An Evaluation of Bitcoin from Shariah Perspective

Zaki Ahmad, Mahvish Nawaz Mokal, Ikhlas al-Amatullah, Mohamed Normen Ahamed Mafaz

School of Economics, Finance and Banking, Universiti Utara Malaysia, Malaysia
School of Language, civilisation and Philosophy, University Utara Malaysia
INCEIF, the Global University of Islamic Finance, Malaysia
Graduate School of Management (GSM), Management and Science University, Malaysia

ARTICLE DETAILS

ABSTRACT

Bitcoin is one of the most successful cases of blockchain use. The objective of this paper is to examine the characteristics of cryptocurrencies, with a specific emphasis on bitcoin. The fundamental attributes, features of bitcoin and how they operate on blockchain are evaluated from the Shariah perspective to determine if they are consistent with Shariah principles. To accomplish the objective, the authors adopted a qualitative secondary analysis (QSA) approach by utilizing the existing data.

JEL Classification:
M19,

DOI: 10.47067/ramss.v6i2.343

© 2023 The authors. Published by SPCR Global Publishing. This is an open-access article under the Creative Commons Attribution-NonCommercial 4.0

1. Introduction

In the era of digital and virtual currencies, cryptocurrency has brought about a new phenomenon in the financial services industry. The first cryptocurrency that entered the public domain in late 2008 was bitcoin, which is currently the most dominant cryptocurrency with the highest market capitalization, accounting for 51.39 percent of the total value (USD1.25 trillion) of all cryptocurrencies (CoinGecko, 2023). The blockchain is the underlying technology that powers cryptocurrency (Dorofeyev et al., 2018). Without the need for banks or other third parties, blockchain enables anybody to transfer money at any time, from anywhere in the world, at little to no cost (Garg, 2023; Gamage et al., 2020). By 2027, up to 10 percent of global GDP may be attributed to blockchain-enabled transactions (McKinsey, 2022). The alleged pseudonymous individual (or individuals) under the alias Satoshi Nakamoto, who founded bitcoin, wrote the bitcoin whitepaper titled “A Peer-to-Peer Electronic Cash System” in 2008 describing the proof of concept to manage its creation and transaction, and built and launched the initial reference implementation of bitcoin. The
first blockchain database was also created by Nakamoto as part of the implementation to serve as the public distributed ledger for cryptocurrency transactions. (Amsyar et al., 2020). It was the first virtual currency ever created, according to Nakamoto, to address the issue of double-spending without the need of a trusted authority or centralized server (Hellani et al., 2018).

Unlike government-issued fiat currency, which may materialize “out of thin air”, cryptocurrencies cannot. A precise procedure is required to produce the supply of cryptocurrencies. This procedure is called “mining” where individuals or entities use high-tech computer hardware and software to solve an intricate cryptographic puzzle. The ones confirming the transactions are called “miners” (Shovkhalov & Idrisov, 2021; Danielsson, 2019; Jamsheer & Muhsina, 2018). The security of the whole network is essentially ensured by this procedure, and the miners’ efforts are rewarded by the creation of cryptocurrency supply. The exertion of computer resources, electricity, time, and labor by the miners signifies value that supports the production of cryptocurrencies (Qian et al., 2023).

However, the speculative nature of cryptocurrencies has sparked controversy over their legality among Islamic scholars (Gaol et al., 2023). Hence, the aim of this paper is to explore the Shariah (Islamic Law) compliance of bitcoin, given it is the most popular and widely used cryptocurrency among others. In order to determine if they are in line with the Shariah principles, this paper looked at the characteristics of bitcoins, primarily from the standpoint of their creation and how they operate on the blockchain.

The remainder of the paper is structured as follows. After briefly stating the problem and the objective of this study, Section 4 provides an overview on the development and the features and functionalities of digital and virtual currencies, cryptocurrencies, bitcoin, and blockchain by reviewing the past literature. The methodology adopted to conduct this study is described in the following section. Section 6 highlights the characteristics of bitcoin and their compliance with Shariah as findings drawn from the analysis of their mechanism, followed by concluding remarks.

2. Problem Statement

With declining faith in fiat money, bitcoin has emerged as a new generation currency (Jasinski et al., 2023; Olowolayemo et al., 2023), enabling broader access to economic activities for the unbanked through digital currency (Kshetri, 2020). Some believe digital currency could outperform fiat money for the global economy (Jamsheer & Muhsina, 2018), driven by blockchain technology advancements (Qian et al., 2023). Bitcoin’s acceptance is growing worldwide, with increasing merchant adoption (International Monetary Fund, 2022). A Deloitte survey found 85% of US retailers plan to accept cryptocurrencies within two years, and bitcoin’s market expansion is projected at 56.4% CAGR (Triple-A, 2023). However, bitcoin’s Shariah compliance is debated due to its decentralized nature, price volatility, and risk potential (Belke & Beretta, 2020; Gaies et al., 2023). These issues may affect wealth preservation, a key Islamic objective (Hifz al-Mal) (Akbar, 2022). This paper aims to explore bitcoin’s Shariah compatibility, given its unique characteristics.

3. Objective

The main objective of this paper is to explore the Shariah compliance of bitcoin. Specifically, in order to determine whether or not they align with Shariah principles, this study will investigate the characteristics of bitcoin, as well as how they run on the blockchain.
4. Literature Review

4.1 Emergence of Digital/Virtual/Cryptocurrencies

In the early stages of civilization, people used to barter as their needs were very limited. They would trade and exchange goods and services for other goods and services. However, this method of payment created a lot of difficulties of finding suitable mutual exchanges as it was very complex and inefficient and led to increased costs for all participants (Bernholz, 2019). The crux of the problem with barter was that it required what economists call “a double-coincidence of wants” in order for the barter to be successful – I must want what you have, and you must want what I have (Astuti et al., 2022). To solve the problems of the barter system, the commodity money system was created.

