2024 International Conference on Next Generation Computing Applications (NextComp) | 979-8-3315-1740-3/24/$31.00 ©2024 IEEE | DOI: 10.1109/NextComp63004.2024.10779646

Mauvote: A Novel Mobile Electronic Voting System Using Blockchain

Junaid Bin Asad Edoo
Dayforce Mauritius, Icon Ebene,
Ebene, Mauritius
junaid.edoo@dayforce.com

Roopesh Kevin Sungkur
Department of Software and Information Systems
University of Mauritius
Reduit, Mauritius
r.sungkur@uom.ac.mu

Jorge Marx Gómez
Department of Business Information Systems
Carl von Ossietzky University of Oldenburg
Oldenburg, Germany
jorge.marx.gomez@uni-oldenburg.de

Hauke Precht
Department of Business Information Systems
Carl von Ossietzky University of Oldenburg
Oldenburg, Germany
hauke.precht@uol.de

Skady Rudolph
Department of Business Information Systems
Carl von Ossietzky University of Oldenburg
Oldenburg, Germany
skady.rudolph@uol.de

***Abstract*—Being able to vote is seen as a key democratic right in many countries. Traditional means and ways of voting include the paper-based means, followed by counting. With this approach, registration procedures are sometimes difficult and the voters are expected to be physically present in the voting centers. This at times can be factors that discourage voters to vote. Electronic voting is also common but the latter can be subject many security threats, including tampering with the voting data and tampering with electronic voting systems. To overcome the issues described above, this research proposes MauVote, a novel blockchain-based voting system. The decentralized nature of blockchain eventually ensures that all transactions are immutable and recorded transparently. This greatly helps to reduce the threats of unauthorized access and alteration of data. The proposed system also makes use of OTP-based recovery and biometric authentication through a mobile app, contributing to the security of the voting process**

Keywords— Blockchain, Voting Systems, Microservices, Non-Fungible Tokens, OTP

I. INTRODUCTION

The voting process in any democracy can be a tedious process. Traditionally a paper-based approach has been used and is still being used in a number of countries. Through an electronic voting system, the process of generating election results is also much faster where there is no need to manually count the votes. Furthermore, electronic voting systems can provide consolidated data through the use of charts and graphs, which can help anyone quickly interpret the data of the voting process obtained. The electronic voting system has gained some momentum but there are always concerns of threats that would make the voting process void. Traditional electronic voting system have faced criticism due to concerns regarding security, privacy, and transparency [1]. Currently, there is a growing demand for a more secure, transparent, and tamper-proof voting system [2]. Blockchain-based voting systems can be seen as a possible solution to address the inherent limitations of traditional electronic voting systems. This research makes a thorough investigation on possible blockchain technologies that can be used for the development of a blockchain-based electronic voting system. Thereafter, a proof-of-concept is proposed to demonstrate the features and functionalities of the proposed system which has been named MauVote. The proof-of-concept is based on the distributed ledger architecture which promotes a decentralised architecture which is maintained by multiple users. So, there is a mechanism that ensures that there is collective verification of ledgers before they are shared. This functions by coming to a consensus among the participants by following possibly globally accepted rules or procedures.

II. LITERATURE REVIEW

A. Smart Contracts

Smart contracts are self-executing agreements in which the terms of the buyer-seller agreement are directly put into lines of code. When the contract's criteria is met, the code executes automatically and the terms of the agreement are honoured ([3]; [4]; [5]). Smart contracts is effectively built on top of the

979-8-3315-1740-3/24/$31.00 ©2024 IEEE

blockchain, and each contract statement's execution is recorded as an immutable transaction saved in the blockchain [6]. Smart contracts guarantee appropriate access control and access permission as developers can assign permission for a specific address to have access to the contract function. For example Person A and Person B agree on a penalty fee for breaching the contract. If one of them violates the contract the corresponding fee will be paid to the other party as specified in the contract [7].

The life cycle of smart contracts is divided into four stages and is shown in Figure 1 below.

a) Smart contract creation

The contract conditions, such as obligations and penalties, will be discussed by the parties concerned. Software engineers will subsequently transform this natural language agreement into logic-based rules in a programming language.

b) Smart contract deployment

After the smart contracts have been confirmed, they are deployed onto the blockchain. Due to the immutability inherent in blockchain technology, these contracts are immune to any alteration or tampering.

c) Execution of smart contracts.

