participants are familiar with. For many users, especially those with limited prior exposure to blockchain-based applications, the transaction and wallet processes may appear less straightforward. Nevertheless, the overall findings indicate that once users became familiar with the system's mechanisms, they strongly appreciated its advantages in providing verifiable, tamper-resistant voting outcomes.

Although the transition to Proof-of-Stake (PoS) and recent scalability upgrades, such as Dencun, have improved energy efficiency and reduced transaction costs, reliance on the public Ethereum infrastructure continues to present challenges. These include fee volatility, latency, and throughput limitations during periods of high network activity. For production deployment requiring predictable costs, fast confirmation, and high scalability, Layer-2 solutions like Polygon or Optimism. These solutions maintain Ethereum's security while delivering the high throughput required for large-scale concurrent voting.

CONCLUSION

This research successfully designed, developed, and validated an innovative contract-based e-voting system, demonstrating that modern blockchain technology offers a secure and transparent alternative to conventional voting methods for competitions. The system’s integrity was ensured through an immutable on-chain ledger and a self-executing smart contract that automatically prevents electoral fraud, such as double voting, by rejecting invalid transactions. Additionally, integrating a public audit trail and a real-time results dashboard highlighted the system’s strong capacity for transparency and verifiability.

From a user-centered perspective, the evaluation using the Technology Acceptance Model (TAM) showed high user acceptance, indicating that participants found the system both valuable for ensuring fairness and reasonably easy to use. The study concludes that the proposed hybrid architecture, which combines off-chain hashed identity management for privacy with on-chain logic for integrity, provides a robust and practical framework. The prototype was evaluated within a limited scope (n=153). Although it demonstrated effectiveness in competition settings, its performance under high-concurrency conditions with thousands of voters has yet to be validated.

Future work should focus on evaluating scalability for larger deployments and on integrating decentralized identity frameworks to enhance privacy and authentication further. Moreover, such systems present significant educational potential. By familiarizing users with blockchain-based voting in low-stakes environments such as competitions, future implementations can encourage broader adoption and understanding of secure e-voting technologies. Overall, this study adds to the expanding body of literature demonstrating how blockchain technology can serve as a bridge between technical transparency and public trust in electronic voting.

REFERENCE

[1] N. Partarakis and X. Zabulis, "A Review of Immersive Technologies, Knowledge Representation, and AI for Human-Centered Digital Experiences," Electronics (Switzerland), vol. 13, no. 2, 2024, doi: 10.3390/electronics13020269.

[2] Y. B. Hamdan and A. Sathesh, "Construction of Efficient Smart Voting Machine with Liveness Detection Module," Journal of Innovative Image Processing, vol. 3, no. 3, pp. 255–268, 2021, doi: 10.36548/jiip.2021.3.007.

[3] M. V. Vladucu, Z. Dong, J. Medina, and R. Rojas-Cessa, "E-Voting Meets Blockchain: A Survey," IEEE Access, vol. 11, no. February, pp. 23293–23308, 2023, doi: 10.1109/ACCESS.2023.3253682.

[4] M. H. Berenjestanaki, H. R. Barzegar, N. El Ioini, and C. Pahl, "Blockchain-Based E-Voting Systems: A Technology Review," Electronics (Basel), vol. 13, no. 1, p. 17, Dec. 2023, doi: 10.3390/electronics13010017.

[5] U. Jafar, M. J. Ab Aziz, Z. Shukur, and H. A. Hussain, "A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems," Sensors, vol. 22, no. 19, 2022, doi: 10.3390/s22197585.

[6] H. Yi, "An Efficient E-Voting System for Business Intelligence Innovation Based on Blockchain," Journal of the Knowledge Economy, no. 0123456789, 2023, doi: 10.1007/s13132-023-01560-x.

[7] B. Ahn, "Implementation and Early Adoption of an Ethereum-Based Electronic Voting System for the Prevention of Fraudulent Voting," Sustainability, vol. 14, no. 5, p. 2917, Mar. 2022, doi: 10.3390/su14052917.

[8] M. S. Farooq, U. Iftikhar, and A. Khelifi, "A Framework to Make Voting System Transparent Using Blockchain Technology," IEEE Access, vol. 10, pp. 59959–59969, 2022, doi: 10.1109/ACCESS.2022.3180168.