In the commodity money system, people selected a few commodities which were widely used and easily available as a medium of exchange and payment, such as salt, wheat, shells, and others. Nevertheless, these commodities were not too easy to carry around, thus metallic monetary system was created where precious metals, such as gold and silver, were used as medium of exchange (Siddiqui, 2019). Precious metals were viewed as an ideal material for money due to their physical characteristics, such as durability and divisibility, with universally accepted purchasing power. However, it did not solve the complicated problems of exchange. It was very difficult to measure the value with these jaw pieces of metal (Kregel, 2021; Ahmad et al., 2020; Mokal & Abd Halim, 2023). As transactions started to become more complex and diverse, then the requirement for a more solid and stable medium of exchange rose. To solve this, standardized coins with specific weight and shape were made. This of course caused additional costs in mining, refining, and minting due to the need for coins (Bernholz, 2019).

The introduction of fiat money, government-issued paper as a means of payment, initially backed by gold or silver, was later detached from precious metals due to difficulties during the interwar period (Siddiqui, 2019). Today, countries issue currencies based on economic needs, often leading to fluctuating exchange rates and higher inflation (Taskinsoy, 2020; Bernholz, 2019). In the 21st century, money has evolved rapidly, embracing new forms like virtual payments and cryptocurrencies, offering cost-effective services and stability (Bavadekar, 2023; Kregel, 2021).

Advancements in technology, particularly computers and e-commerce, have reshaped businesses, replacing traditional cash and checks with electronic transfers (Ahmad et al., 2023). Digital money, or electronic payment, provides rapid transactions, lower fees, and enhanced security, benefiting financial sector businesses (Adrian & Mancini-Griffoli, 2021). This form of currency is known by various terms, including Digital Cash, E-cash, and Digital Tokens (Besson, 1999). Amid these changes, monetary policies are challenged by societal shifts, prompting central banks to consider issuing their own digital currencies (CBDC) (Bavadekar, 2023; Sukumaran et al., 2022).

4.2 Digital and Virtual Currency

Virtual currency, distinct from government-issued fiat currency, is privately issued and operates solely online (Wachira & Wachira, 2021). The European Central Bank (ECB) defined virtual currency in 2012 as unregulated digital money controlled by developers and used within specific online communities. The European Banking Authority (EBA) expanded the definition in 2014, describing virtual currency as a digital representation of value accepted for payment by individuals or entities without central bank or government authority, and transacted electronically (Financial Action Task Force, FATF).
"A virtual currency is a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status in any jurisdiction. It is not issued or guaranteed by any government and fulfills these functions only by agreement within the community of users of the virtual currency. Virtual currency is distinguished from fiat currency (a.k.a. “real currency,” “real money,” or “national currency”), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country. It is distinct from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency – i.e., it electronically transfers value that has legal tender status." (2014)

Digital currency is often used synonymously with the word “virtual currency” since it may refer to a digital representation of either e-money (fiat) or virtual currency (non-fiat) (Narayanan, 2020).

The widespread adoption of digital and virtual currency, along with conducting business through electronic money, has become common due to the banking industry's embrace of these systems, replacing traditional business methods (Hoang et al., 2021). Banks and financial institutions collaborate with electronic money networking processors to facilitate easy transfers from bank accounts to merchant accounts using branded network cards. Similarly, digital wallets utilize comparable transaction mechanisms, relying on centralized banking networks for payment processing and prevention of double-spending (Zhang et al., 2020). Transactions within this system adhere to regulated principles that can impact currency values (Jagtiani et al., 2021). This sparks the idea that if goods and services could be exchanged freely, society could determine the value of money (Armstrong & Siddiqui, 2020). To enable this, a tamper-proof transaction record database is essential, leading to the emergence of the blockchain platform as a recognized digital medium of exchange, including cryptocurrencies like bitcoins (Adrian & Mancini-Griffoli, 2021). This platform supports the creation and use of various cryptocurrencies, expanding beyond just bitcoins.

4.3 Cryptocurrency

Cryptocurrency is best described as a digital or virtual currency as it only operates on computers and has no physical form. It is dubbed “crypto” “currency” because all transaction data are software-encrypted using cryptography. The term “crypto” here refers to the encryption or cryptography upon which the instrument is built, while the term “currency” refers to the user’s acceptance of the instrument as a medium of exchange or a store of value, represented by the ownership of coins or tokens. It leverages the principle of encryption to control the creation of currency and to authenticate transactions, leaving no possibility for counterfeiting. The transactions are conducted between peers in a network without the need for an intermediary as with banks. (Amsyar et al., 2020). Amanzholova et al. (2020) described cryptocurrency as a computer file that cannot be copied or duplicated or used twice. The encryption process renders the encoded data unintelligible and scrambled (Amanzholova et al., 2020).

The two main goals of utilizing encryption are to control the cryptocurrency entering the system via mining and to validate a transaction. As a result, it strengthens and secures the system. The encryption key is often coupled with the encrypted data, and only those who have the key may decrypt it. The purpose is to conceal sensitive information from others by converting plaintext data into a string of random cypher text (encrypted information), which makes it difficult to read the
plaintext without decoding the data using a unique decryption key. (Zohuri et al., 2022). Any transactions that take place are recorded on the blockchain, which is a digital public ledger. The blockchain is distributed across many computers all around the world that host it. The data is stored and transmitted in a very precise manner. The message can only be viewed by those to whom it is directed. (Meunier, 2018). Like precious metals, the purpose of creating most cryptocurrencies is to gradually reduce the production of currency and eventually limit the total amount of currency ever in circulation (Jamsheer & Muhsina, 2018).

