Uluslararası İleri Doğa Bilimleri ve Mühendislik Araştırmaları Dergisi
Sayı 7, S. 134-138, 9, 2023

Araştırma Makalesi

IJANSER
https://as-proceeding.com/index.php/ijanser
ISSN: 2980-0811

International Journal of Advanced Natural Sciences and Engineering Researches
Volume 7, pp. 134-138, 9, 2023

Research Article

A Transparent and Immutable Voting System Utilizing Blockchain

Jian-Him Sam[*a], Ming-Lee Gan [*b]

[*]*Department of Computer and Communication Technology, Faculty of Information and Communication Technology, Universiti Tunku Abdul Rahman Kampar Campus, 31900 Kampar Perak, Malaysia*

[a]*jianhim01@1utar.my*, [b]*ganml@utar.edu.my*

(Received: 23 September 2023, Accepted: 06 October 2023)

(3rd International Conference on Innovative Academic Studies ICIAS 2023, September 26-28, 2023)

ATIF/REFERENCE: Sam, J. H. & Gan, M. L. (2023). A Transparent and Immutable Voting System Utilizing Blockchain. *International Journal of Advanced Natural Sciences and Engineering Researches*, 7(9), 134-138.

Abstract – Democracy has been a major part of many of the current nation's political landscape for many years, it is a form of government and authority selection where power is held by the people of the nation as they would be able to participate in the decision-making process and have a say in the policies and laws that may affect them in terms of the nation's growth and development. However, many countries in the world are still using traditional voting method which is inefficient and inconsistent as there had been major controversies surrounding the usage of the system that it may introduce various exploitation from political parties to increase their chances of winning the election, which would lower the confidence of voters considerably as they may think that their vote is insignificant and would not bring any changes to the overall results. Thus, this paper would like to develop a 3-tier architecture blockchain based electoral system under the local blockchain of Ganache, integrated with front-end interfaces which allows the voters to vote while ensuring their anonymity in the process. The system would introduce verification feature whereby voters could verify their own selection of candidate to ensure scrutiny of the system, without worrying that their selection of votes would be traced back to them.

Keywords – Blockchain, Anonymity, Voting, Verification, 3-tier Architecture, Ganache.

I. INTRODUCTION

Voting has evolved significantly over the past 30 years, transitioning from traditional voting which involved paper to electronic voting and now implementing blockchain onto electronic voting. However, e-voting itself had raised numerous controversies in terms of its effectiveness and security. It has been proven time and time again that e-voting brings lots of security vulnerabilities causing the system to be exploited by malicious actor and ultimately affecting the system's accurateness and trustworthiness [1,2].

Blockchain had emerged and applied in various sectors such as supply chain tracking, NFTs, cryptocurrency transaction etc. The main reasons for using blockchain is because it is decentralized, immutable and its role as a distributed ledger [3]. Decentralization of blockchain allows each user inside the blockchain network to have a copy of the same exact distributed ledger that contain information without the integration of central authority, in this case is the votes casted by voters [4]. Smart contract is another element present in blockchain that runs when predefined conditions are met. It can be related as a digital contract, where when a certain conditions in the contract are met, some actions will be run in the blockchain. Smart contracts abolished the need of middleman to help facilitate the contract as it is composed of programming codes and is self-enforcing, it is

transparent and secure as the contract is immutable and distributed to everyone in the network for validation [5].

By integrating both blockchain technology and e-voting, we can establish a robust foundation for a voting system in which voting records are transparent to everyone while ensuring the anonymity of voters are protected. Not only that, but the security issues regarding the system would also definitely lower by a huge margin when compared to traditional e-voting system as malicious actor would have to target the whole blockchain network and any tampering data would be detected instantly. Lastly by implementing smart contract in blockchain, we can ensure that the procedure of voting is accurate, and verification of votes is achieved without manipulation from third parties.

