



Cryptocurrency Framework Diagnostics from Islamic Finance Perspective: A New Insight of Bitcoin System Transaction

¹Nashirah Abu Bakar, ²Sofian Rosbi, ³Kiyotaka Uzaki

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

²School of Mechatronic Engineering, Universiti Malaysia Perlis, Malaysia

³Department of Business Studies, Oita University, Japan

Abstract: This paper analyses the operation of cryptocurrency system in perspective of Islamic finance. The purpose of this study is to evaluate the cryptocurrency framework whether it is meet the Islamic Finance rule. In addition, this study performed in providing the Islamic minded investor a proper information regarding investment in Bitcoin. Cryptocurrency is a digital currency in which encryption techniques that implement to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank. A transaction is a transfer of Bitcoin value that is broadcast to the network and collected into blocks. A transaction typically references previous transaction outputs as new transaction inputs and dedicates all input Bitcoin values to new outputs. This cryptocurrency has no physical form and exists only in the network. Bitcoin also has no intrinsic value in that it is not redeemable for another commodity, namely gold. Then, this study evaluates the framework according to Islamic Finance rule. The bitcoin account holder is anonymous. Therefore, it is difficult to track the real account holder if any suspicious activity occurs. In addition, the value of Bitcoin is unstable because of high volatility. Bitcoin also suffers variance in perceptions of Bitcoin's store of value and method of value. All of these three conditions contribute to uncertainty in transaction framework of Bitcoin. As a conclusion, Bitcoin transaction is classified as a transaction with high uncertainty (gharar).

Keywords: Cryptocurrency, Bitcoin, Transaction framework, Islamic finance, Uncertainty

1. Introduction

E-commerce is a complex term referring to the process of selling and buying products and services over the Internet or other electronic systems. Considered as the sales aspect of the e-business, the electronic commerce has revolutionized trade as a routine activity for the contemporary man by bringing the marketplace to your home or the office, thus saving you time and efforts. The development of e-commerce has given birth to new terms such as electronic funds transfer, online transaction processing, electronic data interchange (EDI), internet marketing, automated data collection systems, etc. They all designate certain key components of the sophisticated e-commerce system. The concepts of e-business such as e-commerce and e-banking are acceptable in Islam since in Islam anything is halal unless prohibited by Shari'ah, dealing with business by internet is considered as Shari'ah compliant (Alotaib and Asutay, 2015).

Transaction over internet rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust-based model. Completely non-reversible transactions are not possible since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for nonreversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party (From the Shari'ah viewpoint, every single transaction, either in physical or virtual setting, is regarded as a contract.

For the contract to be considered as valid, it must fulfill some requirements stipulated by the Shari'ah (Muhammad et al., 2013).

Therefore, a new method of digital currency is introduced. An electronic payment introduced that system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party (Kristoufek, 2013). Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers (Nakamoto, 2009)

This paper analyzes the operation of cryptocurrency system in perspective of Islamic finance. The purpose of this study is to evaluate the cryptocurrency framework whether it is meet the Islamic Finance rule. The main objective of establishing Islamic financial system is to provide products and services according to shariah law (Abu Bakar and Rosbi, 2017). Shariah is referring to activities that follow Islamic law. All the transaction must be free from the prohibited element such as *riba*, *gharar*, and *maisir*. The main source of Islamic law is Al-Quran and As-Sunnah (Abu Bakar and Rosbi, 2017). Also, this study is performed in providing the Islamic minded investor a proper information regarding investment in Bitcoin.

2. Literature Review Regarding Cryptocurrency Development

Cryptocurrency is defined as a digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank. A cryptocurrency is a digital asset designed to work as a medium of exchange using cryptography to secure the transactions and to control the creation of additional units of the currency. A cryptocurrency is a virtual currency that uses cryptography for security. A cryptocurrency is difficult to counterfeit because of this security feature. A defining feature of a cryptocurrency and arguably its most endearing allure is its organic nature; it is not issued by any central authority, rendering it theoretically immune to government interference or manipulation (Bohme, et al., 2015).

Decentralized cryptocurrency is produced by the entire cryptocurrency system collectively, at a rate that is defined when the system is created and which is publicly known (Moore and Christin, 2013). In centralized banking and economic systems such as the Federal Reserve System, corporate boards or governments control the supply of currency by printing units of fiat money or demanding additions to digital banking ledgers. In case of decentralized cryptocurrency, companies or governments cannot produce new units and have not so far provided backing for other firms, banks or corporate entities that hold asset value measured in it. The underlying technical system upon which decentralized cryptocurrencies are based on a system that created the group or individual known as Satoshi Nakamoto (Decker and Wattenhofer, 2013).

