

CRYPTOCURRENCIES FROM ISLAMIC PERSPECTIVES: A SYSTEMATIC LITERATURE REVIEW

*Baffa, I. Jibrin¹, Sa'id, Abdullahi Doma² & Auwal, Garba³

^{1,2&3} School of Business Education, Federal College of Education Gombe, Gombe State, Nigeria.

*Corresponding Author: +234 8035549494; jibappah4@gmail.com

Abstract

This paper takes into view the conditions that render an investment or transaction forbidden in Islam and relates them to cryptocurrencies through a literature research methodology. Furthermore, elements that exist in the cryptocurrency ecosystem such as tokens, initial coin offerings (ICOs) and cryptocurrency derivatives are assessed to check as to whether they are compatible with Islam. The difference between Bitcoin and its alternatives is also recognized by analyzing their underlying technology and how they could be a major tool in defining whether or not a cryptocurrency falls in the Islamic permissibility criteria. It concludes that although the technology of cryptocurrencies in itself is permissible; different aspects contribute in deciding whether the specific digital currency in question is permissible or forbidden. Future research is needed on a couple of key issues related to Proof of Stake protocol which has been discussed.

Keywords: Blockchain, crypto currency, bit coin, Islamic perspective, sharia compliance.

1. Introduction

Islam welcomes technological development that produces numerous innovations in various sectors around the world, including the financial sector, if it is Shariah compliant. Each country has an authority that controls and administers all matters involved in the production and printing of money. However, cryptocurrency, which emerged over a decade ago, is no longer monitored today by any authority in a certain country (DeVries, 2016; Ammous, 2016; Sungit & Ahmad, 2017; Adam, 2017). Bitcoin is the first cryptocurrency that was developed (2009) and was the first cryptocurrency term that was coined (Albrecht et al., 2019). The term 'cryptocurrency' is used because all transactions and issuance of new units will use the cryptography system that is developed using the blockchain technology. The intended function of the Bitcoin was to be a universal medium of payment that replaces the currency of a certain country (DeVries, 2016). Cryptocurrency is also known as virtual currency or digital currency (Adam, 2017). Scholars and Fatwa institutions all around the world have provided their views related to the use of Bitcoins (Adam, 2017; Oziev & Yandiev, 2017; Meera, 2018; Abubakar et al., 2018). However, those views cannot be generalised to all digital currencies. Various digital currencies have been created based on the original Bitcoin concept with various functions that has expanded the use of digital currencies (Albrecht et al., 2019). An increase in digital currencies with various functions requires different legislation and Shariah

guidelines for each of the function developed. Therefore, there are specific characteristics of these digital currencies outlined by scholars as well as certain countries to classify it into several categories of digital currencies monitored by a specific legislation.

With the rise of Bitcoin compromising the traditional fiat currencies, the world saw governments reacting to it in various manners. Some like Dubai legalized it and proceeded to utilize its underlying technology, 'the Blockchain' to establish plans for a smart city though some even familiarized their own cryptocurrencies like Venezuela. In any case, for Muslims, another problem of the "Halal or Haram" perspective is available which must be managed for progress in the Muslim world. In existing cases, a few researchers have considered Bitcoin as Haram on the accounts of vagueness and excessive risk included, others have expressed it as Halal proclaiming it be even cleaner than the debt-based fiat currencies we use today (Li et al., 2019; Böhme et al., 2015). Nevertheless, moving beyond Bitcoin, not much literature is available to guide Muslim investors in terms of the other cryptocurrencies and tokens that exist like Ethereum, Litecoin, and Golem.

Bitcoin or Virtual currencies are not physical money in kinds, for example, gold, cash or monetary fiat which it gave by the national bank, additionally are not controlled by banks, where the virtual currencies depend on the main bank and the annulment of the role of banks as mediator between the seller and the purchaser (Bakar & Rosbi, 2018; Dyhrberg, 2016; Acquisti et al., 2016). A virtual currency is a digital representation of value that can be digitally exchanged and works as a mechanism of trade, a unit of account as well as a store of value, however doesn't have legal tender status in any jurisdiction. It isn't issued or ensured by any legislature and satisfies these capacities just by understanding inside the network of users of the currency. It is particular from fiat currency or "real currency", which is the physical money that makes up a country's legal tender, and particular from e money, which is a digital representation of fiat currency. Virtual currencies are managed by their users as per the guideline of distributed (Campbell-Verduyn, 2018; Urquhart, 2016). Virtual currencies are portrayed by security, usability, what's more, the people who produce and exchange them are a help to humanity what's more, the individuals of the land since they are creating their own currency (Kaur, 2019; Yermack, 2017; Mettler, 2016). The most famous monetary currencies are Bitcoin, which comprises of a digital address related with an electronic wallet. The wallet is an electronic application when an individual need to convert a specific value from a Bit of coin to someone else; he utilizes the so-called digital signature. This signature contains three things, the first is conversion letter when the Bitcoin is converted to another envelope, and the conversions go to the Bitcoin network and enter the affirmation procedure and are saved in the Chain blocks which are called Blockchain (Cong & He, 2019; Gandal et al., 2018).

