El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

AN ELECTRONIC VOTING SYSTEM WITH DIRECTED ACYCLIC GRAPH (DAG)-BASED BLOCKCHAIN USING ShimmerEVM NETWORK

D. Maliki [1], C. Oruche[2], I. M. Abdullahi[3], B.G. Najashi[4], O.R. Isah[5], A. Ahmed[6], A.S. Gbadamosi[7]

[1,2,3,5,6]Department of Computer Engineering, Federal University of Technology, Minna, Niger State, Nigeria
[4]El Amin University, Minna, Niger State, Nigeria
[6]Electrical and Electronics Engineering Department, Federal University of Technology, Minna, Niger State, Nigeria
Corresponding Author: danlami.maliki@futminna.edu.ng

Abstract

This research introduces an innovative electronic voting system that enhances transparency, anonymity, and reliability, aiming to revolutionize both traditional and existing electronic voting methodologies. The system increases accessibility, security, and efficiency in the electoral process. Advanced web development technologies, including NextJs, TailwindCSS, TypeScript, and JWT tokens, are integrated for an improved e-voting experience. This system employs encryption and cryptographic hashes to secure sensitive information, alongside smart contracts on ShimmerEVM—a Directed Acyclic Graph (DAG)-based blockchain—to ensure data persistence and immutability. A user-friendly front-end interface serves as a portal to the web application, enabling seamless interaction with the ShimmerEVM network. A critical feature of the system is the activation of a biometric hardware component, essential for voter registration and participation. ShimmerEVM facilitates the execution of smart contracts, offering a decentralized, transparent, and secure environment without relying on traditional blockchain technology. The focus of this system is on the implementation of security-centric smart contracts, which are pivotal in maintaining voting data integrity and mitigating the risks of vote count manipulation.

Keywords: e-voting, shimmerEVM, internet voting, electronic voting, blockchain-based voting, voting systems, cryptography-based voting, DLT, distributed ledger voting, blockchain voting

1.0 Introduction

Elections are an essential part of modern democratic societies and determine who can hold political office [1]. Regardless of the scenario, the election outcome has consequences that can affect the livelihoods of the participating parties. Traditional voting systems that require the use of ballots have faced challenges such as fraud, lack of security and election manipulation due to various factors, including human error and fraudulent intent[2]. These issues have created the need for a more secure and efficient voting solution where voters can trust the results and the risk of fraud and manipulation of the results is almost negligible [3]. Current electronic voting systems, which use electronic methods for casting and counting votes, are not only cost-effective but are also recognized as providing a high level of security throughout the voting process [4]. Although, the problem lies in their centralization, where data, including voter information and sensitive voting information, is stored in a single database that can be hacked, creating a single point of failure and potentially damaging effects on democratic outcomes[5].

Various electronic voting mechanisms have been proposed to provide solutions. The best

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

known of these is the use of distributed ledger technology (DLT), with a focus on blockchain systems. The project will consider a different type of DLT, namely directed acyclic graph (DAG), which, although less common, offers faster transaction times than blockchain [6]. Additionally, enabling parallel processing of transactions using DAGs maintains the decentralized, secure and immutable properties of the blockchain while enabling relatively higher speeds with confirmation times in seconds [7].

Introducing the electronic voting system will solve the problems already experienced by traditional voting systems where ballot paper is used and solve concerns related to current voting systems; it will allow for easy onboarding of users (or voters), anonymity, and verification of votes by individual voters after voting events has been completed. The overall goal is to provide a trustable security mechanism that preserves the authenticity of votes, limiting participation from unauthorized [8].

2.0 Reviews of Electronic Voting Systems and Technologies

Electronic voting systems provide an alternative to the more traditional method of ballot voting or mail voting [3]. Efficient electronic voting methods must provide the core features of anonymity, security, and transparency to be considered fit for most electoral purpose [9]. Distributed ledger technologies (DLT) have received great attention in recent years and promise a high level of data security in various areas. One of the main areas of application is electronic voting systems, whose main advantages in terms of immutability, security, consistency and confidentiality lie in the requirement for reliable results. Electronic voting systems help eliminate the need to use the popular vote counting method known for its fairness and political compromises [10].

