JSCDM

http://penerbit.uthm.edu.my/ojs/index.php/jscdm
e-ISSN : 2716-621X

Journal of Soft Computing and Data Mining

UTHM E-Voting System Using Blockchain

Nur Hafizah Mohamed Kassim[1], Noraini Ibrahim[1*]

[1]Software Engineering Research Group (SERG), Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, Parit Raja, 86400, MALAYSIA

DOI: https://doi.org/10.30880/jscdm.2022.03.01.004
Received 01 February 2022; Accepted 01 April 2022; Available online 01 June 2022

Abstract: UTHM E-Voting System using Blockchain is a web-based system that develops to enhance and help to improve the efficiency of the existing system and also make the UTHM election process run smoothly and efficiently. In this system, the advantages of blockchain technology are used in the E-Voting system to make it more secure and effective. Lack of security is a primary concern of the current UTHM voting system, such as authentication, confidentiality, integrity, and non-repetition. Besides, the voting process can be inconvenient due to the limited number of polling stations. The distance between these polling stations and college residences causes difficulties for the students to go to a polling station. Moreover, students have to line up for some time before they can vote, which means that some of them leave without even voting. Finally, communication problems cause much misunderstanding between the election council, which is the Jawatankuasa Pemilihan Majlis Perwakilan Pelajar (JPMPP), which leads to an electoral process that cannot function smoothly. Thus, the UTHM E-voting system using blockchain is developed to overcome those problems in this project. The Prototyping Model drives the activities in this project with five main SDLC phases: planning, analysis, design, prototype, and implementation, which are very flexible compared to other software process models. This system is a web-based system that is developed using PHP as programming language and MySQL as database software. This system uses blockchain technology and the ring signature algorithm when conducting and counting the vote to improve the security of the electronic voting system. The test result shows that the system passed 25 of the 25 test cases, accounting for 100% of all the test cases. To conclude, this system is useful because it can improve the efficiency of the entire electoral process compared to the manual system that facilitates the management of the electoral process.

Keywords: Blockchain, E-Voting system, ring signature algorithm, security

1. Introduction

Universiti Tun Hussein Onn Malaysia (UTHM), is one of the public universities in Malaysia primarily focusing on Engineering and Technology. Currently, UTHM has more than 15,000 students, including international students from 22 countries all over the world. The Student Representative Council, also known as Majlis Perwakilan Pelajar (MPP), is a very important organization in every university to represent the student's voice. They are basically the student representatives of academic as well as the social issues faced by the students.

The student representative election in UTHM has been held for many years. The election is usually held yearly and will be arranged by the *Jawatankuasa Pemilihan MPP (JPMPP)*. It is very important because it symbolizes students being involved in choosing the right student representative and making changes in the Student Representative Council. The flow of the election process is similar to the election process in Malaysia. All the information regarding the election, such as the election date, the nomination process, and the campaign process, are distributed by the *Jawatankuasa Pemilihan MPP (JPMPP)* because they are the organization that is responsible before, during, and after the election process.

The current UTHM E-voting system has been enhanced and improved using blockchain technology. The existing system only provides the normal E-voting system where voters (who are UTHM students) must go through a normal

*Corresponding author: noraini@uthm.edu.my

voting process which is similar to the paper-based voting process with only a slight change where a voter submits his/her vote electronically. However, the voters are still required to cast in appointing polling stations which can be inconvenient due to the limited number of polling stations. The distance between these polling stations and college residences causes difficulties for the students to go to a polling station. During the election day, students need to juggle their responsibilities with learning activities and participate in the election where they can cast their vote. Moreover, students have to queue for so long before they can cast their vote, resulting in some of them leaving without even casting their votes. The current voting system of UTHM consumes a lot of energy, cost, and time which leads to the election process becoming difficult and inconvenient. Last, the communication issues among the departments of the election council, which is the *Jawatankuasa Pemilihan Majlis Perwakilan Pelajar (JPMPP*) have caused a lot of misunderstanding between them, which makes the election process cannot run smoothly.

Thus, the UTHM E-Voting system using Blockchain is developed to address these issues. There are three main objectives of this project. They are designing an enhanced system of the UTHM E-Voting System with blockchain technology, developing the system using an object-oriented approach, and then testing it by conducting several test cases in order to ensure its effectiveness. The system's users can be categorized into the Election Authority (EA), Registration Authority (RA), and Voters. The Election Authority can login into the system, manage the voting event and manage the blockchain. The registration authority can also log into the system, manage candidates, manage voters, and generate results. Lastly, the Voters can cast a vote. Therefore, the development of this system is important to secure the electoral process and engage students in the upcoming elections. The electoral process of the UTHM must proceed smoothly and efficiently.

The following will be organized into four sections. Section 2 discusses the related works of this project. Section 3 focuses on methodology. Section 4 discusses the outcome and discussion of the system results. Lastly, Section 5 addresses the conclusion of the project.

2. Related Works

This section discusses all the related works collected to develop the developed system.