When smart contracts are deployed, the contractual clause are continuously monitored and evaluated. When a specific contractual condition is met, the predetermined contractual procedures are automatically executed. As an illustration, if a certain amount of money is not transferred by the end of each month, the penalty fee will be deducted from the user's wallet as stipulated in the contract.

d) Completion of smart contracts.

When a smart contract is carried out, all parties involved have their information updated and any transactions or changes to their digital assets are recorded on the blockchain.

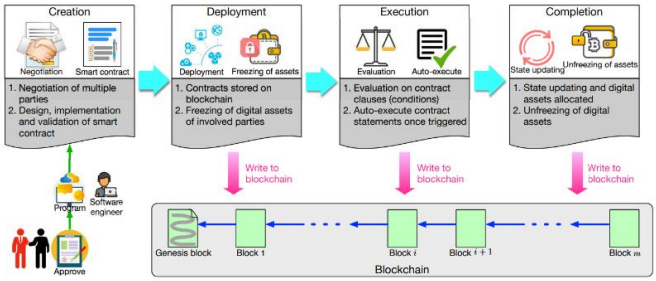

Fig. 1. A life cycle of a smart contract [6]

B. *Existing Systems*

Open for Vote

The Open Vote Network [8] was developed as a smart contract on the Ethereum blockchain and presented a novel solution for conducting boardroom elections. Its unique approach to tally computation and voter privacy protection are the strengths of Open for Vote. The latter introduces a self-tallying protocol that empowers individual voters with full control over the privacy of their votes. Each voter has the ability to ensure the confidentiality of their vote and this eliminates the need for trust in any centralized authority. The system achieves this by employing cryptographic techniques that prevent unauthorized access to sensitive voter information. An individual's vote remains private unless there is a coordinated effort involving all other voters to compromise the privacy of that specific vote. Open Vote Network provides a robust and transparent solution for boardroom elections. It ensures the integrity of the voting process and preserves the privacy rights of individual voters [8].

E-Voting Portal Using Blockchain

[9] presents an e-voting system based on Ethereum that uses blockchain technology to alleviate the limitations of centralized voting systems. To securely record voter accounts, candidate information, and votes, the system use the Ethereum blockchain and smart contracts are employed to facilitate the voting process. This is shown in Figure 2 below.

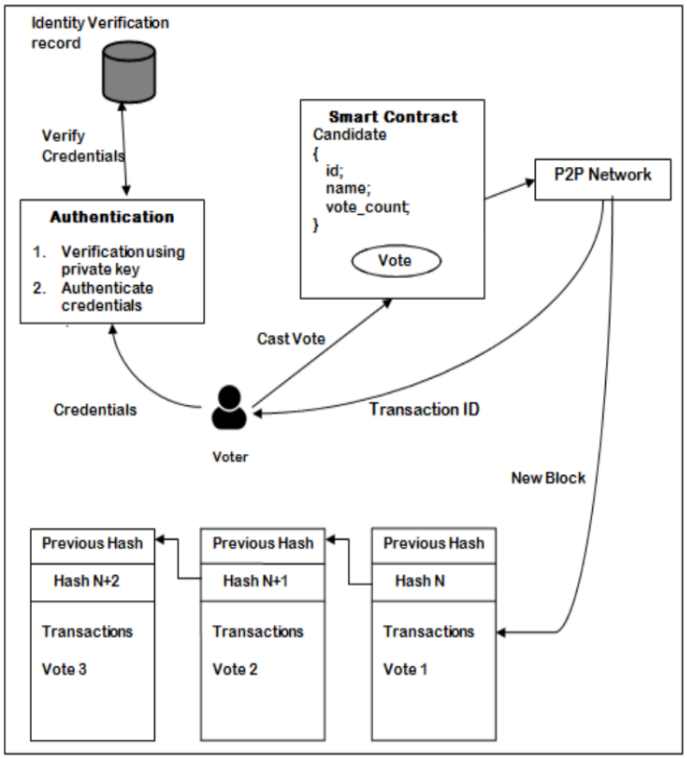

Fig. 2. Voting process [9]

The registration process for voters and candidates in the blockchain-based e-voting system requires prior completion, including identity verification [10]. Authorized individuals are responsible for verifying the identities of eligible users and providing them with a unique coin or token. Because the blockchain's verification method prevents double spending, each user can only vote once with this coin or token [11]. The e-voting system is decentralized and there is no single authority overseeing the elections. This allows a more transparent and trustless voting process [12].