The security of cryptocurrency ledgers is based on the assumption that the majority of miners are honestly trying to maintain the ledger, having financial incentive to do so. Most cryptocurrencies are designed to gradually decrease the production of currency, placing an ultimate cap on the total amount of currency that will ever be in circulation, mimicking precious metals (Barber, et al., 2012).

An electronic payment system based on cryptographic proof is allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms implemented to protect buyers. In the year of 2017, Bitcoin attracts many investors because of high return. Therefore, this study is performed to evaluate the operational framework for Bitcoin from the perspective of Islamic finance.

3. Comparison of Transaction Procedure Between Cryptocurrency and Traditional Currency

In this section, this study describes the overview of transaction procedure for traditional money with a comparison to the digital money (cryptocurrency transaction procedure). Figure 1 shows the traditional money transaction procedure. The process is started when user A transfer money to user B. This transaction will go through the system that provided by the financial provider which is banking sector. This transaction is using centralized management system that is set-up the banking institution. The security of this transaction is monitored and validated by the banking institution. In most cases, a central bank has a monopoly right to issue coins and banknotes (fiat money) for its area of circulation (a country or group of countries); it regulates the production of currency by banks (credit) through monetary policy. In this transaction, the value of the currency is decided using exchange rate value. An exchange rate is a price at which two currencies can

be exchanged against each other. This is used for trade between the two currency zones. Exchange rates can be classified as either floating or fixed. In the former, day-to-day movements in exchange rates are determined by the market; in the latter, governments intervene in the market to buy or sell their currency to balance supply and demand at a fixed exchange rate. In cases where a country has control of its currency, control is exercised either by a central bank or by a Ministry of Finance. The institution that has control of monetary policy is referred to as the monetary authority. Monetary authorities have varying degrees of autonomy from the governments that create them.

Figure 2 shows the cryptocurrency transaction procedure. If user A would like to transfer digital currency to user B, the transaction needs to go through the blockchain path. The blockchain in the ledger system that monitored and validated by the users in involved in ledger validation system using a computer system. Cryptocurrencies make it easier to transfer funds between two parties in a transaction; these transfers are facilitated using public and private keys for security purposes. These fund transfers are done with minimal processing fees, allowing users to avoid the steep fees charged by most banks and financial institutions for wire transfers. There are no physical bitcoins; only balances kept on a public ledger in the cloud. All Bitcoin transactions are verified by a massive amount of computing power.

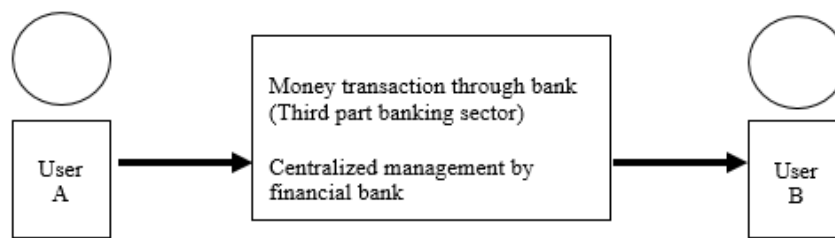


Figure 1: Money transaction procedure

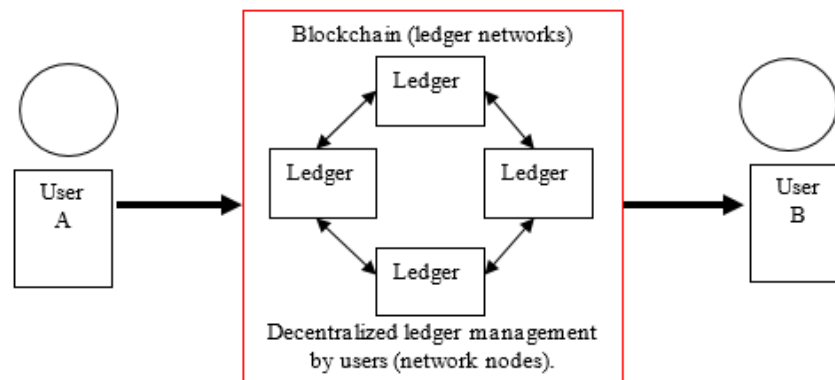


Figure 2: Cryptocurrency transaction procedure

Table 1 shows the comparison between traditional digital currency and cryptocurrency transaction process. In definition, current fiat money is money in any form when in actual use or circulation as a medium of exchange, especially circulating banknotes and coins. This type of money is government-issued currencies. Comparing to cryptocurrency, Bitcoin is digital currency in which encryption techniques are used to regulate the generation of units of currency. Cryptocurrency is a type of currency that is non-physical, of which no banknotes and coins exist. The transaction of Bitcoin only can be performed via electronic means, typically allowing for instantaneous transactions and borderless transfer of ownership.

