ISSN 1816-6075 (Print), 1818-0523 (Online)
Journal of System and Management Sciences
Vol. 12 (2022) No. 5, pp. 121-138
DOI:10.33168/JSMS.2022.0508

Secure E-Voting System based on Blockchain Technology

Chia-Hao Lee, Han-Foon Neo, Chuan-Chin Teo

Faculty of Information Science and Technology, Multimedia University, Malaysia

Abstract. Voting is absolutely important in a democratic society as it gives people a right and a chance to express their voices and opinions. Regardless of whether it is a national election or an internal business decision, a fairness voting process must be uphold. However, there are some situations where the losing party might use electoral fraud as a controversy and disagree with the results. In this research, blockchain technology is proposed to be used to create a secure e-voting system. Blockchain allows digital information to be recorded and distributed, but not edited. Hence, by protecting the anonymity of the vote details, this small piece of high-value data would be stored in the blockchain to make sure it is immutable. Ultimately, the proposed e-voting system is able to avoid any fraud or manipulation.

Keywords: electronic voting (e-voting), blockchain, decentralized, immutable, anonymity.

1. Introduction

Blockchain is an emerging technology that allows digital information to be recorded and distributed, but not edited. Blockchain not only widely used in different industry, but it also creates new industry with its characteristics. For instance, cryptocurrency and non-fungible tokens (NFT) are new area that developed based on blockchain. Besides, secure medical data or processing estate are the example where blockchain improve the industry (Daley, 2022). With the characteristics of not tampered, this technology is having similar attributes with voting.

Nowadays, the biggest problem in e-voting is people do not have enough confidence on the system. They are still questioning and doubting. The most common question asked by the critics is whether the e-voting would be secure. They doubt that by using internet, there is a risk for malicious people to modify the vote or disable the service easily. According to the National Academies of Sciences, Engineering, and Medicine 2018 report, "there is currently no known technology that can guarantee the secrecy, security, and verifiability of a marked ballot transmitted over the Internet" (EPI Center, 2021). Thus, the voting system still facing a lot of controversies especially in the security area.

This research aims to answer the research question on how to integrate blockchain technology and an e-voting system so that it is secure and safe. The objective of this research is to create and develop a secure e-voting system by implementing blockchain technology, which is anonymous, verifiable and accurate.

Based on blockchain technology, it is viable to create a secure e-voting system. Ultimately, it will expedite the election process and the method is environmentally friendly. It will uphold the fundamental of voting where all voters trust the system to make the right decision based on the majority choice of eligible voters.

2. Related Works

2.1. Blockchain technology

Blockchain was first introduced by Satoshi Nakamoto (a pseudonym) (Hayes, 2022). Blockchain is secure by design because there is no trusted centralized coordinator. Instead, every node that engages in the blockchain system holds the data block locally. Blockchain is maintained by a decentralized and open-membership peer to peer network and make it a system with high byzantine failure tolerance.

The blockchain technology revolution has come when Bitcoin become the first and one of the most successful examples with the use of blockchain technology. "Blockchain is to Bitcoin, what the internet is to email," Sally Davoes, a technology reported (Marr, 2022). It is believed that blockchain had trigger the start of a new era in the Internet and online service.

The biggest characteristics of blockchain that attracts many researchers are its immutability in nature. Whenever people create a new block, it will store the previous block's hash data and combine it with the data to be stored, to produce a new hash data. Then, this hash data will be stored to the next new block. The more important part is the copy of whole blockchain is decentralized and distributed to any nodes in this world. Therefore, to modify a data, one has to modify more than half of the nodes in the world which is technically impossible. Therefore, by implementing blockchain technology, a secure e-voting system could be developed.

2.2. E-Voting

Voting is a popular method when deciding and making a choice and it is the fundamental right of democracy. However, during the early of the 19th century, this democracy vote is only eligible to people who own property. This unfairness has been eliminated gradually when people start to fight for their equal voting rights such as Women's suffrage. Finally, the world is changing and start to legislating the Voting Rights Act when the President of America, Lyndon Johnson signed the act in 1965 (Britannica, 2022).

Due to the rapid development of the technology, it has permeated our daily life. For instance, people is relying on internet and social media today. E-voting is one of the systems that exists with the help of technology. E-voting is used to aid casting and counting votes in an election. With e-voting, it can speed up the election results, lower the cost of conducting an election and ensure environment friendly.

2.3. E-voting based on blockchain

An electronic voting system based on blockchain was proposed (Ayed, 2017). In this work, it was posited that the system should not provide a registration function as the verification of a legal voter always requires some documents and the process would be insecure if done online and violate the law. Every legal voter should use their credentials to log in to the system after they register to the authority successfully.

In another similar work, the main property of blockchain, blind signature is used to design a secure e-voting system (Yi and Qi, 2017). Blind signature is used for signing encrypted messages with no need for decrypting them. Hence, the voters' choices on the voters' choices on the ballots while getting signatures is hidden.

Subsequently, BroncoVote, an e-voting system was created (Gaby et al., 2018). It was deployed on Ethereum's Testnet. The process begins with initial setup, register voter, create ballot, load ballot, vote and get votes. They had conducted an analysis on the system's performance to simulate a mature blockchain by observing the gas cost.