C. Critical Appraisal of existing Systems.

Table I below shows a detailed analysis of the similar systems along with the different features that are associated with them.

TABLE 1. COMPARISON OF EXISTING SYSTEMS

	Open for vote	E-Voting Portal Using Blockchain	Securing e-voting
User Friendliness	No	No	No
Require Wallet	Yes	Yes	Yes
Biometric authentication	No	No	No
Anonymity	Yes	No	No
Require voter to pay	Yes	Yes	Yes
Live vote count	No	Yes	Yes
Number of voters	50	No limit	No limit
Can vote multiple candidate	Yes	No	Yes
Candidate Upload image	No	No	No
Forget password	No	No	No

After analyzing the detailed table comparing similar systems and their associated features, several key observations can be made:

1. User Friendliness: None of the examined systems prioritize user friendliness.
2. Wallet Requirement: All systems require users to have a digital wallet.
3. Biometric Authentication: Only one of the systems utilize biometric authentication.
4. Anonymity: Only one system provides anonymity to voters.
5. Payment Requirement: All systems require voters to make payments.
6. Live Vote Count: Two systems support live vote counting.
7. Number of Voters: One system has a limit of 50 voters, while others have no specified limit.
8. Multiple Candidate Voting: Only one system allows voters to choose multiple candidates.
9. Candidate Upload Image: None of the systems support candidate image uploads.
10. Forget Password Functionality: None of the systems offer a forget password feature.

Considering these observations, this project can aim to improve user experience, security, anonymity, accessibility, and the overall integrity of the electoral process.

III. PROPOSED SOLUTION

A. Features of Proposed System and System Architecture

The proposed solution encompasses a blockchain-based e-voting system that addresses the shortcomings of conventional voting methods and existing systems as discussed initially. The system incorporates several key features to ensure secure and transparent electoral processes. A system architecture diagram of the proposed system is shown in Figure 4 below.

User Registration: Prospective voters are required to register in the system by providing their National Identity Card (NIC) number and a password. The registration details are securely transmitted to a dedicated Node.js server. This server possesses an associated account and facilitates interaction with a smart contract. A cryptographic hash function is applied to the NIC number and password to generate a unique Non-Fungible Token (NFT) representing the user's identity within the system.

Party, Constituency, and Candidate Registration: The system facilitate the registration of political parties, constituencies, and candidates, establishing a comprehensive and organized framework for the electoral process. This feature ensures accurate representation and management of political entities involved in the voting procedure.

Login Authentication: Users authenticates themselves by providing their NIC number and password. Subsequently, a hash of the provided information is regenerated and compared against the stored NFT within the system. Successful validation of the NFT ownership grants users access to the system, enabling them to exercise their voting rights securely.

Voting Process: Each vote transaction require the authentication token (hash) and a list of eligible candidates. Once all vote transactions reach the Smart Contract, the system verifies the authenticity of the NFT. This validation step ensures that each user can only cast one vote. Upon successful verification, the NFT is subsequently invalidated (burned) to prevent multiple voting instances.

User-Friendly Web Application: The e-voting system is developed as a responsive and user-friendly web application to cater for a wide range of screen sizes and devices. Angular as the frontend framework provides a seamless and dynamic user interface that adapts its layout and content to ensure optimal viewing experiences. Transactions are streamlined through a Node.js server, eliminating the need for additional tools like MetaMask accounts or browser extensions.

Additional Features: The proposed system incorporate supplementary functionalities to enhance the user experience and security. A "Forget Password" section enables users to recover their accounts by receiving a One-Time Password (OTP) on their registered phone numbers. By integrating these comprehensive features, the blockchain-based e-voting system aims to provide heightened security, user-friendliness, and accessibility, fostering fair and transparent electoral processes.

