SEMARAK ILMU
PUBLISHING
202103268166(003316878-P)

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

e-Voting on Ethereum Blockchain

Muhammad Hilmi Razali[1], Azrul Amri Jamal[1,2], Fadzli Syed Abdullah[3,*], Muhammad D. Zakaria[1,2], Wan Nor Shuhadah Wan Nik[1], Hasni Hassan[1]

[1] Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Besut Campus, 22200 Besut, Terengganu, Malaysia
[2] IoT, Machines, and Systems (iMachS) Special Interest Group, Universiti Sultan Zainal Abidin, Gong Badak Campus, 21300 Kuala Nerus, Terengganu, Malaysia
[3] Faculty of Ocean Engineering Technology and Informatics, Universiti Malaysia Terengganu, 21030 Kuala Nerus, Terengganu, Malaysia

ARTICLE INFO

Article history:
Received 8 December 2023
Received in revised form 28 March 2024
Accepted 28 July 2024
Available online 20 August 2024

Keywords:

Blockchain; electronic voting; authentication; Web 3.0; Ethereum Testnet

ABSTRACT

The act of voting is an inherent and essential entitlement that is universally granted to all individuals. Electronic voting, commonly known as e-voting, is a voting method that utilises electronic equipment to facilitate and manage the process of casting and tallying votes. Electronic voting systems are employed to expedite the process of tallying ballots. Furthermore, it will reduce the amount of money needed to pay for counting staff while also reducing human error. The implementation of remote voting would greatly benefit individuals residing at a considerable distance from their designated polling location, as it would afford them the convenience of casting their vote at any given time and from any geographical area. The utilisation of blockchain technology presents novel opportunities for the creation and advancement of innovative digital services. The implementation of Blockchain-Enabled e-Voting has promise in mitigating instances of election fraud and enhancing voter accessibility. The voting process involved the utilisation of electronic devices, such as computers or smartphones, by those who met the criteria for voter eligibility. This method ensured that the voting process maintained the principle of anonymity. The significance of electronic credibility services has seen substantial development, becoming as a crucial element inside the contemporary information era. This project seeks to implement the objective of constructing an electronic voting system utilising blockchain technology. The two-level architecture ensures secure voting without relying on current (non-blockchain) technologies for redundancy. The blockchain-based voting project is made up of two components that work together to make the whole thing operate. One will be the admin, who will be in charge of creating elections, as well as adding candidates to the smart contract elections. The other type of user is the voter, who can vote for their preferred candidate and have their vote recorded on the blockchain to make it tamper-proof.

1. Introduction

Existing electronic voting systems all have a significant design flaw: they are all designed to be centralised, which means that only one supplier controls the code base, database, and system

[*] *Corresponding author.*
E-mail address: efadzli@umt.edu.my

https://doi.org/10.37934/araset.50.2.186194

outputs, as well as providing the monitoring tools to validate the results. Due to the lack of a third party to verify the system, voters must invest their trust in the organisation that their vote will be recorded and counted correctly once they mark their ballot choice.

Even though many elements of modern life have moved to digitalization, elections are still mainly performed offline such as on paper despite the use of Electronic Voting Machines steadily increasing in recent years. The most frequent voting method is still paper ballots, which are normally recorded by a worker (voter) until being counted by a machine. They put their trust in physical security and voting stations to ensure that their votes are not tampered with or mishandled.

Additionally, absentee ballots use paper ballots to enable citizens to participate without having to actually visit a polling station. These have the same vulnerabilities as regular paper ballots, but they are more vulnerable to attack during their transit through the postal system. Electronic voting (E-Voting) now comes in two forms. For example, instead of a ballot paper and pencil in a voting booth, a polling machine may be used or a vote could be cast over the Internet.

However, many electronic devices are vulnerable to malware or viruses that can alter the software and potentially inject malicious code. Denial of Service Attacks (DoS), Virus Infestation, and Malicious Software are only some of the types of attacks that can occur during the voting process. Electronic voting must cope with difficulties like privacy, fraud, voting under pressure, and corruption and it does nothing to gain voter confidence. Our suggested E-Voting system must be able to give a user-friendly and secured system to be better than existing E-Voting systems. The system will have two users: an administrator and a voter.

