Blockchain-Enabled Election Voting System

Yong Cheng Loke
School of Computing
Asia Pacific University of Technology and Innovation (APU)
Kuala Lumpur, Malaysia
tp042222@mail.apu.edu.my

Nowshath K Batcha
School of Computing
Asia Pacific University of Technology and Innovation (APU)
Kuala Lumpur, Malaysia
nowshath.kb@apu.edu.my

Nik Sakinah Binti Nik Ab Ziz
School of Computing
Asia Pacific University of Technology and Innovation (APU)
Kuala Lumpur, Malaysia
nik.sakinah@staffemail.apu.edu.my

***Abstract*— This study carried out an investigation regarding the election voting system in Malaysia. The current voting method had used the traditional paper ballot as the voting method. Many voters had no trust towards current election voting system due to the weak security and low degree of transparency. The irrecoverable equipment such as paper ballot and indelible ink used during the election also very costly since it scaled based on the number of voters growing by years. Hence a new system had been proposed which is the Blockchain-enabled election voting system. Same as the current voting procedure, the voters also need to vote at the polling station but no longer vote using the physical ballot paper but the virtual vote instead. Blockchain had been recognized for its security and transparency due to its characteristics. The voters will log in the system using the PIN number which they will be noticed by the email. This report had carried the research for the domains and similar voting system implementation to get know of the voting process flow and the challenges met to prepare developer for the development in next semester. The research will used Python as the main language to develop and the environment tools had been specified. 4D methodology will be used as the for the whole development process. Besides that, document review and questionnaire had been selected to collect the data about the election law and the expectations of the voters towards the new system. The deliverables of the system will then suit the data analysed to produce the better one.**

Keywords—*Blockchain, Voting System, Election, security, questionnaire*

I. INTRODUCTION

Malaysia is one of the countries that practices the democracy system to appoint the governments. This process that chosen the government by the preference of the majority in decision-making process known as election. Under this process, citizens have the constitutional right to choose the person they want to governance the country based on their every single vote. Thus, a fair and transparency element are very essentially for this governance democratic system since it carries the ethical responsibility and concern from the people. In Malaysia, there are two types of election which are general election which consists of national and state level while another one is by-election. Different from general election, by-election is small size of the election and aims to fill the seat in Dewan Rakyat when it becomes vacant.

Although they are different type of election, but both use the paper ballot voting and follows the First Past the Post (FPTP) system which the voters only can cast once and the candidates with highest votes count won the election. FPTP is one of the plurality voting system and efficient for large scale of election. Other countries that practices FPTP are Canada, United States, United Kingdom, India and Yemen.

The process will oversee by Election Commission (EC). After the polling done, EC will count the votes publicly and announced the winners based on FPTP system. The elected candidates from by-election only responsible to hold the remaining term of the previous MP which means he or she will not go for full terms of five years.

Election is very important to Malaysia. It is not only the democratic symbolic, but it also represents the patriotisms and concern of the people towards the country. Nothing should affect or modify the results of the election contributed by the people voting. However, there are still several problems exist in our current election.

In the election, process transparency is always the issue. Based on the Malay Mail interview conducted in 2018, towards EC chairman Tan Sri Mohd Hashim Abdullah, he claimed that certain political parties who question the EC's transparency in conducting elections were unfair. This thing can be happened as long as the human are responsible for the monitoring stuffs. Lack of trust towards EC in human factor will keep growing although some efforts had been made such as approach of using indelible ink to indicate those who voted. In addition, EC need to announce each ballot vote publicly at the end of polling process. Due to the inefficiency of the process, the counting section may take sometimes especially there are a large scale of voters. The waiting time will be to long for everyone and unnecessarily if the votes count can be taken simultaneously with the polling.

The unawareness of the voters towards the ballot rules are extremely low. They did not know exactly the rules that will turn the votes cast categorized as spoilt votes. This caused not only the local votes, but the postal votes also cannot reach their support to the candidates. This kind of situation wasted the opportunity of them to fulfil their duty as the part of democracy system of the Malaysian citizens and their patriotism. The spoilage rates in GE13 ranging from 0.4% to 2.6% which estimated as 178,739 votes during the election. Although the rate is quite low, but for the polling results where one candidate won other candidates by less than 1% votes cast, then this situation will become serious matter.

