A Comparative Analysis of Blockchain Consensus Algorithms from Shariah Perspective

Tasneem Darwish[1*], Kamalrulnizam Abu Bakar[1], Gen Matsuda[2], Ahmed Aliyu[1], Abdul Hanan Abdullah[1], Abdul Samad Ismail[1], Raja Zahilah[1], Ahmad Fadhil Yusof [1], Mohd Murtadha Mohamad[1], Mohd Yazid Idris[1], Zuhaimy Ismail[3], Ahmad Che Yaacob[4], Herman[5]

[1]School of computing, Faculty of Engineering,
Universiti Teknologi Malaysia (UTM), 81310 Skudai, Johor, Malaysia
[2]OK Blockchain Centre Sdn. Bhd. Unit B19, level 19, Tower B, Medini 9,
Persiaran Medini Sentral 1, Bandar Medini Iskandar, 79250,
Iskandar Puteri, Johor, Malaysia
[3]Mathematical Sciences Department, Faculty of Science,
Universiti Teknologi Malaysia (UTM), 81310 Skudai, Johor, Malaysia
[4]Faculty of Islamic Civilization, Universiti Teknologi Malaysia (UTM),
81310 Skudai, Johor, Malaysia
[5]Universitas Ahmad Dahlan Indonesia,
Daerah Istimewa Yogyakarta 55166, Indonesia

[*]Corresponding Authors
tasneem83darwish@gmail.com, g_matsuda@okwave.co.jp

Received: 4 June 2020
Accepted: 27 June 2020
Online First:

ABSTRACT

Blockchain provides a distributed digital ledger platform for not only cryptocurrencies but also many other distributed applications. Blockchain platforms work flow and performance are controlled by the used consensus algorithms. Although many studies evaluated cryptocurrency from the Shariah perspective, they focused only on the cryptocurrency concept and did not consider the underlying blockchain technology. However, designing a Shariah compliant application on top of a non Shariah compliant platform does not fulfil the requirements of Shariah. Therefore, it is necessary to

PENERBIT PRESS
UNIVERSITI TEKNOLOGI MARA

use a Shariah compliant blockchain platform in order to produce Shariah compliant blockchain applications. To support the production of Shariah compliant blockchain applications, this study provides a comparative analysis of the most used consensus algorithms in blockchain platforms. In particular, the considered consensus algorithms are evaluated from a Shariah perspective. In conclusion, based on the conducted evaluation some of the widely used blockchain platforms (e.g. Bitcoin and Ethereum) are found to be not compliant with the Shariah rules due to using a consensus algorithm that is not Shariah compliant.

Keywords: *Blockchain, Shariah Compliant, Consensus, Cryptocurrency, Digital Currency.*

INTRODUCTION

Traditionally, the confirmation and record of financial transactions depend entirely on a centralized trusted institution, which may cause many problems of transaction cost, efficiency, and security (Mingxiao et al., 2017). To address this issue the first cryptocurrency "Bitcoin" was introduced as a Blockchain technology application (Nakamoto, 2008). Blockchain technology enables the creation of peer-to-peer transactions which would allow online payment to be sent directly from one party to another without going through a third party or financial institution (Zheng et al., 2017).

After the success of the first cryptocurrency "Bitcoin" (Nakamoto, 2008), Blockchain technology has attracted the industry and academia sectors (Viriyasitavat & Hoonsopon, 2018). Although Blockchain was introduced to serve cryptocurrencies, currently its applications span across diverse areas including various financial services such as digital assets, remittance and online payment (Zheng et al., 2017), insurance (Hess et al., 2017), medical information security management (Liu, 2016; Yue et al., 2016), economics (Huckle et al., 2016), Internet of things (Dorri et al., 2017), smart cities (Biswas & Muthukkumarasamy, 2016), and supply chain (Xu et al., 2016).

Blockchain is a distributed digital ledger which records transactions after verifying them in a block. The blocks are connected together as a chain which continuously grows when new blocks are appended to it (Zheng et al., 2017). In the Blockchain peer-to-peer networks the participants that validate transactions and generate the new blocks are called "validators" or "miners". To manage the process of creating and validating new blocks a consensus algorithm is used.

The core element of any Blockchain application is its consensus algorithm as it controls how the blockchain works (Zheng et al., 2016). The main purpose of using a consensus algorithm is to resolve the problem of reliability in a network involving multiple unreliable nodes (Bach et al., 2018).

In addition, the consensus algorithm plays a crucial role in maintaining the security, robustness and efficiency of blockchain. Using the right algorithm is significant to improve the performance of blockchain applications (Mingxiao et al., 2017).