In another research, Yi (2019) proposed a design for a blockchain-based e-voting scheme using Distributed Ledger Technology (DLT) on a synchronized model of voting records to avoid any tampering of votes. In addition, a user credential model

is designed based on Elliptic Curve Cryptography (ECC) to provide authentication and non-repudiation. A withdrawal model is created that allows voters to change their vote before a preset deadline.

On the other hand, the method of double envelope was proposed. It uses the public key of the election to encrypt the vote in an envelope, then voters use their private key to sign the envelope (Cosmas et al., 2018).

2.4. Case study

Voatz is a private United States company that earns profit by providing a private mobile election voting application based on blockchain. Voatz stated that their company mission is "make voting not only more accessible and secure, but also more transparent, auditable and accountable" (Voatz, 2022). One of the strengths in Voatz is their system will produce three records to let user verify their vote and make sure their votes are counted. It includes Ballot Receipt, Paper Ballot and Blockchain Data. All these records will be encrypted by an "Anonymous ID". By comparison, these three records, the verify process can be done with trust.

Votem is another company that provides a mobile platform e-voting system. Their company mission is having 1 million people around the world using their platform to vote (Votem, 2022). To achieve their mission, they have a strength in which they are supporting hybrid print elections which include online voting, phone voting and paper ballots. Votem offers various secure channels for voting to be integrated into one single platform. Therefore, their consumer has more options of voting channel and ensure all of them are having the same instructions which would not affect the results.

Similarly, Horizon State is a company that plays the role of developing a tamper-resistant digital ballot box and platform that is transparent, verifiable, and trusted by using blockchain technology (Horizon State, 2022). They provide a dedicated server infrastructure to each client. This becomes an edge since the market is not very confident towards e-voting. The unique server cluster has definitely increased the security and the customisation potential.

On the other hand, Clear Ballot provides a modern voting system that enables record speed, accuracy, and transparency. Their system includes browser-based software, used in conjunction with commercial hardware to scale to election of any size (Clear Ballot, 2022). To ensure authorisation, Clear Ballot's software applies role-based access control to limit access to authorised users. Clear Ballot will also record every detail of activities on security audit logs. As Clear Ballot has a huge system which involves many administrators working on it, it is vital to ensure their access is secure.

3. Methodology

3.1. Tools

3.1.1. Truffle framework (solidity)

Truffle framework provides various useful features such as testing, managing networks or communicating with contracts. This environment is convenient regardless of if they are deploying the smart contract or developing the front-end. Solidity is the first smart contract programming language based on object-oriented concept.

3.1.2. Ganache

Using blockchain technology, a digital asset for payment which is called Ether is required and it costs real money. In this research, Ganache is used to build a personal Ethereum blockchain and to test and run the contract with zero cost. Graphical user interface (GUI) with the version 2.5.4. is used.

3.1.3. Metamask

Metamask is a crypto wallet which acts as a bridge to connect the e-voting page with blockchain technology (Metamask, 2022). Ultimately, each user will possess only one account to communicate with blockchain. An important consideration in Metamask is that every time the user performs an update to the blockchain for example register, create new elections or cast a vote, there is a need to make a transaction using the Ether crypto. Fig. 1 illustrate the transaction process.

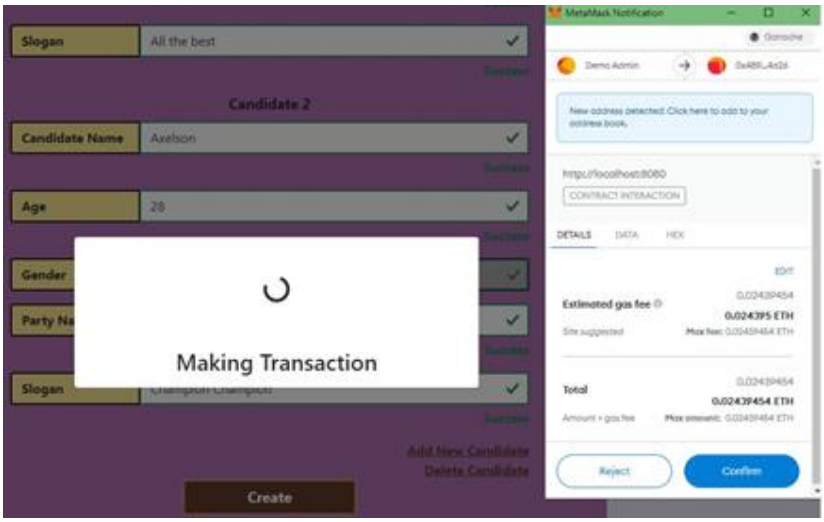

Fig. 1: Example of making transaction using Metamask.

3.1.4. Encryption (@metamask/eth-sig-util)

Encryption is a method used to ensure the voter's choice is encrypted and only the voter who encrypted can decrypt the message as a verification process. Firstly, the voter is requested to obtain their public encryption key. This public encryption key is

computed from entropy associated with the voter's account. Therefore, the generated key will be different for each account.