In 12th election on 2008, a budget of total RM72 million was allocated for the 50,000 ballot boxes to replace the old versions. Besides that, tremendous number of voters also followed by huge amount of the paper ballot printing costs. In election 1995, RM11.42 million of the over RM42 million budget was spent on the paper ballot printing and election documents. In addition, the indelible ink to improve the

transparency costs RM6.9 million with total of 216,600 bottles and another RM200,000 for transport, pack and store the ink. The 48,000 bottles ink that bought with total of RM2.4 million for 2004 elections were not put in use and incinerated later. All of these consumable or non-recoverable will only keep gradually increasing the costs of the subsequent years. Although the election is very important and sacred, but the costs spent maybe too high for it.

Based on the problems mentioned, the proposed system Election Voting System using Blockchain provides a system where every voter can cast their vote using computers in polling station. The system will submit the candidates voted by the voters without any ballots, there would not be any spoilt votes caused by the dirty stain on ballots or the unappropriated marks in the candidates' column. The costs of the voting also can be reduced since the devices can be borrowed and reusable compared to paper ballot and ink. The most advantage of the system is the high transparency and security towards the election result compared to current voting method. People can view the votes count to the candidates during the process while staying anonymous for the name of people who voted to the candidates. The nature of blockchain also make the modification becomes extremely hard and even impossible

II. LITREATURE REVIEW

A. *Blockchain Concepts*

Blockchain, a peer-to-peer network introduced in October 2008 by Satoshi Nakamoto proposed for the Bitcoin which is the currency system that decentralized the centre authority by providing public ledger and shared the transaction records that are irreversible and incorruptible among the participating parties. After Bitcoin had been introduced for the few years, it soon achieved the notoriety in the whole market using the consensus model based on proof-of-work[1].

Proof-of-work records a public history of transactions that quickly makes the records impractical for an attacker to change computationally if majority of CPU power had been controlled by the honest nodes [2].

Another alternative of algorithm also had been proposed as the consensus model which is proof-of-stake to replace proof of work in order to provide most of the network security[3]. The mining power in Proof of Stake is given to the miners which determined by the coin's percentage held by them. Author of [4] supports the proof-of-stake due to numerous of distinct advantages over proof-of-work such as non-wasteful protocol, decreased likelihood of a 51% attack, potentially faster blockchains. There is other consensus algorithm risen that can suit better based on the application needs too such as Proof of Capacity and Proof of Burn. The blockchain is not only limited in cryptocurrency but other industry areas.

According to Iansiti and Lakhani[5] study, it stated that the time needed to transform the complex and novelty kind of applications into blockchain acceptance may take long time, but the last output can impact the economy. This emphasizes, the blockchain already been suggested to implement the applications in the voting. In blockchain, there is one sequence of blocks holds a complete list of transaction records like conventional public ledger [6].

The first block is known as Genesis Block or Block 0. Each block contains the information of the previous block except the first one. The chain line of transactional records is formed by the network participants (miners) by solving the computational problems [7]. The system wide mining power scales with the difficulty of the computational problems required to mine a new block [8].To keep the block-generation pace in a constant way, the difficult level is adjusted to suit that situation [8]. Blockchain also categorized as three types which are permission-less blockchain (Bitcoin), permission blockchain (consortium blockchain) and private blockchain (permitted by one entity) which can be used for different purposes.

B. *Blockchain voting system implementation*

The characteristic of the blockchain makes it no longer limited to crypto currency but also able to implement in the voting system too. There are many countries started to implement the blockchain concepts into the voting system. Estonia was the first country to implement the blockchain into their electronic voting system [9].

Soon after that, Switzerland also followed to adopt the voting system into the statewide election while another country, Norway implemented in council election [10]. Also supported that a blockchain-based voting system is more secured, reliable and anonymous which can increase the trust of people towards the government. In the implementation of blockchain, the study carried by [11] suggested that. the created block proposed shall contains the block ID, timestamp and three section consists of general election result, previous hashed block value and the digital signature which then broadcasting to the entire nodes. According to the experiment analysis carried by Gilbert and Handschuh[12] , the attack towards SHA-256 is very complex due to its characteristic which can produce different types of patterns and high computation probability. In 2016, the Democracy Earth Foundation had used a blockchain to give Colombian expatriates a chance to pass their voice in order to terminate the conflict between the Colombian government and FARC guerrillas. During the implementation of blockchain, the foundation claimed that the immaturity of technology is the main obstacle to pass through. While for the blockchain part, Zheng et al [13] argued that both consensus models in blockchain are having a phenomenon that proof-of-work consumes a lot of electricity energy while proof-of-stake consensus process can cause the phenomenon that the rich get richer.