But, in Islamic rules, the economic activity should be based on real, physical assets (Najeeb, 2014). In the Muslim world, practicing Muslims do not invest in banking products that pay returns via interest. As a result, practicing Muslims do not consider Bitcoin, Ethereum, and other crypto currencies to be compliant with Islamic Shari-ah. Thus, as the influence of cryptocurrencies in our daily life grows, the question of their relevance,

compliance with the requirements of Shari'ah and the permissibility of their use by ordinary Muslims and Islamic financial institutions is also becoming apparent (Ozиеv&Yandiev, 2017).

Therefore, what we attempted to do in this article is to briefly discuss the background of cryptocurrency, followed by Islamic cryptocurrency, what makes an investment and transaction permissible in Islam? Blockchain consensus protocol from Islamic perspectives, and then argued that Islamic crypto currencies can solve many of the economic issues, making them preferred to "traditional" money.

2. Literature review

2.1 What is crypto currency?

Currency is a medium of exchange and measurement of economic value. Creptocurrency is an internet and virtual currency and medium of exchange, which is used in transactions as same way fiat money is used (Irwin & Turner, 2018). Crypto currency can be defined as "a digital asset that is constructed to function as a medium of exchange, premised on the technology of cryptography, to secure the transactional flow, as well as to control the creation of additional units of the currency" (Chohan,2017). However, Different type of cryptocurrency available, but these are the more well-known currencies in the market (Bitcoin, Ethereum, Bitcoin Cash, Tether, Binance Coin, Cardano, EOS) (Coinmarketcap, 2019). Bitcoin is the first virtual currency which created in 2009 by pseudonym Satoshi Nakamoto as decentralized digital currency that can be sent from user to user on the peer-to-peer bitcoin network without the need of intermediaries such as banks (Nakamoto, 2008). The accessibility and acceptance of crypto currency is widespread across regions. It introduced an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to make transaction directly with each other without the need of a trusted third party (Kristoufek, 2013). This system solely depends on "Blockchain" which is a kind of Distributed Ledger Technology (DLT) that has been defined as a "distributed, shared, encrypted database that serves as an irreversible and incorruptible warehouse of information" (Wright, &Filippi, 2015). A defining feature of a crypto currency is that; it is not issued by any central authority, making it theoretically protected from government interference or manipulation (Böhme, Christin, Edelman, & Moore, 2015).

Transaction over internet depends exclusively on financial institutions acting as trusted third parties to process electronic payments. But, in crypto currency, it depends on three correlated elements, which are the users, the Blockchain and the miners (Kerscher, 2014). Blockchain is the backbone of virtual currency. The backbone of this system is secured, decentralized and created by an individual known as Satoshi Nakamoto (Decker, &Wattenhofer, 2013). Here, 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). Therefore, Blockchain consists of three main, complementary parts: a shared state, a set of rules for updating state via blocks and a trust model for time stamping (Williamson, &Andolfatto, 2015). Blockchain allows users to track record and verify all the transactions in network to ensure its validity and security. There are Proof of Stake (PoS) and Proof of Work (PoW) algorithms which are being used in crypto currency mining (Chan, Chu, Nadarajah, &Osterrieder, 2017).

Blockchain is a decentralized database. Crypto currencies such as tokens can fit in this category since they not only can be traded, but they can also be used to build programs or applications into a Blockchain. In the case of Bitcoin, it is a cryptographic ledger shared among all the users on the network to verify transactions and add them to a block of other chained transactions to ensure the reliability of transactions and avoiding issues such as double spending (Mainelli, & Smith, 2015). But, the problem of virtual and digital currencies is that they cannot be considered as a legal tender by the monetary system which created several challenges such as its interaction with the real economy, protecting the consumer from any issues associated with these currencies and crimes and fraud that happened by using these currencies since it is not monitored or properly regulated by a suitable monetary system (Zahudi, & Amir, 2016).. Moreover, Bitcoin transaction is classified as a transaction with high uncertainty (Bakar, Rosbi, &Uzaki, 2017).

