Uluslararası İleri Doğa Bilimleri ve Mühendislik Araştırmaları Dergisi Sayı 7, S. 134-138, 9, 2023 © Telif hakkı IJANSER'e aittir **Araştırma Makalesi**



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 Copyright © 2023 IJANSER **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

^ajianhim01@1utar.my, ^bganml@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 exact distributed ledger that contain same 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 evoting, 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 threearchitecture framework tier 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

| | wallet_address [PK] text | salt text | 1 | key text | / | W text | | |
|--|--|---|--|--|---|--|---|--|
| 91 | d69d1b5b7057034e3980321509cee5f64a8e19ec32897c8a4 | 6e320fc2272b3458 36636438656565373731616136613 | | 5656537373161613661313563633 | 303230616637666464656232343736656563323938643131373035363238623 | | | |
| 92. | d9e3addf3efba2af7c9bb20cf6d77f45f912cc553caa01f365f2 | 5b7d2ea823o44123 32356565 | | | 5313464336135663333356338326 | 1333356038328. 34383231325466336430666138383639653362646138065363335396322233 5430626664396. 373223432636666386283355031664634645316422622439625462652616433 | | |
| 93 | da31a5c192db4d7711013d97dff1f55791ff67c21d3829cd45 | 581d371b166bc7a5 993739636431363664 72b45da85de39c81 3762393531633761660 c8555ac6e72d0599 3838363731326338630 | | 1313636646263376430626664396 | | | | |
| 94 | eaa428bfc722afe36f289517688bc1f12cf8444c2b815365c5a | | | 3762393531633761666336623638666239343. | | 6431356639016235333837663139316161623637653732643233663739616138 | | |
| 95 | f118d14078666866666666666676681ebe74ebdba363071282c931de. | | | 1326338636666356336326438663 | 3635346437353733633264353966333266356635643539393361623234306238 30323036353863626435353034663830646135303331393034303363336533463034 | | | |
| 96 | f85520a01572676c6a3321e10557633714e4e20bd2dd040d8 | 99df20eab7d8e67- | Jeab7d8e674 3565636236313436393862376334646465643 | | | | | |
| 97 | f92652e0cb6fecd9fe6aad77497b05c50d8d1e2b266a723e59 | fee1c055a9f20a41 | | 3264313963356261313833336365653133306. 6433323264666163316636333164308 | | 333164306234646363376165346533613135376638 | | |
| 98. | fc7430ef0f36a9402b6470b7823493d692597b996d67f371c6. | 82f57fd09d3ed5ee | | 6233663134333935653462616633626334313. 313661633765656 | | 313661633765656164373 | 437353937383839383237393061366436663864343133343 | |
| 99 | fe6775913cbe7c0ca1c4a0c54f82e83e3ea68ef9daa8403643f. | 5e8b37c77828ebd | 12 | 623735613 | 2396561393537333666383130353 | 353561353665643631623 | 373939336563396663383434646530343466663664 | |
| | surflat address | | | | home | | Au | |
| a 80 | wallet_address [Pk3Text] d68d1b5b7067034e398032 <u>1509cee5f64a8e19ec32</u> | 897c8a459eb17 | 93d1 | 9210c | key Text e2d4777b19d6b761256eb91 | fa007df456ecb6a4db5 | N Text / 836bcaf3f8876494a559f389a3d66579 | |
| # 80 81 | wallet_address [PK]Text d68d1b5b7067034e3980321509cce5f64a8e19ec32 d9e3addf3efba2af7c9bb20 d68d1b5b7057034e39 | 897c8a459eb17 0321509ccc5/64 | 93d IaBe1 | 9210c 9ec32897 | key Text = | fa007df456ecb6a4db5_ 33e501df591df191199_ | N Text | |
| # 80 81 82 | willet_address [PK]Tex7 d68d1b5b7067034e3980321509cee5f64alle19e-33 d68d3bd73e1ba2af7c9bb20 d68d1a5b70c7034e39 d68d1a5b70c7034e39 d68d1a5b70c7034e39 d68d1a5b70c7034e39 | 897c8a459eb17 0321509ce5154 829cd45b12a5c | 93d1 138e1 | 9210c 9ec32897 5093 | key Text = | fa007df456ecb6a4db5_ 33e501df591df191199_ 748291fe7a9f67722da_ | V Telit | |
| 80 81 82 83 | willet_address [Pk{Text d8ld1b5b7067034a3980321509cee5ff4a3ld19en3 d9e3a6d73efba2a77c9bb20 d831a5c192ab4d7711013a97df1155791ff67c21a3 eaa428b16722afe3f289517688bc1f12cf8444c2b8 | 97c8a459eb17 10321509ce5164 829cd45b12a5co 15365c5a8f5617 | 93d 38e1 c9f5 | 9210c 99232897 9993 cab | key Text e204777b19d6b761256eb91 38459eb1793d592100 n3c864 18a9e157aaad7c5d5351ec0 1acfa6180a2695b72581d1ad | fa007df456ecb6a4db5_ 33e501df591df191199_ 748291fe7a9f67722da_ 17a56b5ce0d2dc8d404_ | V 1682 836bcaf38876494a5597889a3d66579 52b8442b8baf531de59a28d7119728 9aabbfcecC1d8e481a30074914325487 204c7bc2322eb61d5f7920c29a312588a | |