C. *Challenges and Limitation of Blockchain Implementation*

To implement the blockchain in the application is not an easy stuff. According to Boucher[13] study, the complexity of blockchain concepts might hinder public acceptability of Blockchain-enabled Voting(BEV) as the mainstream application. Zheng et al [14] argued that both consensus models in blockchain are having a phenomenon that proof-of-work consumes a lot of electricity energy while proof-of-stake consensus process can cause the phenomenon that the rich get richer. . In addition, the maximum transaction per seconds(tps) in blockchain is 7tps which is much lesser than 2,000 tps in VISA and 5,000 tps in Twitter [15]. Based on the study carried by Eyal and Sirer[16], it stated that 51 percent attack, where the attacker controls more than half of the mining power in the public network can cause anomaly in the public blockchain

system which lead to double spending or even override the transaction block.

III. Existing Similiar Systems

In Geneva election, the citizens still can choose either online voting or ballot voting. Before the polling starts, the voters will receives a voting card attached with the documentation and ballot to fill in. If the voters select the card as their voting method, they need to take the card to the polling station on election day, hands it to the official site and votes in the ballot box. Another alternative will be the remote voting. In this method, they need to send the card back to ensure their votes would not be used. Now the card purpose can be revealed. This card contains unique 16-digit number allocated to the voter, a 4-digit control key and 6-digit secret code hidden under scratch-away opaque layer. Once the layer had been scratched away, the voters are no longer able to choose other methods to vote besides this one. The electronic vote mainly consists of two steps: establishing valid ballot and casting the ballot. Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you.

To establish the ballot, the voter needs to proceed the dedicated website and insert the 16-digit number. Then the server checks the frame and general conditions on the vote valid date, frame not being faked). If the conditions are met, the server immediately sends back the 4-digit key to the voter for self-authentication purpose and proceeds to construct the electronic ballot. When the ballot filling is done, the server invokes the electronic ballot box. Here comes the second layer of authentication by using the hidden secret code (something voter has) and specific information to that person(something voter knows). If the authentication passed, the transaction commits and a confirmation message (date and time the vote successfully registered) sends to the voter. The encrypted electronic ballot will send to one of three servers which running different operating system. After that the votes forwarded to the electronic ballot box in the centralized location. To reveal the votes count in the end of polling, the system requires the presence of two person delegated by each political party. Both has a private key that must be typed into the system so that the ballot count can be deciphered.

Due to the high population in Zurich, the voting system divided them into small communes which each of the communes using its own information system, manages own registered voter's list and its own votes count. For the voters who want to vote electronically, the communities shall enter those names who are eligible into the electronic ballot box. Then the Zurich's Statistical Office will then mail the special password to the citizens as part of the voting forms. For voting device, voters can choose either using one of the devices in the Fig 1.

To cast the vote through internet, voters shall log onto the dedicated website using the identification number and follow the instruction provided by the site. After casting the vote, voters need to enter the personal identification number (PIN) and the system will then compare the security symbol. If the matching passed, the system accepts the vote.

To cast the vote through mobile phone, voters need to enter codes to the dedicated phone number using short message system (SMS). Then insert the personal identification code (for example: g3387y55), name of the referendum (for example: sg1) and the 'Yes' or 'No' response (for example: er2 for 'Yes'). The final SMS message for the voting will be g3387y55 sg1 er2 for 'Yes' response in sg1 referendum. Next the system will ask for the PIN which is separated from the identification access code and the birth date for second authentication purpose. Once the authentication passed, the voter receives the confirmation that the vote had been casted into the electronic ballot box.

