

Robust Framework Diagnostics of Blockchain for Bitcoin Transaction System: A Technical Analysis from Islamic Financial Technology (i-FinTech) Perspective

Nashirah Abu Bakar¹ and Sofian Rosbi²

¹Islamic Business School, College of Business, Universiti Utara Malaysia, Kedah, Malaysia,

²School of Mechatronic Engineering, Universiti Malaysia Perlis, Malaysia,

Abstract: In year 2017, Bitcoin attracted most investors because high return of investment. The system for Bitcoin transaction is known as blockchain. The blockchain is blocks of transaction history that shared publicly using secured cryptography. Each block contains the previous transaction information, timestamp and new transaction data in secured cryptographic hash programming language. This paper evaluates the Bitcoin framework whether the security of the system is satisfied with a definition of reliable computer system. In the same time, this paper discovers the reliability of the programming process that involved in blockchain system. The finding of this paper will help investors to understand the blockchain system properly in developing better understanding of cryptocurrency framework. The better understanding of the blockchain will help investors making proper decision in their investment portfolio to gain better profit and preventing loss.

Key words: *Bitcoin, Blockchain, Cryptography, Transaction Framework, Investment*

INTRODUCTION

The innovation in technology information system have been expanded in varies areas such as financial sector, education sector, retail sector and others sectors. The financial technology (also known as FinTech) is seen as one of the technology that would revolutionize the banking industry. FinTech has received global attention as the challenging technology that would empower firms to compete effectively in the 21st century [1].

Through internet or mobile banking, customers are able to execute online financial transaction from any location. While through social media banking, digital customers can interact online or set up a meeting with their relationship managers via unified communications technology before taking a decision on the best suited product or service offered by bank [2].

Moreover, Islamic financial sectors such as Islamic banking, Islamic capital market and takaful was showed aggressively innovation in their industry especially in FinTech system. FinTech are looking

as a new innovation in promoting Islamic financial products and services. Therefore FinTech become key enabler for future business.

Islamic Financial Technology (*i-FinTech*) was introduced to expanded technology innovation in Islamic banking product and services. *i-FinTech* are looking as a good platform in promoting Islamic financial industry in global site. Islamic Financial industry can be able to outperform its competitors and can sustainable competitive advantage among their competitors by engaged with high technology system. The high Muslim populations in the world also give advantages and opportunities in promoting Islamic banking products and services. Islamic banking that used *i-FinTech* system can easily and quickly advertise their new products and services in the world. This can attract customers to participant with Islamic banking products and services.

The innovation in FinTech was expanded with existent of cryptocurrency or digital currency. The most famous cryptocurrency is Bitcoin. Cryptocurrency is defined as a digital currency in which encryption techniques are used to regulate the

Corresponding Author: Nashirah Abu Bakar, Islamic Business School, College of Business, Universiti Utara Malaysia, Kedah, Malaysia, +6010-4062015

generation of units of currency and verify the transfer of funds, operating independently of a central bank [3]. The system used in cryptocurrency is known as blockchain. A blockchain is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way [4-5].

Blockchain technology enables users to share their ledger of transactions. The record of events gets distributed to all participants in a given network, who in turn use their computers to validate the transactions; thereby removing the need to have a third party intermediary such as a bank. Blockchain records can only be updated by consensus of a majority of the participants in the system and once entered, information can never be erased – providing a detailed audit trail of all associated events [6]. Therefore, this study was investigated the blockchain framework for Bitcoin transaction system. This study was focused on the process of Bitcoin transaction according to Islamic financial technology (*i*-FinTech) perspective.

LITERATURE REVIEWS

In 1950, credit cards were introduced to reduce a customer burden from brings cash money. Credit card was attracted customers to apply a credit card because of the good features such as customer-friendly, easy to bring and useful. Credit cards are regarded as a spending stimulus that allows greater ease of spending than cash [7].