The system will also be based on the Ethereum blockchain testnet which simulating the Ethereum network using simulated ETH cryptocurrency. The main concern that Ethereum-based e-voting seeks to resolve is the absence of trust, transparency, and security in conventional voting systems. Blockchain, the foundational technology of Ethereum, presents a promising remedy by offering a decentralised, transparent, and tamper-proof platform for conducting electronic voting.

The fundamental characteristics of blockchain, including its immutability, transparency, and decentralised consensus, effectively tackle issues associated with voter fraud, manipulation of election outcomes, and the absence of accountability in conventional voting systems. E-voting systems built on the Ethereum platform aim to improve the honesty of the voting process, guarantee transparency, and establish confidence among voters in the electoral system.

2. Related Online Voting System

At present, numerous countries have implemented the computerised voting method. Estonia was the pioneer in implementing and sustaining this initiative. Approximately 30.5% of the total votes in the 2017 Estonian election were submitted electronically [1]. In order to enhance the voting platform, we conducted research on many existing systems, particularly focusing on Estonia, and identified their shortcomings. Consequently, we have devised an improved solution. Estonia implemented a national identification system for its citizens, which served as the central mechanism for the voting process. This card facilitates the distinct identification of the voter. To initiate the voting procedure, the voter must first browse the voting website on a computer that is linked to the internet. Subsequently, the voter is required to insert their card into a card reader. Subsequently, the system requests the user's Personal Identification Number (PIN) and verifies their eligibility to participate in the voting process. Only upon successful authentication, the user is granted the ability to submit their vote. During this procedure, voters have the ability to cast their vote multiple times until four days prior to Election Day. If a card reader for computer is unavailable, customers can utilise their cell phone to cast their vote. This system utilises three servers: the Vote Forwarding Server (VFS), the

Vote Storage Server (VSS), and the Vote Counting Server (VCS). When a voter casts their vote, it is first processed through the publicly accessible Voter File System (VFS) and Voter Storage System (VSS). In these systems, the vote is encrypted and securely stored until the end of the election period. The identifying information of all votes in the VSS is removed and then the votes are transferred to the VCS using a DVD. The VCS operates independently from any networks, decrypting and tallying all votes before presenting the final results. Numerous researchers have extensively examined this method and uncovered multiple security vulnerabilities [2]. The centralised nature of this system allows potential attackers or third parties to manipulate the database. This methodology also permits the voter to cast several votes within the four-day timeframe. In this paradigm, the voter lacks the ability to verify if their vote has been allocated to the intended party, hence leaving room for potential manipulation of the casted vote by a third party [3]. Consequently, the users are unable to reach a consensus over the final tally. We have encountered the New South Wales iVoteSystem and have expanded upon its procedure [4]. This approach generates a solution by allowing the voter to select a 6-digit PIN. The voter authenticates themselves within the system by utilising their ID and PIN. After a voter's authentication is successfully completed, they are issued a receipt number consisting of 12 digits. In order to verify their vote, the voter must provide their identification, personal identification number (PIN), and receipt number.

3. Blockchain and Voting

Numerous digital cryptocurrencies employ blockchain technology as their fundamental framework. In the context of a decentralised and distributed network, the blockchain refers to a sequential arrangement of blocks that serves as a repository for information, which is accompanied by digital signatures. The features of decentralisation, immutability, transparency, and auditability are inherent to blockchain technology, enhancing the security and integrity of transactions by preventing unauthorised modifications. In contrast to conventional methods, Blockchain technology facilitates decentralised digital asset transactions among peers, eliminating the need for intermediaries. The inception of Bitcoin can be attributed to the proposal put out by Satoshi Nakamoto in 2008, with its initial implementation taking place in 2009 [5].

A blockchain is a series of blocks that are linked together to store all committed transactions on a public ledger. A mix of important technologies such as digital signatures, cryptographic hashing, and consensus mechanism procedures enable blockchain to work in a decentralised framework. All transactions are completely decentralised, removing the need for any intermediaries to confirm and verify the transactions. Decentralisation, transparency, immutability, and auditability are some of the major aspects of blockchain [6].