According to [10], Electronic voting systems have proven unsatisfactory for physical security reasons, as the voting system hardware can be sabotaged, rendering the entire voting process unusable. Blockchain technology – a distributed ledger – has been proposed as a solution to this problem. [11] applied Blockchain is a distributed transaction ledger that combines cryptography, distributed computing and networking to ensure the immutability of stored data and the anonymity of network participants, thus meeting some requirements necessary for the security of voting systems

In [12], different methods was examined that have been used to deploy blockchain in electronic voting systems where security is required. One of them is zero-knowledge evidence. It allows you to verify the accuracy of your identity/communications/data without revealing the information contained therein. There is also token-based voting, where cryptocurrencies or tokens are issued over the blockchain protocol, with voting taking place at the voter's wallet address. This token is used for voting, and the voting table is done by counting voter tokens to determine the result. The work of [13] described some current blockchain-based electronic voting systems and their features: Follow My Vote, which allowed voters to vote remotely and used mathematical algorithms to allow voters to identify their ballot and, through identification, ensure the accuracy of the vote cast . Another voting application, Voatz, enables remote voting via a smartphone,

which can be verified using biometric identification. Agora Group worked on a blockchain-based voting system that used the universal token for participation. This was partially used in the 2018 elections in Sierra Leone.

In [10], a licensed Hyperledger blockchain network was used, which leverages robust smart contracts, to develop an electoral system with some of the characteristics of traditional electoral voting. To participate in voting exercises, voters must register and show up at a physical location. Although this provides an additional advantage in terms of voter verifiability, the system is still affected by blockchain scalability issues and the permissive nature of the systems prevents voters from seeing the details of their current votes. Allows only nodes/organizations to access voting data, limiting voting transparency.

In [14], a consensus algorithm was proposed, called Proof of Completeness for use in mock elections in Pakistan, where voting is done on specific voting machines and the presence of presiding officers is required. The algorithm works in four phases: block creation, block sealing, data management and blockchain construction. The problem with this system is that it relies too much on centralized bodies to organize voting. A few weeks before the elections, the voter list must come from a central source. The end of voting at a polling station depends on the polling station control, which is obliged to confirm the end of voting at their polling station. In the consensus model, blocks are only closed when an election official makes a decision. Most of the features of this system remove the decentralized functionality of the blockchain. There is no way to check verifiability and invalid votes are not verified.

In [15] and [16], "DVTCain" system was developed, where voters have the option to vote using their smartphone or go to a specific polling station to vote. It ensures voter anonymity by storing hash values of details on the blockchain during registration, which are ultimately used to verify the voter's identity during voting. Before voting, those entitled to vote receive a coin (symbolic vote). which they use to cast vote for specific candidates/option. To check that a voter has taken part in the election, their wallet balance is checked. 1 coin means vote not casted, and zero coins means vote has been casted by the voter. DVTChain also carries identity checks using private-public key pairs which is a core feature of the blockchain identities. Overall,

The privacy is preserved, transparency is achieved and voting outcome can be trusted. One downside of DVTChain is in the use of Ethereum blockchain which has a high probability of slow confirmation time for transaction in congested network states.

According to [27] and [10] a blockchain-based voting system called "TrustVote" which uses Hyperledger Fabric as underlying protocol for voting was proposed. It faces the same problems as the proposed system from where the protocol is permissioned to specific nodes/organization and transparency may not be guaranteed with a centralized controlling entity. It proposes the visit of established voting body to verify the authenticity of transaction ID which is generated after a voter casts their vote. The characteristics of different DLTs are shown in Table 1.

In [28], a technique was created that enable voters to cast their ballots via a website interface, eliminating the need to visit their preferred polling station. Additionally, voters can register on the day of the election itself.

This process involves the verification of the voter's ID card and eligibility to vote, as confirmed by the relevant authorities based on the provided documents. However, this method does not ensure voter anonymity. According to [29], a Tangle was presented, a directed acyclic graph (DAG) structure, as a method for reaching consensus in distributed ledger systems. It adopts a theoretical perspective, offering an in-depth exploration of Tangle's fundamental concepts. Popov delves into the mathematical basis of Tangle's consensus process and explores its impact on scalability. Yet, the article's primary shortcoming is its theoretical focus, lacking a thorough assessment of Tangle's practical effectiveness or potential weaknesses in real-world scenarios.

[30] research on addressing scalability issues found in networks based on Tangle. The approach integrates empirical analysis with simulations to assess how Tangle performs under different circumstances. The team pinpoints challenges and suggests enhancements to improve scalability. Nevertheless, the study's drawbacks lie in its dependence on simulated environments, which might not accurately mirror actual conditions, and the difficulty in forecasting the behavior of future networks.