B. *Stakeholder Interactions*

Figure 3 below shows the interaction between the different stakeholders and the system.

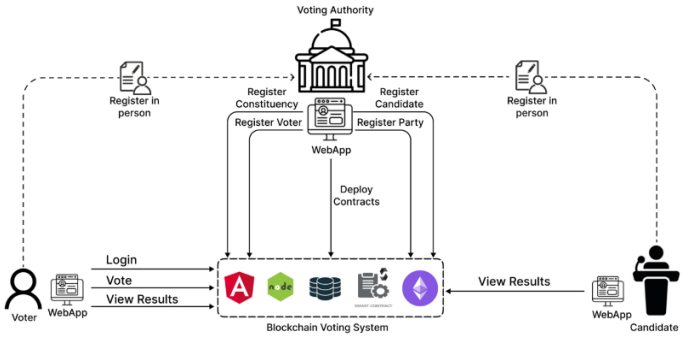

Fig. 3. Stakeholder Interactions

C. *Distributed Microservices Setup with Docker Swarm and Nginx Load Balancers*

The microservices architecture described in Figure 6 showcases a highly resilient and scalable system design, leveraging fault tolerance and high availability principles. By utilizing Docker Swarm and load balancers, the architecture ensures continuous operation even in the face of failures or disruptions. Fault tolerance is achieved through the redundancy of components. Multiple manager nodes within Docker Swarm enable fault-tolerant management and coordination of the microservices. Replicated Nginx load balancers ensure that even if a replica becomes unavailable, the system can seamlessly distribute incoming requests across healthy replicas, preventing single points of failure. It exemplifies the utilization of Docker Swarm and load balancing techniques to deliver a resilient, responsive, and scalable platform for the applications and services involved.

D. *Voting Process*

There are a number of processes that have not been shown for the sake of simplicity but one of the most important processes is the voting process and this is shown in Figure 5 below.

