International Journal of Engineering & Technology, 7 (4.11) (2018) 156-162

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Blockchain in Voting System Application

Nur Sakinah Burhanuddin, Fadhlan Hafizhelmi Kamaru Zaman*, Ahmad Ihsan Mohd Yassin, Nooritawati Md Tahir

Faculty of Electrical Engineering, Universiti Teknologi MARA, 40450 Shah Alam Selangor, Malaysia
**Corresponding author E-mail: fadhlan@salam.uitm.edu.my*

Abstract

Two of the most familiar method of voting is through voting polls and online voting. The main problem with conventional method is the insecurity of the votes to be untemper. Another problem of voting methods is the existence of fraud in voting system. This paper is to propose a method in overcoming these flaws and problems by using the Blockchain technology. Blockchain technology is a secured database and has very high security. The technical concept of the Blockchain technology has many advantages and benefits that could be applied to many technical sectors and have the possibility in changing the world. The concept for this project is to develop a cryptocurrency implementation in the voting system. From there, the transaction votes are kept in the blockchain could be illustrated by examining the block hashes. The outcome of the project shows a transaction of coins from one voter's wallet into two candidates' wallet. The transactions were approved through a process of mining and the transactions of coins were a success. The data of the transactions were kept in the blockchain where unique blockhash, which acted as the block's fingerprint were generated. From there, the integrity of the blockchain technology is illustrated.

Keywords: *Blockchain Technology; decentralized cryptocurrency; integrity; security; voting system.*

1. Introduction

Voting is vital in determining the disposition of any men in a society respecting to the adoption or acceptation of their position and their contribution to the community. It has been the method used since ancient history and are introduced and implemented largely in politics. Voting system is the basis of any elections in a democratic country, being the core of any elections.

In this advanced technological era, there are a couple of conventional voting methods ranging from manual ballot system to online voting system. These methods are used largely in the electoral system. Malaysia is one of the countries that are still using the manual ballot count voting system in their diplomat politics. Alternatively, advanced and more developed countries such as Estonia in the Europe have implemented and shifted into the online voting poll for their elections [2].

The main issue of current conventional voting system is the existing of the possibility of frauds in the electoral system itself. From year 1946 to 2000, the number of independent countries has increased from 67 countries to 190 and many of these countries have shifted into the democracy system since independence [4], Malaysia being one of it. Electoral institutions have much great importance in political science. There was a study made on the voting fraud in early twentieth-century in Pittsburgh, United State of America. The study mentioned how it is possible for current voting system could be padded with ghost voters [5]. In conclusion, there are still improvements that need to be implement on the voting system in order to eliminate the possibility of voting fraud.

With the possibility of this fraud, comes the issue of voter's confidence in the conventional voting method. The conventional method of voting polls does not have a system or proof that guaranties the security of the votes. Due to this reason, the voters lack confidence in the purity of the election's result. An example that shows in the insecurity of the vote result is in Estonia, who is the country to apply digital voting. During their 2013 Local Election, it was highlighted on the potential security risk within the system through malware infecting the system and allowing vote change [16]. Therefore, the system requires a more secure database in order to guaranty the reliability of the voting system.

Another matter in question that needs to be highlight is the low number of turn out due to the indolence of community in the actual voting process. In [3] states that in the United Kingdom, a result on a research conclude people who vote through posting, has a high report level of satisfaction and confidence in the whole voting process. An ideal alternative that could improve the voting system is voting through a secure online platform.

Every project proposed has its own objectives and purpose. The main objective of this project is to implement blockchain technology into voting system. Aside from that, the project is to evaluate the effectiveness of the Blockchain technology in the confidence of its security to protect information, specifically for voting. This technology is also believed to improve the reliability of current voting system and the process flow of voting to increase the voting turn-up.

The application of blockchain technology can be implemented on this problem where data or votes will be stored in a decentralized database, where security is verified by the public within nodes of network and are impossible for alterations [17]. Information in the sequential database of a blockchain is protected by methods of cryptographic proof and is a digital alternative to the conventional ledger. Thus, this technology promises a greater security in the election system to secure it against frauds.