2.1 E-Voting System

Democracy is a system of voters electing representatives by voting [1], [2]. Electronic voting systems have been in use since the 1960s, and it has been an area of research focus for many years. The term electronic voting refers to the use of computers, computerized equipment, or any electronic means and the incorporation of information technology to cast votes in an election process. The direct electronic recording systems (DRE) with interfaces almost just like an automated teller machine (ATM) have also successfully introduced e-voting technology to be used by the voters. These systems are nearly the same as the regular voting system, with a little difference. Besides, casting the votes is usually called the front-end of the election, while counting the ballot is known as the back-end. [3]. Suppose voters grasp the voting system very well. In that case, the usability of the system can be significantly improved, and the purpose of this e-voting system is to increase the number of voters that cast a vote, decreasing the cost of the election process and enhancing the accuracy of the voting result can be achieved [4]. However, the technical threat to the e-voting system has always been a concern [5], but this problem can be overcome with the use of distributed ledger technology such as blockchain.

2.2 Blockchain Technology

Nakamoto [6] was the first to introduce the blockchain and proposed a peer-to-peer (P2P) electronic cash system, which describes the decentralized P2P network that allows a transaction by using the Internet without the need for any central authority. Fig. 1 shows the method of generating a Bitcoin address from the public key. The blockchain is the backbone of bitcoin as it can create a transaction and verify it but can remain transparent to any users with the use of cryptography to secure the transaction. For addressing and transaction signing, bitcoin uses public and private keys. A Bitcoin private key is a random 256 bits. Users use this key to sign their transactions every time they transfer Bitcoin. Users randomly generate the private key. The public key is derived from the private key through an elliptic curve crypto- algorithm, specifically `secp256k1`. The public key is an (x,y) pair resulting from the `secp256k1` equation multiplied by the generator. This generator is fixed in Bitcoin systems, which means that the public key uniqueness is not guaranteed by the generator but is guaranteed by the private key's uniqueness. A public key hash is produced using `SHA256` and `RIPEMD160` hashing algorithms. The fingerprint of a public key, called the public key hash, has 160 bits. The public key is `Base58Check` encoded to generate the Bitcoin address. Since this address is generated from a private key that contains no secret information, addresses can be known to the public [7]. Fig. 2 shows the structure of blockchain. The blockchain is a data structure that contains a block of transactions. The first block of the blockchain is known as 'Genesis Block', which is a special block and also known as the foundation of the stack because it does not refer to the previous block as the other block in the chain that will be linked to the previous block in the chain. Each

block has a transaction data part, copies of the transaction that has been hashed, and then the hashes are paired and hashed again; this continues until a single hash remains.

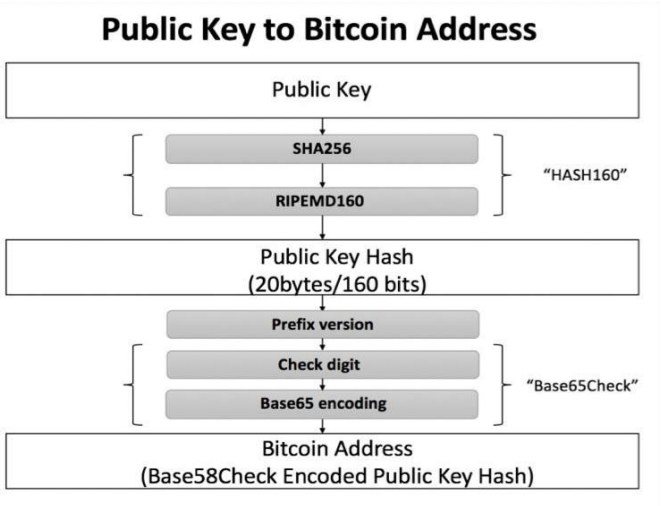

Fig. 1 - Method of generating Bitcoin Address from public key [7]

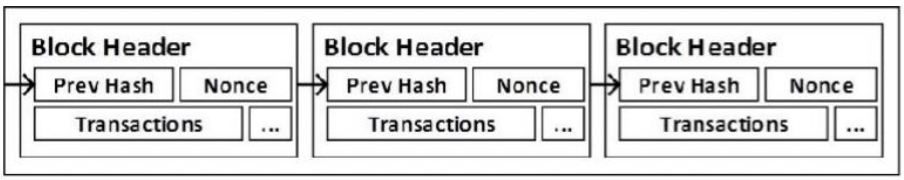

Fig. 2 - The structure of blockchain [7]

2.3 Ring Signature Algorithm

Rivest [8] first proposed the ring signature algorithm. The technology is in the simplified group signature [9], which is a type of digital signature that can be performed by using the cryptographic keys of any ring members in the group. Each ring member in the ring signature scheme is anonymous and equal. This ring signature scheme will be divided into three-part: generating a key pair, generating a ring signature, and verifying the signature. Firstly, the signer will randomly select the public keys of multiple ring members and combine their public and private keys, random numbers, and other technologies to complete the signature. Then, only the verifier of the signature can verify that the signature comes from this signature set, but the verifier would not know who signed the signature [10]. Therefore, with an in-ring signature, we can conclude that the security feature is its anonymity. Even if anyone has stolen the voter's private key, the possibility of exposing the identity is almost impossible. Hence, this ring signature algorithm is suitable for a voting system because all transactions default to an anonymous transaction. The anonymous functionality will not be affected by any centralized organization.