II. MATERIALS AND METHOD

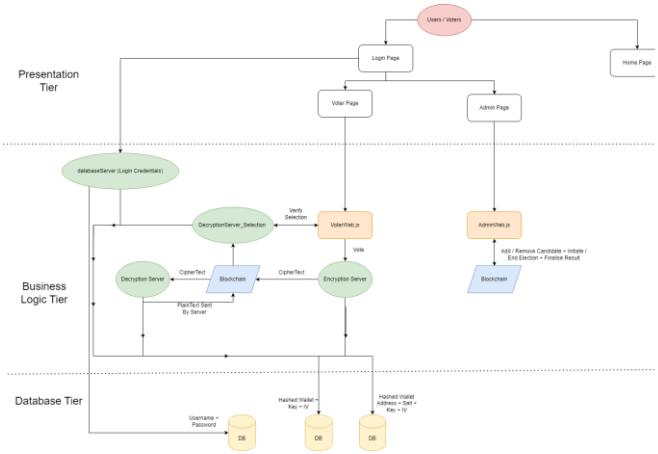

Fig. 1 System Design Diagram

The system's design utilizes the concept of three-tier architecture framework consisting of presentation, business logic, and database tier. The overall flow of the system starts when voter proceeds to the login page and enters their credentials which would then be used to match the existing credentials from the database to authenticate the voters from using the system. If the user is a valid voter, the voter would be redirected to their own respective voting page where they could cast their vote and verify their selection.

When a voter had casted their vote for a respective candidate in the election, the name of the candidate would be encrypted twice using asymmetric encryption within the encryption server, the ciphertext of the candidate's name would then be sent to the blockchain corresponding to the voter's wallet address. At the same time, two sets of the encryption keys would be stored inside two databases along with the voter's wallet address that will be hashed with salt.

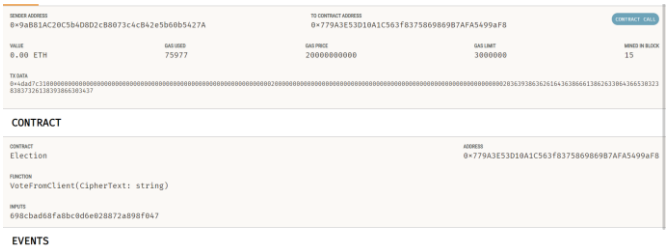

Fig. 2 Transaction of Voter sending candidate (Ciphertext) to Blockchain

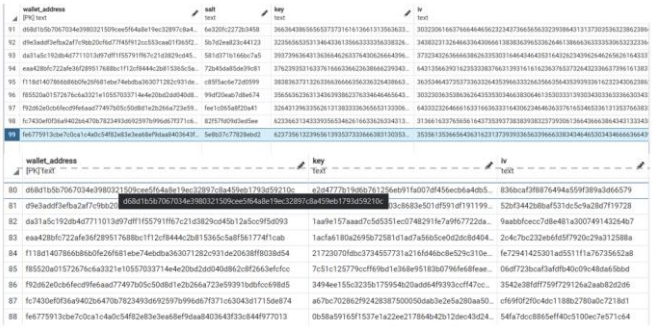

Fig. 3 Encryption Keys in Databases

Decryption Server would have a listener function that intercepts and retrieve the recently appended ciphertext in the blockchain for decryption. After the ciphertext had been decrypted into plaintext by the server, it is once again sent back to the blockchain in the name of the server's wallet address instead of the voter's wallet address. Since the name of the candidate is now in plaintext form, there will be a function inside the blockchain that would match the name of the candidate and increase the overall vote count for that respective candidate by 1. By utilizing the servers for encryption and decryption, the system can protect the anonymity of the voters as the public would not be able to gain any meaningful information from viewing the transaction that corresponds to the voter's wallet address as the input by the voter had been encrypted by the system.

Fig. 4 Transaction of Server sending candidate (Plaintext) to Blockchain

After voting, voter could verify their own selection of candidate as the system would take the ciphertext from the correspond voter's wallet address and send it for decryption in the server and display the plaintext back to the voter inside the voting web page.

The system would also include three administrative tasks for the system, in which one of them is the adding and removing of candidates in the election. Additionally, the initialization and ending of the election session would be another administrative task of the system as voters could only start to login to the voting and vote for their respective candidate only after the election period is initiated by the admin. Finally, the finalization of the election would conclude the election and come out with a winner, on the prerequisite where the election period must be ended before the election could be finalized.