| 80 81 82 83 84 | wallet_address print_text disid1b5b706703443900321509cm6564a38019cm12 disid1b5b706703443900321509cm6557070704843 disid1b5b706703443900321509cm6557070704843 disid1b5b70970483917080507070474853 disid1b5b7097048391708050512047110139970411655911672c1203 disid1b5b70970483917080505120411655911672c14442038 disid1b5b7097048442038 disid5550562052456316567426436316274 | 1897c8a459eb17 10321509ce5154 829cd45b12a5o 15365c5a8f5617 82c931de20638f | 93d 138e1 c9f5 74f1 f803 | 0210c 09032897 1093 cab 8d54 | key Text e2d4777h1966b761256eb91 84659eb1798d59210c 13c86 13a9e157aaad7c5d5351ec07 13cfa6180a2695b72581d1ad 21722070fdbc3734557731ad | fa007df456ecb6a4db5. 33e501df591df191199. 748291fe7a9f67722da. 17a56b5ce0d2dc8d404. 116fd46bc8e529c310e. | M 1683 836bcaf38876494a5597389a3d66579 52b8442b8baf531de559a28d7119728 9aabbfcecc7/d8e481a300749143264b7 2c4c7bc232ab61d57920c29a312588a fe72941425301ad5511f1a76735652a8 | |
| 80 81 82 83 83 84 85 | walke_address PRYLext | 1897c8a459eb17 10321509cee5154 829cd45b12a5co 15365c5a8f5617 82c931de20638f 8dd040d862c8f20 | 93d 38e1 c9f5i 74f1 f803 663e | 9210c 92032897 2093 cab 8d54 fcfcc | key Text e2:04777b19:05b761256eb91 33559eb17920552100 13:0565 13:0596 13:05965100 13:059572581101 21722070fb:0-3734555773142 7c51c125779ccff69bd1e369 | 1a007df456ecb6a4db5. 38e501df591df191199. 148291%7a9f67722da. 17a56b5ce0d2dc8d404. 116fd46bc8e529c310e e95183b0796fe68feae | N 1ex 352bca/18876-044a5597893930465579 552b1344288ba/531c55-9a28d7119728 9abb/cecc/08e4813030749143264b7 2c-67bc2228e6/6579202c93125888 fc7294142501ac55111a5r7355528 fc7294142301ac55111a5r7355528 | |
| 4 80 81 82 83 84 85 85 | wildt_dddess prifter: dilattibio7667034790721500cccff4483b19er25 dilastibio77667034790721500cccff4483b19er25 dilastibio7204764790715080ccff120787484 asa428050722af6347299317688bccff120f844c2b3 111381439785888806226581abc74cbaba303712 8555202015772764c633231e105570337144e42bb3 | 1897c8a459eb17 10321509ces556 829cd45b12a5cc 15365c5a8f5617 82c931de20638f 2dd040d862c8f2 5a723e59391bd0 | 93d1 88e1 74f1 7803 663e foo6 | 9210c 99232897 8093 cab 8d54 fcfco 98d5 | key Text 204777b1966b761256eb91 84659eb1798559210c 1acfa6180a2995b725811d1ac 21723070fdbc373452731ac 7551c125779cff6bd1216b8 3494ee155c3235b175954b2 | fa007df456ecb6a4db5. 838501df591df191195. 838501df591df19172da. 7/856b5ce0d2dc8d404. 15f464bc85230310e. e95183b0796fe68feae. 3add64f9393ccff47cc. | N Exit B36bcat318876494a55097897a30466579 S2054424288a45514 S2054424288a45514656792027384132848 6r234142301a6551711a723565288 06d722bcat33a67b40c09c48a4636b3 06d722bcat33a67b40c09c48a463ba22d6 | |
| a 80 81 82 83 84 85 85 86 87 | wildle, doktemis profiltant dielen to boly 2004 and 2002 12 000 ceed friedelie 19 vorzi- dielen to boly 2004 and 2005 12 000 ceed friedelie 19 vorzi- dielen to boly 2004 and 2005 2006 17 000 ceed friedelie 19 vorzi- dielen to 2004 and 2005 2006 17 000 ceed friedelie 10 vorzi- 10 001 and 2006 and 2004 2006 ceed friedelie development 10 001 and 2006 and 2004 2006 ceed friedelie development 10 001 and 2006 and 2004 2007 2006 ceed friedelie development 10 001 and 2006 and 2004 2007 2007 and 2007 2006 ceed friedelie development 10 001 and 2006 and 2004 2007 2007 and 2007 2006 ceed friedelie development 10 001 and 2006 and 2004 2007 2007 2006 ceed friedelie development 10 001 and 2006 ceed friedelie development | 1897c@a459eb17 10321509ce555 829cd45b12a5cc 15365c5a8f5617 82c931de20638f 2dd040d962c8f2 5a723e59391bdb 67f371c63043d1 | 93d1 88e1 74f1 7803 663e fcc6 715e | 9210c 9232897 4093 605 8d54 4cfco 98d5 56874 | key Text Cold:77701906b7612564591 204572701906b7613564591 1acfe6180a269507258101ac 21722070febc3724557731ac 7c51c125779ccff69bd1e368 3e94ec155c2258175954820 a67bc7026629242838475000 | fa007df456ecb6a4db5. 83e501df591df191109109. 7482911e7a9/67722da. 17356b5ce0d2dc8dd40. 16f46bc58e529c310e. e9518380796fe68feae. 3add54f9393ccff47cc. 150dab3e2e5a280aa50. | P Test 8386-ex1518074444559718943646579 52874442888451511654-ex286719728 9aabdecex508e481.a0074914325497 264-bc222686457202-b315111a75725652a8 6472541425301ad551111a75725652a8 04677226-bc1882678046564 3542a384671597791242aaab822036 | |