Table 1: Comparison between traditional digital currency transaction and cryptocurrency transaction

	Traditional digital currency transaction	Bitcoin (Cryptocurrency) transaction
Definition	Money in any form in actual use or circulation as a medium of exchange, especially circulating banknotes and coins. Money is government-issued currencies.	Digital currency in which encryption techniques are used to regulate the generation of units of currency. Type of currency that is non-physical, of which no banknotes and coins exist, and which can only be transmitted via electronic means, typically allowing for instantaneous transactions and borderless transfer of ownership.
Example	Two monetary systems: fiat money and commodity money	Virtual currencies and cryptocurrencies
Verification	The transaction using code from financial institution	A transaction using a digital signature that represented by a code that is generated by the algorithm.
Transaction path	The transaction path is monitored by trusted third part	Ledgers in blockchain monitor the transaction path. This ledger is open for public access and maintained by users.
Transaction cost	There is transaction cost	Minimal transaction cost that lower compared to traditional money transfer method
Volatility	Price of exchange rate fluctuates according to economic condition.	Price of Bitcoin is based on supply and demand. The exchange rate of cryptocurrency fluctuates widely depending on the news.

4. Technical Aspects of Cryptocurrency

4.1 Distributed Open Ledger Networks

A ledger is the principal book or computer file for recording and totaling economic transactions measured regarding a monetary unit of account-by-account type, with debits and credits in separate columns and a beginning monetary balance and ending monetary balance for each account (Ron and Shamir, 2013). A blockchain is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way (Reid and Harrigan, 2013).

Figure 3 shows the distributed open ledger networks as a peer-to-peer cryptocurrency platform. This platform is acting as the host, skeleton, and tool for constant innovation, designed for high-speed transactions, allowing users to trade assets in near-real time, securely and with ultra-low fees. The operation procedure of Bitcoin is the blockchain that uses to store an online ledger of all the transactions that is conducted using bitcoins, providing a data structure for this ledger that is exposed to a limited threat from hackers and can be copied across all computers running Bitcoin software.

A transaction is a transfer of Bitcoin value that is broadcast to the network and collected into blocks. A transaction typically references previous transaction outputs as new transaction inputs and dedicates all input Bitcoin values to new outputs (Miers, et al., 2013). Ledger is open to all users in the networks, and all users refer to one public ledger of transaction chain (Moore and Christin, 2013).

The data profile shows that the age range of women legislative members ranges from 20 to 50 years old. There are only people with a single status. A number of children data also shows that generally, everyone has three or more children. Only one woman legislative member that has a high school, the majority has a bachelor degree. Many informants have a background of working in a formal sector such as banking and informal sector such as businesswoman. The informant data also show that the circumstances in which women successfully obtain a position as members of legislative in Medan and Deli Serdang are those who have a relatively high education background with a working experience. Marriage Status and a number of children also show a family condition that allows them to have careers. We could assume that the strict values of patriarchy in this family have shifted. The patriarchy values in this family have shifted towards women participation in parliament/politics. The patriarchy value in those families became more flexible and adjusted based on the role of women in parliament. This proves that shift of patriarchy value is an important note in this research.

In the context of a merit system, we can note that leaders of political parties mentioned that they select women legislative members based on formal education and the ability of each women legislative members. Formal education data show that chosen women legislative members have a higher formal education, but this not as guarantee them to have sufficient political skills. Considering every women legislative member does not have a background in political science, law, or any other political education background. The background of active participation in social organization certainly can be an asset come election time. But this is not enough because their integrity as an elected women representative, their political competence such as negotiation skill, legislation skill and critical skill and issues of gender bias toward women become a requirement for the merit system.