2.4 UTHM E-Voting System

The current UTHM E-Voting System consists of eight modules: the vote session module, voter module, candidate module, open session module, voting results module, user account module, logs, and reset vote count module. Fig. 3 shows the As-Is Model for the current UTHM E-Voting system. Firstly, the election authority needs to log in to the system with a valid ID and password and activate the open session so that the voter can log in to the voting system. Once the voter has logged in to the system, they cannot exit from the system until they have finished their voting process. In order to log out from the page, a security password is required. Then, the voter needs to cast a vote by choosing the candidate list that has been displayed on the screen. Finally, the vote will be counted, and the result will be produced.

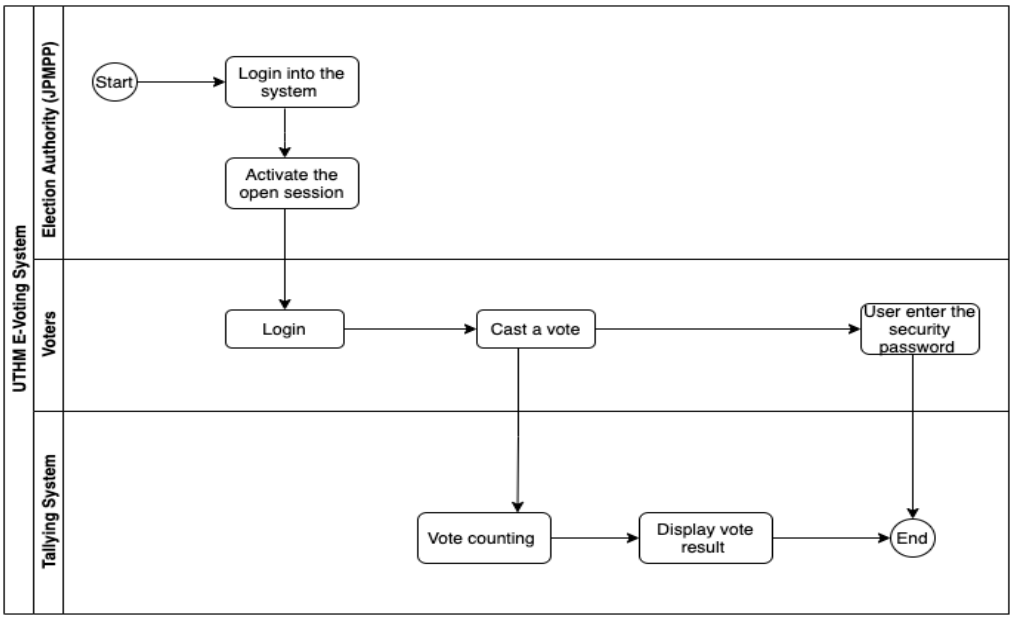

Fig. 3 - The as-is model of the UTHM E-Voting system

2.5 Study of Existing Related Systems

A study of the existing system has been conducted on three existing systems in the market. This study is conducted so that the system developer can analyze and identify the advantages and disadvantages of the existing systems to use them as a reference when developing the system. The three existing related systems that have been chosen are The Brazil Smartmatic E-Voting System [11], Estonian Internet Voting System [12], and The Votebook New York University Voting System [13]. Table 1 shows the comparison between the existing related systems and the developed system based on the characteristics and features of the systems.

Table 1 - Comparison of the system

Features/ System	Smartmatic E-Voting System [11]	Estonian Internet Voting System [12]	Votebook New York University Voting System [13]	UTHM E-Voting System using Blockchain
Platform	Local Software	Local Software	Local Software	Web-based
Technology / Algorithm	Biometric	Asymmetric Cryptography	Permission Blockchain & Key Pair Encryption	Blockchain & Ring Signature Algorithm
Log In	No	Yes, for Voters (ID Card & Pin Code)	No	Yes, for Election Authority & Registration Authority
Verification Process	No	No	Yes	Yes
Ballot Confidentiality	No	No	Yes	Yes
Transparency	No	No	Yes	Yes
Data Anonymity	No	No	Yes	Yes
Remote E-Voting	No	Yes	No	Yes
Universal Usability	Yes	No (only available in Russian language)	Yes	Yes
Users	Voters & Election Authority	Voters & Certificate Authority	Voters & Election Administrators	Voters, Election Authority & Registration Authority

Table 1 shows that every system has its advantages and disadvantages. It also shows some similarities to the other system, such as using blockchain technology to improve the system's usability and make the system more safe and secure to be used. Hence, this developed system will consider adapting the same similarities in the existing system with an enhancement.