4.4 Blockchain

Blockchain is the technology behind the existence of cryptocurrencies, among other things. Blockchain is a decentralized, public database or ledger that maintains a continuously growing list of records called blocks, digitally distributed among the nodes or participants of a P2P network. This is known as distributed ledger technology (DLT). The database chronologically stores time-stamped records of all transactions, both old and new, in blocks that are securely linked together in a chain via cryptographic hashes. The nodes collectively adhere to a consensus algorithm protocol to add and validate new transaction blocks. Since each block contains cryptographic hash-based information of the previous block, they effectively form a chain, with each additional block linking to the ones before it. (Meunier, 2018). As a result, it allows for the permanent, immutable, and transparent recording and tracking of data and transactions shared across the network. Blockchain transactions are immutable in that, once they are recorded, the data in any given block cannot be altered retroactively without altering all subsequent blocks. (Xu & Zou, 2020). The system has built-in mechanisms that prevent unauthorized transaction entries and create consistency in the shared view of these transactions. The information is stored and managed in a decentralized manner, without intervention of outside parties or an intermediary, giving full control to the users and computer software algorithms. (Niranjanmurthy et al., 2019). Hence, no central authority owns or controls the blockchain. Instead, most decisions are based on a consensus of all the participating nodes of the network spread all over the world (Ertz & Boily, 2019). One of the most well-known public blockchain networks is the bitcoin blockchain (Srivastava et al., 2019).

4.5 Bitcoin

Bitcoin is the most popular and commonly used cryptocurrency. Nakamoto defined bitcoin as “a purely peer-to-peer version of electronic cash [that] would allow online payments to be sent directly from one party to another without going to a financial institution.” (Rahardja et al., 2021). It is a decentralized virtual currency with no central issuing authority. Once a bitcoin is mined, they can be sold, used as payment for retail purchases, or held as an investment to be traded later. Cryptocurrency trading websites are available around-the-clock and run independently to facilitate the buying and selling of bitcoin. The functionality of these websites is the same as that of traditional foreign exchange trading and brokerage platforms. (Caliskan, 2020). Nakamoto designed bitcoin to ultimately create 21 million bitcoins as rewards for solving mathematical algorithms which is crucial to maintain the bitcoin ledger for its mining. Of which, almost 83.21 percent have already been mined. Since the reward drops after every 210,000 blocks that are mined, bitcoin will continue to exist at least until 2040. (Srivastava et al., 2019).

Bitcoin comprises two key virtual components. The first is the blockchain, a distributed ledger that every computer (node) on the network possesses, containing a complete history of bitcoin transactions (Meunier, 2018). Bitcoin transactions occur over a peer-to-peer (P2P) network governed by the bitcoin protocol (Dotan et al., 2020), and the blockchain records these transfers. Each user
with the full bitcoin software has a local ledger copy, housing transaction records (Schilling & Uhlig, 2019; Ahmad et al., 2023). The second component involves key pairs, which consist of mathematically related large numbers. They enable actions by one party, verifiable by another, enhancing anonymity (Murty, 2019), thanks to the bitcoin protocol's encryption and verification, maintaining user privacy (Manimuthu et al., 2019).

Bitcoin transactions are validated by network nodes or miners to prevent double-spending, achieved through cryptographic puzzles (Hazari & Mahmoud, 2019). Miners then update the blockchain with solved transactions and receive bitcoins as compensation (Gamage et al., 2020). The security of this ledger depends on the incentive-driven efforts of miners to maintain it (Gamage et al., 2020). Bitcoin's decentralized structure, public transaction visibility, and protocol-based verification eliminate the need for centralized trust or intermediaries (Manimuthu et al., 2019). Individuals can easily create bitcoin wallets or join the network as nodes, while acquiring bitcoins involves purchasing them on cryptocurrency markets using traditional fiat money like the US dollar (Arslanian, 2022; Schilling & Uhlig, 2019). With these features, bitcoin emerges as a disruptive technology poised to challenge authorities (Zhang et al., 2020; Cumming et al., 2019), making it a significant contender in future disruptive technologies.

4.6 Bitcoin from Shariah Perspective

Some scholars do believe that cryptocurrencies are Shariah compliant (Sekaringsih & Al-Banna (2022), or at least found no conclusive evidence indicating that bitcoin violates Shariah principles (Pa & Hasan, 2021). Khan and Rabbani (2022) and Saleh et al. (2020) asserted that bitcoin or other cryptocurrencies may comply with the Shariah requirements and could be a better medium of exchange than fiat currencies. The fact that the price of bitcoin has recently soared to record highs – USD56,000 for one bitcoin as of 2021 (CNBC, 2021), is not an indication of its impermissibility from Shariah perspective. If anything, it is merely a hint that the demand for bitcoins is growing (Erwin et al., 2022).

In an effort to understand the volatility of bitcoin, Yermack (2014) discovered that it was 142 percent more volatile in 2013 than other currencies. While acknowledging its highly speculative nature, Siswantoro et al. (2020) did not dismiss its practical use in commercial transactions. Despite claims that cryptocurrencies are the preferred form of payment for money laundering, analytics reveals that fiat currency is used 800 times more often than cryptocurrencies for money laundering (Messari, 2020). Although bitcoin is not fully immune from unlawful activities, fiat currency continues to be the favored option for money laundering. Abubakar et al. (2018) opined that blockchain may possibly aid in the battle against money laundering. They opposed declaring cryptocurrencies illegal under Shariah owing of their volatile value.