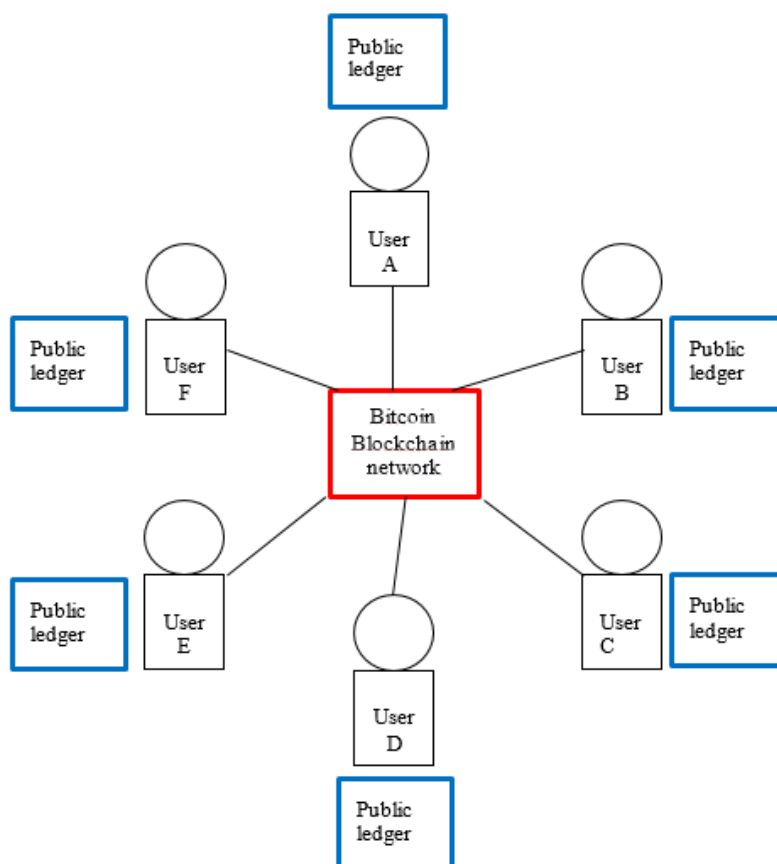


Figure 3: Blockchain network (open ledger network)

4.2 Transaction Chain

A transaction is a transfer of Bitcoin value that is broadcast to the network and collected into blocks. A transaction typically references previous transaction outputs as new transaction inputs and dedicates all input Bitcoin values to new outputs. Transactions are not encrypted, so it is possible to browse and view every transaction ever collected into a block. Once transactions are buried under enough confirmations they can be considered irreversible (Gennaro, et al., 2007).

Figure 4 shows the transaction procedure in cryptocurrency. A transaction is a transfer of Bitcoin value that is broadcast to the network and collected into blocks. A transaction typically references previous transaction outputs as new transaction inputs and dedicates all input Bitcoin values to new outputs. Bitcoin transaction defined as a chain of digital signatures.