2. Related Works

2.1 Blockchain Technology

2.1.1. What is Blockchain Technology?

Blockchain technology is a peer-to-peer secured, transparent, and decentralized public ledger that can be accessed and shared through any Internet network. An anonymous programmer known as Satoshi Nakamoto first introduced the blockchain technology, applying it in cryptocurrency [8]. It is a database that is made out of transactional record blocks that are chained together. Each block is validated by users within the network (also known as miners). This involves the validation of chain by solving complex computational functions.
The blockchain technology promises high-level security due to its decentralization characteristics. There is no centralized organization or party that controls it. The data in the network is an open access and can be viewed by anyone within the Internet network. The data in blockchain will have an exact copy in every node of network, resulting the alteration of information in the chain very complex, near to impossible. In the blockchain, any transactions of information require the exchange of public keys by the user which will generate addresses cryptographically and stored in the blockchain. Although the transaction is traceable, the identity of the user will not be disclosure and this transparency is one of the striking characteristics of the blockchain technology [12].

2.1.2. Mining, Hash Functions and Proofs

The blockchain technology is a public transaction ledger that involves a subset of network volunteers who are known as the miners, to validate the chain by solving some complex computational functions known as hash functions. When miners successfully solve the equation hash function, the next new block is added into the blockchain database [9]. The more miners involved in the mining process, the more complex the computational problems are. Primitively, individuals that use their home computers central processing units are sufficient. Since the blockchain technology has attract many attention, the rising complexity of solving algorithm requires greater power mining techniques such as using application-specific integrated circuits (ASIC), pool mining and cloud mining [9]. Every miner that successfully solve the functions will have their Proof-of-Work, which is a requirement to proof that the user have done the work to solve the problem. Proofs are also required for a new block to be generated. Another term that Proof-of-Work is always compared to is the Proof-of Stake. Proof-of-Stake is when the transaction block is generated based on the miner's or creator's digital wealth [10].

2.2 Cryptocurrency

Those who have heard about blockchain technology must have heard about cryptocurrencies as it has close relation and blockchain technology is originated from a cryptocurrency that is widely known, which is the Bitcoin. One of the top and legendary digital currencies that have stayed long in the industry is Bitcoin and Ethereum.

2.2.1. Bitcoin

Satoshi Nakamoto, an anonymous programmer has discovered the blockchain Technology through the production of Bitcoin. In another word, Bitcoin is the first byproduct of the blockchain technology and is now leading at top in the crypto market. Bitcoin works in a peer-to-peer network for payment transfer that can be done digitally without the third party. Bitcoin also proposes to prevent double spending by a peer-to-peer network that has a timestamp with hash algorithm that are attached to the particular transaction chain as a proof. The work done to solve the hashing function is called the proof-of-work [11]. Bitcoin is now on the top chart of the Cryptocurrency Market Capitalizations, standing on the first rank [12].

2.2.2. Blockchain Technology Applications and Related Research

With the striking characteristics of the Blockchain technology (a decentralized, reliable and redundant network where transactions and programs are not reversible), it has been implemented in other sectors than in the digital financing area. There are many related researches that have been found through this literature study, whether it is implemented in the voting system or not.
In [16], the authors elaborated on the digital voting system especially by examining the first country to implement a digital voting system, Estonia. Blockchain is the base underline architecture design for cryptocurrencies where the system is robust and highly secure, which transactions are stored in a block that will eventually be complete as many transactions are chained in. The Estonian Local digital voting elections uses the voter's identification number to identify their eligibility to vote and is then allowed to vote. The votes will be passed through a server and are encrypted and stored. The data are transferred to a DVD vote counting server that is private. However, in their 2013 elections some number of potential security risks was highlighted, where the risks are some possible malware in the clients and servers that allows change of votes. An implementation of the blockchain technology in the voting system was proposed.
Similar to the review done that was mentioned above, describe the potential applicability of blockchain technology and its characteristics to be implement in Canadian electronic voting system [17]. It is proposed that a system would require voters to vote in the system and be provided with random key pair for voting. Particular software is to require ensuring the voter's eligibility. The votes are visible, and a tally will be resulted. However, implementing the technology will require high cost, a board for integrity assurance and accommodation for voters. It will also be required to run in synchronized with the paper balloting system. Nonetheless, it is still concluded that blockchain technology is an excellent method in the vote result transmission and its implementation in the Canada electoral system was considered.
However, even though digital voting system is considered advanced and implementing the 21st century advances, it is still full of holes in the architecture, that blockchain could overcome. A paper written in [18] reviews and provides a proof on the integrity flaws of Electronics voting system. This review deploys the election legitimacy of Direct Recording Electronic (DRE) voting system. The project is aimed to assess the ease of bug introduction into a system, and their detection difficulties. The security oversight of DRE voting system is undetected multiple voting cast, possible access to voting machine to perform administrative actions and improper voting terminals and central server encryption. The assessment is done by conducting a project called Hack-a-Vote to proof that electronics voting system is not resistant to those security concerns.
A paper reference in [19] elaborates on the maximum voter's privacy by using a smart contract for boardroom voting. It develops a system called The Open Vote Network that uses an Internet voting protocol that self-tallies with a maximum voter privacy using smart contracts. This network does not rely on any authority to compute the tally of the result, nor does it rely on any authority to protect the voter's privacy in the voting process. Using the consensus mechanism of smart contract that is used in the Ethereum Blockchain enforces the Open Vote Network protocol. This implementation of network was tested with forty simulated voters, and the minimal setup for the elections cost only for $0.73 per voter.
In [a] states that despite being electronically online or not, the conventional method of voting has low level of transparency. Thus creating the lack of voter's confidence in the result, as it is impos-