The integration of blockchain technology and a robust cryptographic protocol results in the establishment of a safe encryption block, thereby guaranteeing the authenticity, security, and transparency of public voting outcomes, while also preventing any unauthorised modifications [7]. The block consists of block headers, whereas the core block comprises plain serial transactions. The hash value event refers to an unprocessed transaction that encompasses the unique identifier, often known as the Transaction ID (TxID).

The values that identify all transactions within each block are subsequently utilised to construct the leaf node of the Merkel tree [8]. Sandi Rahmadika *et al.,* conducted a study on blockchain technology, which is a cost-effective digital security platform that has been decentralised to ensure data confidentiality without the need for third-party involvement [9].

According to the findings of Mustofa Kamila and his research team, the implementation of blockchain technology in electronic voting systems can effectively minimise the necessity for individuals to be physically present at voting booths during election activities. This reduction in physical contact among individuals can significantly mitigate the occurrence of human physical touch, as demonstrated in their study [7].

A recent innovation in the field of voting systems has proven to be not only time and cost effective, but also safe and secure [10]. Because the vote is directly recorded in the system, a blockchain-based electronic voting system eliminates the need for a third party. Transparency may be assured by using blockchain as a backbone for the election process. As a result, the voter can be comfortable that his vote is secure [10]. These enhancements to the current voting system would not only protect the voter's vote, but they would also increase turnout in election booths since people would know that their vote would be recorded [11].

4. Ethereum

According to Sri Raksha and his research team, Ethereum is an open-source, public, blockchain-based distributed system architecture trying to operate systems with smart contracts [12]. The Ethereum Wallet is a doorway to decentralised apps on the Ethereum blockchain, where miners earn Ether instead of bitcoin. Ether is a crypto coin that serves as a digital bearer asset for the network. In addition to becoming a marketable coin, Ether is utilised by software developers to charge for transaction cost and operations on the Ethereum network. It doesn't require a third party to execute or approve a transaction, just like cash [12].

All generated transactions will be verified by looking at the timestamp, nonce combinations, and availability of sufficient execution costs. Every action in Ethereum demands the use of crypto fuel or gas. For simplicity of calculation, gas is used instead of ether as a fee. The fundamental reason for this is that gas is a cryptocurrency that is unaffected by market valuation for transaction and computation fees [6]. Gustavo A. Oliva and colleagues assert that the Ethereum platform employs the computationally intensive Proof-of-Work (PoW) consensus mechanism, necessitating nodes to solve a challenging mathematical problem [13].

5. e-Voting Framework

Figure 1 shows the e-Voting framework. The framework may be categorised into three primary components, namely the Ethereum Virtual Machine (EVM), the server-side, and the client-side. The current EVM in use is the Rospten EVM integrated with an Ethereum smart contract. The server is the designated location for the placement of the candidates and voting portal. The client side refers to the component of the system where the wallet, such as Metamask, is utilised to store a single vote on behalf of the user. The front-end component encompasses the web application that is being developed using web3 technology.