According to several studies (Abozaid & Khateeb, 2021; Saleh et al., 2020; Oziev & Yandiev, 2018), bitcoin like any other currency is regarded as money within its community, and therefore some conditions that apply to currency exchanges from a Shariah perspective will apply when exchanging bitcoin for other currencies. The conditions are: (i) exchange must be made on spot; and (ii) there shall not be speculations on currencies. This indicates that the intention must be to use the currency for both buying and selling, and not only for exchange of currency (Oziev & Yandiev, 2018). However, in the opinion of Khan and Hakami (2022), there is still a significant potential of manipulation until bitcoin is traded on an open market like other currencies. This is due to the fact that a small number of early investors still own a sizable majority of bitcoins (Brown, 2019). As of
2017, about 40 percent of bitcoin is held by about 1,000 users (Kharif, 2021). Nakamoto alone is believed to possess about five percent, i.e., approximately 1.1 million, of the entire bitcoin (CNBC, 2021).

On the contrary, the use of bitcoin is frowned upon by some scholars. Turkey’s Directorate of Religious Affairs (Diyanet), a state organization dealing with religious matters, ruled that cryptocurrencies are open to speculation; they are not yet appropriate for Muslims to use. Their decision states that: “Buying and selling virtual currencies is not compatible with religion at this time because of the fact that their valuation is open to speculation, they can be easily used in illegal activities like money laundering, and they are not under the state’s audit and surveillance.” (Ensonhaber, 2017). Bahar (2022) found a strong correlation between bitcoin and the element of risk (maysir) and uncertainty (gharar) due to the anonymity of bitcoin holders. The anonymous nature of bitcoin would make it nearly impossible to track the actual account holder in the event of any suspicious behavior (Ayedh et al., 2021; Siswantoro et al., 2020). Bitcoin may be appropriate for limited usage (Khan & Hakami, 2022). Implementing it across all economic sectors must have a clear mandate since fraud is a possibility in the absence of a centralized authority (Cumming et al., 2019). Therefore, this paper will analyze the true nature and characteristics of bitcoin from Shariah perspective based on the classical fiqh (Islamic Jurisprudence) rulings.

5. Methodology
This study adopted a qualitative secondary analysis (QSA) method by utilizing the existing secondary qualitative data in order to investigate if the characteristics of bitcoin are consistent with Shariah principles. The major secondary sources of information that the authors mostly relied on were desktop research tools, which included research papers, journals, textbooks, news reports, and other publications that are available in print or online. The data gathered were then analyzed, organized into themes, and discussed in this paper. The paper mainly focuses on the key characteristics of bitcoin as determined by an analysis of its mechanism and the compliance of these characteristics with Shariah principles according to the classical fiqh viewpoints.

6. Findings and Discussion
This section will present the key characteristics of bitcoin and their compliance with Shariah as findings drawn from the analysis of their mechanism based on the existing literature.

6.1 Key Characteristics of Bitcoin
6.1.1 Mechanism of Blockchain
Blockchain technology is used by bitcoin as its transaction ledger. Whether bitcoins are being stored in a digital wallet or used for trade, blockchain ensures that they are all tracked. Any user who is hosting a copy of the blockchain receives notification of any bitcoin transaction that is made. The miners then use specialized software to attempt to crack a cryptographic puzzle, which enables them to add a “block” of transactions to the ledger. (Ertz & Boily, 2019). A ledger is updated with several transactions at once. Miners sequentially add these “blocks” of transactions. Because of this, the ledger and the underlying technology are referred to as “block” and “chain.” A “chain” of “blocks” of transactions makes up the system. (Schilling & Uhlig, 2019).

It is difficult to alter the historical records of bitcoin transactions or at least simple to spot attempts to tamper since each block in the blockchain is cryptographically linked to the preceding block. Cryptography is what keeps the blockchain secure. (Xu & Zou, 2020). As the blockchain is a
distributed file system with participants having copies of the file, any changes are made by consensus. This file is composed of blocks, each of which contains a sequence of transactions with the primary data consisting of a timestamp, the cryptographic signature (hash) of the previous block, the hash of the current block, and additional information. The current block is connected to the previous block via the hash of the previous block, and the following blocks will also need the hash of the current block, forming a chain. If a block is modified in any way, it is possible to compute its hash and come up with a result that differs from the one that was expected, in which case the block would be rejected. The entire history of the system is thereby integrated into the current block by incorporating the hash of the previous block. (Meunier, 2018).

6.1.2 Mechanism of Bitcoin

Simply put, the transfer of bitcoins is very much like regular online bank accounts in that when one person transfers money to another, their account balance is adjusted accordingly (Rahardja et al., 2021). Since the data stored in blockchain are irreversible, it compels everyone to “play fair”, eliminating the possibility of double-spending. A user who attempts to spend the same bitcoin twice is said to be double-spending. Blockchain stops double-spending by broadcasting groups of transactions to all nodes in the bitcoin network and timestamping them. (Hellani et al., 2018). The blockchain’s public nature allows all network participants to monitor and evaluate bitcoin transactions in real-time (Rahardja et al., 2021).