An adopted a methodical strategy for evaluating the security of the IOTA Tangle was developed. This involves employing a mix of penetration testing, formal verification, and cryptographic scrutiny to uncover possible security weaknesses. While the approach is robust, a key limitation of the study is the ever-changing landscape of security threats, posing a challenge to fully addressing every conceivable attack scenario. Furthermore, as the Tangle network develops, the efficacy of implemented security measures may change over time[31]

Table I: Different DLTs and their characteristics.

Blockchain /DLT	**Consensus Mechanism**	**Typical Time to Finality**	**Typical TPS**	**Transaction Characteristic**
Bitcoin	PoW	~60 minutes[17]	7[18]	Can vary depending on network congestion
Ethereum	PoS	13-20 minutes [19]	<25[20][21]	Transactions are divided into 12-second slots
Solana	PoS with a unique hybrid consensus mechanism	~12 seconds[22]	~2000 [23]	Time varies depending on network conditions and contract complexity
Avalanche	PoS with a fast finality protocol	2 seconds[24]	40-100 [24]	Prioritizes rapid transaction confirmation
IOTA Tangle	Shimmer DPoS	10-30 seconds[25]	700 [26]	Boasts high speed and scalability
Blockchain /DLT	**Consensus Mechanism**	**Typical Time to Finality**	**Typical TPS**	**Transaction Characteristic**
Bitcoin	PoW	~60 minutes[17]	7[18]	Can vary depending on network congestion
Ethereum	PoS	13-20 minutes [19]	<25[20][21]	Transactions are divided into 12-second slots

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

Solana	PoS with a unique hybrid consensus mechanism	~12 seconds[22]	~2000 [23]	Time varies depending on network conditions and contract complexity
Avalanche	PoS with a fast finality protocol	2 seconds[24]	40-100 [24]	Prioritizes rapid transaction confirmation
IOTA Tangle	Shimmer DPoS	10-30 seconds[25]	700 [26]	Boasts high speed and scalability

A comparative study was performed to assess the appropriateness of Blockchain and Tangle technologies for Internet of Things (IoT) applications. The research focuses on evaluating aspects like transaction velocity, scalability, and efficient use of resources. The approach entails setting up experimental IoT environments and tracking the performance of each technology. However, the study is limited by the particular nature of IoT settings and the potential for varying outcomes based on different network setups. In essence, the effectiveness of both networks is still constrained by the robustness of the networks they function within[32].

Description of transaction architecture for DLTs based on the Tangle (DAG) and the Blockchain is given in Figure 1.

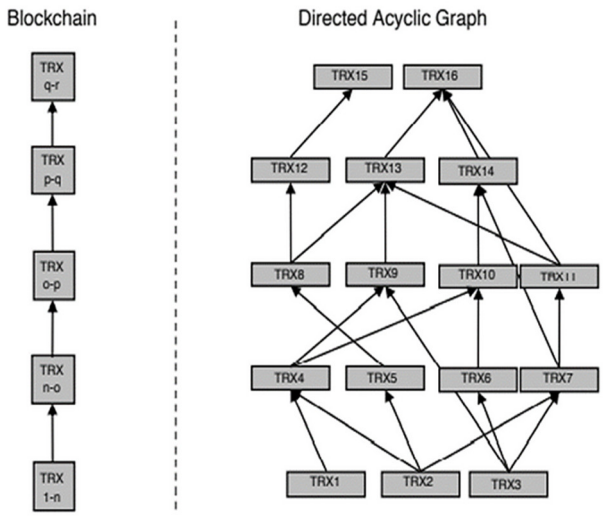

Fig 1: Difference in transaction architecture for blockchain and DAG distributed ledgers *[33]*

3.0 Methodology

3.1 System Implementation & Overview

The developed system integrates hardware components, software components and uses smart contracts (enabled by decentralized ledgers) to achieve its intended purpose of allowing transparent and secure elections. To measure the effectiveness of the electronic voting system, parameters included response time, reliability, security, and user-friendliness. Response time was measured in seconds by observing elapsed time between the start of a task and the end of that same task. Specific parameters like the time to finality (TTF) which implies the time to not only record a transaction on chain, but when it becomes "immutable" was also considered in evaluating response time. Reliability was evaluated through system stability and accuracy of results when registering a voter and identifying a voter for carrying out ballot casting. Security covered the resilience against unauthorized access and data manipulation. User-friendliness was assessed based on the simplicity of the interface and overall voter experience.