3. Methodology

A prototyping model has been chosen to drive the development of the UTHM E-Voting System using blockchain. The prototyping model is a systems development method that involves exploring ideas and quickly developing a prototype based on preliminary requirements revised through the end-user's feedback [14]. The system is developed in 2 iterations. This model works best in conditions where the project requirements are not fully known in detail and are unclear. It also requires a full commitment between the developer and the stakeholders. This model consists of five main phases: planning, analysis, design, prototype implementation, and final implementation. Figure 4 shows the phases of the prototyping model. Table 2 shows the software development activities and tasks conducted for the entire project development.

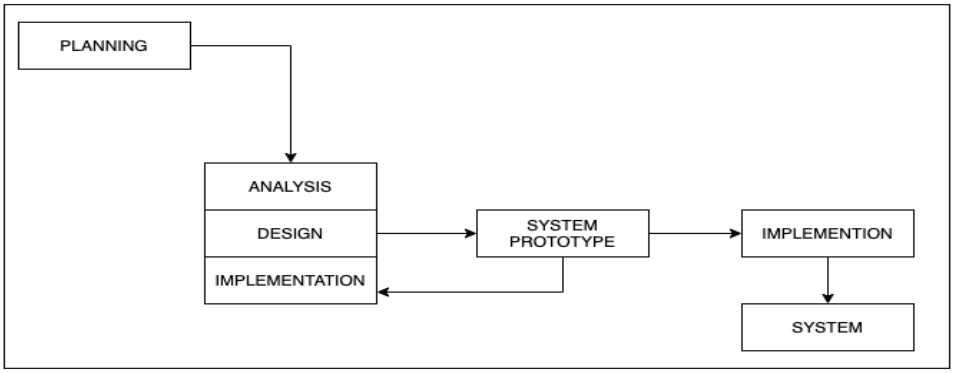

Fig. 4 - The phases of prototyping model [13]

Table 2 - Software development activities and their task

Phase	Task	Output
Planning	• Proposed the project • Determine the project scope, objectives, problem statements, and significant and expected results. • Determine the project schedule, activities and output • Interview the stakeholders.	• Project proposal • Gantt chart
Analysis	• Analyse the existing system. • Analyse the software and hardware requirements. • Choose the best methodology. • Develop the use case diagram, activity diagram, sequence diagram, and class diagram using Draw.io	• Literature review • Swimlane diagram (As-Is and To-Be Diagram) • Requirement specification • Hardware and software specification • Use a case diagram • Activity diagram • Sequence diagram • Class diagram
Design	• Design the system interfaces. • Design the database.	• System interfaces • Data dictionary
Prototype Implementation	• Develop 2prototypes. • Collect the feedback from stakeholders. • Refined the prototype • Develop and connect to the database (MySQL)	• Prototype 1 (The interfaces of the system) • Prototype2 (The connection between the interfaces and the database) • Stakeholder's feedback

Phase	Task	Output
Final Implementation	• Develop the program code using PHP. • Develop the system. • System testing.	• The UTHM E-Voting System using blockchain • Test cases report • Requirement Traceability Matrix (Test cases vs. Requirement)

4. Result and Discussion

This section will discuss and show the outcome of this system's analysis, design, implementation, and testing in detail.

4.1 Analysis

The analysis outcome for this system is specified in the forms of a Swimlane diagram, use case diagram, activity diagram, class diagram, and requirement definition. The UTHM E-Voting system using blockchain has three users. They are the election authority that focuses on managing the vote and blockchain. The registration authority focuses on managing the voter by sending them an email of the voting system link and managing the candidates and the voter, which focuses on the verify access before and during the election day and casting a vote. The current business process (As-Is Model) mentioned in Figure 3 is improved to the new business process (To-Be Model) as shown in Fig. 5.