In 1960, ATM machine was introduced in order to replace tellers and branches system. While, electronic stock trading began on exchange trading floors in 1970. The rapid development of Islamic Capital Market (ICM) started in 1990 when Shell MDS Sdn. Bhd. issued the country's first Islamic bond. In 1994, Malaysia's first full-fledged Islamic stock broking company, BIMB Securities Sdn, Bhd, was formed [8].

Financial technology was continuously developing with introducing of bank mainframe computers, more sophisticated data and record-keeping systems in year 1980. Internet and e-commerce business models flourished in year 1990. Now, in the early part of the 21st century, retail financial services are being further digitized via mobile wallets, payment apps, robo-advisors for wealth and retirement planning, equity crowdfunding platforms for access to private and alternative investment opportunities and online lending platforms [9].

Therefore, FinTech innovations are looking as a good platform in the financial industry. The new system that was introduced in FinTech system is known as blockchain. The blockchain fundamental was developed in 2008 by developer known as

Satoshi Nakamoto. Bitcoin is the digital currency that was established based on the blockchain system. Blockchain was published a technical white paper which laid the foundation of an open source, public, distributed and peer-to-peer exchange of Bitcoin, a digital currency which allowed pseudonymous, verifiable and immutable online payments without the need of a financial intermediary [3].

Then the second cryptocurrency came into market in 2014, when Vitalik Buterin and his core team of developers, in recognition of the limitations of the Bitcoin blockchain (Bitcoin was designed to be used only as a payment system), developed a second-generation blockchain called Ethereum [10]. Bitcoin and Ethereum are built on top of novel internet protocols, the latter inspired many other financial and non-financial applications, including private blockchains (e.g. developed by banks), resulting in a vibrant and constantly growing ecosystem [11].

There are many researches that focus on the performance of the Bitcoin. Study from Abu Bakar and Rosbi [12] regarding volatility of Bitcoin found that standard error indicates the volatility for Bitcoin is 4.458 % . This value is considered as high value of volatility. High value of volatility indicates the investment in Bitcoin is categorical as high risk investment.

Bariviera, [13] found the long memory content of daily volatility of Bitcoin is stronger than in daily returns. This feature gives some hints on the characteristics of Bitcoin cryptocurrency market. In particular, volatility of Bitcoin transaction is clustering as a key feature of the Bitcoin market.

The others study regarding Bitcoin cryptocurrency found that the Bitcoin data distribution of exchange rate for Bitcoin follows non-normal distribution. Therefore, the normality transformation is important to make sure the distribution of data follows normal distribution. The results show that the Bitcoin data is highly volatile with existence of many outliers [14].

Balcilar, et al, [15] investigate a non-parametric causality-in-quantiles test to analyze the causal relation between trading volume and Bitcoin returns and volatility, over the whole of their respective conditional distributions. The causality-in-quantiles test reveals that volume can predict returns over the quantile range of 0.25 to 0.75, i.e. except in Bitcoin bear and bull market regimes. This result highlights the importance of modelling nonlinearity and accounting for the tail behavior when analyzing causal relationships between Bitcoin returns and trading volume.

FRAMEWORK ANALYSIS

The transaction of Bitcoin is between peer-to-peer system that managed by decentralized system. Figure 1 shows the comparison between current