On the backend as well, security was important as the backend provides an interface to database and modifying of data on shimmerEVM DLT storage. JSON Web Tokens (JWT) facilitated secure user

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

authentication, sessions and authorization with cryptographic hashes to ensure data integrity between client and server. Cryptography played a pivotal role in securing sensitive data, using cryptographic hashes for tasks such as data integrity verification. Smart contracts, necessary for transparent and automated voting processes, were deployed on the Tangle – a Directed Acyclic Graph (DAG)-based Distributed Ledger Technology (DLT) which ShimmerEVM is built on. Leveraging the Tangle's structure provided cost efficiency and scalability advantages over traditional blockchain frameworks.

For biometric verification, an Arduino ESP32 module and JM101 model fingerprint scanner were programmed using the Arduino IDE. The I2C 0.9-inch OLED display facilitated a user-friendly interface during voter registration. The system underwent rigorous testing, including unit testing for individual components and end-to-end testing for the entire system. User feedback and iterative development cycles were crucial for refining the implementation, addressing issues, and optimizing performance and user experience. The hardware implementation for biometric requirements of the system is given in Figure 2

3.2 Tangle's Directed Acyclic Graph (DAG) DLT

Unlike blockchains, where transactions are sequentially chained in blocks, the Tangle adopts a web-like structure. Each transaction references two previous transactions, creating a directed acyclic graph. This eliminates the need for miners and block size limitations, resulting in unbounded scalability where transaction volume increases, the Tangle simply becomes denser, enabling it to handle massive workloads without performance degradation. The absence of miners eliminates transaction fees, making the Tangle ideal for micropayments and resource-constrained environments like IoT devices.

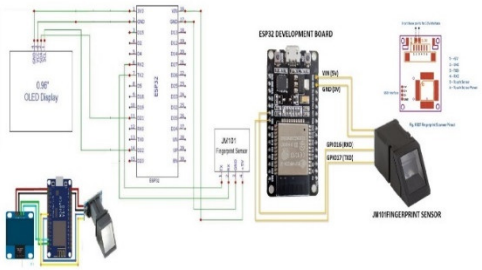

Fig 2: Circuit Diagram of the Fingerprint Component showing circuitry between ESP32, JM101 scanner, and 0.9" I2C OLED display

While Tangle excels in transaction handling, smart contract functionality, the core characteristic of blockchains like Ethereum — which allowed smart contract execution — was initially absent. This gap is bridged by IOTA Smart Contracts, deployed on the Tangle through ShimmerEVM based on a layer two architecture.

The mathematical representation of the Tangle's DAG involves the linking of transactions. Let Tx_n be the nth transaction, and Txn−1 and Txn−2 represent the two previous transactions that approve Tx_n. This relationship can be expressed as in equation (1)

$$Tx_n \rightarrow Tx_{n-1}, Tx_{n-2} \quad (1)$$

In the context of smart contracts, a mathematical or algorithmic representation of a simple condition might involve a conditional statement C that triggers the execution of a smart contract SC when satisfied as given in equation (2)

If C is true, execute SC (2)

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

Shimmer Consensus Mechanism uses Delegated Proof of Stake (DPoS) consensus mechanism. It ensures secure and decentralized smart contract execution. Based on Delegated Proof of Stake (DPoS) algorithm, Shimmer selects nodes for contract validation based on their stake in IOTA tokens. This incentivizes honest participation and mitigates the risks of manipulation. Shimmer's DPoS utilizes complex calculations to determine node selection probabilities for contract validation. These calculations involve weighting nodes based on their IOTA holdings and employing a "weighted random walk" algorithm to select validators.

3.3 Time to Finality

For distributed ledger technology (DLT), time-to-finality refers to the point at which a transaction becomes irreversible and permanently etched into the ledger. Time to finality is not synonymous with transaction speed. Understanding time to finality is crucial for assessing the speed and reliability of different blockchain and DLT systems. Here, we compare the time to finality for prominent blockchains with that of ShimmerEVM.