[9] S. Ramasamy, A. K B, and P. K, "Blockchain-Based Online Voting System," ECS Trans, vol. 107, no. 1, pp. 13195–13203, Apr. 2022, doi: 10.1149/10701.13195ecst.

[10] L. Theodorakopoulos, A. Theodoropoulou, and C. Halkiopoulos, "Enhancing Decentralized Decision-Making with Big Data and Blockchain Technology: A Comprehensive Review," Applied Sciences (Switzerland), vol. 14, no. 16, 2024, doi: 10.3390/app14167007.

[11] A. Shaikh, N. Adhikari, A. Nazir, A. S. Shah, S. Baig, and H. Al Shihi, "Blockchain-enhanced electoral integrity: a robust model for secure digital voting systems in Oman," F1000Res, vol. 14, p. 223, 2025, doi: 10.12688/f1000research.160087.2.

[12] M. Goyal and A. Kumar, "Sustainable E-Infrastructure for Blockchain-Based Voting System," in Digital Cities Roadmap, Wiley, 2021, pp. 221–251. doi: 10.1002/9781119792079.ch7.

[13] C. Onur and A. Yurdakul, "ElectAnon: A Blockchain-Based, Anonymous, Robust and Scalable Ranked-Choice Voting Protocol," Mar. 2022, [Online]. Available: http://arxiv.org/abs/2204.00057

[14] R. Fatih, S. Arezki, and T. Gadi, "A Review of Blockchain-Based E-Voting Systems: Comparative Analysis and Findings," International Journal of Interactive Mobile Technologies (iJIM), vol. 17, no. 23, pp. 49–67, Dec. 2023, doi: 10.3991/ijim.v17i23.45257.

[15] P. Kumbharkar, S. Pawtekar, S. Javeer, and P. Abhale, "Blockchain-based e-voting systems: Enhancing security, transparency and trust," International Journal of Science and Research Archive, vol. 12, no. 1, pp. 635–642, May 2024, doi: 10.30574/ijsra.2024.12.1.0707.

[16] P. McCorry, M. Mehrnezhad, E. Toreini, S. F. Shahandashti, and F. Hao, "On Secure E-Voting over Blockchain," Digital Threats: Research and Practice, vol. 2, no. 4, 2021, doi: 10.1145/3461461.

[17] S. A.-B. Salman, Sufyan Al-Janabi, and A. M. Sagheer, "Valid Blockchain-Based E-Voting Using Elliptic Curve and Homomorphic Encryption," International Journal of Interactive Mobile Technologies (iJIM), vol. 16, no. 20, pp. 79–97, Oct. 2022, doi: 10.3991/ijim.v16i20.33173.

[18] R. S. Bhadoria, A. P. Das, A. Bashar, and M. Zikria, "Implementing Blockchain-Based Traceable Certificates as Sustainable Technology in Democratic Elections," Electronics (Basel), vol. 11, no. 20, p. 3359, Oct. 2022, doi: 10.3390/electronics11203359.

[19] A. Mukherjee, S. Majumdar, A. K. Kolya, and

S. Nandi, “A Privacy-Preserving Blockchain-based E-voting System,” Jul. 2023, [Online]. Available: http://arxiv.org/abs/2307.08412

[20] H. Hassan, R. Hassan, and E. Gbashi, “E-voting System Based on Ethereum Blockchain Technology Using Ganache and Remix Environments,” Engineering and Technology Journal, vol. 41, no. 4, pp. 1–16, Mar. 2023, doi: 10.30684/etj.2023.135464.1273.

[21] H. Herman and F. Frederick, “Progressive Web Apps: Pengembangan dan Studi Penerimaan pada Mahasiswa Indonesia Menggunakan Scrum dan UTAUT,” jurnal teknologi terpadu, vol. 9, no. 1, pp. 22–28, 2023.

[22] T. Wibowo and Y. Christian, “Usage of blockchain to ensure audit data integrity,” vol. 24, no. 1, pp. 47–58, 2021, doi: 10.34209/equ.v24i1.2357.