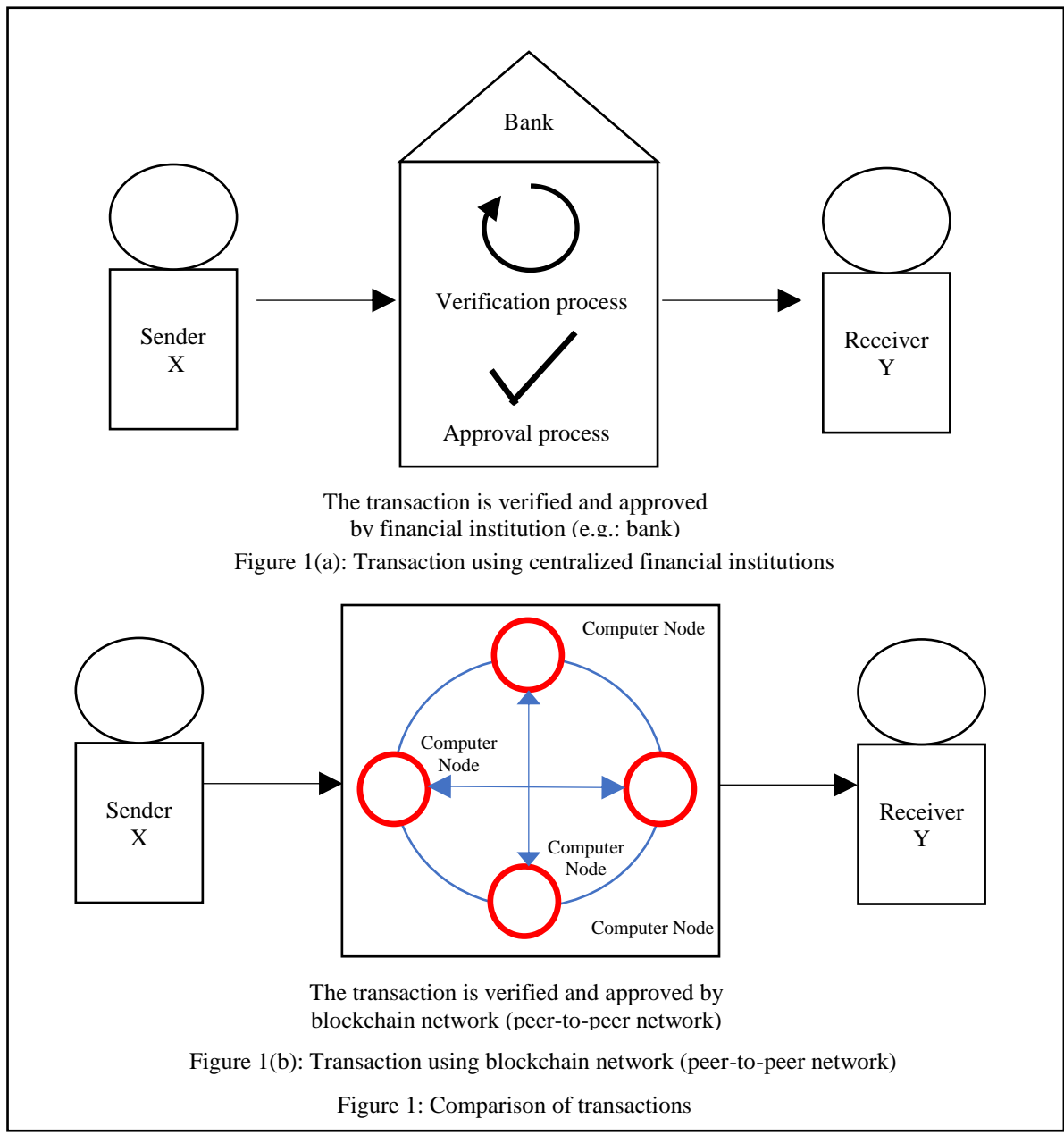
system for transaction and transaction system using blockchain.

Figure 1(a) shows the current transaction process. If a sender X would like to send an amount of money to receiver Y, the transaction process need to be verify and approved by central financial institutions. However, Bitcoin transaction is performed without the centralized authority. This transaction of the system is validated using public ledgers that maintain by computer node in the network. This system is called peer-to-peer system. The benefit of this system is, the entire computer node have a similar open ledger that can be access by users in the computer network of Bitcoin. In the same time, the verification process and the approval process can be performed in short time which is every 10 minutes. The main advantages of Bitcoin network system is

the fee of the transaction is very low when comparing to the centralized system using financial institutions.