Several factors influence time to finality, including:

i. Consensus Mechanism: The algorithm used to reach agreement on the state of the ledger, such as Proof of Work (PoW) or Proof of Stake (PoS), among others.

ii. Block Size: The amount of data contained in each block of the chain.

iii. Network Congestion: The number of transactions competing for space on the ledger.

3.4 System Overview

The Figure 3and Figure 4 describes the different phases of the voter registration process. The voter's fingerprint and email are obtained for their first registration, after which they can complete the remaining process by themselves to obtain their unique token and password (the two requirements for the voting exercise). The prominent feature here is that voter's details are not stored on the server, nor is there a collection of any personal information. A means of verification can be obtained and checked for validity before a voter is allowed to register for a particular event.

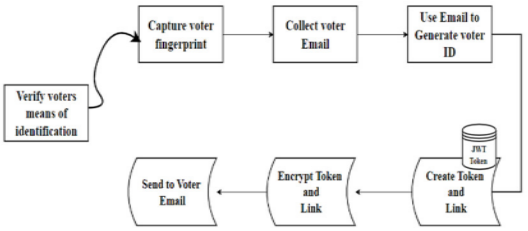

Fig 3: voter registration first phase

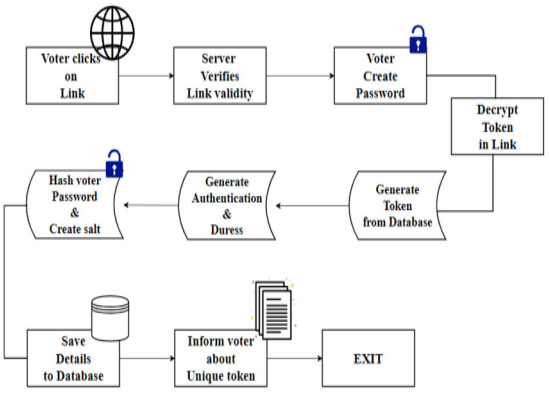

Fig 4: voter registration final phase

Figure 5, describes the vote/ballot casting process where a voter's biometric (fingerprint) is first captured to verify they can vote before given access to the voting screen.

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

4.0 Experimental Results

The electronic voting system was developed which that allows anonymity, a core characteristic of traditional voting systems. The system was run on HP EliteBook 850 G3 with Microsoft Windows 10 Pro version 10.0.19045 Build 19045 OS. All network-based tests were carried out on a 3G Network with an up/down speed range of 600kbits/sec to 1.5mbits/sec.

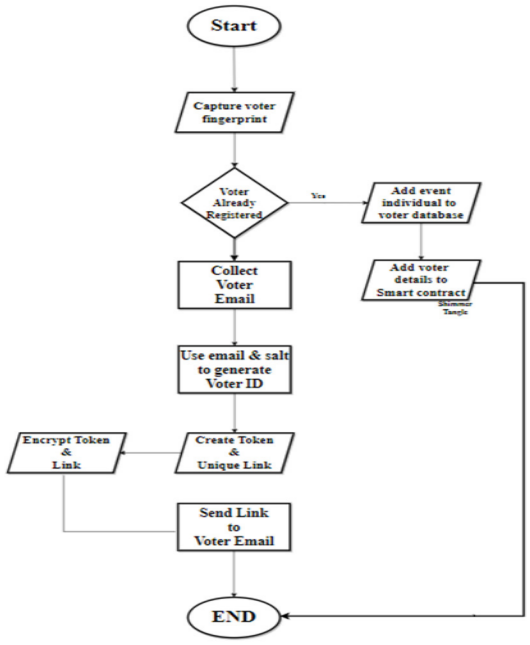

Fig 5: Voting Flow Process for the DAG-based electronic system

In order to obtain reliable results, multiple transactions were taken to obtain results with higher level of accuracy. Response time results from fingerprint scanner was obtained to verify performance after specific operation times has elapsed. Figure 6 shows fingerprint scanner response time. It describes the speed to detect a finger when placed on the scanner after several uses measured in minutes. It should be noted that for every five minutes of a transaction, the fingerprint scanner is used between 5-8 times.

Figure 6 and Figure 7 shows a graph description and snapshot of some of the transactions that happened on chain and the time to confirmation (for creating event, registering voter, allowing voting, etc.).