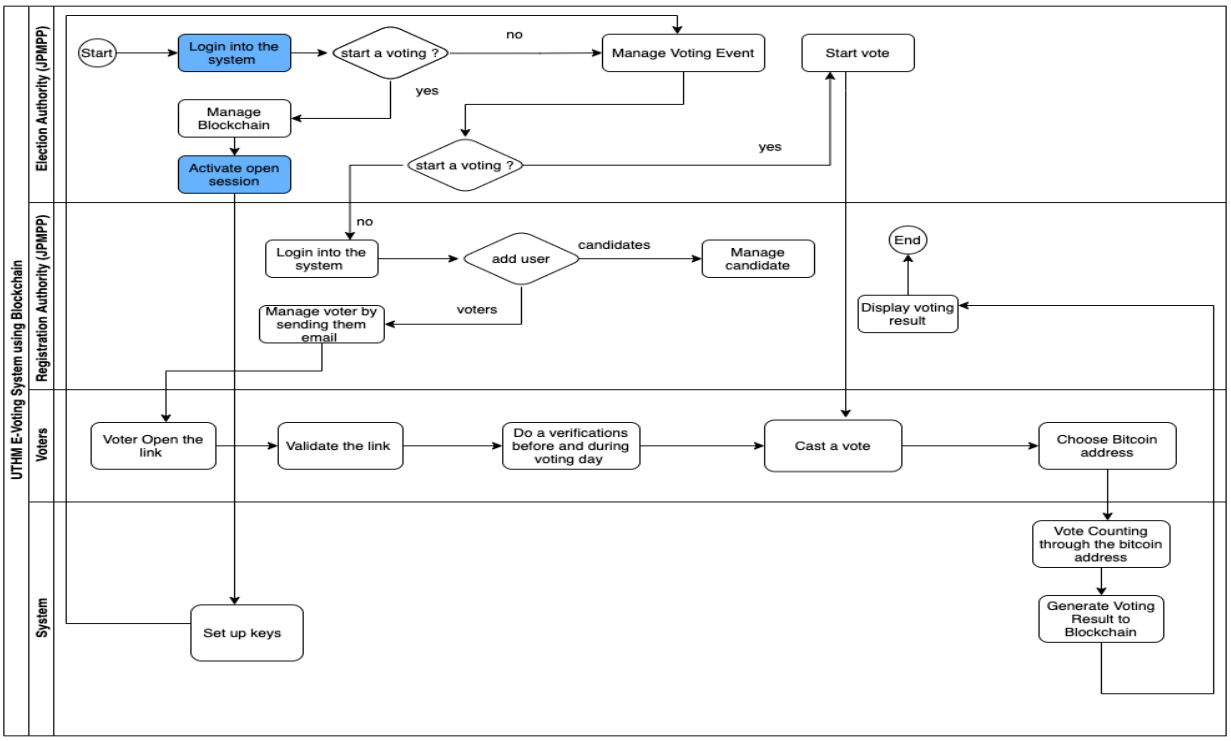

Fig. 5 - The to-be model of the developed system

Three actors are involved in the UTHM E-Voting system using blockchain. They are voter, election authority, and registration authority. There are seven prominent use cases in this system. They are shown in Fig. 6.

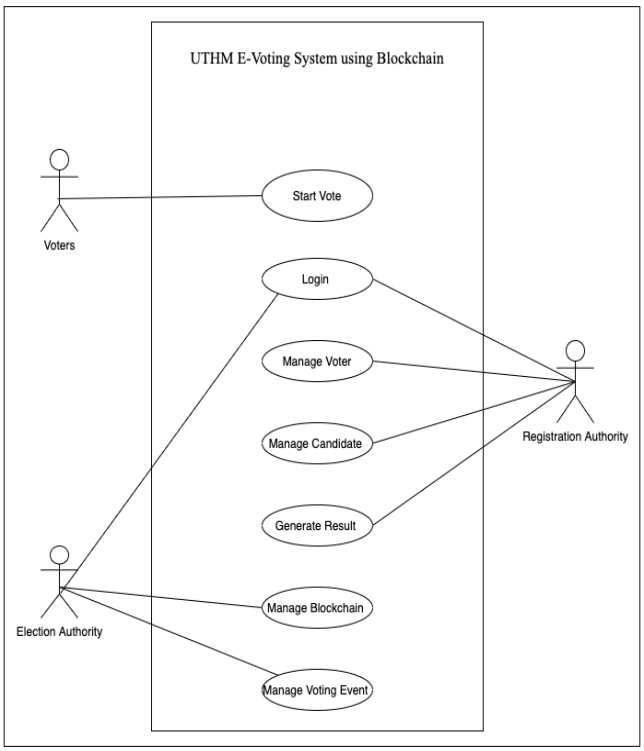

Fig. 6 - The use case diagram of the developed system

There are six classes in the system as shown in Fig. 7. They are *user*, *candidate*, *vote*, *key*, *signature*, *faculties*, and *code.*