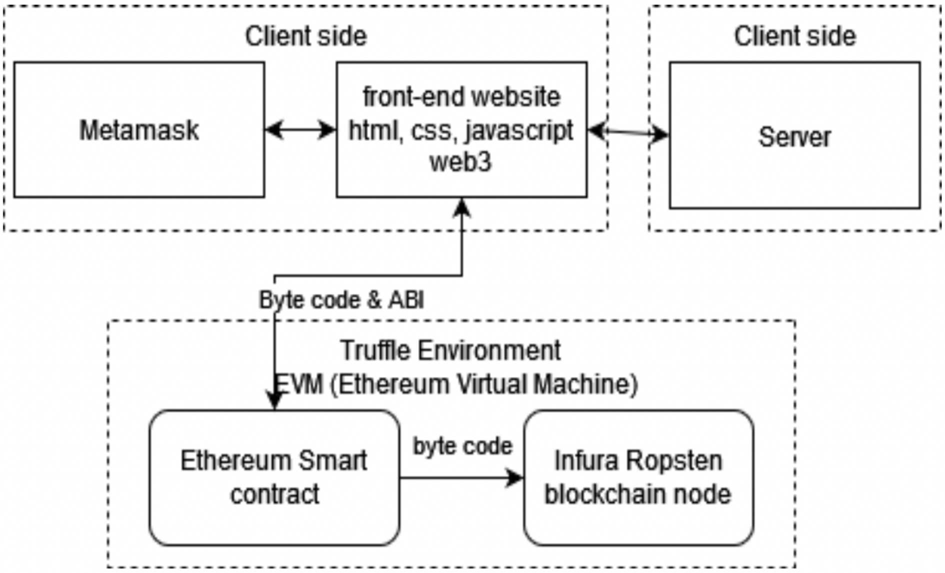

Client side
Metamask
front-end website html, css, javascript web3
Client side
Server
Byte code & ABI
Truffle Environment
EVM (Ethereum Virtual Machine)
Ethereum Smart contract
byte code
Infura Ropsten blockchain node

Fig. 1. e-Voting framework

The user's validation is successfully conducted by verifying the wallet ID, enabling them to successfully access the system. Subsequently, the user is directed to the voting platform. The voting portal would provide a roster of candidates. In the voting process, individuals are required to designate their favourite candidates by assigning numerical values. The candidate with the least favourable standing is assigned the lowest number, while the candidate with the highest level of preference is assigned the highest number.

In our system, each voter's preferred list is regarded as a singular transaction. A transaction is appended to the blockchain network whenever a user or voter expresses their preference for candidates and submits their list. As widely acknowledged, in order to initiate a transaction on the Ethereum blockchain, it is vital for a user to furnish a certain amount of fuel or petrol. Ether, often known as ETH, is the designated term for the gaseous substance or fuel utilised within the Ethereum blockchain network. In the proposed system, it is envisaged that each voter will get a unit of Ether from the designated chairperson or administrator in order to exercise their voting rights. Consequently, each individual voter would have the capacity to cast a single vote.

There would be no alternative method for a voter to acquire an Ether and subsequently exercise a second voting privilege. Consequently, every individual voter is limited to providing a single response, which is subsequently documented as a transaction and disseminated across the blockchain network. Subsequently, miners append a block to the blockchain that encompasses the aforementioned transactions. Miners are individuals responsible for verifying the legitimacy of transactions and appending blocks to the blockchain network.

6. Deployment and Configuration

The installation of the system requirements that enable the development of this project takes place at this stage. Several tools and extensions must be installed, configured, and tested to ensure that they are compatible with this project. Deployment and configuration of E-Voting based on Ethereum Blockchain which is integrated into Truffle Suite and connects to the smart contract via the Metamask wallet. The process of ensuring that the system is completely functional and tested by involving software, tools, and decentralised application requirements based on system design.

6.1 Ethereum Virtual Machine (EVM)

The Truffle Framework requirement enables the development of decentralised Ethereum applications. It offers a set of tools for writing, testing, and deploying smart contracts to blockchain using the Solidity programming language, as well as a platform for developing client-side applications. First, the command "truffle unbox pet-shop" will be executed. This command contains the configuration for a simple Decentralized Application for a petshop. We will then adapt this template to fit the E-voting on the Ethereum blockchain project. After creating the truffle suite project, you will have a project structure with the following elements:

i. /contracts: Listing of Solidity contracting resources.
ii. /migrations: Directory for deployment files that can be scripted.
iii. /test: Directory for testing your application and contracts using test files.
iv. /Truffle-config.js: Truffle configuration file.

6.2 Smart Contract

The contract will be saved in the contract folder as Election.sol. After you've saved the Smart Contract, you'll need to run the command "truffle compile" to compile it. The output of your compilation process is saved by default in the build/contracts/Election.json file. It's a JavaScript Object Notation (JSON) document. The two most crucial keys in this JSON object are Application Binary Interface (ABI) and bytecode. The smart contract's bytecode will be saved on the blockchain, and it will yield the smart contract's address known as contract address. It is nearly impossible to understand the functionality of a smart contract using only bytecode therefore, ABI is essential. Application binary interface is shortened as ABI. To connect with the deployed smart contract via contracts address, ABI is required.