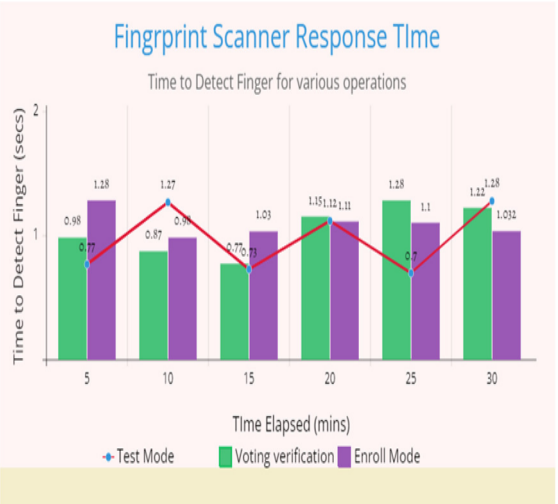

Fig 6: fingerprint response time after specific number of uses

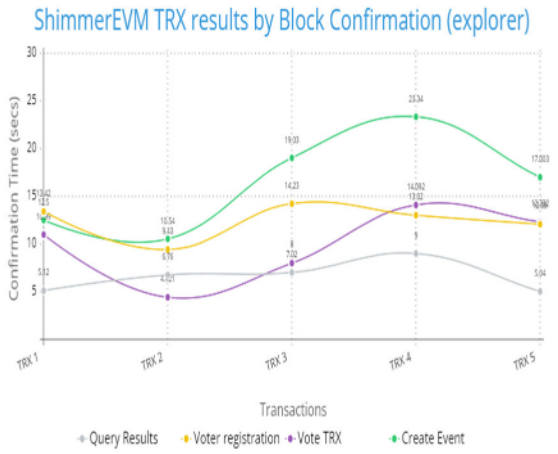

Fig 7: Block TRX confirmation time for different operations

The failed transaction in Fig 8 is for specific cases where a specific smart contract condition required for calling a function in the contract is not satisfied. For example, a voter who has already been registered for an event is attempting double registration; or a voter attempting double voting.

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

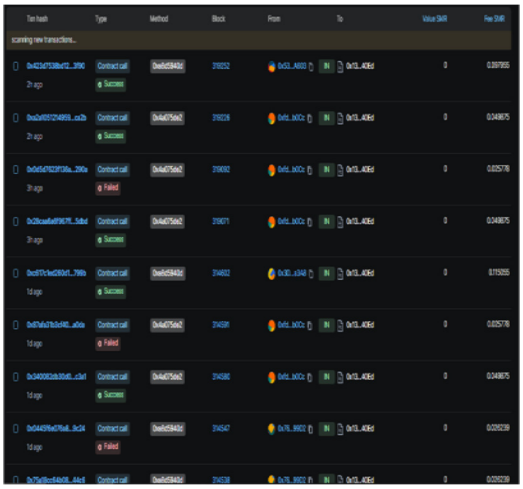

Fig 8: transactions on chain

Figure 9 shows experimental results for a specific election from the web interface/UI.

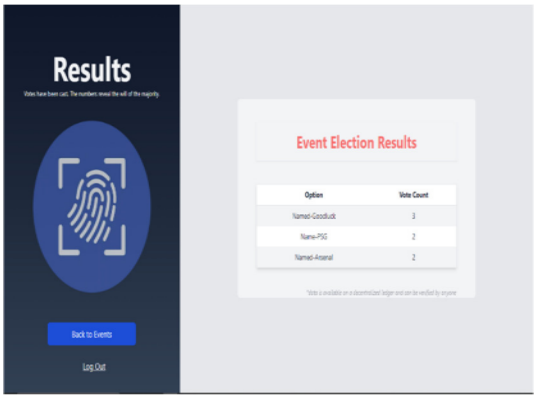

Fig 9: Results view for voting event

5.0 Conclusion

The primary objective was to develop a system that ensures voter anonymity, authenticity, and integrity, utilizing the IOTA Tangle Directed Acyclic Graph (DAG) for decentralized and secure implementation of smart contracts. The central issue addressed is the susceptibility of conventional voting systems to problems like coercion, duplicate voting, and the absence of a transparent, automated procedure. By incorporating cryptographic techniques, a Tangle-based smart contract framework, and a hardware-based biometrics component, this system offers a strong solution that enhances the reliability and efficiency of the voting process. Nonetheless, certain challenges persist, such as the necessity for comprehensive testing to confirm the system's reliability and security, which are critical in electronic voting. Additionally, safeguarding against coercion, essential for preserving voting integrity, requires ongoing refinement and awareness of potential weak points. Despite these obstacles, this research marks a considerable stride in the development of more secure and transparent electronic voting systems.