BLOCK STRUCTURE OF BLOCKCHAIN

The transactions of Bitcoin are translated to hash programming to produce hash code. Figure 2 shows the chaining process of the blockchain. The process of chaining started with the first block of transaction. Then, the current has code need to link with previous code to validate the content of transactions. Next, the current hash code in second block of transaction is created using hash programming. This hash code need to link with previous hash code which is in first block. Again, when the hash code for third block is created, it must be evaluated and synchronized with hash code in previous block.



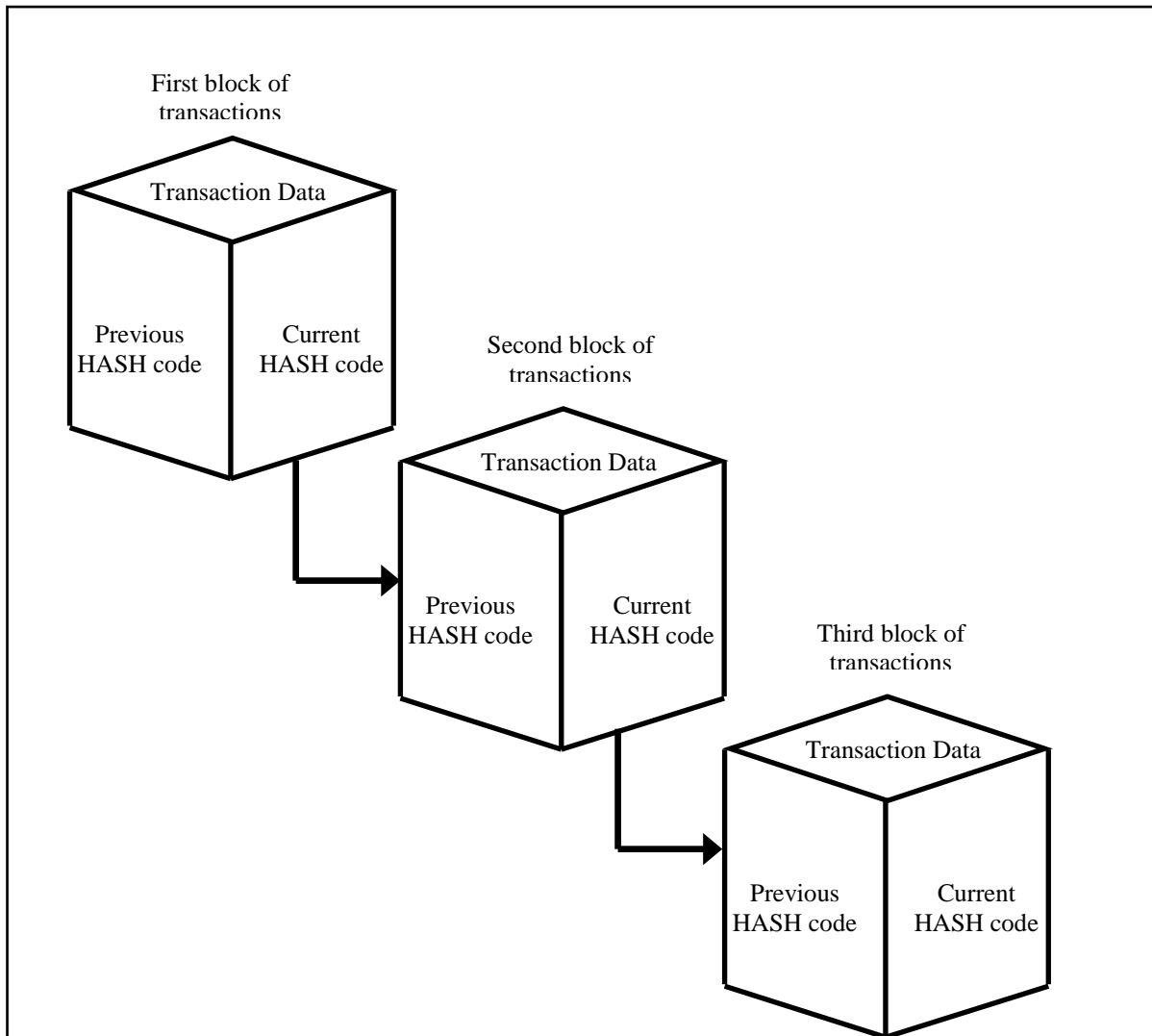


Figure 2: Blockchain chaining procedure

Table 1: Hash code chaining process

First stage		Second stage		Third stage	
Current hash	12FH	Current hash	34HQ	Current hash	6BH2
Previous hash	0000	Previous hash	12FH	Previous hash	34HQ