III. RESULTS

a. Voters

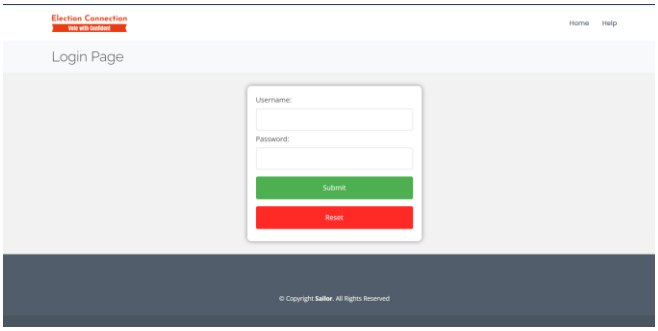

Fig. 5 Login Page

In the perspective of the user of the system, voters would first need to authenticate themselves as eligible voters of the election by inputting their credentials into the login page, in which the credentials inputted would be authenticated by a server.

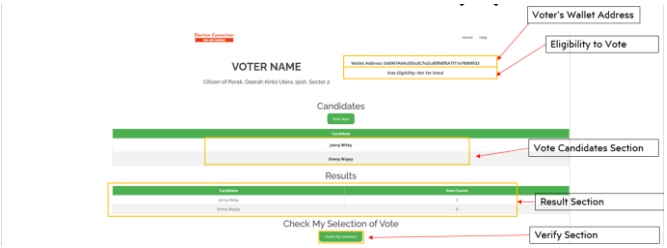

Fig. 6 Login Page

After logging into their own respective voter page, the voter would be able to check and verify their own wallet address and the state that they are voting for, as well as their eligibility of voting in the election. Besides from those, voter could also check the current result of the ongoing election, including which candidate is currently leading in the election.

Voter would be able to vote for their own respective candidate in the "Vote Candidate Section" by clicking on their name as shown in Figure 3. The name of the candidate would then be encrypted and sent to blockchain which would then be decrypted by another server and append it back to blockchain which would increase the vote count of the chosen candidate. If the voter would like to verify their own selection of candidate, they can do so by clicking the verify button located at the bottom of the page which in turn would decrypt the ciphertext and display it into the web page.

b. Admin

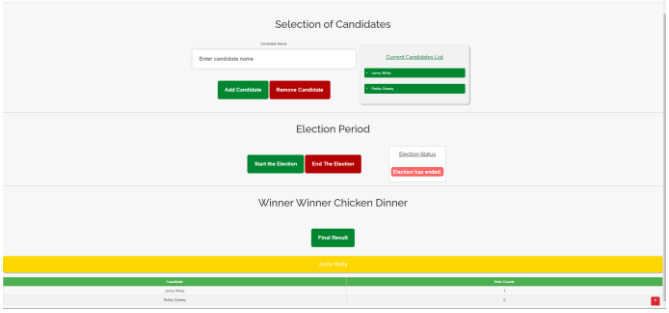

Fig. 7 Admin Page

In the perspective of the admin of the system, as mentioned earlier, there are three main administrative tasks that can be performed. One of them is the adding and removing candidate for the election, whereby admin can add or remove candidate by typing their name inside the text box. Additionally, there will be a candidate list that shows the existing candidate in the election to avoid any confusion.

Furthermore, admin could also initiate and end the election period with the click of a button and

the section would include a status bar to indicate the existing status of the election.

Lastly, the admin could finalize the election and come out with a winner a table displaying the existing candidate and their corresponding vote counts.

IV. DISCUSSION

There exist many different ideas and modifications in the development of a secure e-voting system utilizing blockchain. Some of the system had utilized other encryption methods such zero knowledge succinct non interactive arguments of knowledge (zkSnarks). In such systems, voters are able to authenticate themselves and perform voting without revealing their wallet address as they would be given a secret phrase as a proof of knowledge during the registration stage, which would be used to authenticate the voter during the voting session without needing any additional information such as their wallet addresses [6,7]. Such method does not require servers as per our current system as the cryptographic method is implemented inside the smart contracts corresponding to the voters, making it much safer as it eliminates point of failure of having servers and would improve performance of the system as the method does not require back and forth communication and had proven to be fast and lightweight cryptographic method.

[8] proposes a new authentication method for the voters to authenticate themselves as eligible voter by utilising biometric fingerprint and iris authentication, whereby voter would need to match their fingerprint or iris through a device to check their eligibility to vote and could eliminate any repetition of voting from a particular voter. However, such system may fail to recognize the voter's biometrics if there is any changes or injury toward their thumb. Furthermore, breaches onto the biometric database server would be devastating as voters cannot change their identification trait as they can change their passwords [9].