6.0 References

[1] S. H. Rome, “Why Voting Matters,” in *Promote the Vote: Positioning Social Workers for Action*, S. H. Rome, Ed., Cham: Springer International Publishing, 2022, pp. 31–49. doi: 10.1007/978-3-030-84482-0_2.

[2] M. Bernhard *et al.*, “Can Voters Detect Malicious Manipulation of Ballot Marking Devices?,” in *2020 IEEE Symposium on Security and Privacy (SP)*, May 2020, pp. 679–694. doi: 10.1109/SP40000.2020.00118.

[3] R. K. Esteve Jordi Barrat i, “Electronic Voting,” in *Routledge Handbook of Election Law*, Routledge, 2022.

[4] H. Yi, “Securing e-voting based on blockchain in P2P network,” *EURASIP J. Wirel. Commun. Netw.*, vol. 2019, no. 1, p. 137, May 2019, doi: 10.1186/s13638-019-1473-6.

[5] A. S. Yadav, A. U. Thombare, Y. V. Urade, and A. A. Patil, “E-Voting using Blockchain Technology,” *Int. J. Eng. Res.*, vol. 9, no. 07, Jul. 2020.

[6] PixelPlex, "DAG Technology Definitive Guide: Protocols & Use Cases," PixelPlex. Accessed: Jan. 15, 2024. [Online]. Available: https://pixelplex.io/blog/dag-technology/

[7] K. Lasya, "A Detailed Guide to DAG Technology," Vegavid Technology. Accessed: Jan. 12, 2024. [Online]. Available: https://vegavid.com/blog/dag-technology-guide/

[8] P. Baudier, G. Kondrateva, C. Ammi, and E. Seulliet, "Peace engineering: The contribution of blockchain systems to the e-voting process," *Technol. Forecast. Soc. Change*, vol. 162, p. 120397, Jan. 2021, doi: 10.1016/j.techfore.2020.120397.

[9] A. Petitpas, J. M. Jaquet, and P. Sciarini, "Does E-Voting matter for turnout, and to whom?," *Elect. Stud.*, vol. 71, p. 102245, Jun. 2021, doi: 10.1016/j.electstud.2020.102245.

[10] Md. A. H. Wadud, T. M. Amir-Ul-Haque Bhuiyan, M. A. Uddin, and Md. M. Rahman, "A Patient Centric Agent Assisted Private Blockchain on Hyperledger Fabric for Managing Remote Patient Monitoring," in *2020 11th International Conference on Electrical and Computer Engineering (ICECE)*, Dec. 2020, pp. 194–197. doi: 10.1109/ICECE51571.2020.9393124.

[11] Z. Guo, X. He, and P. Zou, "Voting System Based on Blockchain," *J. Comput. Sci. Res.*, vol. 3, no. 2, Art. no. 2, Apr. 2021, doi: 10.30564/jcsr.v3i2.2797.

[12] S. Donepudi and K. T. Reddy, "Comparing and Elucidating Blockchain Based Voting Mechanisms," in *2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, Apr. 2022, pp. 1181–1185. doi: 10.1109/ICSCDS53736.2022.9760775.

[13] U. Jafar, M. J. A. Aziz, and Z. Shukur, "Blockchain for Electronic Voting System—Review and Open Research Challenges," *Sensors*, vol. 21, no. 17, Art. no. 17, Jan. 2021, doi: 10.3390/s21175874.

[14] B. Shahzad and J. Crowcroft, "Trustworthy Electronic Voting Using Adjusted Blockchain Technology," *IEEE Access*, vol. 7, pp. 24477–24488, 2019, doi: 10.1109/ACCESS.2019.2895670.

[15] S. T. Alvi, M. N. Uddin, L. Islam, and S. Ahamed, "DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 9, pp. 6855–6871, Oct. 2022, doi: 10.1016/j.jksuci.2022.06.014.

[16] A. Sabharwal, M. Saifullah, P. Grover, and N. Batra, "Comparative Study of Blockchain Techniques in Electronic Voting System." Rochester, NY, Jul. 11, 2021. doi: 10.2139/ssrn.3884390.