Table 1 shows the example of the hash code chaining process. Consider the initial block of transaction is represented by hash code of 0000. In the first stage of block transactions, new hash code generated is 12FH. The transactions in 12FH, need to evaluate and link to hash code of 0000. When there is synchronization, then hash code of 12FH is accepted in the network as legal hash code. Next, the second block of hash code is 34HQ. This code need to verify and validated with hash code of previous block which is 12FH. Then, the hash code in the third stage is 6BH2. This code need to synchronize with the second stage of transaction. This process is called as

proof of work that contributes to the security of the system.

BLOCKCHAIN FRAMEWORK

Blockchain framework is a system that involved from starting process of transaction until the completion of transaction.

Figure 3 shows the blockchain framework for Bitcoin. The process starts with the issuance of payment by user X to user Y. The value of Bitcoin that own by user X is stored using Bitcoin e-wallet.

This wallet is protected using private key. The private key is the unique for each user in network. Then, the request to make a payment is consider as a transaction. The transaction message is send to

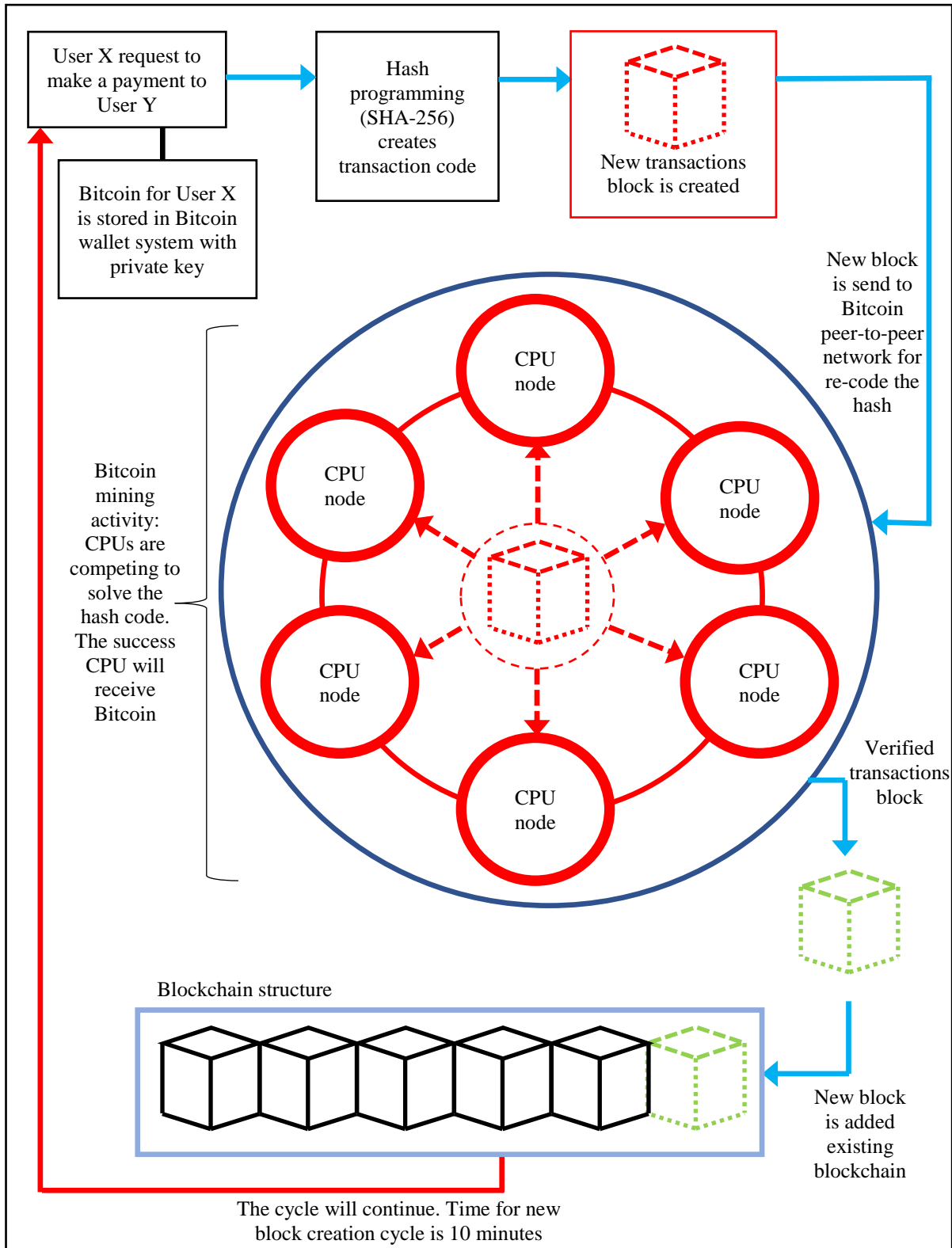


Figure 3: Blockchain framework

Hash programming to create hash code using secure Hash Algorithm (SHA 256). Next, the hash codes of transaction are created and are represented by a block.

Next, the block is transferred to Bitcoin peer-to-peer network for evaluation and synchronization with previous of block transactions. In this network, computer with public ledgers will compete with each other's to solve the hash code in determining the transaction. The success computer that can translate the meaning of the codes will receive Bitcoin reward. This activity is called Bitcoin mining.

The solved block will be added to main blockchain after it is evaluated and verified by all computer nodes regarding the reliability of the transactions. Then, the cycle will start again from a user who is request to make payment.

BLOCKCHAIN PATH ANALYSIS

Blockchain is transactions history recorded in block and validated using chain system. Figure 4 shows the path analysis for the main blockchain system. In initial stage, the blockshain is developed using block A, B and C. Then, there are two blocks are added to the main chain in the same time, namely Block E and D. After F block is added, Block E will be accepted and Block D will be deleted. The chain with reliable and longest chain will be selected for main blockchain. Then, block G and H are created simultaneously after block F. After Block I is created, Block G will deleted and Block H will be accepted as path of main chain.

This path analysis is to make sure the path of blockchain is reliable for storing transaction history. In the same time, the path development can prevent any suspicious block that insert into the blockchain.