6.3 Ropsten Migration

HD Wallet-enabled Web3 provider, also known as @truffle/hdwallet-provider, must be installed in the project's root directory to connect to the Ropsten Ethereum network. This enables the client site to communicate with Metamask for this project. Register an account with Infura at https://infura.io. then create a project and click the settings button. Choose Ropsten in the key section and paste the API key into the truffle- config.js file.

After the migration process is complete, the displayed contract address is intended to be the smart contract address used for auditing and transparency purposes. The smart contract will generate a new address whenever the migration is deployed. This means that each time an election is held, a new address for smart contracts is deployed.

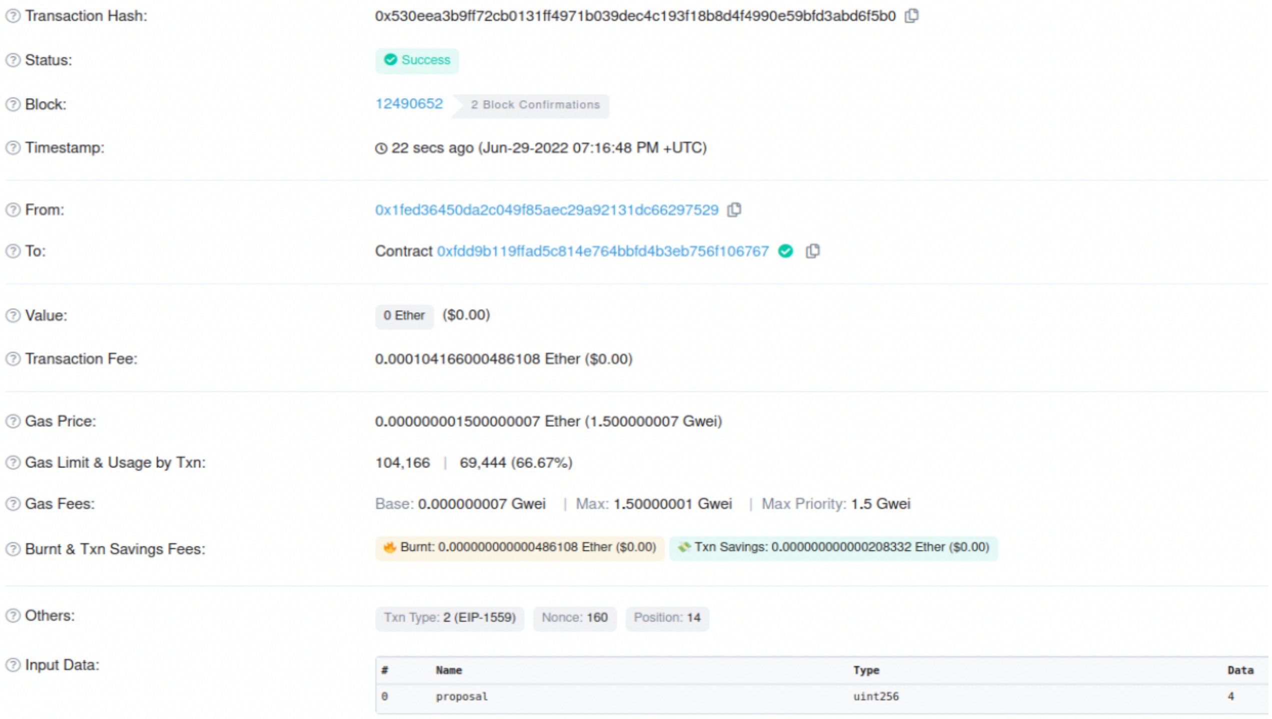
By executing the command 'npm run dev', a local development server will be started. users can access the application's front end by navigating to "http://localhost:3000".

7. Result

This project restricts voters to a single vote per smart contract deployment, while the administrator can add new candidates to the application. The website will automatically disable the voting button for voters who have already cast a vote. The utilisation of blockchain technology, which enables the tracing of every transaction, ensures the prevention of illicit votes and tampering with the results inside the voting system. Despite the ability to detect the wallet ID, the anonymity of the voter is intact, ensuring the enforcement of the one person, one vote constraint.