Subsequently, the key is encrypted by using the encrypt() function from @metamask/eth-sig-util to encrypt the data with an algorithm called ''x25519-xsalsa20-poly1305'. The encrypted message will be stored in a mapping object in the contract. The mapping logic works as the first uint256 is the election ID, this ID will map to another mapping with the key is the voter's signature and the value is the encrypted message.

By doing this, everyone will know who has voted by verifying the signature of the voter. However, the encrypted message remains a secret.

3.1.5. Homomorphic encryption (paillier-bigint)

In the e-voting system, the crucial concept to ensure anonymity is homomorphic encryption. As all the transaction information including sender and data is recorded on blockchain, so encrypting the total votes while maintain the ability of calculation will be a better and suitable solution to achieve anonymity and confidentiality (Fleming, 2020). As the ability to perform calculation without compromising the data is the priority of this research, homomorphic encryption is chosen as compared to zero-knowledge proof which is more suitable to preserve an identity or attribute.

To ensure the security, public and private keys are stored separately and is not public to avoid putting those keys in plain text and having the risk of being exposed. After getting these two keys, encryption, decryption and addition can be performed easily. In homomorphic encryption, addition can be done with two encryption numbers to ensure no one knows what the total number is (Clark, 2020).

For example, if there are three candidates (A, B and C) in Election X, the candidates will have a voteGet value with default encrypted zero. When a voter votes for Candidate A, the total voteGet from the three candidates is loaded. Hence, the Candidate A's voteGet will be a homomorphic add with an encrypted value of one while the other two candidates will have a homomorphic add with an encrypted value of zero. The examples of the result are illustrated in Fig. 2 and 3 respectively.

Fig. 2: Example of addVote function performed at Election with ID 1 by one of the users.

Fig. 3: Example of addVote function performed at Election with ID 1 by one of the users.

To proof the concept, data from Etherscan can be retrieved to view the details of the addVote function which indicates that the votesGet array consists of long encrypted strings that will change everytime when the addVote function being called. This encrypted number will only be decrypted when the election is ended so that the public can view the result.

Moreover, if the candidates are having similar value, such as zero vote, they would have the same voteGet value. However, as every encryption performed generates a random integer, it ensures that the encrypted value would not be the same (even though the plain text values are the same) (Juan, 2022).

3.2. Architecture diagram

Fig. 4 shows the architecture diagram of the secure e-voting system based on blockchain technology. There are three main components which include the smart contract that deployed on blockchain (Ganache/Infura), the front-end interface for users and a bridge that connects both (Metamask).

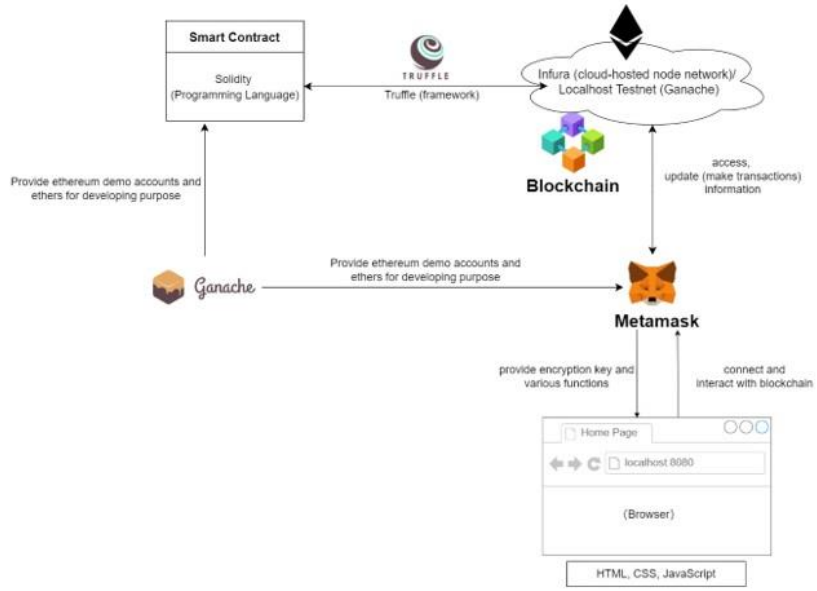

Fig. 4: Architecture diagram of the e-voting system.

4. E-Voting System

4.1. Voter's view

Voter's main page as illustrated in Fig. 5 introduces the secure e-voting system and provide brief guidance such as to cast a vote, view the election result, verify the vote, and view their profile. Fig. 6 shows the "Cast a Vote" page, where the available election is arranged in an organised category which include "Yet to Vote" and "Voted". When a voter selects the preferred candidate, the system will ask the voter to confirm their choice again (Fig. 7) as this is an unchangeable process once the voter confirms the vote and makes the transaction.