The authors believe it is essential to understand the basic difference between a cryptocurrency and a token in order to have a sense of what one is investing in. Cryptocurrencies are coins that are specifically created to be used as digital currencies, as a medium of exchange. On the contrary, tokens serve as a fundraising tool used by startups related to the crypto sphere as opposed to traditional finance raising methods such as venture capital. Tokens are released to the public through an Initial Coin Offering (ICO) just as shares are issued by a public limited company (plc) through an Initial Public Offering (IPO). The latter is strictly regulated whereas ICOs have been exploited to pull off scams in the past. Although this is changing with countries such as America placing regulations on how these are conducted, the fraud can easily be avoided by due diligence, hence it does not go against Islam's principles. The value of a token depends on how the company who issued it in the first place is retaining demand and performing. This can be seen as owning a share in a company but with less right such as no equity, no say in the startup's decisions and no say in the direction the startup takes. This also conforms to the Islamic principles of an investor knowing as to what they are buying with no deception involved. So, cryptocurrencies are digital currencies whereas a token is an asset much like a share(Asif, 2018).

2.2 Salient Characteristics of Cryptocurrency

Cryptocurrency is a computer file that cannot be copied or used twice. Since cryptocurrency can be used for trading transactions and savings and exchange for other currencies, they are considered similar to any existing undocumented money circulating only in the Internet (Oziev&Yandiev, 2017).

There are three distinct levels of working with cryptocurrency (taking bitcoins as example).

Firstly: any legal or real physical person can own bitcoins and use them for transactions. The client will need to download on his computer a special software program which will enable him to open a wallet for storing his bitcoins. The client, using ordinary fiat money (USD, EURO, etc), can buy bitcoins on the special cryptocurrency market and place the acquired bitcoins in his wallet (Oziev, &Yandiev, 2017).

Secondly: bitcoins can be generated or emitted: To do this, the user needs to download on his computer a special software program that solves sophisticated mathematical equations/puzzles generated by the bitcoin system. The user whose computer first solves the equation/puzzle (known as hash) gets a bitcoin as a reward. Figuratively, the process of generating or emitting bitcoins is called mining (as if it is a work in a mine where something valuable, for example, gold is mined). The process takes time and considerable amount of electricity. For a long time, especially at the initial stage, the market value of bitcoins was lower than the cost of electricity.

However, the truth is that in the current situation only those with specialized, high-powered machinery will have a greater chance to profitably extract bitcoins compared with the home miners. That's because they actually have no chance to compete in such a challenging environment, unless they have access to free or extremely low-cost electricity (Mukhopadhyay, & Suryadevara, 2014).

Thirdly: the user, having solved a sophisticated mathematical equation/puzzle faster than other players gets the right to execute transactions performed by bitcoins' holders at that particular time. Owners of bitcoins can perform transactions either way: with or without payment of commission. The user proposes a commission to prioritize his deal, in about 10 minutes time, while regular transaction - without commission - can take longer, up to few hours. High security of bitcoins is provided in addition to encryption by the use of blockchain technology (decentralized maintenance of registries). In other words, each owner of bitcoins has a complete database of all transactions made with all the bitcoins from the first time of their appearance. The complete database is about the transaction time of all bitcoins, the transferred amount and the approximate location of the payer (however, the database is anonymous and therefore to find the exact location of the bitcoin holders in most cases is impossible (Khalilov, & Levi, 2018).

The transaction mechanism works as follows. A person, for example, sold something and received bitcoins in his wallet. The record of this transaction is automatically sent to all computers connected to the bitcoin system, and all bitcoin owners learn that a certain owner of an electronic wallet with a certain number has acquired a certain number of bitcoins from such a wallet under certain number. After sometime this person decides to buy something using his bitcoins. In this case he instructs his wallet to transfer a certain sum of bitcoins to such and such an address/wallet. At this point, his computer sends a request to all computers connected to the bitcoin system to confirm the validity of such a transaction. The computers of other participants check their records and send confirmation when they see that, indeed, this buyer (they see only the electronic name/code of his wallet) possesses the necessary number of bitcoins. When a certain number of confirmations are received, the participants of the second level form a special record. Next, the claimed amount is transferred and all the computers of the system receive a message to add a new record to the database: deduct bitcoins from this person's wallet and add to his partner's wallet (Swan, 2018).

Bonneau, Miller, Clark, Narayanan, Kroll, & Felten, (2015), deduce the following key characteristics of cryptocurrencies (using bitcoin as example):

- i. decentralized emission;
- ii. absence of the regulator;
- iii. the primary distribution of bitcoins among users is carried out based on competition whose criterion is a successful solution for sophisticated mathematical equations/puzzles;
- iv. They are not backed by any asset;
- v. the maximum amount of emission is limited (21million), the terms and volumes of current emission are known to all participants of the system;
- vi. It is impossible to recover lost or stolen funds;
- vii. It has high degree of secrecy of the users;
- viii. They operate with full and transparent information for all users;
- ix. They have relatively high transaction speed;
- x. There is no mandatory commission for money transfer;
- xi. Their transactions currently are speculative in nature in most cases;
- xii. They are unable to eliminate the social stratification.