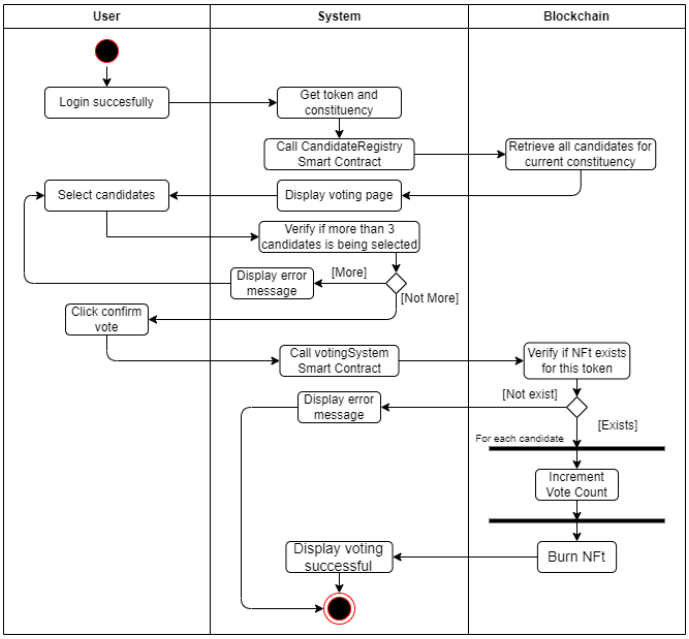

Fig. 5. Voting Process

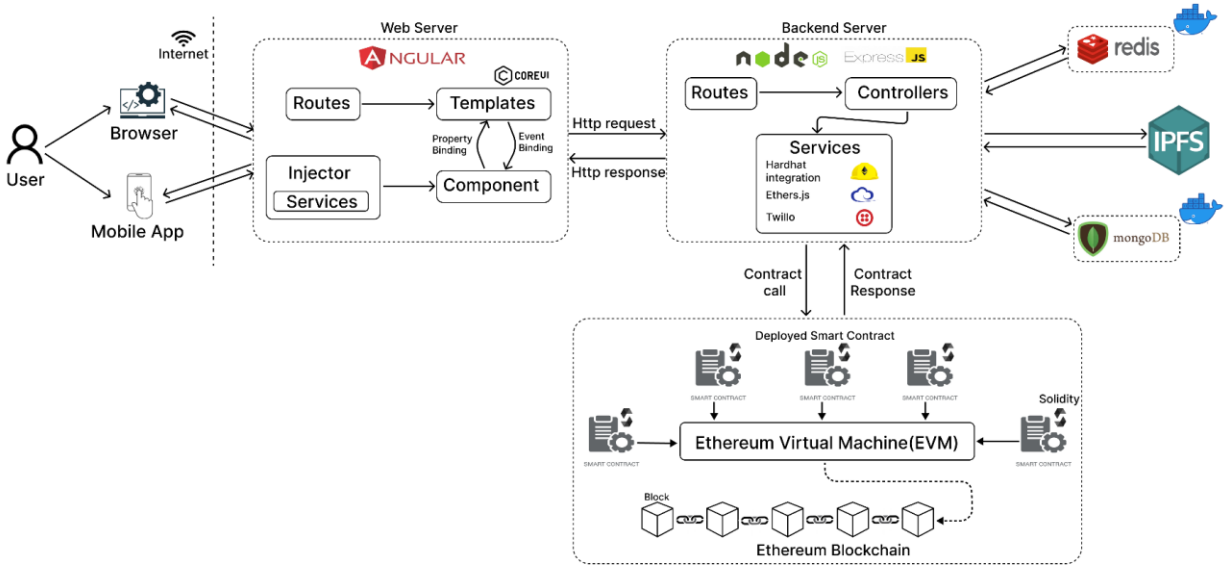

Fig. 4. System Architecture of Proposed System

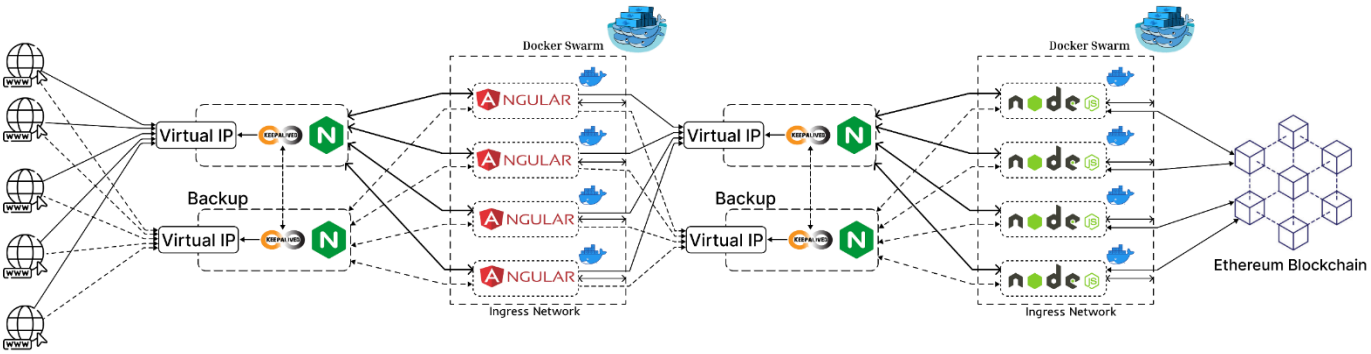

Fig. 6.Distributed Microservices Setup with Docker Swarm & Load Balancers

IV. IMPLEMENTATION

This section provides an overview of the implementation of the different modules within the system. It includes discussions on the development environment, tools utilized, and specific examples of the user interface for the web application.

A. Development Environment

The software components used to implement the system is shown in table II below.

TABLE II. SOFTWARE COMPONENTS

Component	Description	Version
Integrated Development Environment (IDE)	IntelliJ, Vs Code	1.80.1
Programming Language	Solidity.javascript, TypeScript	0.8.8
Web Framework	Angular	14.2.1
Web Template	CoreUi	4.2.6
Blockchain	Ethereum	2
Containerisation	Docker	20.10.24
Container Orchestrator	Docker Swarm	0.1.0-beta.2
Blockchain Framework	Hardhat	6.1.2
Messaging Services	Twillo	4.13.0
Database	Mongo DB	6.0
Load Balancer	Nginx	*1.23.4*
One Time Password Generation	speakeasy	2.0.0
Routing Software for high availability	Keepalived	2.1.5
Scheduler	Node cron	3.0.2
Smart Contract Deployment	Hardhat	6.1.2
Web Server	Nginx	1.23.4
Mobile Development Framework	Flutter	3.7.0
Image storage	Moralis	2.18.1

B. User Interface for Voting

The system consists of a number of interfaces for registration and other processes and Figure 7 below shows the interface for voting.