sible to assure that the voter's vote is being counted for in the election result. Other than that, [a] mentioned on the electronic voting system that can be hacked, by giving Virginia's WIN voting machine as an example. The possibility level of hacking on that machine is high, until the responsible agency decided to discontinue the usage of that machine for official elections. There were many cases mentioned in [a], including the decision of the U.S president, Barrack Obama, to expel 35 Russian diplomats due to concerns in interference of Russia with the 2016 election. The adoption of blockchain network in the voting system was proposed to be a better-secured alternative in the voting system. Its trust ability, decentralized and distributed architecture could bring benefits in the voting system. In conclusion, blockchain in the voting system has attracted many attentions, to create a transparent, trustworthy and reliable voting mechanism.

3. Methodology

3.1. How Does It Work?

- Candidates – Each candidate will be assigned as a public key (transaction address) to the voter. To keep the secrecy of ballot, the public key (transaction address) is different for each voter. For the project simulation however is done using only one voter's wallet only, where it cast transaction votes to two candidates simultaneously.
- Voters – Each voter is also assigned their own wallet and public key (transaction address)
- Ballots – By using the public keys from candidates, voters, and organizers that have been recorded by the application, it can create a transaction sent to it once the voter confirms the vote. When the voter has confirmed the vote, the voter's ballot now has cryptographically secure representation in the transaction, and it is then broadcasted to the coin network nodes. However, even though the verification of the vote is not yet confirmed, the transaction will be shown after the voter's confirmation. After mining, the ballot is securely logged on the blockchain with an increasing number of networks.

3.2. Implementation of Blockchain Technology and Its Application

The blockchain technology is based fully on programming language codes. Thus, it is important to determine the programming language for this project. To structure the system of this project, C++ language will be used to write the blockchain system. The project will take the cloning of the Litecoin C++ Language, and alterations will be edited to the program.

Litecoin codes was forked as the base of the programming that later was modified to satisfy based on the characteristics and quality of this project. There are several reasons in choosing the Litecoin as the base of code, to be forked. One of it is because Litecoin has the similar features, as the first and predominant cryptocurrency existed, Bitcoin. In fact, Litecoin was forked from Bitcoin itself. A difference of Litecoin that is an upgrade from Bitcoin is that Litecoin is faster in the sense of transaction capacity, as its blockchain block confirmation is generated on average two and a half minutes, whereas Bitcoin's blocks are created every ten minutes. This feature is the main reason why Litecoin is chosen. The system needs to be able to create a block faster, so that the votes could be submitted into the blocks faster and does not lag the voting process.

3.3. Evaluation of the Blockchain Technology System

Upon completion of the structure of the database, an evaluation of the blockchain system itself needs to be monitored. A data test was conducted within small number of network. Any errors within the test was monitored and corrected. It is important that the blockchain database works, as it is the base system of the project. Monitoring the blocks' hash algorithm does the evaluation of this system.

3.4. Creating Custom Coin Called Kinakoin

The first step in creating the custom altcoin and its wallet for the use in the voting system was to clone the Litecoin. This was done successfully using the Linux command on a Virtual Machine of Ubuntu. The image below shows the success in cloning of the Litecoin git file.