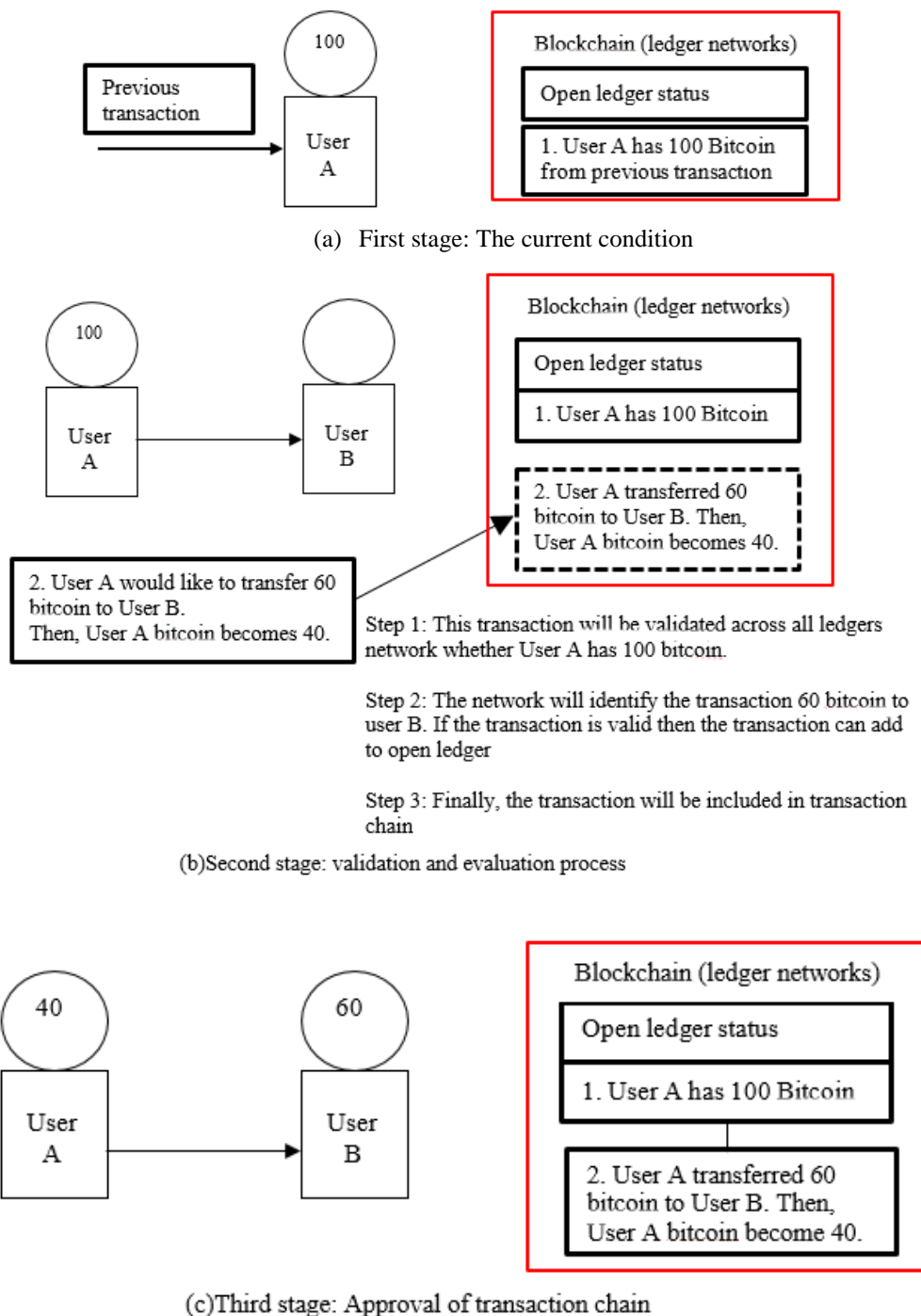


Figure 4: Transaction process of cryptocurrency

4.2 Bitcoin Mining and Implementation of Cryptographic Hash Functions in Transaction

Cryptocurrency defines an electronic coin as a chain of digital signatures (Okamoto, 1995). Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership. Bitcoin miners help keep the Bitcoin network secure by approving transactions (Kroll et al., 2013). Mining is an important and integral part of Bitcoin that ensures fairness while keeping the Bitcoin network stable, safe and secure (Ron and Shamir, 2013).

Figure 5 shows the proses of Bitcoin mining and implementation of cryptographic hash functions in the transaction. Bitcoin is a type of cryptocurrency that balances are kept using public and private keys, which are long strings of numbers and letters linked through the mathematical encryption algorithm that was used to create them. The public key (comparable to a bank account number) serves as the address which is published to the world and to which others may

send bitcoins. The private key (comparable to an ATM PIN) is meant to be a guarded secret and only used to authorize Bitcoin transmissions.