[17] Fantom foundation, "Time to Finality." Accessed: Jan. 12, 2024. [Online]. Available: https://docs.fantom.foundation/technology/blockchain-basics/time-to-finality

[18] Ledger Academy, "Transactions Per Second (TPS) Meaning," Ledger. Accessed: Jan. 15, 2024. [Online]. Available: https://www.ledger.com/

academy/glossary/transactions-per-second-tps

[19] F. D'Amato and L. Zanolini, "A Simple Single Slot Finality Protocol For Ethereum." 2023. Accessed: Jan. 12, 2024. [Online]. Available: https://eprint.iacr.org/2023/280

[20] Supra Oracles, "Transactions Per Second (TPS): The Complete Guide," https://supraoracles.com/. Accessed: Jan. 05, 2024. [Online]. Available: https://supraoracles.com/academy/transactions-per-second/

[21] Corey Barchat, "What is the Ethereum Merge? ETH 2.0 explained," MoonPay. Accessed: Jan. 05, 2024. [Online]. Available: https://www.moonpay.com/learn/cryptocurrency/ethereum-merge-eth-2

[22] C. Research, "The Time to Finality for Solana," Crypto Research Report. Accessed: Jan. 12, 2024. [Online]. Available: https://cryptoresearch.report/crypto-research/the-time-to-finality-for-solana/

[23] P. Pontem, "A detailed guide to blockchain speed | TPS vs.," Medium. Accessed: Jan. 04, 2024. [Online]. Available: https://pontem.medium.com/a-detailed-guide-to-blockchain-speed-tps-vs-80c1d52402d0

[24] B. Liu, "Avalanche gets the 'Ordinals' bump, sets new transaction record," Blockworks. Accessed: Jan. 04, 2024. [Online]. Available: https://blockworks.co/news/avalanche-ordinals-asc20-transaction-record

[25] N. Labs, "The Magic of ShimmerEVM: Redefining Web3's Potential," Medium. Accessed: Jan. 04, 2024. [Online]. Available: https://medium.com/@NakamaLabs/the-magic-of-shimmerevm-redefining-web3s-potential-b0c0be3149c4

[26] B. Akolkar, "IOTA's ShimmerEVM Resilience Tested Again: Defending Against 700 TPS Spam Attack," Crypto News Flash. Accessed: Jan. 04, 2024. [Online]. Available: https://www.crypto-news-flash.com/iotas-shimmerevm-resilience-tested-again-defending-against-700-tps-spam-attack/

[27] M. Soud, S. Helgason, G. Hjálmtýsson, and M. Hamdaqa, "TrustVote: On Elections We Trust with Distributed Ledgers and Smart Contracts," in *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, Sep. 2020, pp. 176–183. doi: 10.1109/BRAINS49436.2020.9223306.

[28] S. Danwar, J. Mahar, and A. Kiran, "A Framework for e-Voting System Based on Blockchain and Distributed Ledger Technologies," *Comput. Mater. Contin.*, vol. 72, no. 1, pp. 417–440, 2022, doi: 10.32604/cmc.2022.023846.

[29] W. F. Silvano and R. Marcelino, "Iota Tangle: A cryptocurrency to communicate Internet-of-Things data," *Future Gener. Comput. Syst.*, vol. 112, pp. 307–319, Nov. 2020, doi: 10.1016/j.future.2020.05.047.

[30] N. Sealey, A. Aijaz, and B. Holden, "IOTA Tangle 2.0: Toward a Scalable, Decentralized, Smart, and Autonomous IoT Ecosystem." arXiv, Sep. 11, 2022. Accessed: Jan. 03, 2024. [Online]. Available: http://arxiv.org/abs/2209.04959

[31] B. Wang, Q. Wang, S. Chen, and Y. Xiang, "Security Analysis on Tangle-based Blockchain through Simulation." arXiv, Aug. 11, 2020. doi: 10.48550/arXiv.2008.04863.

[32] N. Živi, E. Kadušić, and K. Kadušić, "Directed Acyclic Graph as Tangle: an IoT Alternative to Blockchains," in *2019 27th Telecommunications Forum (TELFOR)*, Nov. 2019, pp. 1–3. doi: 10.1109/TELFOR48224.2019.8971190.

[33] M. Ashouri, "Directed Acyclic Graph (DAG) vs Blockchain," Medium. Accessed: Jan. 04, 2024. [Online]. Available: https://ashourics.medium.com/directed-acyclic-graph-dag-vs-blockchain-b16a85a95c30