Fig. 1: Cloning Litecoin Process

From this cloned coin, the parameters in files were changed and altered to satisfy the characteristics of the desired custom altcoin that is named Kinakoin. The parameters that were changed was:

- Prefix initials was changed to k, which sets all Kinakoin addresses to start with initial k.
- Number of coins per block was set to 10 coins per block.
- Total number of Kinakoin exists is set to be 22500
- Priority is set to 144, which means that the rate of blocks that was expressed within the difficulty period of 144 coins, then the difficulty will readjust.

After the parameters have been changed, the Kinakoin is then deployed and run. The image below shows that the Kinakoin and wallet is being built. After the process of coin building, we run everything on the testnet basis.

Fig. 2: Process of building the custom coin, Kinakoin

4. Results and Discussion

There are three Kinakoin wallet set up on three different Virtual Machines, with respect to their connections. The main Virtual Machine will contain the files and run the coin's wallet as the server and as well as simulated as the wallet where voters will cast their votes. The other two cloned virtual machines with their respective wallets act as the clients and will be simulated as the wallet of the candidates. The transaction of the coins from the voter's wallet to the wallet of the two candidates will be shown below.

Due to previous test and wallet testing and mining, the wallet of Candidate 1 has a balance of 668.90 KIN and Candidate 2 has a balance of 120.00 KIN. These values will be the reference value for the respective candidates as the initial Kinakoin balance in the wallet, before any transactions. The Immature shows the value of coins that has been mined into the wallet but has not yet been confirmed by miners.

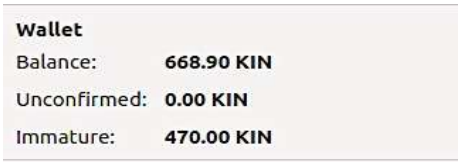

Fig. 3: Balance of Candidate 1's Wallet Before Any Transaction Simulation

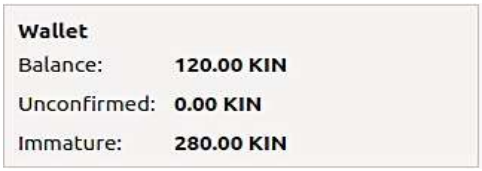

Fig. 4: Balance of Candidate 2's Wallet Before Any Transaction Simulation

It is given from the organizer to voters, the public address (public key) of the candidates and the address for the candidate. The transaction address of candidate 1 is kE94QQC6zgXFYLLgR21j8bheQXHgWdXg9V and the address of candidate 2 is kLojcXu7BpMNYeYeBRx2C31DALCtQMB9Xh. Below shows the transaction of money sent from the voter's wallet, to the candidates' respective address. The amount of coins was transferred were set to be 10 KIN. Thus, when voter sent 10 KIN to the candidate's wallet, the respective candidate wallets should receive and has increase amount of balance by 10 KIN. A notification of transaction will be popped up simultaneously on the voter wallet and candidates' wallet. Transactions to candidate 1 were done four times with total of 40 KIN and candidate 2 was done three times with total transfer of 30 KIN.

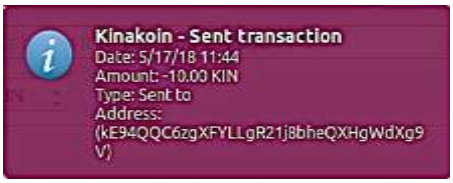

Fig. 5: Sent Transaction Notification on the Voter's Wallet (Transaction to Candidate 1)

Fig. 6: An Incoming Transaction Notification on the Candidate 1's Wallet

Fig. 7: Sent Transaction Notification on the Voter's Wallet (Transaction to Candidate 2)

Fig. 8: An Incoming Transaction Notification on the Candidate 2's Wallet

However, since this system is implemented under the Blockchain Technology, the transactions are not simply transferred just like that. The transactions require block confirmations from miners, which require the voter's account to be mined first to validate the confirmations. Before the blocks are confirmed, even though the transaction is done, the coins are not yet transferred.

The question mark symbol on the list of transaction on the voter's wallet indicates that the transaction block requires mining and not yet mined. At the same time, on the candidate's wallet, the coins transferred are considered as immature and is not added into the wallet balance.

Fig. 9: List of transactions from voter's wallet made to Candidate 1's wallet

Fig. 10: Overview of Candidate 1's Balance After Transaction from Voter Was Made, Before Mining Process

Fig. 11: List of transactions from voter's wallet made to Candidate 2's wallet

Fig. 12: Overview of Candidate 2's Balance After Transaction from Voter Was Made, Before Mining Process

Time taken for the mining depends on the connectivity of the Internet connection. Below shows the graph of the blocks created versus the time taken for block creation.