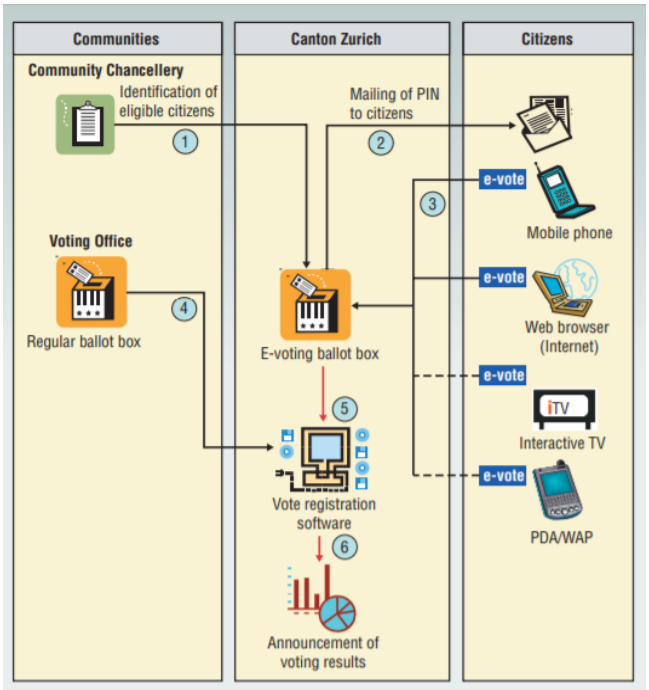

Fig. 1. Zurich e-voting process [17]

IV. Methodology of the Proposed System

4D phases consists of 4 main phases which are define, design, develop and deliver. In define stage, the basic requirements how the voting system should be worked will be gathered. Then a simple design for the diagram, process flow and database design can illustrate as the prototype blueprint. The developer will then develop the system based on it and finally delivered to the client to review it. The review collected is essential for the next cycle. After the review, the developer will start another cycle again. If there are additional requirements added, the developer needs to define them again and adds into the design parts. A new system developed from the previous will be presented to the client again for the review. This cycle ends once the requirements are met and the client is satisfied with the whole system.

The proposed system for this study is the election voting system that uses the blockchain implementation. The main concept of the blockchain used is to provide the decentralized of the voting record which avoid any tampering action towards the result. Based on the research found, the current voting system is using traditional paper ballot to cast the vote. There are also additional resources like the polling station setup, physical ballot box, indelible ink and lots of workforces

to ensure the election can run successfully. Therefore, the developed system has provided a platform for the Election Commissioner (EC) to conduct the election. The platform can record the voters who had been casted the vote and insert their vote into the Ethereum blockchain. No one is able to change the vote casted for the candidates selected in this process. The Fig. 2 and 3 illustrate the overall architecture for the core functions developed in both voter and officer side.

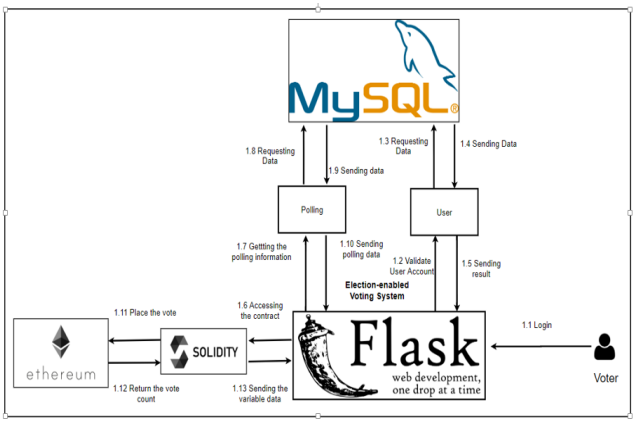

Fig. 2. System Architecture for Blockchain-enabled Voting System for Voter

The main users in this system are the EC officer who is able to create the polling events and view that information while the voters are able to cast the vote for their preference candidate and view the polling results. The application used the Flask as the web development framework which use Python. To access the data, the system needs to access the MySQL Workbench to retrieve the polling data and users account. Furthermore, there is no registration option for both officers and voters as the assumption stated that all of their data had been successfully inserted into database earlier.

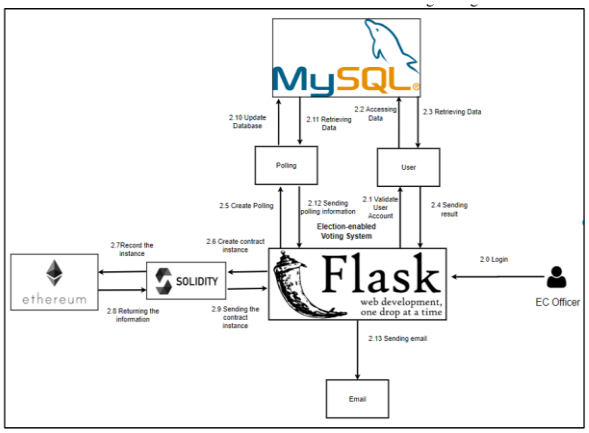

Fig. 3. System Architecture for Blockchain-enabled Voting System for Voter

For the EC officer, the accounts are already created at the beginning. He can create the polling events which included adding the candidates, selecting the date and time, and the polling location that determines the voters who can vote. After the polling created successfully, the system will auto generate the verification code for the eligible voters. The officer can then send the verification email carried with the PIN to those voters. Besides that, the polling created also has its own address value that associated with each unique Solidity contract.