One of the main characteristics of a consensus algorithm is its incentives or rewards method. Basically, when validators or miners validate and create new blocks, they are given some incentives or rewards for their participation. In some types of consensus algorithms, the participants are required to stake some amount of money in order to participate in the consensus process. In particular, the consensus algorithm uses the concept of rewards and money staking to secure the consensus process against the malicious participants.

The Shariah governs every aspect of a Muslim's religious practices and everyday life including economic activities. Although there are many studies discussing whether or not cryptocurrency is Shariah compliant, to the best of our knowledge this is the first study that evaluates the core of Blockchain technology (i.e. consensus algorithms) from a Shariah perspective. To this end, this study conducted a comparative analysis of the most used consensus algorithms in the current blockchain platforms. Particularly, the rewarding or incentivizing methods used by existing consensus algorithms are evaluated from the Shariah perspective. Our analysis focused on explaining the principle steps of the consensus algorithm and the method that the algorithm employs to reward or incentivize the participants in the consensus process. Due to the lack of related information to this study topic in the academic publications, we used various information resources such as journal articles, books, conference proceedings, blogs, wikis, and forum posts.

After this brief introduction, this paper explains the blockchain characteristics and structure in section 2. The concept of Islamic finance and Sharia compliant is explained in section 3. The most used blockchain consensus algorithms are analyzed, evaluated and compared in section 4. A discussion and our remarks are presented in section 5. Finally, section 6 concludes this work.

BLOCKCHAIN CHARACTERISTICS AND ARCHITECTURE

A blockchain is a sequence of blocks, where each block holds a complete list of transaction records like conventional public ledger (Chuen, 2015). Diagram 1 illustrates an example of blockchain. Each block is connected to the immediately previous block via a reference which is a hash value of the previous block (i.e. parent block). The first block of a blockchain is called genesis block which has no parent block (Zheng et al., 2016). A blockchain platform is built on a peer-to-peer network, where each node in the network keeps a copy of the whole chain of blocks.

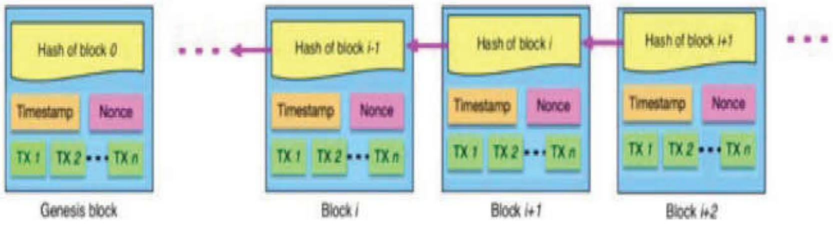


Diagram 1: Example of Blockchain Structure (Zheng et al., 2016)

A block consists of the block header and the block body as shown in Diagram 2. The block body is composed of a transaction counter and transactions. The maximum number of transactions that a block can contain depends on the block size and the size of each transaction. The block header includes (Zheng et al., 2016):

1. Block version: indicates which set of block validation rules to follow.

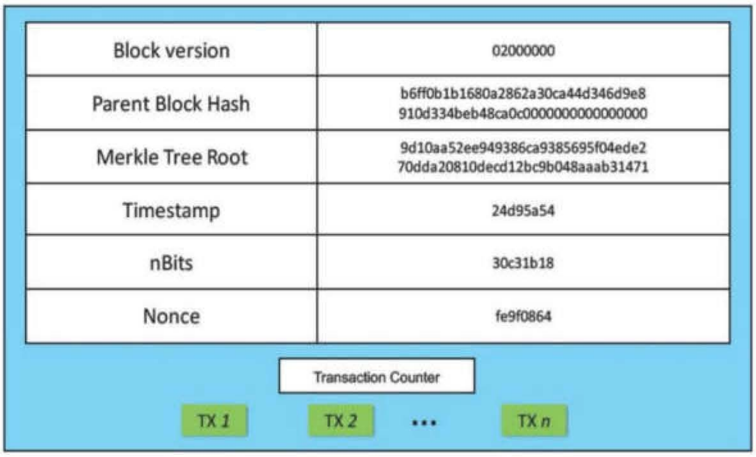
2. Parent block hash: a 256-bit hash value that points to the previous block.

3. Merkle tree root hash: the hash value of all the transactions in the block.

4. Timestamp: current timestamp as seconds since 1970-01-01T00:00 UTC.

5. nBits: current hashing target in a compact format.