Another electoral system utilized permissioned blockchain (private blockchain) under the platform of Go-Ethereum and employing the consensus algorithm of Proof of Authority [10]. The system would have district node that verify the votes and append it to the blockchain, the other node is Bootnode which act as discovery and coordination service that helps the district nodes to communicate with each other. During the election session, voters can vote for their candidate after authenticating themselves. After voting, each voter would get their own transaction ID that could be paste into a blockchain explorer and verify the selection of candidate. The transaction in the permissioned blockchain works in a way that every transaction would not include the sender address, which mask the voter's wallet address and ensure the anonymity of the voter.

V. CONCLUSION

In the transitioning toward the era of Industry Revolution 5.0, blockchain has been a emerging technology that offers multitude of benefits, including transparency, security, verifiability and accessibility in the voting process. By harnessing the features that blockchain brings, elections could be revolutionized to become more resistant to fraud and manipulation, while maintaining the integrity of the democratic process. However, it is important to acknowledge that the implementation of electoral blockchain system requires meticulous planning onto factors that might affect the overall system such as the blockchain network, consensus algorithm, scalability and security. While challenges remain, the potential benefits make it a convincing opportunity for the evolution of electoral system in the digital age.

ACKNOWLEDGMENT

This project is developed and guided by Dr Ming Lee Gan, who has given me this bright opportunity to engage in the development of blockchain electoral system as your guidance and advice has been instrumental on understanding the complexities of blockchain technology which had sparks ideas and solutions when developing the electoral system. The authors would also like to express gratitude to the Universiti Tunku Abdul Rahman for the necessary resources and knowledge that have been provided.

REFERENCES

[1] W. M. Grossman. "Why machines are bad at counting votes." The Guardian. https://www.theguardian.com/technology/2009/apr/30/e

-voting-electronic-polling-systems (accessed April. 30, 2009).
[2] M. Safi and G. Chan. “NSW election result could be challenged over iVote security flaw.” The Guardian. https://www.theguardian.com/australia-news/2015/mar/23/nsw-election-result-could-be-challenged-over-ivote-security-flaw (accessed March. 23, 2015).
[3] M. Safi and G. Chan. “NSW election result could be challenged over iVote security flaw.” The Guardian. https://www.theguardian.com/australia-news/2015/mar/23/nsw-election-result-could-be-challenged-over-ivote-security-flaw (accessed March. 23, 2015).
[4] R. Tas and O. O. Tariover., “A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting.” in Symmetry, Aug. 2020. [Online]. Available: https://www.mdpi.com/2073-8994/12/8/1328
[5] IBM. “What are smart contracts on blockchain?” IBM. https://www.ibm.com/topics/smart-contracts (accessed n.d).
[6] A. Fatrah et al., “Transparent Blockchain-Based Voting System: Guide to Massive Deployments” in Proceedings of the International Conference on Advanced Intelligent Systems and Informatics 2020, S. Cham, 2020, pp. 237-246. [Online]. Available: https://www.researchgate.net/publication/344440372_Transparent_Blockchain-Based_Voting_System_Guide_to_Massive_Deployments
[7] M.H. Murtaza, Z. A. Alizai, and Z. Iqbal, “Blockchain-Based Anonymous Voting System Using zkSNARKs,” National University of Sciences and Technology (NUST), Islamabad, Pakistan, 2019. Available: https://ieeexplore.ieee.org/document/8853836
[8] J. A. Samsul and M. B. Limkar, “A biometric-secure cloud-based e-voting system for election processes,” International Journal of Electrical and Electronics Engineering Research (IJEEER), 2014.
[9] V. N. S. R. Aswin, P. G. Vijay, T. R. S., and D. Dath, "EVO: An E-Voting System using Blockchain," in 2021 5th International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, Jan. 2021. [Online]. Available: https://www.ijert.org/research/evo-an-e-voting-system-using-blockchain-IJERTCONV9IS13036.pdf
[10] G. Hjalmtysson. (July. 2018). Blockchain-Based E-Voting System. Presented at IEEE 11th International Conference on Cloud Computing. [Online]. Available: https://www.researchgate.net/publication/327812253_Blockchain-Based_E-Voting_System.