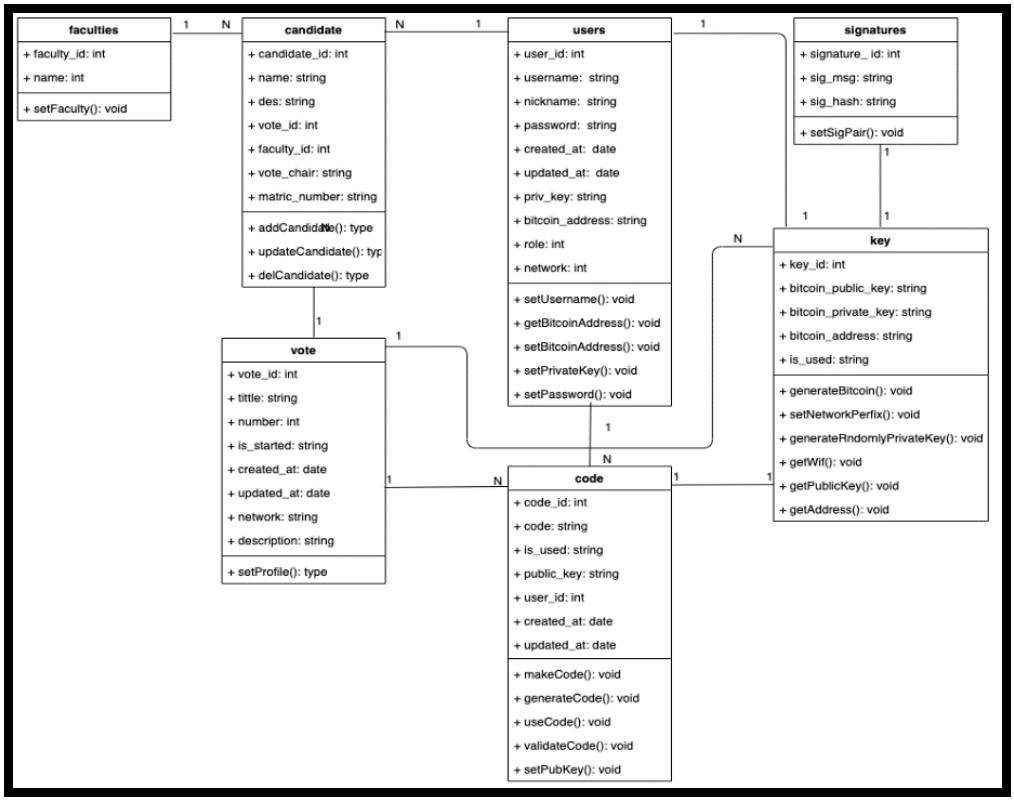

Fig. 7 - The class diagram of the developed system

4.2 Design and Implementation

There are several different processes in implementing an E-Voting system using blockchain than conventional systems. In this UTHM E-Voting system using blockchain, the election authority has to set up the address of the blockchain, as shown in Fig. 8.

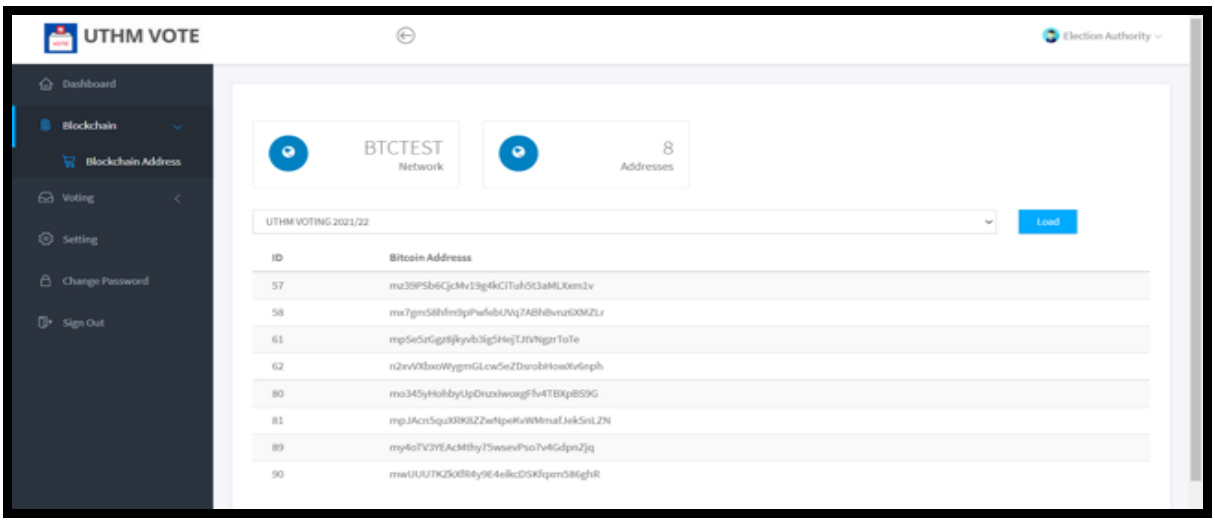

Fig. 8 - The manage blockchain interface

Before the voting starts, the voter will receive an email, and they need to complete the first verification process. Then, they can cast a vote and do the second verification on the day of the election. They will receive a receipt at the end of the process. The Registration Authority can choose the voting item at the end of the voting session, as shown in Fig. 9.