The process requires the user to first sign up for an account to create a bitcoin wallet. This digital wallet allows users to transfer funds between accounts. The user must have the private key, which functions like a password, to be able to access the account to manage their cryptocurrency funds and authorize any transactions. (Murty, 2019). The private key is formed by the wallet and is used to create the user’s public key (their wallet address), that acts similarly to a bank account number, using Elliptic Curve Cryptography (ECC). The private key is used to generate digital signature based on cryptographic algorithm, while the public key is used to verify the digital signature. (Xiao et al., 2021). These P2P transactions are encrypted before being broadcast to the bitcoin network and queued up for around ten minutes to be recorded in the public ledger via mining process by the miners (Arslanian, 2022). All bitcoin transactions are stored publicly and permanently in the P2P network (Gamage et al., 2020). Bitcoin does not take into consideration any information relevant to a user’s actual identity due to the wallet address that is obtained via ECC, therefore enabling participants to become pseudo-anonymous in the bitcoin network to protect their privacy, unless details are made known during a transaction or in other situations (Xiao et al., 2021). Thus, even though it can be used multiple times, it is best practice to use the wallet address only once since anybody can view the public ledger and know how many transactions are made (Murty, 2019). Figure 1 below illustrates an example of a simple bitcoin transaction.
6.1.3 Mining Process of Bitcoin

Bitcoin mining involves the process of validating transactions and adding them to the blockchain ledger, which results in the generation of new bitcoins – like a central bank printing new fiat money. The process works similarly to how gold is extracted and circulated, hence the term “mining”. (Schilling & Uhlig, 2019). Bitcoin miners solve complex hash equation-based cryptographic puzzles using sophisticated hardware, i.e., a blockchain node, which runs the protocol software, to create a new block for the purpose of validating and logging the new transactions on the blockchain ledger. When a block is validated, the transactions bundled in it are verified and the block is then added to the chain, and this happens every ten minutes. In return for their computational efforts, the miners are rewarded with transaction fees and newly created cryptocurrencies, which are volatile and speculative in value, in their wallet for the new block. (Aljabr et al., 2019).

Since bitcoin mining is an open source, anybody with specialized hardware can be a miner and validate a transaction. The first miner to successfully crack the puzzle gets to add the new block of transactions to their blockchain ledger and broadcast it to the network. Once added, the block gets chained, creating a chain of transactions that are in effect permanent and irrevocable; they cannot be altered or removed. This process is called the “proof-of-work system.” (Fullmer & Morse, 2018). The interplay between transactions, blocks, and the public blockchain ledger makes it impossible for anybody to arbitrarily add or change a block. Since this decentralized network is not owned or controlled by a central authority and is run on a peer-to-peer basis, with the control being equally distributed among its users across the entire network and the fact that anybody may participate in mining, a system is required for every bitcoin transaction to avoid abuse by one governing member (Arslanian, 2022). Based on their mechanism from the above, the following characteristics of bitcoin are deduced:

- Anonymous and decentralized
- Requires mining
- Volatile and speculative
- Not backed by any authority
6.2 Evaluation of Bitcoin’s Characteristics from Shariah Perspective

This section will discuss the four aforementioned characteristics of bitcoin from the perspective of Shariah. As the characteristics will be evaluated using the Islamic Legal Characterization (takyif fiqhi), they are divided into internal and external characteristics. The internal characteristics will include: (i) anonymous and decentralized; and (ii) requires mining, while the external characteristics will comprise: (i) volatile and speculative; and (ii) not backed by any authority.

6.2.1 Internal Characteristics

This subsection will assess the internal characteristics of bitcoin, such as it operates anonymously and in a decentralized system and that it requires to go through the process of mining, from the Shariah perspective to confirm if they comply with the tenets of Islam.

(i) Anonymous and Decentralized

As discussed earlier, the blockchain is a platform used for bitcoin transactions. Blockchains are open-sourced ledgers that record every transaction, making it incredibly simple to determine if fraud is occurring. Miners, who verify transactions continuously 24 hours a day, monitor and protect the integrity of blockchain networks. The world’s blockchain transactions are constantly being verified by tens of thousands of miners at any one time. (Aljabr et al., 2019). Due to this, decentralized bitcoins built on blockchains are subject to a massive degree of monitoring and are almost completely protected against fraud risk (Meunier, 2018). Decentralized blockchains have this as a major advantage.

Although Nakamoto, who invented bitcoin, remains anonymous to this day, users do not need to worry about whether he or anybody else has complete control over the currency. This is due to the fact that bitcoin’s source code is open source, meaning that everyone can see it. Because of openness, it is possible for any software developer to research the protocol and produce a newer version of their own for future development. (Garg, 2023). In fact, bitcoin is programmed to function only when the whole network of users has agreed upon it. This makes sure that no developer may alter bitcoin without breaking the network’s interoperability as a whole (Adrian & Mancini-Griffoli, 2021).

As shown in Figure 1 above, a bitcoin wallet is a set of bitcoin addresses and private keys that is managed by bitcoin software. An alphanumeric string of characters or a cryptographic hash is what makes up a bitcoin address. There is no other information provided that may help trace the real identity of the sender and the recipient behind the bitcoin wallet address (Xiao et al., 2021).

The idea that bitcoin is an anonymous form of payment is a prevalent misconception. This misconception often results from a lack of familiarity with the underlying technology itself. Unlike cash, a bitcoin transaction is recorded on the blockchain without any involvement of third-party intermediaries, thus nobody knows the real identities of the bitcoin holders. The sender and recipient’s public keys, the amount, and a time stamp are just some of the details that are saved. Every transaction that has ever occurred in the history of bitcoin is documented, stored on the blockchain, and accessible to everyone. (Murty, 2019). Bitcoins may be anonymous similar to cash in that transactions may take place between parties without having their identities disclosed, but they differ from cash in that it is possible to track transactions to and from any bitcoin address (Fullmer & Morse, 2018). Bitcoin is therefore not anonymous, but rather pseudonymous.
From the Shariah perspective, this anonymity is not purely anonymous. Bitcoin transactions with their pseudonymity still satisfy the four essential elements of a valid (sahih) contract (aqd), namely: (i) sigah - offer (ijab) and acceptance (qabul) – one party to the contract makes an offer while the other party accepts the offer; (ii) aqidan - contracting parties which are the buyer and the seller must have the ability and legal capacity (ahliyyah) to enter into a contract for their mutual contract; (iii) subject matter (ma'qud alayh) – must be lawful, in existence, deliverable, precisely determined and owned by the offeror; and (iv) consideration (price) – must be something capable of being given like money and goods. Therefore, if the subject matter satisfies the conditions, such as being a permitted (halal) commodity, existing, and being lawfully owned, as well as having all of its characteristics described and its price disclosed, then the offer and acceptance should be fulfilled successfully, even if there is bargaining (Muneeza & Mustafa, 2019).