6. Nonce: a 4-byte field, which usually starts with 0 and increases for every hash calculation.



Block version	02000000
Parent Block Hash	b6ff0b1b1680a2862a30ca44d346d9e8 910d334beb48ca0c0000000000000000
Merkle Tree Root	9d10aa52ee949386ca9385695f04ede2 70dda20810decd12bc9b048aaab31471
Timestamp	24d95a54
nBits	30c31b18
Nonce	fe9f0864

Diagram 2: The structure of a Blockchain Block (Zheng et al., 2016)

The key characteristics of blockchain technology are its decentralization and security (Mingxiao et al., 2017; Zheng et al., 2016). All the nodes in the blockchain have equal status. These nodes achieve consensus by using the prior agreement of the rules and following the principle of majority dominance (Mingxiao et al., 2017). In addition, blockchain is persistent and auditable. A transaction cannot be tampered once it is saved into the blockchain. As blockchain is distributed, it can avoid the single point of failure situation (Zheng et al., 2017). Blockchain is classified into three types: public blockchain, private blockchain and consortium blockchain (Zheng et al., 2017). The public blockchain system is also known as permissionless blockchain while the other two classifications come under the category of permissioned blockchain (Zheng et al., 2016).

ISLAMIC FINANCE AND SHARIAH COMPLIANT CONCEPT

Islamic banking and finance is a financing activity that complies with Shariah guidelines and its practical applications and aims to develop the Islamic economics. The Shariah guidelines forbid interest (*riba*), gambling, speculations, excessive uncertainty (*gharar*), and illegitimate transactions that are related to pigs, alcohol, pornography, tobacco, short-selling, and any other activities considered to be harmful to society. In addition, it condemns exploitation and focuses on real economic activities that promote social well-being through the concept of profit-and-loss sharing (PLS) (i.e. rewards and risk sharing) of businesses outcomes between/among the parties involved. Basically, the prohibited ex-ante fixed rate of return in financial contracting is replaced with a rate of return that is uncertain and calculated after obtaining the profit. Only the profit-sharing ratio between the capital provider and the entrepreneur is determined in advance (Hassan & Aliyu, 2018).

1. The three financial activities that must not be presented in a Shariah compliant financial system are explained in more details in the following points (Chong & Liu, 2009):

2. Interest: is offering a predetermined return on deposits or charging interest on loans. Muslims are prohibited from taking or offering *riba* or dealing with any transaction involves *riba*.

3. Uncertainty or ambiguity is not permitted in Islamic contracts as the contract terms must be well defined and have no ambiguity. For example, the sale of fish from the ocean that has not yet been caught is prohibited. The prohibition of *gharar* is to protect people from being exploited.

4. Gambling (*Maisir*) is defined as wishing something valuable with ease and without paying an equivalent compensation for it or without working for it, or without undertaking any liability against it by way of a game of chance (not by effort) (Muhammad, 2007). It is involved in contracts where the ownership of an item depends on the occurrence of a predetermined, uncertain condition in the future. Gambling or any games of chance (including lotteries, lotto, casino-type games and betting on the outcomes of animal races) are all considered prohibited.

COMPARATIVE ANALYSIS OF BLOCKCHAIN CONSENSUS ALGORITHMS

In blockchain, nodes do not trust each other and there is no central node to ensure that ledgers in distributed nodes are all the same. To ensure that ledgers in different nodes are consistent, blockchain depends on the concept of consensus (Zheng et al., 2016). The following subsections analyse and evaluate the most used consensus algorithms in blockchain from Shariah perspective.

Proof of Work (PoW) Consensus Algorithm

PoW is the consensus algorithm used in bitcoin (Nakamoto, 2008) and Ethereum (Wood, 2014), which generates, validates, and adds new blocks that record new groups of transactions. The nodes that participate in the PoW consensus are called miners and the PoW procedure is called mining. To add a block to the blockchain, each node has to show that it has performed some amount of work, also known as Proof-of-Work (Baliga, 2017). The procedure of PoW which is applied by each node in the blockchain network is summarized in the following steps (Zheng et al., 2016; Zheng et al., 2017):

1. Each node (miner) has to calculate the hash value continuously using different nonces as inputs to the hashing algorithm. This calculation stops when the calculated hash value is less than or equal to a target value. This process consumes a long time and energy.

2. The node that manages to finish the calculation first will broadcast the new block and all the other miners will stop trying to find a hash value

for this block. Subsequently, all the nodes must mutually confirm the correctness of the obtained value of the broadcasted block.

3. After validating the transactions in the new block to ensure that there is no fraud, the new block is approved in the blockchain.

4. Since the hash calculation is a time and energy consuming process, the miner that finds the hash value first gets some incentives or rewards in the form of cryptocurrency.

PoW takes the workload as the safeguard. All nodes trust the longest chain. If anyone wants to tamper with the blockchain, he needs to control more than 50% of the world's hashing power to ensure that he can become the first one to generate the latest block and master the longest chain (Ming xiao et al., 2017). Consequently, the block cannot be changed without redoing the work for the specific block and all the subsequent blocks after it (Bach et al., 2018).