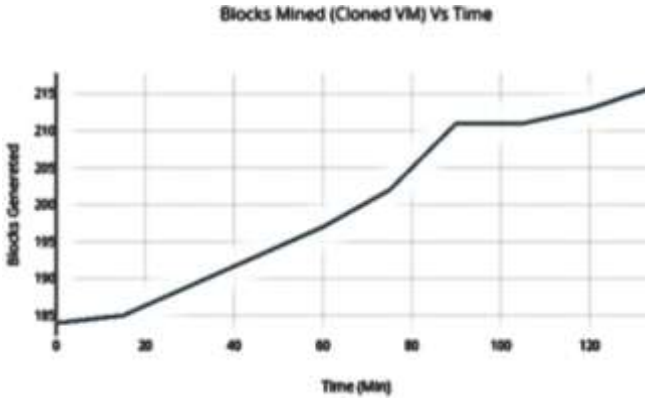

Fig. 13: Graph of Blocks Mined from First Candidate's Account vs. Time Taken

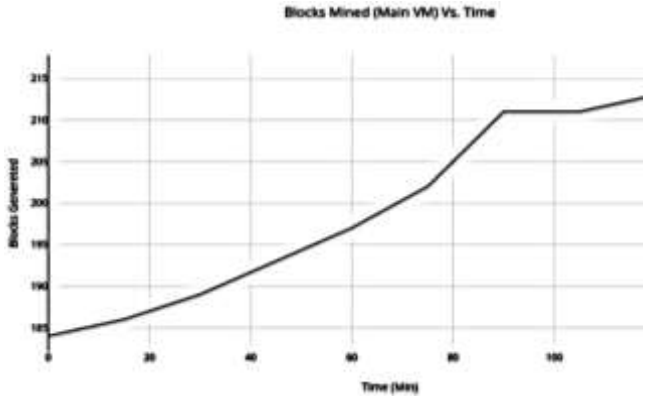

Fig. 14: Graph of Blocks Mined from Voter's Account vs. Time Taken

The blocks created are linear to the time taken. After the 210th blocks, the Internet connectivity was disconnected for a while which results in the mining process to be disturbed.

Once the transaction block has been confirmed, then the coins will be released to the candidates' respective account. Before the blocks were confirmed, Candidate 1 had 40 KIN coin immature in the wallet with 668.00 KIN but after transactions were approved, the 40 KIN coins were added to the total balance of Candidate 1's wallet. There was an additional transaction that were done to Candidate 1 due to testing that added another 40 KIN, which is why the total balance in the simulation is 748.90. Whereas, for Candidate 2, the wallet had 30 KIN immature coins with 120.00 KIN but after transactions were approved, the 30 KIN coins were added to the total balance of Candidate 1's wallet.

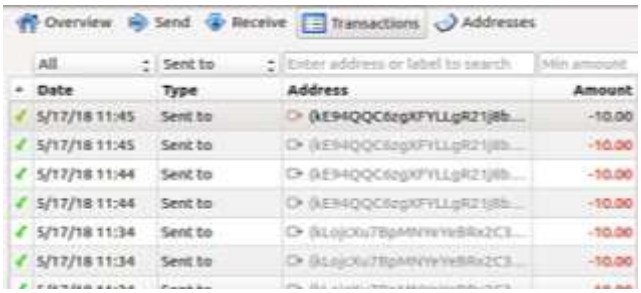

Fig. 15: List of Approved Transactions from Voter's Wallet

Fig. 16: Balance of Candidate 1's Wallet After Approved Transactions

Fig. 17: Balance of Candidate 2's Wallet After Approved Transactions

Each transaction that were performed and confirmed at the same time has the same block hash, which means that the record of transactions that were mined simultaneously was recorded and stored in one same unchangeable block with the same blockhash. From the result above, to show that a different transaction confirmed groups are added to different blocks, another 10 KIN coin transfer was done to each candidate's wallet.

The first earlier transactions that was confirmed and mined at the same time (the transactions explained above) has the same blockhash of:

Candidate 1	13826745ebc22f747be4cb1035568b15895fe5bdc15532241604ef62a333bada
Candidate 2	9baf5b8f822a2415cb039220732c14cb2127ea71e4b3c40cb4c909f4fd8fd168

Each transaction has a different transaction ID or transaction hash. Transaction hash is an identifier used to uniquely identify a particular transaction. All on-chain transactions have the unique transaction ID that can be seen in transaction's details. The hash of your transaction usually looks like a random set of letters and numbers. In one block, there can be multiple transactions, just as illustrate below.