2.3 Classification of Digital Currency

Bitcoin was the first term used to describe a cryptocurrency or digital currency because it was the first digital currency that used the cryptographic system with blockchain technology (Albrecht et al., 2019). The emergence of other digital currencies produced by improving the original Bitcoin concept had various functions and characteristics and was called cryptocurrency (Joo et al., 2019). Now, this term does not only focus on the medium of payment function alone but includes various financial infrastructure and instruments built on the smart contract platform that issues digital currencies with various functions.

Islamic scholars had classified digital currency into several different categories without a specific guide so that it can be uniformly used by all countries. There are three different views about the classification of digital currency according to its functions (Mukhopadhyay, 2018; FINMA, 2018; Howell et al., 2018; Asif, 2018; Sockin&Xiong, 2018; Wu et al., 2018; Deloitte, 2019; Victor & Luders, tt). According to several studies (Victor & Luders (tt), Asif, 2018, Sockin&Xiong, 2018, Howell et al., 2018, Wu et al., 2018 and Mukhopadhyay, 2018), digital currency can be divided into two categories, which are coins and tokens. Tokens are created through the smart contract platform that is built on the blockchain technology used by other digital currencies, such as ERC-20, that can only be developed using the Ethereum blockchain (Mukhopadhyay, 2018). A token represents an asset or various commodities that can be distributed, such as physical or digital assets, shares, votes, membership, loyalty bonuses and other utilities. Sockin&Xiong (2018) and Howell et al., (2018) had divided tokens into two categories according to different functions, namely utility and security tokens. Coins represent a digital form currency and is created using a blockchain of its own, such as Bitcoin and Ethereum. Coins have limited function, which is a store of value, compared to tokens that have numerous functions.

Deloitte (2019) and Maxson et al., (2019) had used the term ‘crypto asset’ because the term ‘cryptocurrency’ usually refers to a medium of payment, such as Bitcoin. ‘Crypto assets’ is a much wider term and refers to security tokens or other innovations developed by using the crypto system. Crypto assets comprise three categories, namely payment or exchange tokens, utility tokens and security tokens (Deloitte, 2019; Maxson et al., 2019).

3. Methodology

To examine beyond the extent of the current literature that exists on digital currency and concentrate on different parts of the cryptocurrency ecosystem, a literature research approach was utilized. Various sources of information are utilized comprising of journal publications, books and articles. So as to progress in the direction of keeping up the credibility of the information sought, sound sources are focused on. The credibility of these sources can be judged by the way that they were produced by reputable researchers and experts in existing fields. Since the existing literature on Islamic finance is immense, however, limited about cryptocurrencies, this paper means to gather together the information that exists, distinguish the gaps that exist and prepare towards future study on the Shariah consistence of different cryptocurrencies and tokens beyond Bitcoin. Besides, notwithstanding examining Islamic financial principles, the very technology that administers cryptocurrencies is likewise analyzed to give a contention that can be applied in various cases. Real world examples are likewise given to make it simpler to Muslims to comprehend the specific context of these regulations as opposed to being bound theoretically.

4. What makes an Investment and Transaction permissible in Islam?

The main source of Islamic shari`ah is Al-Quran and As-Sunnah (Bakar, Rosbi, & Uzaki, 2017). Hence, it might be a kind of opportunity to look after the potential of adapting these currencies and their respective payment technologies. Islamic law provides a set of certain conditions which must qualify for an asset to be Halal. Although cryptocurrencies are in the literal sense to be used as a medium of exchange, they also qualify as assets along with Tokens since they serve as a store of value as the traditional fiat currencies may while the latter resembles a share of a company as mentioned earlier. Islamic crypto currency must comply with the following Shari-ah requirements (Alzubaidi, & Abdullah, 2017).

Riba – Interest:

One of the thumb rules of Islamic finance is that Riba (Interest) is strictly forbidden. Similarly as covered in section 3.2, there are digital currencies and tokens that make use of any of the two types of Riba - Riba Al Fazl and Riba Al Nasee’ah.- to facilitate the running of the coin’s network on a daily basis falls into the impermissible. Hence, all cryptocurrencies or tokens involved in activities that are related to Riba are Haram. This is further clarified by the Prophet Muhammad PBUH’s Hadith: “Allah has cursed the one who consumes riba, the one who gives it, the one who witnesses over it, and the one who writes down the transaction. “(Sahih Muslim) And a verse of the Holy Quran, “Allah has permitted trade and has forbidden Riba.” (Quran 2:275)

Unlawful Industry:

Judging from over hundreds of cryptocurrencies and tokens that exist in the market today, many of them are targeted to serve industries that are regarded impermissible in Islam. An example is of the Funfair token – explained in section 3 - which aims to deliver casino gaming to the public. As gambling is Haram, this automatically makes this token Haram regardless of other properties that may be permissible in themselves. Tron is another token aimed at serving the entertainment industry which directly correlates to music, movies, dancing and other acts which fall out of the permissibility criteria in Islam rendering it Haram. Other industries Muslims should beware of include Pornography, Non-Islamic Banking, Alcohol, Pork and Tobacco. This concept can be understood with an analogy to the widely understood stock market. If someone invests in a company like Microsoft which is developing software products, this is Halal and hence the investment is Shariah Compliant whereas if one invests in a Company like Diageo which is involved in the production of alcoholic beverages, this investment would be haram (Asif, 2018).

Gharar– Uncertainty:

Gharar is the Islamic term for transactions or investments that involve uncertainty consisting of two types: Gharar-e-Fahish(excessive) and Gharar-e-Yasir(minor), the latter one being permissible as a trivial amount of uncertainty is present in every kind of contract and transaction, hence it is considered tolerable.(Uddin, M. 2015, October 13). On the other hand, Gharar-e-Fahish is strictly forbidden.

To demonstrate this, here's an example: A retailer promised to buy the rice harvest of a farmer next year for a fixed price of \$20,000 regardless of the number of rice crops grown. This means that even if all the crops are burned or even if the product is worth \$40,000, the retailer will still pay the fixed amount of \$20,000. This introduces the concept of uncertainty (Gharar) in 3 ways.

- i. The commodity that is being sold does not exist yet.
- ii. The quantity and quality of the crops are unknown.
- iii. The farmer is selling something that he does not own which imposes upon him a debt. The buyer also now owes an amount of money to the seller resulting in debt in both cases, hence the transaction being a debt to debt one becomes prohibited according to the Shariah (Asif, 2018).

These facts are evident from the Hadith of the Prophet Muhammad PBUH in which a man asked him, “People ask me to sell them things I don't have. Should I say yes, and go buy them?” and the Messenger of Allah PBUH said, “No, go buy them first, and then sell them.” However, as Mufti Taqi Usmani states, with 2 exceptions namely Salam and Istisna such deals are allowed.

a. Salam.

In Salam, a future contract is permissible under certain conditions. This was allowed at the time of the Holy Prophet Muhammad PBUH because after the prohibition of Riba, it was difficult for traders and small farmers to finance themselves. In order to solve this, Salam was allowed which is a transaction in which the seller agrees to sell goods to the buyer on a future date but the buyer must make the full payment at the time of the contract in order for the deal to be beneficial to the seller. The buyer benefits from this due to getting a lower price than the market price. However, there are certain strict conditions under which this contract is valid:

- i. The payment must be made at the time the contract is made.
- ii. The buyer must give the seller at least one month for the time of delivery of goods.

This is because the seller might not be able to deliver before which will undermine the basic reason of granting relief to the seller in terms of finance.

b. Istisna.

Istisna also allows future contracts but is distinguished from Salam by a few conditions:

- i. In an Istisna contract, the seller must be a manufacturer whereas, in Salam, this is not a requirement – the seller could be a retailer or of any other profession.
- ii. Payment in advance is not a requirement.
- iii. It is possible to cancel the contract before the seller starts the work of manufacturing.
- iv. The time of delivery does not have to be fixed.

Maysir (Gambling):

Maysir is the gaining of wealth through very easy means without any effort and purely depends on speculation without the person having any control of the outcome. It is strictly forbidden in Islam, in any form.

Allah says, “O you who have believed, indeed, intoxicants, gambling, [sacrificing on] stone alters [to other than Allah], and divining arrows are but defilement from the work of Satan, so avoid it that you may be successful.” (Quran - 5:90)

5. Blockchain Consensus Protocols

For the purposes of efficiency and security, consensus protocols are used to ensure the network operates smoothly with every user having a common version of the blockchain avoiding conflicts and attacks from opponents.