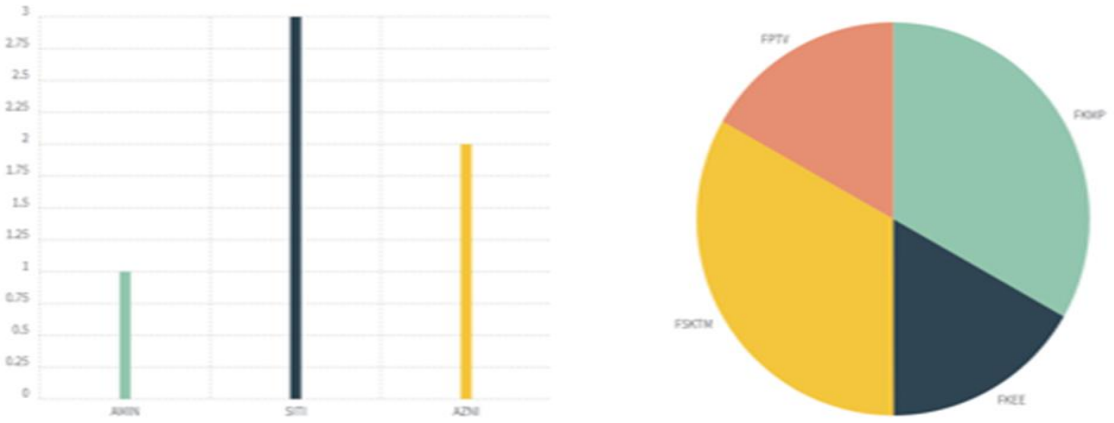

Fig. 9 - The results

4.3 Testing

Functionality testing has been conducted on the system. The testing has been conducted driven by the test cases listed in Table 3. The testing status of each test case is also included in the table.

Table 3 - List of test cases

Test Cases	Software Requirement	Description	Status
STD TEST_100	**SRS REQ_100**	**Login Module**	**Pass/ Fail**

Test Cases	Software Requirement	Description	Status
TEST_100_001	REQ_100_101	The Election Authority and Registration Authority log in to the system by entering their valid ID and password.	Pass
TEST_100_002	REQ_100_101	The Election Authority and Registration Authority cannot log in into the system by entering their invalid ID and password	Pass
STD TEST_200	**SRS REQ_200**	**Manage Voter Module**	**Pass/ Fail**
TEST_200_001	REQ_200_201	The Registration authority adds a voter by completely filling the form.	Pass
TEST_200_002	REQ_200_201	The Registration authority cannot add a voter if the form is not completely filled.	Pass
TEST_200_003	REQ_200_202	The voter receives an email from the Registration Authority.	Pass
STD TEST_300	**SRS REQ_300**	**Manage Candidate Module**	**Pass/ Fail**
TEST_300_001	REQ_300_301	The Registration Authority adds a candidate by completely filling the form.	Pass
TEST_300_002	REQ_300_301	The Registration Authority cannot add a candidate if the form is not completely filled.	Pass
TEST_300_003	REQ_300_302	The Registration Authority edits the candidate.	Pass
TEST_300_004	REQ_300_303	The Registration Authority delete the candidate.	Pass
STD TEST_400	**SRS REQ_400**	**Manage Voting Event Module**	**Pass/ Fail**
TEST_400_001	REQ_400_401	The Election Authority creates a voting event by completely filling out the form.	Pass
TEST_400_002	REQ_400_401	The Election Authority to create a voting event if the form is not completely filled.	Pass
TEST_400_003	REQ_400_402	The Election Authority edits a voting event.	Pass
TEST_400_004	REQ_400_403	The Election Authority start a voting event.	Pass
TEST_400_005	REQ_400_404	The Election Authority start a voting event.	Pass
TEST_400_006	REQ_400_405	The system should allow the Election Authority to view the candidate of a voting event.	Pass
STD TEST_500	**SRS REQ_500**	**Manage Blockchain Module**	**Pass/ Fail**
TEST_500_001	REQ_500_501	The Election Authority set up the address of the blockchain	Pass
STD TEST_600	**SRS REQ_600**	**Generate Result Module**	**Pass/ Fail**
TEST_600_001	REQ_600_601	The result of the whole election process can be generated.	Pass
STD TEST_700	**SRS REQ_700**	**Start Vote Module**	**Pass/ Fail**
TEST_700_001	REQ_700_701	The voters open the code link from the voter's email.	Pass
TEST_700_002	REQ_700_701	The voters open the code link from the voter's email when it is already expired.	Pass
TEST_700_002	REQ_700_702	The voters open the link that will redirect the voter to a different page which is the voting system.	Pass
TEST_700_003	REQ_700_703	The voters do the verification process if the link has expired.	Pass
TEST_700_004	REQ_700_703	The voters do the verification process before the election by generating the public key and saving it in the system.	Pass
TEST_700_005	REQ_700_703	The voters do the verification process before the election by generating a private key and saving it on the device.	Pass
TEST_700_005	REQ_700_703	The voters cannot cast a vote during the election day before doing the verification.	Pass
TEST_700_006	REQ_700_704	The voters do the verification process again by pasting the same private key in order to allow the voter to cast a vote on the election day.	Pass
TEST_700_007	REQ_700_704	The voters cannot do the verification process again if pasting the wrong private key and are not allowed to cast a vote on the election day.	Pass

Test Cases	Software Requirement	Description	Status
TEST_700_008	REQ_700_705	The voters cast a vote on the election day.	Pass

The summary of the overall test case result is recorded in Table 4. It shows that the system passed 25 of the 25 test cases, accounting for 100% of all the test cases.