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.

| -ыкк ТХ Ө×ее80 | abf7824d9072c9105d6d7b33 | 1e356dac4954279d217a785148 | Sef021fbfbe | | | | | | |
|--|--------------------------|---|---|-----------------------|--|--|--|--|--|
| SENDER ADDRESS 8×819F128f9AA9b0B7B4 | DCcab5b07B8cBd192486E5 | TO CONTRACT ADDRESS 0×779A3E53D10A1C563f83 | 10.09/TMACF.AD04E00 0×779A3E53D10A1C563f8375869869B7AFA5499aF8 | | | | | | |
| WLUE 0.00 ETH | GAS UND 39829 | GAS PRICE 20000000000 | DAS LIMIT 30000000 | MINED IN BLOCK 16 | | | | | |
| | | | | | | | | | |
| CONTRACT | | | | | | | | | |
| CONTRACT Election | | | ADDRESS 0×779A3E53D10A1C563f8 | 37586986987AFA5499aF8 | | | | | |
| RMETTON VoteFromServer(_Cand | idateNames: string) | | | | | | | | |
| ынита Jonny Wicky | | | | | | | | | |
| EVENTS | | | | | | | | | |

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.





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.





Fig. 7 Admin Page

In the perspective of the admin of the system, as mentioned earlier. there three are 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

different exist There many ideas and modifications in the development of a secure evoting 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 the smart inside 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 fingerprint utilising biometric and bv 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 acknowledge that the implementation of to 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/australianews/2015/mar/23/nsw-election-result-could-bechallenged-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/australianews/2015/mar/23/nsw-election-result-could-bechallenged-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_T ransparent_Blockchain-Based_Voting_System_Guide_to_Massive_Deploymen
- ts [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/evoan-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_B lockchain-Based_E-Voting_System.