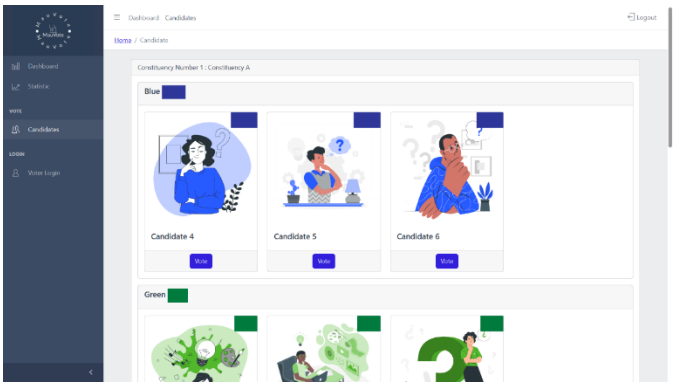

Fig. 7. Voting Interface

This section describes some of the interesting features of the proposed system.

C. Dashboard and Statistics

For the dashboard each constituency has a card which contains all the candidates sorted in number of votes. The statistics page is created using several different endpoints that feeds data into the charts. This is shown in Figure 8 below.

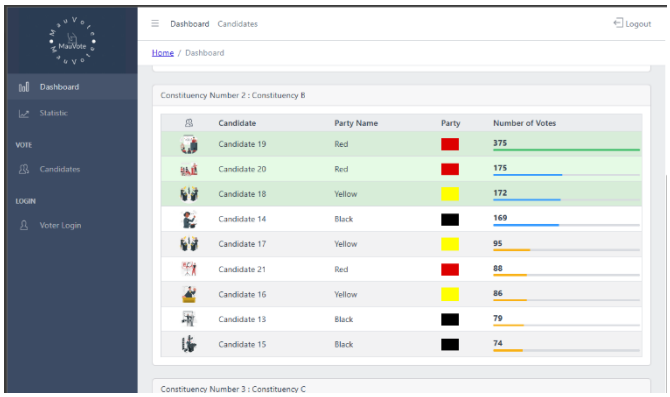

Fig. 8. Dashboard Page

The charts are created using chartJS module. The line chart data is made using a scheduler that store the time stamp and the current number of votes per party inside a mongo DB collection.

D. Device Registration

When registering a voter. If the user wishes to use the mobile app for biometric authentication a checkbox will be set to true and subsequently a one-time password will be sent to the user. The user then enters this OTP in his app to register his device. After entering the OTP. The app will open a WebView of the system where it will register the device.

E. Biometric Authentication

When the user clicks on the Login and vote card the device local biometric authentication is called. Only after being authenticated is the user given access to the device token. This device token is then verified in the backend and used to login the voter similar to the forget password functionality. After the user is logged in successfully a web view of the system is shown to the user. The system is responsive to various screen sizes. This is shown in Figure 9 below.