While the bitcoin system is anonymous, it technically is not since a buyer and a seller genuinely exists in their legal capacity. For a contract to be valid under Shariah, both parties must fulfill the required conditions of legal capacity, i.e., have reached the age of puberty and are mentally competent. A person must possess this legal capacity in order to be eligible to exercise their rights and carry out their contractual obligations and responsibilities (Lateh & Rejab, 2021). As such, anonymity is not an issue from in the case of conducting bitcoin transactions from the Shariah standpoint since it is not required that the parties to a contract know one another, present their identification, or reveal their faces (Siddique & Shah, 2021). In the supermarket, for instance, there is a self-checkout system that allows customers to choose, purchase, and pay for their items without the assistance of a cashier.

Nonetheless, in a decentralized system, the identity of the bitcoin holder is kept in an encrypted address that they can control, but it is not linked to an individual’s identity; as a result, this makes it more desirable and alluring to conduct financial crimes. Since there is an additional layer of secrecy within the industry concealing their identity, the absence of regulatory controls and complicated technology make it enticing to hackers and fraudsters. (Kethineni & Cao, 2020). Such nature of bitcoins violates some of the Shariah principles. For example, they include gharar (uncertainty) due to the users’ anonymity, as well as tadlis (deceit), fraudulent behavior, and crimes (Bahar, 2022). No single passage in the Qur’an explicitly mentions gharar, however it is said:

وَلاَ تَقْتُلُواْ أَمْوَالَكُمْ بِالْبَاطِلِ إِلَّاَّ أَنْ تَكُنْ تَأْكُلُواْ فَرْقًا مِّنْ أَمْوَالِ النَّاسِ بِالْأَدْمَ رَبُّكُمْ تُعْلَمُونَ

“Do not devour one another’s property wrongfully, nor throw it before the judges in order to devour a portion of other’s property sinfully and knowingly.” [al-Baqarah: 188]

Another evidence to support this prohibition is:

بَا أَيُّهَا النَّاسُ لَا تَكُنَّ تَأْكُلُواْ أَمْوَالَ الْكُتَّابِ بِالْبَاطِلِ إِلَّاَّ أَنْ تَكُنْ تَأْكُلُواْ فَرْقًا مِّنْ أَمْوَالِ النَّاسِ بِالْأَدْمَ رَبُّكُمْ تُعْلَمُونَ

“You who have believed, do not consume one another’s wealth unjustly but only in lawful business by mutual consent. And do not kill yourself [or one another]. Indeed, Allah is to you ever Merciful.” [an-Nisa:29]

From the interpretations made by various Shariah scholars it was found that the Hanafi School of Thought defined gharar as “that whose consequences are hidden.” According to certain
scholars from the Shafi’i School of Thought, it is “something which in its manner and its consequence is hidden.” Hanbali, on the other hand, referred to it as “that whose consequences are unknown.” (Al-Saati, 2003). Islam explicitly prohibits any economic transactions that result in exploitation and injustice of any kind to the contracting parties. By forbidding gharar in any commercial exchange contracts that are not free from risk, hazard, or speculation about the crucial components of the transaction to either party, or uncertainty of one party’s capacity to honor its rights and obligations, it seeks to protect the parties involved from deceit and ignorance. In order for any party to uphold its rights and duties, it mandates that all Islamic financial transactions to be founded on accuracy, completeness, truth, openness, and disclosure of all relevant facts to ensure that neither party has an unfair advantage over the other. (Al-Suwailem, 2000). The possibility of fraudulent conduct is another breach of Shariah principles. Literally, the word “fraud” refers to deliberate deception to get an unjust gain or deprive someone of their right. Fraud is morally reprehensible, both logically and in conformity with civil and criminal law. (Lateh & Rejab, 2021). It is mentioned in the Qur’an:

وَمَا كَانَ لِنَبِيٍّ أَنْ يَغْلَّ ۚ وَمَنْ يَغْلُلْ يَأْتِ بِمَا غَلَّ يَوْمَ الْقِيَامَةِ ۚ ثُمَّ تُوَفَّىٰ كُلُّ نَفْسٍ مَّا كُسبَتِ

“It is not [attributable] to any prophet that he would act unfaithfully [in regard to war booty]. And whoever betrays, [taking unlawfully], will come with what he took on the Day of Resurrection. Then will every soul be [fully] compensated for what it earned, and they will not be wronged.” [al-Imran:161]

Therefore, it may be concluded that bitcoin does not transgress the Shariah principles due to its inherent characteristics of a decentralized system and pseudonymity among the user base. It must be taken into account, nevertheless, that such nature of bitcoin may open door for criminal activity and fraudulent conduct (Panda & Jani, 2019), necessitating the implementation of certain risk management strategies (Cumming et al., 2019).

**(ii) Requires Mining**

As previously explained, the method of creating bitcoins is known as mining. As new block transactions are verified, they are added to the public ledger as part of the mining process, which keeps the blockchain up to date. Some claimed that mining bitcoins was generating income out of thin air (Ayedh et al., 2021). To address this, it is important to understand that the creation of bitcoins requires more technological labor than it does manual labor by actual people.