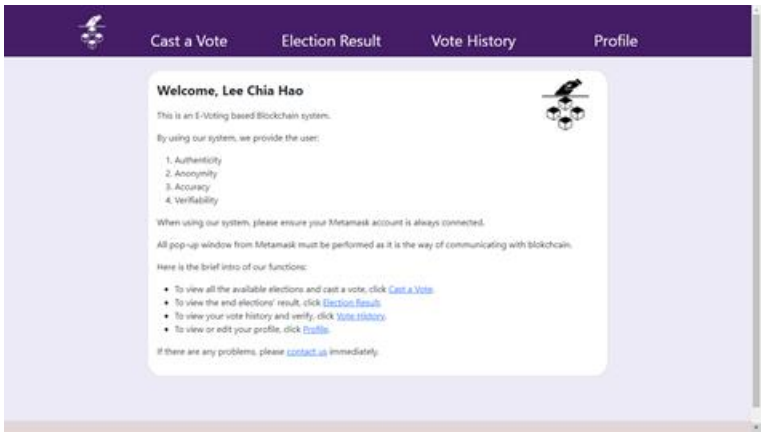

Fig. 5: Voter's homepage.

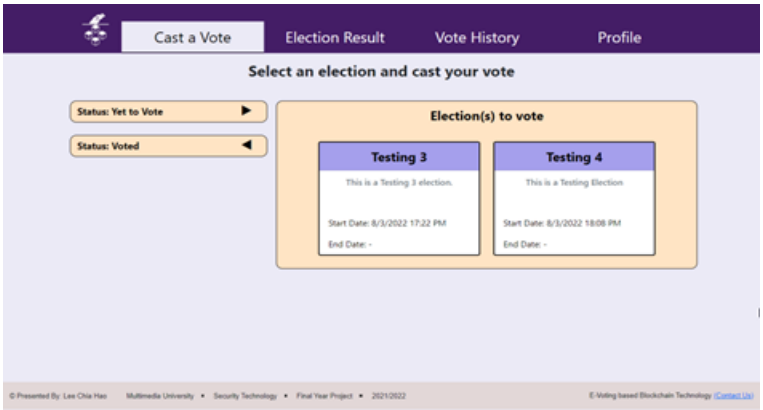

Fig. 6: Cast a vote.

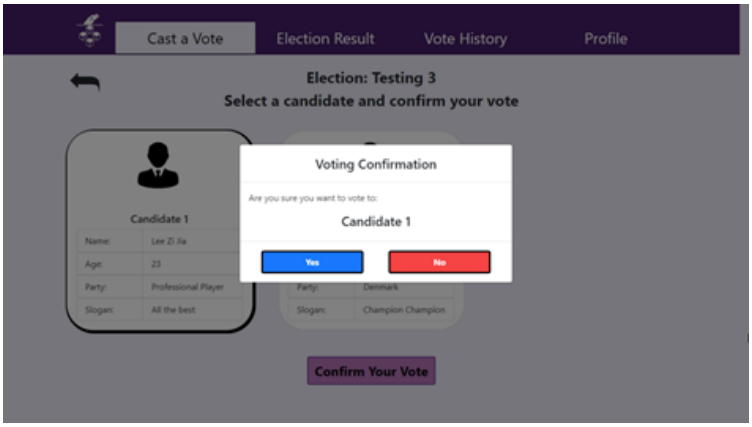

Fig. 7: Confirmation on the vote.

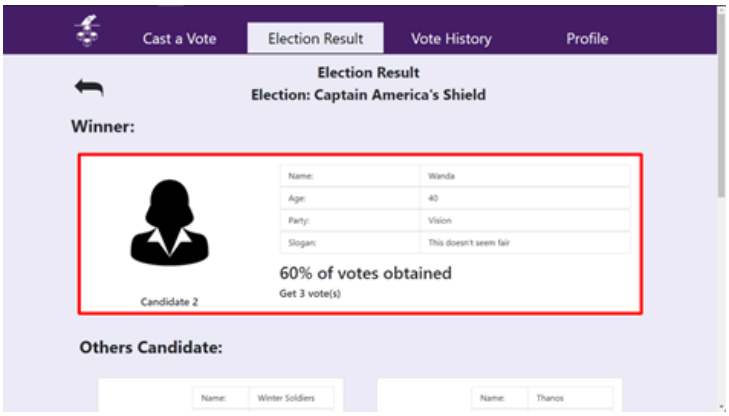

Fig. 8: Election's detail result.

Fig. 9: Verification result.

Fig. 8 shows the detailed result of the election like candidate's information and the number of votes that they obtained. The layout is separated as "Winner" and "Other Candidates". Once the voter has decrypted the message, the verification result would be displayed as illustrated in Fig. 9. It displays the detailed voting information of who they have voted other information such as Candidate, Time, Transaction ID, and Block Number. The transaction ID is unique and can be checked on platforms like etherscan to ensure the voting function from this voter has been executed (if the contract is developed on public blockchain). However, in this research, it would be checked via Ganache as this operation is performed in the local blockchain. The example of Block 2000 and its transaction ID in Ganache is shown in Fig. 10.

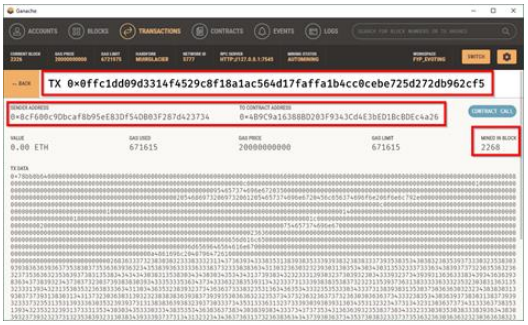

Fig. 10: Transaction ID in Ganache.