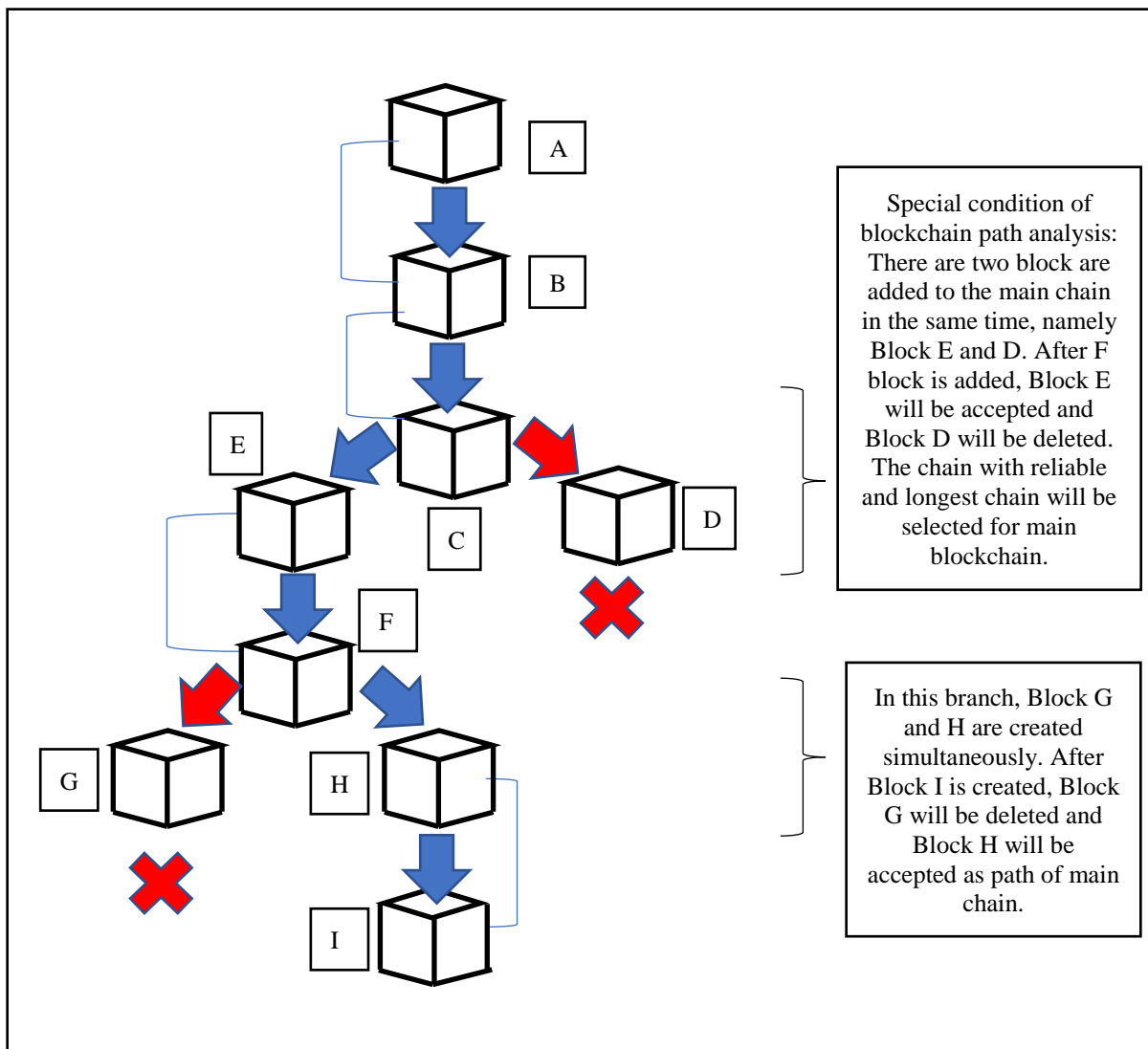


Figure 4: Blockchain path selection

CONCLUSIONS

The objective of this study is to evaluate the blockchain system from technical perspective. The purpose of this analysis is to make sure the reliability of the system in storing the transaction data including the security level of the system. The main findings of this study are:

- (a) The decentralized system is developed to reduce the transaction fee by the central financial institutions namely Bank institutions. Therefore, the transactions fee of Bitcoin using blockchain in decentralized system is lower compared to existing exiting payment system. This methods is supporting the digital community in e-commerce.
- (b) The security of blockchain is highly reliable because the implementation of hash algorithm. Hash algorithm is a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size (a hash) and is designed to be a one-way function, that is, a function which is infeasible to invert.
- (c) However, the account holder of bitcoin including the receiver identity is anonymous exist in the system. Therefore, the account holder are undetected if any suspicious activities occurs in the transaction activity.
- (d) From the Islamic Financial technology perspective, the blockchain idea is reliable in recording the transactions. However, the anonymities including the setting of Bitcoin programming setting is still unclear and untransparent. The anonymities characteristic has a tendency that contributes to participation in illegal transactions and illegal online gambling activities.