While for the voters, their credential account is only given through the email when they are eligible to vote. They can then log in the system to cast the vote in the polling duration but they only able to view the result after the polling ends. The vote casted will then be added into the smart contract in the Ethereum blockchain. The polling result will then be inserted into the database for recording purposes but the final result will be based on the blockchain one instead. Hence, there is no reason to tamper the result in the database as it would not affect the original one.

V. Conclusion

Although the system has finally successfully developed there are functionalities that could be further enhanced or implemented. The developed contract only able to store the candidate names with the total votes received but not the complete candidate information which includes the political party and the personal photos. Since the current system is already able to handle the by-election. the future investigation can be carried out in conducting the General Election. The scope and more functionalities need to be identified correctly in order to ensure the performance and availability of the system in handling such a tremendous workload. The statistical feature also can be provided to assist the officer in promoting the election or taking as the measure to optimize the system performance. The smart contract also can be further enhanced to cover the necessary polling rules and agreements inside.

References

[1] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Tim´on, and P. Wuille, “Enabling Blockchain Innovations with Pegged Sidechains,”, 2014 Retrieved from http://www.blockstream.com/sidechains.pdf

[2] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2019.

[3] King, S. and Nadal, S., 2012. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. self-published paper, August, 19.

[4] V. Buterin, ‘‘Bitcoin network shaken by blockchain fork,’’ Bitcoin Mag., vol. 12, Mar. 2013. Available at: https://bitcoinmagazine.com/3668/bitcoin-network-shaken-byblockchain-fork/

[5] M. I. K. R. Lakhani, “The Truth About Blockchain,” The truth about blockchain,” Harvard Business Review, 95(1), pp.118-127.

[6] Lee, P., Lee, P., Guan, H., Dienstfrey, A., Theofanos, M., Stanton, B. and Schwarz, M.T., 2018. Forensic Latent Fingerprint Preprocessing Assessment. US Department of Commerce, National Institute of Standards and Technology.

[7] Böhme, R., Christin, N., Edelman, B, & Moore, T. (2015). Bitcoin: Economics, Technology, and Governance. Journal of Economic Perspectives, 29(2): 213-38, DOI: 10.1257/jep.29.2.213

[8] Dwyer, G. (2014). The Economics of Bitcoin and Similar Private Digital Currencies. July 8. dx.doi.org/10.2139/ssrn.2434628

[9] Madise, Ü. and Martens, T., 2006. E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world. Electronic voting, 86 (2006).

[10] Stenerud G.S and C. Bull, “When reality comes knocking Norwegian experiences with verifiable electronic voting”, Electronic Voting. Vol. 205. (2012), pp. 21-33.

[11] Kirby, K., Masi, A. and Maymi, F., 2016. Votebook. A proposal for a blockchain-based electronic voting system. The Economist. Accessed December, 14.

[12] Gilbert, H. and Handschuh, H. , " Security analysis of SHA-256 and sisters," In International workshop on selected areas in cryptography pp. 175-193. Springer, Berlin, Heidelberg, 2003.

[13] P. Boucher, What If Blockchain Technology Revolutionised Voting?, European Parliamentary Research Service, 2016; http://www.europarl.europa.eu/thinktank/en/document.html?reference 5EPRS_ATA(2016)58191

[14] Zheng, Z., Xie, S.,Dai, H-N., Chen, X. and Wang, H, " Blockchain challenges and opportunities: a survey," Int. J. Web and Grid Services, Vol. 14, No. 4, pp.352–375, 2018.

[15] Yli-Huumo, J., Ko, D., Choi, S., Park, S. and Smolander, K., " Where is current research on blockchain technology?—a systematic review,". PloS one, Vol. 11, p.e0163477, 2016

[16] I. Eyal and E. G. Sirer, " Majority is not enough: Bitcoin mining is vulnerable. Communications of the ACM, 61(7), pp.95-102, 2018.

[17] G. E. G. Beroggi, "Secure and Easy Internet Voting," *Computer*, Vol. *41*(2), pp.52-56, 2008.