4.2. Administrator's view

Admin 's main page as shown in Fig. 11 introduces the system briefly and guide the basic functions that can be performed which include creating a new election and viewing existing elections. If the transaction is performed successfully, then a success message is prompted as shown in Fig. 12. Admin can view all the elections in this page (Fig. 13). All the created elections would have a default "initial" status, which means that the admin is still allowed to edit or delete the election's information. Fig. 14 shows a checklist form to enable the admin to choose who can or cannot vote in this election. Fig. 15 shows the detail of the election result and the details such as the winner candidate's information and total of votes obtained.

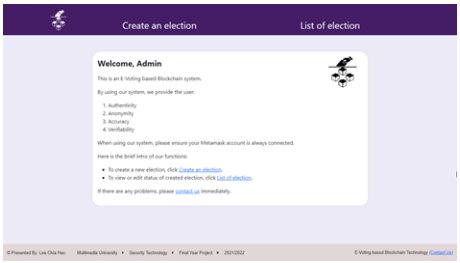

Fig. 11: Admin's home page.

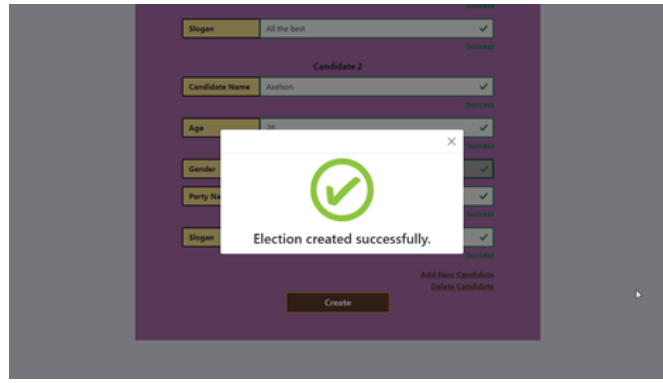

Fig. 12: Election successfully created message.

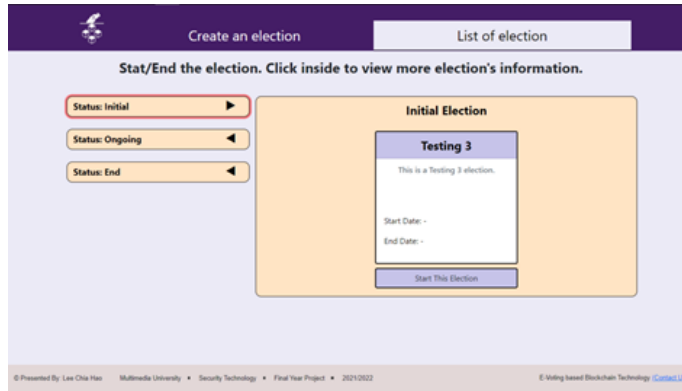

Fig. 13: List of "Initial" election.

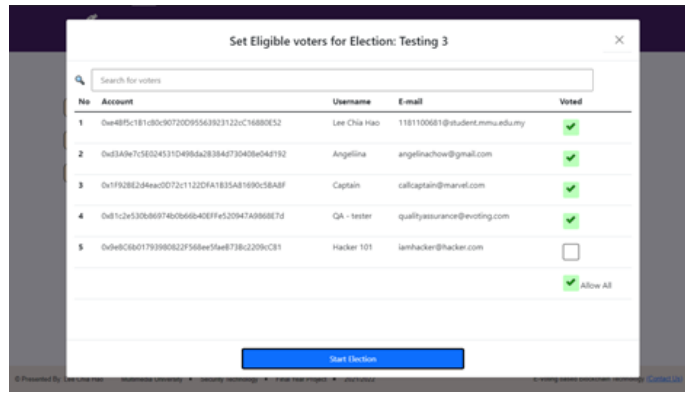

Fig. 14: Select eligible voters for the election.

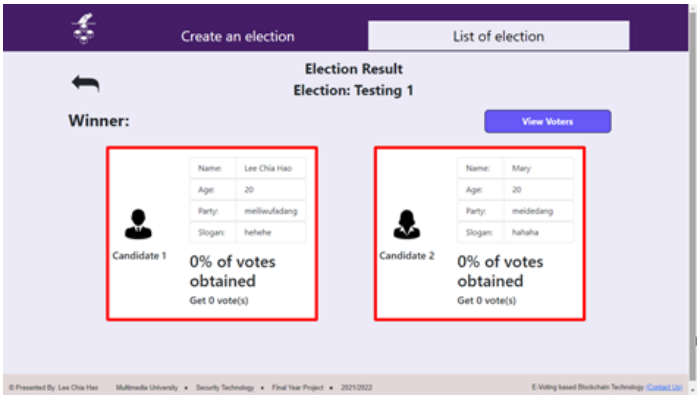

Fig. 15: Election detail result.