The findings of this study will help government agencies, public, and investors to understand the nature of Bitcoin structure. The finding will help the policy makers in making better policy regarding cryptocurrency.

FURTHER STUDY

The findings of this study can be extending to analyze the reliability hash programming structure including the volatility of Bitcoin exchange rate. In addition, this further level of this study can be analyzed the performance of Bitcoin exchange rate with correlation to other cryptocurrency such as Ethereum, Litecoin, Ripple, Dash and Monero.

REFERENCES

- [1] Wonglimpiyarat, J., (2017). FinTech Banking Industry: A Systemic Approach, *Foresight*, Vol. 19, No. 6, pp. 590-603.
- [2] Malaysia International Islamic Financial Centre (MIFC), (2016). Financial Technology (FinTech) in Islamic Finance, available at: <https://www.islamicfinance.com/wp-content/uploads/2016/05/Islamic-Finance-Technology-and-Innovation.pdf> (accessed 10 April 2018)
- [3] Nakamoto, S., (2009). Bitcoin: A Peer-to-Peer Electronic Cash System, available at: <http://bitcoin.org/bitcoin.pdf> (accessed 20 October 2017)
- [4] Abu Bakar, N., Rosbi, S. and K. Uzaki, (2017). Cryptocurrency Framework Diagnostics from Islamic Finance Perspective: A New Insight of Bitcoin System Transaction, *International Journal of Management Science and Business Administration*, Vol. 4, No. 1, pp. 19-28.
- [5] Reid, F. and Harrigan, M., (2013). *An Analysis of Anonymity in the Bitcoin System*, Springer, New York, NY.
- [6] Standard Chartered, (2017). Blockchain, available at: https://www.sc.com/fightingfinancialcrime/av/SCB_Fighting_Financial_Crime_Deep_dive_Blockchain_August_2017.pdf (accessed 10 April 2018)
- [7] Awanis, S. and Chi Cui, C., (2014). Consumer Susceptibility to Credit Card Misuse and Indebtedness, *Asia Pacific Journal of Marketing and Logistics*, Vol. 26, Issue: 3, pp. 408-429.
- [8] Laldin, M.A., (2008). Islamic Financial System: The Malaysian Experience and The Way Forward, *Humanomics*, Vol. 24, Issue: 3, pp. 217-238.
- [9] Desai, F., (2015). The Evolution of FinTech, available at: <https://www.forbes.com/sites/falgunidesai/2015/12/13/the-evolution-of-fintech/#7bde08b67175> (accessed 10 April 2018)
- [10] Bajpai, P. (2018), Bitcoin Vs Ethereum: Driven by Different Purposes, available at: <https://www.investopedia.com/articles/investing/031416/bitcoin-vs-ethereum-driven-different-purposes.asp#ixzz5BODKZUe4> (accessed 10 April 2018)

- [11]Zalan, T., (2018). Born global on blockchain, *Review of International Business and Strategy*, Vol. 28 Issue: 1, pp. 19-34.
- [12]Abu Bakar, N. and Rosbi, S. (2017), High Volatility Detection Method Using Statistical Process Control for Cryptocurrency Exchange Rate: A Case Study of Bitcoin, *The International Journal of Engineering and Science*, Vol. 6, Issue: 1, pp. 39-48.
- [13] Bariviera, A.F. (2017). The Inefficiency of Bitcoin Revisited: A Dynamic Approach, available at: <https://arxiv.org/pdf/1709.08090.pdf> (accessed 10 April 2018)
- [14]Abu Bakar, N. and Rosbi, S. (2017) Robust Statistical Normality Transformation method with Outlier Consideration in Bitcoin Exchange Rate Analysis, *International Journal of Advances in Scientific Research and Engineering*, Vol. 3, No. 9, pp. 80-91.
- [15]Balcilar, M., Bouri, E., Gupta, R., and Roubaud, D. (2017). Can Volume Predict Bitcoin Returns and Volatility? A Quantiles-Based Approach, *Economic Modelling*, Vol. 64, pp. 74 – 81.