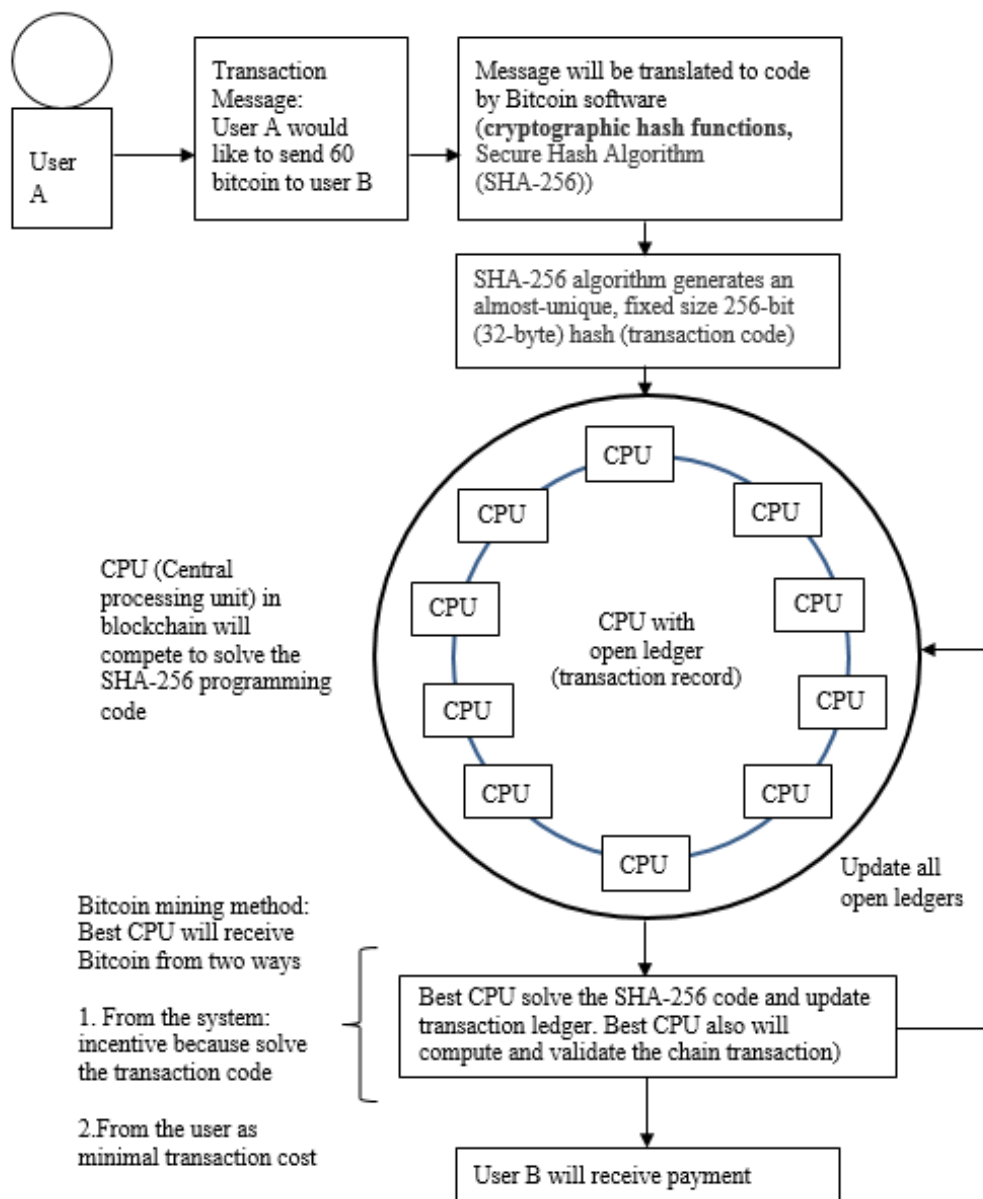


Figure 5: Bitcoin mining and implementation of cryptographic hash functions in transaction

5. Bitcoin Transaction System from Islamic Finance Perspective

Bitcoin is one of the first digital currencies to use peer-to-peer technology to facilitate instant payments. The independent individuals and companies who own the governing computing power and participate in the Bitcoin network, also known as "miners," are motivated by rewards (the release of new bitcoin) and transaction fees paid in bitcoin (Yermack, 2013). These miners can be thought of as the decentralized authority enforcing the credibility of the Bitcoin network. New bitcoin is being released to the miners at a fixed, but periodically declining rate, such that the total supply of bitcoins approaches 21 million (Grinberg, 2012). One bitcoin is divisible to eight decimal places (100 millionths of one bitcoin), and this smallest unit is referred to as a Satoshi.

Table 2 shows the analysis of cryptocurrency issues respect to Islamic finance perspective. The result shows the system of Bitcoin has uncertainty (gharar) elements.

Table 2: Issues of cryptocurrency concerning Islamic Finance perspective

Issues	Analysis from Islamic finance perspective
An unknown individual under the pseudonym Satoshi Nakamoto who revealed little about himself and left the project in late 2010 published the first Bitcoin specification and proof of concept in 2009.	The inventor of Bitcoin is still unknown. This element is associated with uncertainty (<i>gharar</i>) element.
Bitcoin system is the first decentralized peer-to-peer payment network powered by its users with no central authority or intermediaries.	The proposed system of Bitcoin is suitable for a certain community of internet users. However, to implement in all sectors of the economy, authority is needed to confirm the validity of the transactions. There is a possibility of a fraud case if there is no central authority that validates and monitoring transaction system. This element is associated with uncertainty (<i>gharar</i>).
The system is relying on the cryptographic hash function. A cryptographic hash function is a special class of hash function that has certain properties that make it suitable for use in cryptography. It is a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size (a hash function) which is designed to also be a one-way function, that is, a function that is infeasible to invert.	This system is vulnerable to hacking activity. This element is associated with uncertainty (<i>gharar</i>). In addition, this cryptocurrency has no physical form and exists only in the network. Bitcoin also has no intrinsic value in that it is not redeemable for another commodity, namely gold.
Government regulation or law does not support Bitcoin.	The value of Bitcoin is not tied to a tangible asset or government regulation or law. Therefore, Bitcoin validity in a current economic system is still in uncertainty status. This element brings questionable (<i>gharar</i>) status.
Bitcoin is high volatility cryptocurrency because of the following factors (Jonathan,2017): <ol style="list-style-type: none"> 1. Bad press hampers rate of adoption. 2. News about security breaches makes investors react: Bitcoin can also become volatile when the Bitcoin community exposes security vulnerabilities in an effort to produce massive open source responses in the form of security fixes. 3. Too much variance in perceptions of Bitcoin's store of value and method of value. 4. Bitcoin is much more volatile versus the USD than the high inflation country. 	The value of Bitcoin is unstable because of high volatility. Therefore, the operation of Bitcoin is classified as uncertainty (<i>gharar</i>) in Islamic Finance perspective.
Bitcoin volatility is also stretched to an extent driven by holders of large proportions of the total outstanding float of the currency. For Bitcoin investors with current holdings above around \$10M, it is not clear how they would liquidate a position that large into a fiat position without severely moving the market. Since Bitcoin's volume resembles a small cap stock, the currency has not hit the mass-market adoption rates that would be necessary to provide option value to large holders of the currency.	Bitcoin offers little option value to large holders of the currency. In this operation, there is an undefined operation to provide option value to large holders of the currency. Therefore, the system of Bitcoin has uncertainty (<i>gharar</i>) elements.
Bitcoin purchases are discrete. Unless a user voluntarily publishes his Bitcoin transactions, his purchases are never associated with his identity, much like cash-only purchases, and cannot be traced back to him. In fact, the anonymous Bitcoin address that is generated for user purchases changes with each transaction (Androulaki, et al., 2013).	The bitcoin account holder is anonymous. Therefore, it is difficult to track the real account holder if any suspicious activity occurs. This creates uncertainty (<i>gharar</i>) condition.