5. Performance TESTING and Results

5.1. INFURA vs localhost testing

Infura is used to develop the secure e-voting system onto a Testnet (Ropsten). Infura provides a convenient environment to test or fully develop the blockchain application on Ethereum. As an Infrastructure-as-a-Service (Iaas) and Web3 backend infrastructure provider, it is uncomplicated to use (Ivan, 2021).

All the operations (transactions) occured in Ethereum are published and can be checked at Etherscan regarding whether it is a mainnet or testnet. For instances, the transaction ID of the Elections Contract can be checked by using the url: (https://ropsten.etherscan.io/address/0xD1c5A50d47fE6B083063772971e4F71c5ae6912A) and Voters Contract: (https://ropsten.etherscan.io/address/0xE3b422B3C0089a24A7db268E7B13D40319eb782E).

Table 1 shows the functions used to test the all eight transactions. Fig. 16 shows the test result of using Infura-Ropsten and Localhost. The significant difference includes the time taken to conduct a transaction where it is faster in Localhost as compared to Infura-Ropsten. This is reasonable as in Localhost, there is only one transaction at a time while in Infura-Ropsten, the amount of transaction in one time is unpredictable since the blockchain can be used by anyone at the same time (ETH Gas Station, 2022).

Table 1: Transactions and its function.

Transaction ID	Function Performed
Transaction 1	Deploy the contracts (Elections and Voters)
Transaction 2	Create Election (2 candidates)
Transaction 3	Create Election (4 candidates)
Transaction 4	Start Election (2 candidates, 3 eligible voters)
Transaction 5	Start Election (4 candidates, 3 eligible voters)
Transaction 6	Register
Transaction 7	Cast Vote
Transaction 8	Edit profile

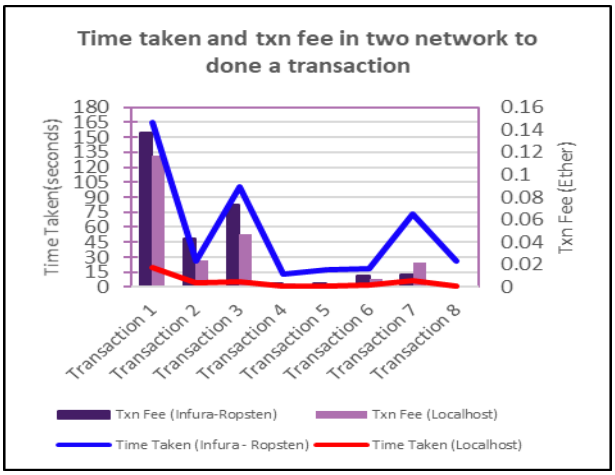

Fig. 16: Time taken and transaction fee between Infura-Ropsten and Localhost.

It is noticeable that when the amount of transaction is high, the average gas fee in the network becomes higher. For example, Transaction 3 is creating an election with four candidates as compared to two in Transaction 2, the total time consumed and gas fee are unarguably higher.

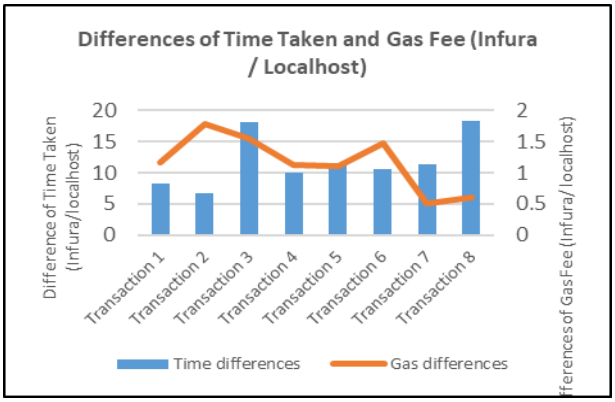

Fig. 17: Differences of time taken and transaction fee between Infura-Ropsten and localhost.

However, there exists variant such as for Transaction 7, the gas fee for Localhost is much higher as compared with Infura-Ropsten. Fig. 17 shows the differences of time taken and gas fee by calculating the data for Infura-Ropsten divided by the data for Localhost. It demonstrated that the time taken for Localhost is 6 to 18 times faster as compared with Infura-Ropsten overall.

However, it is observed that there is a significant different of gas fee for the transactions. Generally, transactions in Localhost require higher gas fee as compared with Infura-Ropsten. For example, in Transaction 7 and Transaction 8, although the transaction's gas fee in Localhost is higher, the time taken to complete the transaction is faster than Infura-Ropsten. This does not imply that a higher gas fees is useless because of the circumstances of two different networks.

Overall, the test result shows the average time taken and gas fee to complete a transaction in localhost is 11.8 times shorter and 1.17 lesser than Infura-Ropsten network. From this result, we can conclude that although the required gas fee is not obvious, the time taken is a major issue as it will affect the user experience especially if this research were to extended to develop the contracts on the mainnet.

5.2. User acceptance testing

A user acceptance testing (UAT) was conducted to a group of 37 respondents. The participant is required to watch three demo videos before proceed to answer the survey form. The survey form is assessed using 5-point Likert Scale, ranging from 1 (Strong Disagree) to 5 (Strong Agree) for a total of 10 statements. The three demo videos include Cast a Vote (https://youtu.be/jlBPGu6YSTo), Election Result (https://youtu.be/TuiuQpbciuE) and Vote History (https://youtu.be/ONH5Jrbd3I0).