Several factors, including the cost of mining and the degree of difficulty, must be considered. To continue boosting computational power, miners must employ several types of hardware. In fact, specialized software is needed to connect the miners to the blockchain and mining pool. This software is in charge of assigning tasks to the miners, collecting completed tasks from the miners, and transmitting this data back to the blockchain. To secure a transaction from the usage of the mining hardware and software, the miners must invest a significant amount of their time, effort, and money on computational power and electricity consumption (Srivastava et al., 2019).

The cost of mining equipment is influenced by the hashrate as well as the time it will take to receive the product after placing the order. The lifespan of mining equipment is typically between three and six months. (Aljabr et al., 2019). As a result, the miners in this industry are required to continually invest any profits earned in order to keep the hardware and software upgraded used in
mining. To prevent bitcoin mining from being unfairly exploited, proof-of-work schemes utilize computational puzzles that are difficult to solve but simple to verify. This resembles a “captcha” that takes intensive computational resources to solve (Xiao et al., 2021).

Given the value placed on the work and services provided by miners, it is only reasonable for them to get compensation in the form of a fee. The miners are rewarded with newly minted bitcoins and transaction fees as payment for contributing their computational power to the network. Regarding this payment of fees, there is no Shariah concern since Islam recognizes labor and effort and hence urges that the job done be properly compensated as long as it is lawful (Muneeza & Mustafa, 2019). Prophet Muhammad (peace be upon him [PBUH]) said:

“He upon whom his brother has a right, be it of the nature of money or honor, let him compensate for it before he is made to compensate for it on a day when there will be neither dinar nor dirham to deal with. Instead, if he has a good deed in his account it will be taken away from him and given to the person he had wronged. And if he has no good deeds in his account, sins of the other person will be taken from him and added to his account.” [al-Bukhari 6534]

It is against Islamic doctrine to employ an individual to undertake a job and then fail to pay them their due. In a Hadith Qudsi, narrated by Abu Huraira, Allah (God) sent a warning via the Prophet (PBUH), saying:

“I will be an opponent to three types of people on the Day of Resurrection: one who makes a covenant in My name but proves treacherous; one who sells a free person and eats his price; and one who employs a worker and takes full work from him but does not pay him for his labor.” [Sahih al-Bukhari 2270]

The difficulty level that miners encounter in securing a bitcoin network and solving the algorithm must also be taken into account, in addition to the amount of computing resources and electricity is required. The fact that these two elements may also influence the price of each token demonstrates the significance of the mining process and the expertise needed to be a miner. Prophet Muhammad (PBUH) warned:

“You should pay the laborer his wages before his sweat dries.” [Sunan ibn Mâjah 2443]

This Hadith makes it very plain and obvious that workers must be paid on time. A worker should be compensated right away if they are hired to perform a task. However, if a contract stipulates that salaries must be paid weekly or monthly, this is how it must be done. In contrast, this is true of miners who toil and achieve since only then would they be paid (Abubakar et al., 2018).

### 6.2.2 External Characteristics

Under external characteristics, the volatile and speculative value of bitcoin, as well as the fact that it is not backed by any authority are evaluated from the Shariah perspective.

#### (i) Volatile and Speculative

The majority of bitcoin users profit from bitcoin as a short-term investment by capitalizing on its price fluctuations. As a result, many are making money by buying cheap and selling high, while others use bitcoin as a long-term investment in the hopes that the price would rise over the years.
Numerous factors contribute to the volatility of bitcoin. One of them is bitcoin, like most cryptocurrencies, is unregulated, and hence they will continue to be traded on free markets (Patel et al., 2022).

The free or open market is a kind of economic system that is based on supply and demand with little to no intervention from the government. The open market and the consumers, where the law of supply and demand is unhindered by government influence or monopolization, determine the pricing of goods and services. Price swings of 20 percent or more in a single day are not uncommon for bitcoin as it is mostly influenced by supply and demand, investment and user sentiments, and media hype due to the lack of a centralized regulatory regime (Gaies et al., 2023). This explains why bitcoin and other cryptocurrencies will continue to be volatile up until they hit their market capitalization and saturation, which nobody can predict with certainty (Zhang et al., 2020). Another reason is that there are only 21 million bitcoins available in total as how it was designed by Nakamoto, and not all of them have yet been mined. This makes bitcoin highly illiquid. The majority of the ones that are available are owned by a small number of individuals, limiting their liquidation. When liquidity is low, few individuals are either willing to sell or to purchase. (Srivastava et al., 2019). Therefore, there would not be enough bitcoin available for someone to purchase a large quantity at once. This would raise the price until more people started selling. The same holds true in reverse: if someone wants to sell their bitcoins but finds nobody to buy, in which case the price will fall until far lower prices entice buyers (Kharif, 2021).

Additionally, the extreme volatility of bitcoin limits its usefulness as a store of value. A stabilizing element, which is redundant to the volatile nature of cryptocurrencies, is necessary for a currency to be considered legal tender (Amsyar et al., 2020; Belke & Beretta, 2020). Consider the scenario where a loaf of bread that costs RM0.20 today costs RM2.00 tomorrow owing to currency fluctuations. The way bitcoin behaves with its prices moving more in sync with the stock market, bitcoins are unlikely to be used as an alternative medium of exchange (Baur & Dimpfl, 2021). In regard to that, Imam Malik said:

لا خير فيها نظرة بالذهب ولا بالورق, ولو أن الناس أجازوا بينهم الجلود حتى تكون سكة, وعين لكرهتها أن تباع بالذهب والورق نظرة

“There is no good in the sale of fulus for gold or silver by deferred payment. And if the public were to accept leather (as medium of exchange) and turned it into minted money, I would detest its sale for gold and silver for deferred payment.” [Al-Mudawwanah]