The ‘ropsten.etherscan.io’ website can be used to verify votes and candidates by checking transaction details. Etherscan is among the most reliable and widely known Ethereum block explorers. Etherscan enables you to search across all public interactions on Ethereum. A transaction hash (transaction ID) can be used to verify all associated activity, including tokens, smart contracts, and wallet addresses. Etherscan serves as a tool for analysing the data transmitted to a smart contract upon the initiation of a transaction directed towards its designated address. However, in the event that the transaction results in the formation of a contract, the bytecode of that contract is inserted into the input data field.

Figure 2 depicts the transaction that occurs on the Ropsten network when a vote is cast. Once a user successfully casts a vote and the transaction is verified, the blockchain node will proceed to store the proposed candidate within its Input Data. The voting transaction information will remain on the 'ropsten.etherscan.io' network to be viewed and assessed at any time.



Transaction Hash:	0x530eea3b9ff72cb0131ff4971b039dec4c193f18b8d4f4990e59bfd3abd6f5b0
Status:	Success
Block:	12490652 2 Block Confirmations
Timestamp:	22 secs ago (Jun-29-2022 07:16:48 PM +UTC)
From:	0x1fed36450da2c049f85aec29a92131dc66297529
To:	Contract 0xfdd9b119ffad5c814e764bbfd4b3eb756f106767
Value:	0 Ether ($0.00)
Transaction Fee:	0.000104166000486108 Ether ($0.00)
Gas Price:	0.000000001500000007 Ether (1.500000007 Gwei)
Gas Limit & Usage by Txn:	104,166 | 69,444 (66.67%)
Gas Fees:	Base: 0.000000007 Gwei | Max: 1.50000001 Gwei | Max Priority: 1.5 Gwei
Burnt & Txn Savings Fees:	Burnt: 0.000000000000486108 Ether ($0.00) Txn Savings: 0.000000000000208332 Ether ($0.00)
Others:	Txn Type: 2 (EIP-1559) Nonce: 160 Position: 14
Input Data:	

#	Name	Type	Data
0	proposal	uint256	4

Fig. 2. Voting transaction

8. Conclusion

E-voting systems built on the Ethereum platform aim to guarantee the security, anonymity of voters, and the integrity of the voting process by employing a range of features and cryptographic approaches. Security can be guaranteed by the implementation of decentralisation and consensus mechanisms. Ethereum functions on a decentralised network of nodes, which enhances its resilience against individual points of failure and reduces its vulnerability to attacks. Ethereum employs a Proof-of-Stake (PoS) consensus mechanism, which is in the process of migrating to Ethereum 2.0. The network safeguards by requiring members to have a financial stake in upholding its integrity.

To maintain voter anonymity, two techniques can be employed: the utilisation of public and private addresses, as well as the implementation of zero-knowledge proofs. Ethereum supports the utilisation of both public and private addresses. Cryptographic techniques can be employed to ensure the privacy of voter identities, with only public addresses being available on the blockchain. Smart contracts can be programmed to incorporate zero-knowledge proofs, enabling voters to provide evidence of their legitimate vote without disclosing the specific details of their vote. This increases the level of anonymity.

In real world scenario with large number of online voters, several blockchain technologies can be implemented including layer 2 scaling, sharding, and a shift towards relying on proof of stake instead of proof of work, which is a more energy-efficient approach. By integrating layer 2 scaling solutions, such as sidechains or state channels, we may alleviate the burden on the main blockchain by diverting transactions, resulting in reduced congestion and improved throughput. By employing sharding technologies, the blockchain is divided into smaller sections (shards) that can independently handle transactions, hence enhancing scalability. The consensus mechanism can be improved by implementing the PoS algorithm. This approach, exemplified in Ethereum 2.0, intends to promote scalability by enabling the processing of a higher number of transactions concurrently.

There are inherent risks associated with the implementation of an Ethereum-based electronic voting system. One potential risk is the possibility of unauthorised access or identity theft, which might undermine the integrity of the voting process. This risk can be reduced by implementing strong voter authentication methods, such as biometrics or cryptographic keys. Consistently revise and enhance authentication systems to proactively address evolving risks.