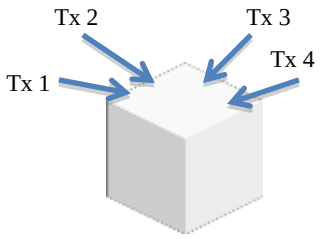

Fig. 18: One Block in a Blockchain that has several transactions that were mined together

Then, to prove that different transactions that were confirmed differently are added to different blocks, the transaction was made and the blockhash is different.

New transaction that was made to Candidate 1's and Candidate 2's wallet account and being mined at different time than the previous transactions.

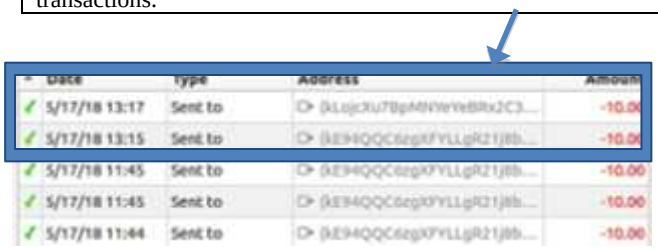

Fig. 19: New Transactions That Was Mined Differently

The block hash for the new transactions is:

Candidate 1	852a9d6bcf44bdc238086881c1c797a10844f5e948f586899f4082fa195f22a1
Candidate 2	852a9d6bcf44bdc238086881c1c797a10844f5e948f586899f4082fa195f22a1

Once data are recorded inside the Blockchain it becomes very difficult to change it. One block contains the transaction data, the hash of the block, and the hash of previous block. The next content of the block is also the block hash that is like the fingerprint of the block, which means one single block that contains the transactions data has a unique block hash in the block. Once a block is created which is through mining, its blockhash is calculated.
Changing any data in that particular block will cause the hash to change, thus making it not the same block. This hash is important in avoiding any alterations of data in the blocks. The other important element on the block is the previous hash block and this effectively creates the chain of blocks as one block is connected to the previous block via the block hashes. This characteristic is what makes the Blockchain very secure. The figure below will illustrate this. The result of the voting could be taken on which candidates have more blocks.

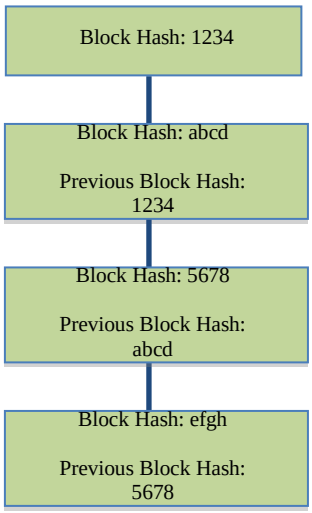

Fig. 20: Illustration of the blockchain untemper

If there is any slight alteration of data on any blocks, its hash will change. Let's say the system was hacked and data was changed on the second block, the blockhash will be changed and it will not tally with the previous block hash in the third block, and the whole blockchain system will not be validated. Since blockchain has copies on every network node, this chain will be terminated, just as illustrated in Figure 21.

5. Conclusion

It is believed that it is possible to implement the blockchain technology in the voting system application. Using cryptocurrency transactions as the determination of the results seems to be an alternative to the voting method, in order to apply the characteristics of integrity and security of the blockchain in the system. The output of the project proves effectiveness of the Blockchain technology in the confidence of its security to protect information. This can be seen through the block hashes generation. Lastly, with the blocks of transactions having a unique fingerprint shows that blockchain technology could improve the reliability of current voting system, as the data in the blocks could not be altered without changing the blockhash and terminating the chain. With improvements, it is believed that this project could be a stepping-stone in changing the voting system. Some of improvements that could apply for future are by deploying the coins as this project only work based on the testnet basis. Another recommendation to refine the project is by mining using a Graphics Processing Units (GPU) as mining without graphic cards takes such longer time.