Table 4 - The overall result of the test case

Test Cases ID	Total Test Cases	Total Success	Total Fail
STD TEST_100	2	2	-
STD TEST_200	3	3	-
STD TEST_300	4	4	-
STD TEST_400	6	6	-
STD TEST_500	1	1	-
STDTEST_600	1	1	-
STD TEST_700	8	8	-
Total	25	25	-

5. Conclusion

In conclusion, the UTHM E-Voting System using blockchain technology has been completely developed into a complete system. This system has several advantages, such as it can minimize human activity where the student (voter) does not have to go to the polling station to cast a vote and have high security and privacy with the use of the blockchain because no one will know who the voters vote for, it can improve the efficiency of the entire election process compared to the current system because it can help save the student time because the student no longer has to queue for so long to cast a vote, only the legal voter can vote because the RA will send the link code to the voter's email. They need to verify it before casting a vote, and the result of the voting cannot be influenced or modified by anyone or anything because all votes have been sent to the blockchain. However, there are some limitations of this system. It needs high technical understanding from the stakeholder to use this system because they must understand how blockchain works before using this system. It consumes a lot of effort from the stakeholders to use this system. This system also needs several preliminary steps before and during the election session, like verification. The system cannot combine the general and faculty representatives' votes in the same voting event. The complexity of blockchain may make it difficult for people to accept blockchain-based electronic voting, which could be a substantial obstacle to the widespread adoption of blockchain-based electronic voting. Hence, some recommendations for improvement in the future can be made, such as improving the user interfaces design and expanding its use through the development of mobile phone website technology that can be applied to this system when students can easily cast a vote using their smartphone and improve the system by combining the vote for general and faculty representative on the same voting event. Hopefully, this system can help the JPMPP UTHM in conducting the election process, making the election process more manageable, convenient, and efficient, and will attract the voters (who are UTHM students) to participate in the election process.

Acknowledgement

The authors would like to thank the Software Engineering Research Group (SERG) and Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia for their support and encouragement throughout the process of conducting this study.

References

[1] Racsko, P. Blockchain and Democracy. (2019). Soc. Econ. 41, 353–369.
[2] Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. (2019. Blockchain technology overview. arXiv, arXiv:1906.11078.
[3] Riera, A., & Brown, P. (2003). Bringing Confidence to Electronic Voting. Electronic Journal of E-Government, 1(1), 43–50.
[4] Ghassan Z. Q., Rani T. (2007). Electronic voting systems: Requirements, design, and implementation, Computer Standards & Interfaces, 29(3), 376-386.
[5] Ahmed, B. A. (2017). A Conceptual Secure Blockchain-Based Electronic Voting System. International Journal of Network Security & Its Applications (IJNSA), 9(3), doi: 10.5121/ijnsa.2017.9301.

[6] Nakamoto, S. (2018). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved on January 30, 2021, from https://bitcoin.org/bitcoin.pdf.
[7] Lee, K., James, J. I., Ejeta, T. G., and Kim, H. J. (2016). Electronic Voting Service Using Block-Chain, Journal of Digital Forensics, Security and Law, 11(8), doi: 10.15394/jdfsl.2017.1383.
[8] Rivest, R. L., Shamir, A., and Tauman, Y. (2001). How to Leak a Secret. Proc. ASICRYPT. New York, NY, USA: Springer-Verlag, 2248, https://doi.org/10.1007/3-540-45682-1_32
[9] Bleumer, G. (1991). Group signatures. Advances in Cryptology – EUROCRYPT. New York: Springer-Verlag, 250–252.
[10] Li, X., Mei, Y., Gong, J., Xiang F., and Z. Sun, Z. (2020). A Blockchain Privacy Protection Scheme Based on Ring Signature. IEEE Access, 8, 76765-76772, doi: 10.1109/ACCESS.2020.2987831.
[11] Sheeba, A., Vinaye,A., Sameer, S., and Yatin, D. (2012). Comparative study of electronic voting models and a proposed security framework for the implementation in Mauritius, IEEE Symposium on Humanities, Science and Engineering Research, 1187-1192, doi: 10.1109/SHUSER.2012.6268798.
[12] Clarke, D., & Martens, T. (2016). E-voting in Estonia. ArXiv, abs/1606.08654. Retrieved on January 30, 2021, from https://arxiv.org/abs/1606.08654.
[13] Kirby,K., Masi, A., Maymi, F. (2016). Votebook: A blockchain-based electronic voting system. The Economist. Retrieved on January 30, 2021, from https://www.economist.com/sites/default/files/nyu.pdf.
[14] Dennis, A., Wixom, B.H., & Tegarden, D. V. (2021). Systems Analysis Design UML Version 5.0 An Object-Oriented Approach, 5th ed. John Wiley & Sons, Inc.
[15] Kshetri, N.; Voas, J. (2018). Blockchain-enabled e-voting. IEEE Softw. 2018, 35, 95–99.