Smart contracts are susceptible to vulnerabilities that can result in the manipulation of votes or other harmful actions. To mitigate this risk, it is essential to perform comprehensive code audits and testing. Employ well-established coding methodologies and adhere to rigorous security protocols. Ensure that smart contracts are regularly updated to rectify any identified issues.

In addition, there is a potential risk of Distributed Denial of Service (DDoS) assaults, which include overwhelming the e-voting system with enough traffic to disrupt its availability. To address this issue, one might employ DDoS prevention strategies, such as implementing traffic filtering and load balancing techniques. Employ Content Delivery Networks (CDNs) to disperse traffic and minimise the possibility of outage.

Acknowledgement

The authors like to acknowledge the Centre for Research Excellence & Incubation Management (CREIM) at Universiti Sultan Zainal Abidin (UniSZA) for their provision of facilities, and encouragement in the pursuit of research and development. The authors would like to express their gratitude to the Research Management Office (RMO) of Universiti Malaysia Terengganu (UMT) for providing sponsorship for the publication of this article.

References

[1] Springall, Drew, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, and J. Alex Halderman. "Security analysis of the Estonian internet voting system." In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pp. 703-715. 2014. https://doi.org/10.1145/2660267.2660315

[2] Kovic, Marko. "Blockchain for the people: Blockchain technology as the basis for a secure and reliable e-voting system." (2017). https://doi.org/10.31235/osf.io/9qdz3

[3] Essex, Aleksander. "Internet voting in Canada: a cyber security perspective." *Brief submitted to the House of Commons Special Committee on Electoral Reform (Canada). Retrieved from< https://www. ourcommons. ca/Content/Committee/421/ERRE/Brief/BR8610535/br-external/EssexAleksandere. pdf* (2016).

[4] Ayed, Ahmed Ben. "A conceptual secure blockchain-based electronic voting system." *International Journal of Network Security & Its Applications* 9, no. 3 (2017): 01-09. https://doi.org/10.5121/ijnsa.2017.9301

[5] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

[6] Monrat, Ahmed Afif, Olov Schelén, and Karl Andersson. "A survey of blockchain from the perspectives of applications, challenges, and opportunities." *Ieee Access* 7 (2019): 117134-117151. https://doi.org/10.1109/ACCESS.2019.2936094

[7] Kamil, Mustofa, Ankur Singh Bist, Untung Rahardja, Nuke Puji Lestari Santoso, and Muhammad Iqbal. "COVID-19: Implementation e-voting blockchain concept." *International Journal of Artificial Intelligence Research* 5, no. 1 (2021): 25-34. https://doi.org/10.29099/ijair.v5i1.173

[8] Wu, Yifan. "An e-voting system based on blockchain and ring signature." *Master. University of Birmingham* (2017).

[9] Rahmadika, Sandi, Diena Rauda Ramdania, and Maisevli Harika. "Security analysis on the decentralized energy trading system using blockchain technology." *Jurnal Online Informatika* 3, no. 1 (2018): 44-47. https://doi.org/10.15575/join.v3i1.207

[10] Choudhary, Kushal Chaganlal, Saurabh Achal Agrawal, Mihir Manohar Gadhe, and Mrs Rohini Pise. "Decentralised voting with Ethereum blockchain."

[11] Arun, V., Aditya Dutta, Sourav Rajeev, and Rohan Varghese Mathew. "E-Voting using a Decentralized Ethereum Application." *International Journal of Engineering and Advanced Technology (IJEAT)* 8, no. 4 (2019): 830-833.

[12] Arun, S. S., S. Spoorthi Shibani, Vaishnovi R. Kamath, and D. C. V. Raj. "Blockchain Enabled E-Voting System." *Int. J. Adv. Res. Comput. Commun. Eng* 8, no. 4 (2019): 77-81. https://doi.org/10.17148/IJARCCE.2019.8412

[13] Oliva, Gustavo A., Ahmed E. Hassan, and Zhen Ming Jiang. "An exploratory study of smart contracts in the Ethereum blockchain platform." *Empirical Software Engineering* 25 (2020): 1864-1904. https://doi.org/10.1007/s10664-019-09796-5