Table 2: Analysis of demo video rating.

No	Survey Questions	Mean	Mod	Standard deviation
1.	Video 1 (Cast a Vote): I think this function is easy to use.	3.78	4	1.004
2.	Video 1 (Cast a Vote): I think this is a useful function.	3.97	4	1.067
3.	Video 2 (Election Result): I think this function is easy to use.	4.43	5	0.729
4.	Video 2 (Election Result): I think this is a useful function.	4.30	5	0.878
5.	Video 3 (Vote History): I think this function is easy to use.	4.08	5	0.862
6.	Video 3 (Vote History): I think this is a useful function.	4.03	5	1.118

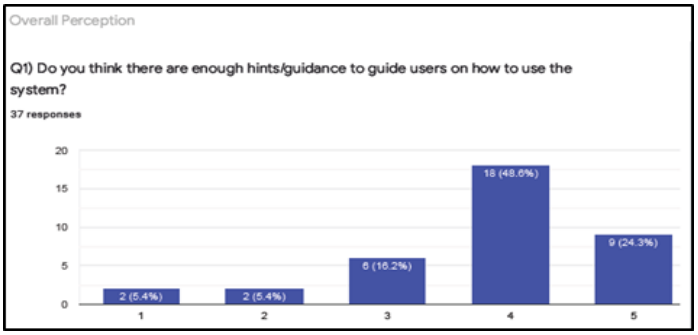

Fig. 18: E-voting system's facilitating conditions.

Table 2 shows the statistical results of respondent's perception of the ease of use and usefulness. Overall, the respondents have provided positive feedback (Mean between 3.78 to 4.43). This is encouraging to know that the respondents are confident of the secure e-voting system. It is noticeable that the average of the first demo video (Cast a Vote) is lower compared to others. This might be due to the reason that the steps needed to perform a complete cast vote are much more and the respondents felt too much a burden. Fig. 18 shows that 48.6% of respondents felt agree and 24.3% strongly agree that there are sufficient facilitating conditions to use the secure e-voting system. Guidance is important as it provides a basic tutorial or especially to the new users so that they would not feel intimidated to use the e-voting system.

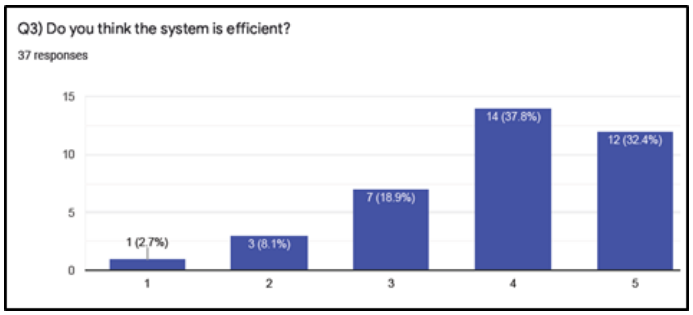

Fig. 19: E-voting system's efficiency.

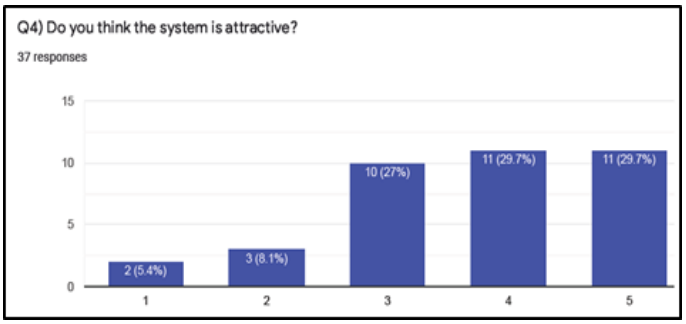

Fig. 20: E-voting system's attractiveness.

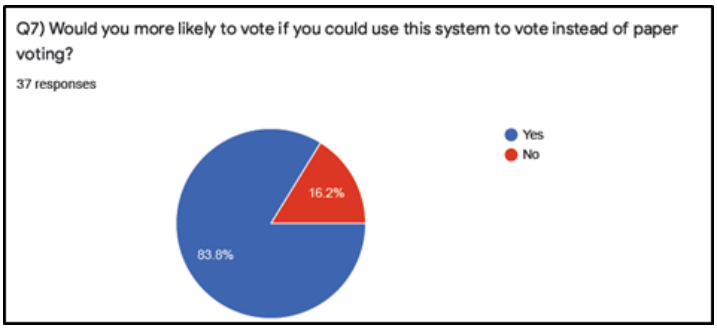

Fig. 21: E-voting system's overall perception.

Fig. 19 shows that about a total of 70% of respondents agree that the e-voting system is efficient. Efficiency of the secure e-voting system means that the user can perform all necessary steps in an election within a short period of time successfully. Fig. 20 shows that 27% of respondents are neutral on the interface design of the e-voting system. Although about 60% of respondents agree that the system is attractive, the user interface has rooms for improvements such as incorporating more images, icons and colors in the future. Fig. 21 shows that 83.8% of respondents are more likely to vote if the election is conducted using the secure e-voting system instead of the traditional paper-based voting.