5. Conclusion

Cryptocurrency is a medium of exchange created and stored electronically in the blockchain using encryption techniques to control the creation of monetary units and to verify the transfer of funds. Bitcoin is a type of cryptocurrency: Balances are kept using public and private "keys," which are long strings of numbers and letters linked through the mathematical encryption algorithm that was used to create them. The public key (comparable to a bank account number) serves as the address, which is published to the world and to which others may send bitcoins. The private key (comparable to an ATM PIN) is meant to be a guarded secret, and only used to authorize Bitcoin transmissions (Abdalla, et al., 2009).

Bitcoin has advantages of low transaction fee and no third party interruption. Standard wire transfers and foreign purchases typically involve fees and exchange costs. Since Bitcoin transactions have no intermediary institutions or government involvement, the costs of transacting are kept very low. One of the most widely publicized benefits of Bitcoin is that governments, banks and other financial intermediaries have no way to interrupt user transactions or place freezes on Bitcoin accounts. The system is purely peer-to-peer; users experience a greater degree of freedom than with national currencies (Canard and Gouget, 2007).

This paper analyzes the operation of cryptocurrency system in perspective of Islamic finance. The purpose of this study is to evaluate the cryptocurrency framework whether it is meet the Islamic Finance rule. Also, this study is performed in providing the Islamic-minded investor a proper information regarding investment in Bitcoin.

The main finding from this study described in the following explanation.

1. Bitcoin is a type of cryptocurrency. Balances are kept using public and private keys, which are long strings of numbers and letters linked through the mathematical encryption algorithm that was used to create them. The public key (comparable to a bank account number) serves as the address which is published to the world and to which others may send bitcoins. The private key (comparable to an ATM PIN) is meant to be a guarded secret and only used to authorize Bitcoin transmissions. The proposed system of Bitcoin is suitable for a certain community. However, to implement in all sectors of the economy, authority is needed to confirm the validity the transaction. If without the monitoring authority, there is a possibility of manipulation of the system. Therefore, the Bitcoin system is associated with uncertainty (gharar).
2. A transaction is a transfer of Bitcoin value that is broadcast to the network and collected into blocks. A transaction typically references previous transaction outputs as new transaction inputs and dedicates all input Bitcoin values to new outputs. Transactions are not encrypted, so it is possible to browse and view every transaction ever collected into a block. Once transactions are buried under enough confirmations, they can be considered irreversible. This system is vulnerable to hacking activity. This element is associated with uncertainty (gharar). Also, this cryptocurrency has no physical form and exists only in a network. Bitcoin also has no intrinsic value in that it is not redeemable for another commodity, namely gold.
3. Bitcoin volatility is also stretched to an extent driven by holders of large proportions of the total outstanding float of the currency. For Bitcoin investors with current holdings above around \$10M, it is not clear how they would liquidate a position that large into a fiat position without severely moving the market. Since Bitcoin's volume resembles a small cap stock, the currency has not hit the mass-market adoption rates that would be necessary to provide option value to large holders of the currency. Bitcoin offers little option value to large holders of the currency. In this operation, there is unclear operation to provide option value to large holders of the currency. Therefore, the framework of Bitcoin system is associated with uncertainty (gharar).