Proof of Work: the very first cryptocurrency, Bitcoin made use of the Proof of Work (PoW) protocol, hence it does not come as a surprise that it's the most popular and frequently used protocol today. In PoW each coin is generated by solving tough cryptographic puzzles through the use of computational power. In this way, money isn't created from thin air and is backed by an asset, in this case, electricity. This also serves as a mechanism to regulate the supply of currencies as the difficulty factor in solving the cryptographic puzzles are directly

proportional to the number of computational power being invested into the network. In 2009, Bitcoins were mined using personal computers due to the low amount of computational power required whereas now in 2021, specialized hardware exists to cater to the miner’s market. In Islam, one of the requirements for something to be legal tender is it to have an intrinsic value. Bitcoin has been criticized in the Islamic world on the basis of having no intrinsic value but this fact is easily debunked in the case of the PoW protocol as electricity serves as the asset backing the currency in question without any debt being used. (Maierbrugger, 2017). However, there is a limitation to this argument which is put forward by Alzubaidi& Abdullah (2017) in which it is argued that electricity does not qualify as the physical existence of an asset which holds its value in the real world. Nevertheless, the author believes that this does not render the PoW protocol impermissible; further research still needs to be undertaken regarding this specific issue.

Proof of Stake (PoS): While Bitcoin is regarded as one of the greatest achievements of our time due to the technological advancements it has brought forward, there has been much criticism on the amount of electricity that is wasted to generate new coins through the process of mining. In Bitcoin’s infancy, coins could be mined using the graphical processing unit (GPU) of a normal computer machine but with the passage of time, the difficulty of the network has increased. Now miners need to purchase specialized equipment which can compete with the rest of the participants on the Bitcoin network for solving tough cryptographic puzzles. The miner to solve the puzzle in the fastest time gets to validate the transaction block and is rewarded a certain sum of Bitcoins which decreases over time.

Table 1: Estimated Bitcoin Energy Consumption Statistics.

Description	Value
Bitcoin's current estimated annual electricity consumption* (TWh)	62.06
Annualized global mining revenues	\$7,082,886,904
Annualized estimated global mining costs	\$3,102,851,896
Current cost percentage	43.81%
Country closest to Bitcoin in terms of electricity consumption	Switzerland
Electricity consumed per transaction (KWh)	939
Bitcoin's electricity consumption as a percentage of the world's electricity consumption	0.28%

Retrieved from <https://digiconomist.net/bitcoin-energy-consumption> Copyright 2021 by Digiconomist.

As seen in Table 1, the amount of electricity dedicated to Bitcoin mining operations leads to immense wastage and increased costs. In response to this, in 2012 Scott Nadal and Sunny King introduced the Proof of Stake (PoS) protocol incorporating it first in a new

cryptocurrency called Peercoin. PoS aims to minimize on electricity usage with the transactions in the network being validated through another way as opposed to the use of computational power in PoW. This involves the method in which a person can validate the percentage of transactions according to the amount of stake they hold in the coin. Along with this, investors can earn interest based on the amount they have put on stake for the purpose of validation in the network. As a thumb rule of Islamic finance, interest (Riba) is strictly forbidden. On the other hand, so is the creation of legal tender without an intrinsic value. In the case of Proof of Stake, both of these become true hence ruling that any digital currency following the Proof of Stake (PoS) protocol is Haram. Other variations of the PoS also exist, one being the Delegated Proof of Stake (DPoS). In DPoS, a representative democratic process is applied in which the users of the currency vote for delegates to serve on a panel that may contain a different number of witnesses. These panel members are responsible for confirming transactions, setting transaction fees and transaction sizes. Just like in PoS, the influence or power each delegate holds is directly proportional to the stake they contain in the coin.

The benefits of PoS can be seen in the non-Islamic world which has urged several cryptocurrency projects to make the transition from PoW to PoS in order to save the high electricity consumption. One of these is Ethereum, the second largest network by market capitalization after Bitcoin. To make this change, the lead developers of the network have decided to apply a gradual change in which every-one transaction block out of 100 that are processed will be secured via the PoS protocol whereas the rest will continue to use the PoW protocol (Heritage, A). This results in a hybrid system different from the pure PoW or PoS cryptocurrencies we have mentioned above which pose a problem from a Shariah compliance perspective.

Apart from the 2 widely used above mentioned protocols, a variety of others such as Proof of Funds, Proof of Activity and Proof of Capacity exist and before investing in any such coin that makes use of these, a Muslim should be well informed on their status in respect to the financial rules in Islam. One way to ensure this is to check that every protocol is in agreement with the requirements laid down by Islam which have been mentioned above.

6. Conclusion and Recommendations

In light of the above discussion, it can be concluded that the cryptocurrency ecosystem consists of both permissible and forbidden elements. In analyzing any digital currency or token, one must look at different aspects both from a technological and a religious point of view. Technologically, the consensus protocols must be analyzed logically to assess whether they are in line with Islamic conjunctions. Currently, the authors believe the Proof of Work (PoW) protocol as permissible whereas the Proof of Stake (PoS) protocol as forbidden. Religiously, the prohibitions of Riba, Gharar and Maysir must be checked against in every transaction or investment.