6. Conclusion

In this research, a secure e-voting system based on blockchain technology is proposed. The e-voting system is secure because every user is authenticated by using a private key to login to an account in metamask, and the authorization is controlled by the admin. Besides, by using the homomorphic encryption and public key encryption, the anonymity is achieved. Hence, only the voters will know who they have voted while others would only get to see a series of encrypted messages. At the same time, the voter can verify their vote information by using the same account that they voted. By implementing the blockchain technology, the accuracy is achieved in at the same time.

In terms of limitation, although it can be ensured that no third party would know the choice of a voter, the identity of voter is not exactly private as all users are using the public key. For example, people may find out this public key belongs to Bob, but no one will know who has Bob voted in an election as long as the private key is secure. Besides, it takes quite a long time for a block to be mined in blockchain so the transaction and data can be saved successfully. However, the time taken is not always the same as blockchain may have unexpected traffic and affected by the ethers that the user spent. This issue may affect the performance of the user experience. Besides, the crypto that must be used in a transaction may cost a higher price as compared to traditional voting methods. For example, 1 ether costs about USD 3,066 (RM 13,500) and the costs fluctuates and varies every day. Further study has to be made to compare

the difference of cost between the traditional voting and e-voting based on blockchain technology.

Authors' contributions

Lee Chia Hao has contributed in application development and original draft preparation. H.-F. Neo is the corresponding author and is the supervisor for this research. She has contributed to reviewing and editing the research paper. C.-C. Teo is responsible for providing overall research guidance and proofreading the research paper.

Acknowledgments

This work is supported by funding of IR Fund, from Multimedia University (MMU/RMC/IR FUND/2020/38612-MMUI/210035).

References

Ayed, A. B. (2017). A conceptual secure blockchain-based electronic voting system. *International Journal of Network Security & Its Applications,* 9(3), 1-9.

Britannica. (2022). Voting rights act. Retrieved from https://www.britannica.com/event/Voting-Rights-Act.

Clark, W. (2020). What is the paillier cryptosystem? Retrieved from: https://blog.openmined.org/the-paillier-cryptosystem/.

Clear Ballot (2022). Innovation for our nation's elections, Retrieved from: https://clearballot.com/.

Cosmas, K. A., Rikard, H. & Hiroyuki, S. (2018). A proposal of blockchain-based electronic voting system. *2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, 22-27.

Daley, S. (2022). 34 blockchain applications and real-world use cases disrupting the status quo. Retrieved from: https://builtin.com/blockchain/blockchain-applications.

EPI Center (2021). Internet or online voting remains insecure. Retrieved from: https://www.aaas.org/epi-center/internet-online-voting.

ETH Gas Station (2019). How long does an ethereum transaction really take? Retrieved from: https://legacy.ethgasstation.info/blog/ethereum-transaction-how-long/

Fleming, S. (2020). What is homomorphic encryption and how can it help in elections? Retrieved from: https://news.microsoft.com/on-the-issues/2020/04/13/what-is-homomorphic-encryption-and-how-can-it-help-in-elections/.

Gaby, G. D., Praneeth, B. M., Matea, M. & Jordan, M. (2018). BroncoVote: Secure voting system using Ethereum's Blockchain. *4th International Conference on Information Systems Security and Privacy,* 96-107. DOI:10.5220/0006609700960107.

Hayes, A. (2022). Who is Satoshi Nakamoto? Retrieved from Investopedia: https://www.investopedia.com/terms/s/satoshi-nakamoto.asp.

Horizon State (2022). Simpler, trusted decisions, Retrieved from: https://horizonstate.com/.

Ivan (2021). Infura explained – what is infura? Retrieved from: https://academy.moralis.io/blog/infura-explained-what-is-infura#:~:text=Infura%20is%20a%20Web3%20backend,of%20the%20Infura%20Web3%20service.

Juan, H. S. (2022). An implementation of the Paillier cryptosystem using native JS implementation of BigInt, Retrieved from: https://github.com/juanelas/paillier-bigint.

Marr, B. (2022). A very brief history of blockchain technology everyone should read. Retrieved from: https://bernardmarr.com/a-very-brief-history-of-blockchain-technology-everyone-should-read/#:~:text=%E2%80%9CBlockchain%20is%20to%20Bitcoin%2C%20what,Sally%20Davies%2C%20FT%20Technology%20reporter.&text=Even%20today%2C%20there%20are%20many,even%20though%2.

Metamask, (2022). Introduction, Retrieved from: https://docs.metamask.io/guide/

Votem, (2022). The current voting system is ripe for disruption, Retrieved from: https://votem.com/about/#our-story

Yi, H. (2019). Securing e-voting based on blockchain in P2P network. *Journal on Wireless Communications and Networking*, 137, 1-9.

Yi, L. and Qi, W. (2017). An e-voting protocol based on blockchain. *IACR Cryptol. ePrint Arch.*, 1043.

Voatz. Secure, accessible voting at your fingertips, the future of voting is mobile, Retrieved from: https://voatz.com/.