References

- Abdalla, M., Boyen, X., Chevalier, C., Pointcheval, D.: Distributed Public-Key Cryptography from Weak Secrets. In: Jarecki, S., Tsudik, G. (eds.) PKC 2009. LNCS, vol. 5443, pp. 139–159. Springer, Heidelberg (2009) [Crossref](#)
- Abu Bakar, N. and Rosbi, S. (2017) Data Clustering using Autoregressive Integrated Moving Average (ARIMA) model for Islamic Country Currency: An Econometrics method for Islamic Financial Engineering, The International Journal of Engineering and Science, Vol. 6 (6), pp. 22-31 [Crossref](#)
- Abu Bakar, N. and Rosbi, S. (2017) Data modeling diagnostics for share price performance of Islamic Bank in Malaysia using Computational Islamic Finance approach, International Journal of Advanced Engineering Research and Science, 4 (7), 174-179 [Crossref](#)

- Alotaibi, M.N. and Asutay, M. (2015) Islamic Banking and Islamic e-commerce: Principles and Realities, *International Journal of Economics, Commerce and Management*, III (4), 1-14
- Androulaki E., Karame G.O., Roeschlin M., Scherer T., Capkun S. (2013) Evaluating User Privacy in Bitcoin. In: Sadeghi AR. (eds) *Financial Cryptography and Data Security. FC 2013. Lecture Notes in Computer Science*, vol 7859. Springer, Berlin, Heidelberg [Crossref](#)
- Barber, S., Boyen, X., Shi, E. and Uzun, E. "Bitter to better - how to make bitcoin a better currency," in *Financial Cryptography 2012*, vol. 7397 of LNCS, 2012, pp. 399-414.
- Böhme, R., Christin, N., Edelman, B., and Moore, T. (2015). Bitcoin: Economics, technology, and governance. *The Journal of Economic Perspectives*, 29(2), 213-238. [Crossref](#)
- Canard, S., Gouget, A.: Divisible E-Cash Systems Can Be Truly Anonymous. In: Naor, M. (ed.) *EUROCRYPT 2007. LNCS*, vol. 4515, pp. 482–497. Springer, Heidelberg (2007) [Crossref](#)
- Decker, C. and Wattenhofer, R., "Information propagation in the Bitcoin network," *IEEE P2P 2013 Proceedings, Trento, 2013*, pp. 1-10. doi: 10.1109/P2P.2013.6688704 [Crossref](#)
- Gennaro, R., Jarecki, S., Krawczyk, H., and Rabin, T. (2007) Secure distributed key generation for discrete-log based cryptosystems. *Journal of Cryptology*, 20(1), 51-83. [Crossref](#)
- Grinberg, R. (2012). Bitcoin: An innovative alternative digital currency. *Hastings Sci. & Tech. LJ*, 4, 159.
- Jonathan T.B. (2017). Why Is Bitcoin's Value So Volatile?
- Kristoufek, L. (2013). BitCoin meets Google Trends and Wikipedia: Quantifying the relationship between phenomena of the Internet era. *Scientific reports*, 3, 3415. [Crossref](#)
- Kroll, J. A., Davey, I. C., & Felten, E. W. (2013, June). The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In *Proceedings of WEIS (Vol. 2013)*.
- Miers, I., Garman, C., Green, M. and Rubin, A. D. "ZeroCoin: Anonymous Distributed E-Cash from Bitcoin," 2013 *IEEE Symposium on Security and Privacy*, Berkeley, CA, 2013, pp. 397-411. doi: 10.1109/SP.2013.34 [Crossref](#)
- Moore, T., and Christin, N. (2013, April). Beware the middleman: Empirical analysis of Bitcoin-exchange risk. *International Conference on Financial Cryptography and Data Security* (pp. 25-33). Springer, Berlin, Heidelberg. [Crossref](#)
- Muhammad, M., Muhammad, M.R. and Mohammed Khalil, M. (2013) Towards Shari'ah Compliant E-Commerce Transactions: A Review of Amazon.com, *Middle-East Journal of Scientific Research*, 15(9), 1229-1236
- Nakamoto, S. (2009) "Bitcoin: A peer-to-peer electronic cash system", Retrieved from <http://www.bitcoin.org/bitcoin.pdf>
- Okamoto, T.: An Efficient Divisible Electronic Cash Scheme. In: Coppersmith, D. (ed.) *CRYPTO 1995. LNCS*, vol. 963, pp. 438–451. Springer, Heidelberg (1995) [Crossref](#)
- Reid, F. and Harrigan, M., "An analysis of anonymity in the Bitcoin system," in *Privacy, security, risk and trust (PASSAT)*, 2011 *IEEE Third International Conference on Social Computing (SOCIALCOM)*. IEEE, 2011, pp. 1318-1326.
- Retrieved from <http://www.investopedia.com/articles/investing/052014/why-bitcoins-value-so-volatile.asp>
- Ron D., Shamir A. (2013) Quantitative Analysis of the Full Bitcoin Transaction Graph. In: Sadeghi AR. (eds) *Financial Cryptography and Data Security. FC 2013. Lecture Notes in Computer Science*, vol 7859. Springer, Berlin, Heidelberg [Crossref](#)
- Yermack, D. (2013). Is Bitcoin a real currency? An economic appraisal (No. w19747). National Bureau of Economic Research. [Crossref](#)