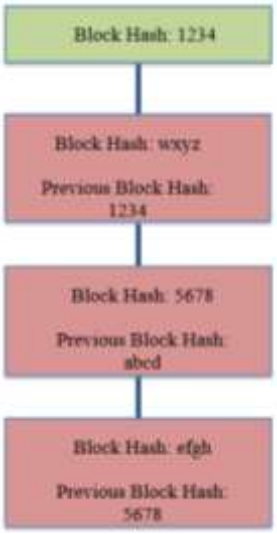

Fig. 21: Illustration of the blockchain tempered

Acknowledgement

This research is funded by Institute of Research Management and Innovation (IRMI), Universiti Teknologi MARA (UiTM), Shah Alam, Selangor, Malaysia under the Research Grant Scheme No: 600-RMI/DANA 5/3/PSI (195/2013) and Faculty of Electrical Engineering UiTM Shah Alam for all the support given during this research. Gratitude and appreciation to Electrical Engineer Mr Mohd Badri Mohd of Ifcon Technology Sdn Bhd as well as Ifcon Technology Sdn Bhd for all the assistance and support given in this project specifically introducing the technology to the authors and implementation of the Blockchain Technology.

References

[1] Lieber, F. (1889). Manual of political ethics, Part 2: Political ethics proper (for the use of colleges and students at law). Charles C Little and James Brown.
[2] Popescu, B. M. (2013). Electoral fraud: Few thoughts and insights about the phenomenon. Cogito (2066-7094), 5(1), 94-108.
[3] Electoral Commission. (2014). Electoral fraud in the UK: Final report and recommendations. Electoral Commission.
[4] Golder, M. (2005). Democratic electoral systems around the world, 1946–2000. Electoral Studies, 24(1), 103-121.
[5] Mayfield, L. (1993). Voting fraud in early twentieth-century Pittsburgh. The Journal of Interdisciplinary History, 24(1), 59-84.

[6] Noizat, P. Blockchain electronic vote. https://www.weusecoins.com/assets/pdf/library/blockchain-electronic-vote.pdf .
[7] Kaleem, J. (2016). Here's what we know so far about voter fraud and the 2016 elections. http://www.latimes.com/politics/la-na-pol-voting-irregularities-snap-story.html.
[8] Pierro, M. D. (2017). What is the blockchain? Computing in Science and Engineering, 19(5), 92–95.
[9] Pilkington, M. (2016). Blockchain technology: Principles and applications. In F. X. Olleros, & M. Zhegu (Eds.), Research Handbook on Digital Transformations. Cheltenham: Edward Elgar, pp. 225–253.
[10] Blockgeek, Proof of work vs proof of stake. https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/.
[11] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://s3.amazonaws.com/academia.edu.documents/32413652/BitCoin_P2P_electronic_cash_system.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1534387951&Signature=9k5FhInrT6iJ1FYAvhUhLO6%2BRJg%3D&response-content-disposition=inline%3B%20filename%3DBitcoin_A_Peer-to-Peer_Electronic_Cash_S.pdf.
[12] CoinMarketCap. Cryptocurrency market capitalizations. https://coinmarketcap.com/.
[13] GitHub. A next-generation smart contract and decentralized application platform. https://github.com/ethereum/wiki/wiki/White-Paper.
[14] Biswas, K., & Muthukkumarasamy, V. (2016). Securing smart cities using blockchain technology. Proceedings of the IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems, pp. 1392-1393.
[15] Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here. Proceedings of the IEEE 18th International Conference on e-Health Networking, Applications and Services, pp. 1-3.
[16] Economist. Digital voting with the use of blockchain technology. https://www.economist.com/sites/default/files/plymouth.pdf.
[17] Bogucki, B. (2017). Buying votes in the 21st century: The potential use of bitcoins and blockchain technology in electronic voting reform. Asper Review of International Business and Trade Law, 17, 59.
[18] J. Bannet, D. Price, A. Rudys, J. Singer, and D. Walach, (2004). Hack-a-vote: Security issues with electronic voting systems. IEEE Security and Privacy Magazine, 2(1), 32–37.
[19] P. Patrick McCorry, S. F. Shahandashti, F. Hao, “A smart contract for boardroom voting with maximum voter privacy,” Proceedings of the International Conference on Computer Science and Technology, pp. 357-375, 2017.
[20] D. Han, H. Kim, and J. Jang, “Blockchain based smart door lock system,” Proceedings of the IEEE International Conference on Information and Communication Technology Convergence, pp. 1165-1167, 2017.
[21] J.-H. Lee, “BIDaaS: Blockchain based ID as a Service,” IEEE Access, 6:2274-2278, 2018.