Cryptocurrencies should not be rejected as a whole, and the technological developments should not be ignored. These tools might be used in favour of Muslims. Halal cryptocurrencies can be developed jointly by Islamic countries and this can help the countries support each other in terms of trade and borrowing. Thus, Islamic digital currency model is necessary for applying Islamic law to the use of cryptocurrency. Hence, cryptocurrencies might be a suitable tool for Muslim countries.

Although the technical aspects of the cryptocurrency ecosystem were analyzed along with assessing the permissibility criteria according to Islamic teachings, further research is required to tackle more complex issues which are of significance in making cryptocurrency adaption possible in the Islamic world. Nevertheless, Islamic Shari'ah compliant Crypto currency can be feasible if and only if it is able to provide solutions to overcome the current vulnerabilities of Crypto currencies related to value creation and regulatory system.

References

- Abubakar, Y. S., Ogunbado, A. F., & Saidi, M. A. (2018). Bitcoin and its legality from Shariah point of view. *SEISENSE Journal of Management*, 1(4), 13-21.
- Abu Bakr, M. (2017, April 5). Is Bitcoin Halal? A Shariah Analysis. Retrieved August 21, 2021, from: <https://blossomfinance.com/is-bitcoin-halal-shariah-analysis-of-bitcoincryptocurrency-and-blockchain>.
- Adam, M. (2017, December 30). Shariah Interpretations of Bitcoin. Retrieved August 22, 2021 from <https://afinance.org/2017/12/30/shariah-interpretations-of-cryptocurrencies>.
- Al-Khalifa, S. (2022). CryptoHalal: An Intelligent Decision-System for Identifying Halal and Haram Cryptocurrencies. *Journal of Islamic Banking and Finance*, 3(1), 1-11.
From: *arXiv preprint arXiv:2211.06305*.
- Alzubaidi, I. B., & Abdullah, A. (2017). Developing a Digital Currency from an Islamic Perspective: Case of Blockchain Technology. *International Business Research*, 10(11), doi:<https://doi.org/10.5539/ibr.79-87>.
- Asif, S. (2018). The halal and haram aspect of cryptocurrencies in Islam. *Journal of Islamic Banking and Finance*, 35(2), 91-101.
- Bakar, N. A., Rosbi, S., & Uzaki, K. (2017). Cryptocurrency framework diagnostics from Islamic finance perspective: A new insight of Bitcoin system transaction. *International Journal of banking and finance*, 2 (5), 22-32.
- Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *The Journal of Economic Perspectives*, 29(2), 213-238.
- Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015, May). Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In *2015 IEEE symposium on security and privacy* (pp. 104-121). IEEE.
- Chan, S., Chu, J., Nadarajah, S., & Osterrieder, J. (2017). A statistical analysis of Cryptocurrencies. *Journal of Risk Financial Management*, 10(12), 214-221.
- Chohan, U. W. (2017). Cryptocurrencies: A brief thematic review. *Management Science and Business Administration*, 4(1), 19-28.
- Dorofeyev, M. A., Kosov, M., Ponkratov, V., Masterov, A., Karaev, A., & Vasyunina, M. (2018). Trends and prospects for the development of blockchain and cryptocurrencies in the digital economy. *European Research Studies*, 21(3), 429-445.
- Evans, C. W. (2015). Bitcoin in Islamic Banking and Finance. *Journal of Islamic Banking and Finance*, 3 (1), 215-231 from doi:10.15640/jibf.V3n1a1.