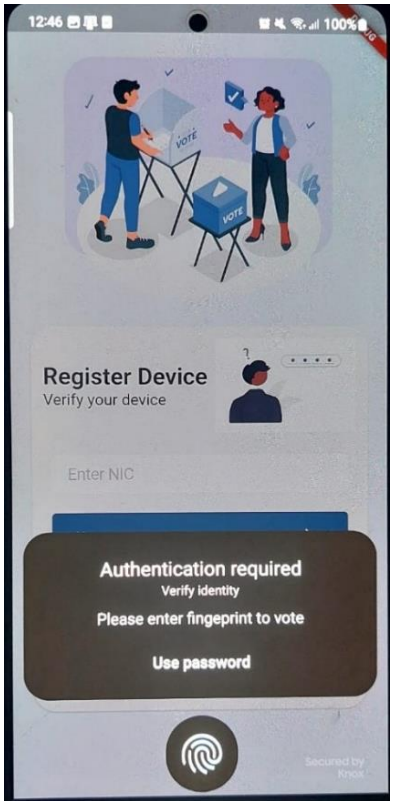

Fig. 9. Biometric Prompt

V. CONCLUSION

The proposed system displays several strengths that add to its novelty and effectiveness. The use of blockchain technology guarantees the integrity and immutability of voting transactions whilst NFTs provide secure and tamper-proof authentication. The web-based system implemented in Angular and Node.js, offers a user-friendly interface. The centralized transactions carried out by the Node.js server enhance user convenience and eliminate transaction fees. The proposed system was evaluated using different metrics and the results obtained were very promising. The system provides enhanced security, transparency, and tamper-proofing capabilities to ensure the integrity of the election process. It enhances the integrity of the voting process, provides a user-friendly experience and addresses the limitations of traditional voting systems.

REFERENCES

[1] S. Tanwar, N. Gupta, P. Kumar, et al. (2024). Implementation of blockchain-based e-voting system. Multimed Tools Appl 83, 1449–1480. https://doi.org/10.1007/s11042-023-15401-1

[2] M. Vladucu, Z. Dong, J. Medina and R. Rojas-Cessa, (2023). E-Voting Meets Blockchain: A Survey, in IEEE Access, vol. 11, pp. 23293-23308, doi: 10.1109/ACCESS.2023.3253682.

[3] Z. Zheng, S. Xie, H. Dai, W. Chen, X. Chen, J. Weng and M. Imran (2020) 'An overview on smart contracts: Challenges, advances and platforms', *Future Generation Computer Systems*, 105, pp. 475–491. Available at: https://doi.org/10.1016/j.future.2019.12.019.

[4] V. Chukowry, G. Nanuck, and R. K. Sungkur (2021). The future of continuous learning–Digital badge and microcredential system using blockchain, Global Transitions Proceedings, Volume 2, Issue 2, Pages 355-361, ISSN 2666-285X, https://doi.org/10.1016/j.gltp.2021.08.026.

[5] H.A.M. Deenmahomed, M.M. Didier and R.K.Sungkur (2021). The future of university education: Examination, transcript, and certificate system using blockchain. Comput Appl Eng Educ ; 1– 23. https://doi.org/10.1002/cae.22381

[6] Z. Zheng, S. Xie, H. Dai, W. Chen, X. Chen, J. Weng and M. Imran (2020) 'An overview on smart contracts: Challenges, advances and platforms', Future Generation Computer Systems, 105, pp. 475–491.

[7] D.P. Oyinloye, J.S. Teh, N. Jamil and M. Alawida (2021) 'Blockchain Consensus: An Overview of Alternative Protocols', Symmetry, 13(8), p. 1363. Available at: https://doi.org/10.3390/sym13081363.

[8] P. McCorry, S.F. Shahandashti and F. Hao (2017) 'A Smart Contract for Boardroom Voting with Maximum Voter Privacy', in A. Kiayias (ed.) *Financial Cryptography and Data Security*. Cham: Springer International Publishing (Lecture Notes in Computer Science), pp. 357–375. Available at: https://doi.org/10.1007/978-3-319-70972-7_20.

[9] K. Patidar and S. Jain (2019) 'Decentralized E-Voting Portal Using Blockchain', in 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT). 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India: IEEE, pp. 1–4. Available at: https://doi.org/10.1109/ICCCNT45670.2019.8944820.

[10] B. Lashkari and P. Musilek (2021) 'A Comprehensive Review of Blockchain Consensus Mechanisms', IEEE Access, 9, pp. 43620–43652. Available at: https://doi.org/10.1109/ACCESS.2021.3065880.

[11] A.A. Monrat, O. Schelén, and K. Andersson (2019) 'A survey of blockchain from the perspectives of applications, challenges, and opportunities', *IEEE Access*, 7, pp. 117134–117151.

[12] Q. Wang, R. Li, Q. Wang, and S. Chen (2021) 'Non-fungible token (NFT): Overview, evaluation, opportunities and challenges', *arXiv preprint arXiv:2105.07447* [Preprint].