Such volatility carries substantial risks of speculation leading to maysir (gambling). Islam clearly prohibits all forms of gambling. Shariah deems maysir and qimar, the two types of gambling transactions, to be wholly inequitable. Maysir refers to the effortless acquisition of wealth via luck, whether or not it violates another person’s right (Gaol et al., 2023). Therefore, it is prohibited for anybody to benefit from investing in bitcoin merely on the basis of speculation, without sufficient knowledge or a thorough analysis (Abubakar et al., 2018). This prohibition under Shariah does not apply to activities that include knowledge, skill, the investment of assets, and labor, as well as those that rely on the analysis of economic and financial data (Lateh & Rejab, 2021). Instead, it is the one that involves making an effortless gain based on chance or wagering. It is considered gambling because there is no assurance that the large sums of money invested in the creation of cryptocurrencies will be profitable or not. In order to earn money, the miners strive to solve complex mathematical puzzles; if they fail, they get nothing (Bahar, 2022).
(ii) Not Backed by Any Authority

Since Bitcoins operate on a decentralized network, there are no authorities to oversee the system and serve as an undertaker in the event of a problem. Moreover, bitcoins are not backed by any precious metals, such as gold or silver (Murty, 2019). Due to the risks involved, most countries do not agree to regulate bitcoin (Sukumaran et al., 2022). As such, bitcoins are seen by most people as being unreliable and untrustworthy (Scharding, 2019). Bitcoin's greater adoption would be discouraged by the uncertainty of the network's security. Due to the lack of regulation and insurance, as well as the fact that most central banks and monetary authorities do not permit the production, trade, or use of virtual currencies, including bitcoins, users are exposed to a variety of hazards. There is also no viable customer remedy available for bitcoins, unlike conventional financial products that have robust consumer protections. (Prayogo, 2018). There is no intermediary with the authority to control customer losses in the event that bitcoins are lost or stolen (Niranjanmurthy et al., 2019). Because most regulators appear reluctant to oversee, there is a lack of security and an absence of a well-established consumer protection framework in terms of protecting customers (Scharding, 2019).

Apart from a few countries, such as Egypt, China, and Indonesia, where bitcoin is banned, most bitcoins and its system are not restricted by any laws (Neti, 2022). This makes the regulation of bitcoin exceedingly difficult as there is no governing body or applicable legislation. If fraud or scam occurred during bitcoin transactions, no one would be able to control it (Sukumaran et al., 2022). Any principle of human justice and their rights will be broken when there is no legislative body or act to govern. It is clarified in the Qur'an to be truthful and equitable in dealings:

وأوقوا الكبائر إذا كنتم وزنوا بالقسطاس المستقيم

“And give full measure when you measure, and weigh with an even balance. That is the best [way] and best in result.” [Surah al-Isra: 35]

This may be in conflict with Hifz al-Mal (preservation of wealth) – one of the five objectives of Shariah (Maqasid al-Shariah). Hifz al-Mal goes beyond wealth preservation; it encourages the creation, accumulation, and preservation of wealth as well as the degree of protection of property rights and ownership, transparency in financial transactions, and the equitable and just distribution of wealth. This will contradict the concept of maslahah (public interest) due to the unpredictable nature of bitcoin in the absence of any regulatory legislation (Akbar, 2022).

7. Conclusion

This study was conducted to evaluate bitcoins' conformity with Shariah. In light of this, a conclusion may be drawn that bitcoins are by their very nature acceptable and do not violate the Shariah principles. This is evident from bitcoin's fundamental existence, which involves mining, that obviously requires work and effort when looked into its internal characteristics. In addition, cryptocurrency is not completely anonymous as long as the conditions for a transaction contract are satisfied. The blockchain provides the foundation for bitcoin, as was explained in the examination of the internal factor. The requirements of Shariah for disclosure and openness may be aided by blockchain. It has the potential to enhance current notions of trust in trade and transactions. Blockchain may further help to uphold the principle that only cash should be used to trade currency and goods. Issues with decentralized systems and anonymity may also result in gharar (uncertainty) and non-compliance with Shariah only if they are tied to illicit activities like fraud and scams. This is an outside aspect that has no immediate impact on the bitcoin legal requirements under Shariah. In
general, anything being used for an illegal purpose does not make it illegal in and of itself. It is recommended that regulations be established in order to address this issue.

However, based on the external characteristics discussed, it may be said that bitcoin does not adhere to Shariah, since market speculation about price and value contains gharar and has other elements of gambling. Speculation is an uncontrollable external factor that is unconcerned with determining the legitimacy of currency. Like with all other assets, prices are always dependent on the law of supply and demand. Therefore, the fact that bitcoin is subject to speculation cannot be used to deem it haram (unlawful). Even fiat money has the same issue, proving that the volatility of bitcoin’s value is insufficient to render it unlawful from a Shariah perspective. Furthermore, because bitcoin is not supported by any government, there is a potential that it may violate the principle of maslahah (public interest). One of the main factors that causes confusion among Islamic scholars is the absence of a regulator for cryptocurrencies. High levels of maysir (risk) and gharar, a lack of actual tangible assets, and governmental assurances are some of the key criticisms against bitcoin. To sum up, bitcoin is legal and compliant with Shariah in its most basic form. In general, there does not seem to be any conclusive proof that utilizing bitcoin is Islamically prohibited. Dealing with bitcoins is acceptable from a Shariah perspective. However, one of the primary objectives of Shariah (Maqasid al-Shariah) is the preservation of wealth (Hifz al-Mal). It is thus essential for cryptocurrency users, especially bitcoin holders, to be aware of the hazards involved.

References


merchant-getting-ready-for-crypto.pdf


Multidisciplinary Conference on Engineering Technology (IMCET), Beirut, Lebanon. https://doi.org/10.1109/IMCET.2018.8603029