- Fokri, N. I. M., Ali, E. M., T. E., Nordin, Chik, N., M. Y. Sumayyah Abdul Aziz, S. A., & Jusoh, A. J. M. (2021). Classification of Cryptocurrency: A Review of the Literature, *Turkish Journal of Computer and Mathematics Education* 12 (5), 1353-1360.
- Goleman, T. (2018). Cryptocurrency: mining, investing and trading in blockchain for beginners. How to buy cryptocurrencies (Bitcoin, Ethereum, Ripple, Litecoin or Dash) and what wallet to use. Crypto currency investment strategies. Zen Mastery. *SSRN Electronic Journal*, 2 (4), 18-26. Available at [SSRN-id3101981.pdf](https://ssrn-id3101981.pdf) (boiv.org.au).
- Hertige, A. (2017, May 16). Ethereum's Big Switch: The New Roadmap to Proof-of-Stake. Retrieved April 08, 2018, from <https://www.coindesk.com/ethereums-bigswitch-the-new-roadmap-to-proof-of-stake/>
- Irwin, A. S. M., & Turner, A. B. (2018). Illicit Bitcoin transactions: challenges in getting to the who, what, when and where. *Journal of MoneyLaundering Control*, 21(3), 297–313.
- Kerscher, D. (2014). Bitcoin: Funktionsweise, risiken und chancen der digitalenwährung.
- Khalilov, M. C. K., & Levi, A. (2018). A survey on anonymity and privacy in bitcoin-like digital cash systems. *IEEE Communications Surveys & Tutorials*, 20(3), 2543-2585.
- Kristoufek, L. (2013). BitCoin meets Google trends and Wikipedia: Quantifying the relationship between phenomena of the Internet era. *Scientific reports*, 3, 3415.
- Maierbrugger, A. (2017, February 07). Islamic finance and digital currencies: The halal aspect. Retrieved August 22, 2021, from <http://www.gulf-times.com/story/532032/Islamic-finance-and-digital-currencies-The-halal-a> Digiconomist.(n.d.). Bitcoin Energy Consumption Index. Retrieved from <https://digiconomist.net/bitcoin-energy-consumption>
- Mainelli, M., & Smith, M. (2015). Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology). *The Journal of Financial Perspectives*, 3(3), 38-69.
- Maxson, S. Davis, S. and Moulton, R. (2019). UK Cryptoassets Taskforce publishes its final report. *Journal of Investment Compliance*. 20(2), 28-33.
- Meera, A.K.M. (2018). Cryptocurrencies from islamic perspectives: The case of bitcoin. *BuletinEkonomiMoneter Dan Perbankan*, 20(4), 475-492.
- Mukhopadhyay, S. C., & Suryadevara, N. K. (2014). Internet of things: Challenges and opportunities. *Internet of Things*, 1-17.

- Najeeb, S. F. (2014). Trading in Islam: Shari` ah rules and contemporary applications in Islamic financial transactions. *Journal of Emerging Economies and Islamic Research*, 2(2).
- Nakamoto, S.(2008). Bitcoin: A peer-to-peer electronic cash system. *Proceedings, Trento*,1-10.
- Ozиеv, G., &Yandiev, M. (2017). Cryptocurrency from Shari’ah perspective. *SSRN Electronic Journal*, 2 (3), 1-18. Available at [SSRN-id3101981.pdf \(boiv.org.au\)](https://ssrn.com/abstract=3101981).
- Polas, M. R. H., Muhibbullah, M., & Bhattacharjee. A. (2020). Is Bitcoin Halal or Haram in The Islamic Banking and Finance? An Overview, *Journal of Economics, Business and Market Research*.1 (2), 96-104.
- Saleh, A. A. I., Ibrahim, A. A. Noordin, M. F., &Mohadis, H M. (2020). Islamic Approach toward Purification of Transaction with Cryptocurrency *Journal of Theoretical and Applied Information Technology*, 98 (6), Retrieved August 18, 20221 from www.jatit.org p1050-1067.
- September 16, 2021, from <https://coinmarketcap.com/>.
- Sudais Asif, S., (2018)*. The Halal and Haram Aspect of Cryptocurrencies in Islam, *Journal of Islamic Banking and Finance* 2 (35) 91- 101. Retrieved August, 18 2021 from: external.worldbankimflib.org/uhtbin/cgiirsi/x/0/0/5/?searchdata1=37177{ckey}.
- Swan, M. (2018). Blockchain for business: Next-generation enterprise artificial intelligence systems. In *Advances in computers* (Vol. 1(11), 121-162. Elsevier.
- Tikhomirov, S. (2020). Security and Privacy of Blockchain Protocols and Applications (Doctoral dissertation, University of Luxembourg, Esch-sur-Alzette, Luxembourg).
- Uddin, M. (2015, October 13). Retrieved August 12, 2021, from <https://mpa.ub.unimuenchen>.
- Usmani, M. (n.d.). Forward Sales and Manufacturing Contracts: Salam AndIstisna. Retrieved
- Victor, F., &Luders, B.K. ttMeasuring Ethereum-based ERC20 Token Networks.
- Williamson, S., &Andolfatto, D. (2015). Scarcity of safe assets, inflation, and the policy trap. *Journal of Monetary Economics*, 73, 70-92.
- Wright, A., &Filippi, P. (2015, March 10). Decentralized Blockchain technology and the rise of lex
- Wu, K., Wheatley, S., &Sornette, D. (2018). Classification of cryptocurrency coins and tokens by the dynamics of their market capitalizations. *Royal Society open science*, 5(9), 180-381.

Zahudi, Z. M., & Amir, R. A. T. R. (2016). Regulation of virtual currencies: Mitigating the risks and challenges involved. *Journal of Islamic Finance*, 5(1), 63-73.

Zuckerman, M. J. (2018, January 18). First Bitcoin Futures Contract Expires At \$10,900, Win for Bears. Retrieved August 10, 2021, from <https://cointelegraph.com/news/firstbitcoin-futures-contract-expires-at-10900-win-for-bears>.