PoW Evaluation from Shariah Perspective

In a PoW based blockchain all miners can participate in the mining process. The mining process consumes a long time and excessive energy. However, only the miner who first finds the required hash value gets the reward and all the other miners have wasted their resources for no rewards. Basically, getting the rewards from a mining process depends on luck and the amount of computing power devoted to it (Hertig, 2016). Thus, the miners are not always rewarded for their work and the chance of getting a reward has a high level of uncertainty. From the Shariah perspective, this rewarding process has a high level of uncertainty and it has the same concept of the game of chance (Gambling). In addition, this mining process wastes the resources of miners with no guarantee of getting any rewards or profits. Based on the aforementioned analysis of the PoW rewarding method, it is obvious that PoW is not Shariah compliant.

Proof-of-Stake (PoS) Consensus Algorithm

Unlike PoW, where participants need to spend time and energy as well as buying mining equipment to engage in the consensus algorithm, PoS requests participants to stake some money to buy proportionate block creation chances and become a validator (Baliga, 2017). With PoS, the creator of a new block is chosen in a deterministic way, depending on the participants' stakes (Blockgeeks, 2017). Thus, if a participant owns 10% of the total stakes, then his probability of validating the next block will be 10%. Validators get paid transaction fees for validating blocks of transactions and no new coins are minted or mined (Jenks, 2018). In addition, a participant with a large stake will receive a greater reward than a participant with a small stake as the former has more opportunities to validate blocks (Rammeloo, 2017).

The PoS security concept is that when people stake some money, they are less likely to attack the network as they will lose their staked money (Zheng et al., 2017). In particular, the attacker would need to obtain 51% of the total stakes to carry out a 51% attack. However, a participant with 51% stake is not interested in attacking a network which he holds a majority share (Frankenfield, 2018).

Giving block generation rights based on participants' stake is quite unfair because the rich people will be dominant in the network. As a result, many solutions proposed other parameters to combine with the stake size to decide which participant generates the next block (Zheng et al., 2017). For example, Peercoin (King & Nadal, 2012) favours participants with large stakes of old coins (cryptocurrency) to be chosen as validators. The coin-age value is obtained by multiplying the number of coins by the time period after it was created. Thus, holding 10 coins for 10 days equates to 100 coin-days (Bach et al., 2018). The longer one node holds the coins, the more rights it can get to mine blocks. In addition, the rewards that miners receive are based on the amount of coins that they stake and the coins' ages (Zheng et al., 2016). However, spending these coins in a transaction rests the age of the coin to zero. Unlike PoW where the chain with the most work is seen as the main chain, Peercoin considers the chain with the highest consumed coin-age (Bach et al., 2018).

PoS Evaluation from Shariah Perspective

To be considered in the list of potential validators of the PoS consensus algorithm the participant must stake some cryptocurrency, which is similar to depositing money in a bank account. Participants with higher stakes have higher probability of being chosen as validators. Validators get paid transaction fees for validating blocks of transactions. Therefore, the rewards that a validator receives is proportional to the amount of money he stakes. Thus, a validator with a large stake receives larger rewards than a validator with small stake. As mentioned by many Muslim scholars, depositing money in a bank account and receiving a fixed and known-in-advance interest rate from the bank is considered *riba* and not Shariah complaint (Kahf, 2014). Although in PoS the validation work does not consume much resources and the participant rewards are proportional to his stake, this case cannot be considered as receiving interest (*riba*) as the rewards are not given as a fixed ratio of the stake. Basically, the rewards are obtained from transaction fees, thus, the reward amount depends on the number of validated blocks, the number of transactions each block has, and the charged fees per transaction. Accordingly, the participant rewards are variable and not given as a fixed rate of his stake. This is similar to investing in a project that has a variable profit rate. It can be concluded that PoS is Shariah compliant.

Delegated Proof of Stake (DPoS) Consensus Algorithm

The major difference between PoS and DPoS is that in PoS the participants who stake their money (i.e. stakeholders) work as validators while in DPoS stakeholders elect their delegates to generate and validate blocks. With significantly fewer validators, the block can be confirmed quickly, making DPoS faster and more efficient than PoS and PoW (Zheng et al., 2016). DPoS has already been implemented, and is the backbone of Bitshares (Mingxiao et al., 2017). The following steps summarizes the DPoS consensus algorithm (Rammeloo, 2017; Bach et al., 2018; Zheng et al., 2016):

1. To become a stakeholder a participant has to stake some money in the blockchain network.

2. Stakeholders vote to select their delegates who will generate and validate the new blocks. A stakeholder can elect any number of delegates and his vote weight is based on his stake size.

3. In the entire network, the top delegates that have participated in the campaign and got the most votes have the block creation and validation right in the next maintenance interval.

4. During each maintenance interval, each elected delegate takes a turn in creating and validating a new block and getting the reward. The rewards are shared with the voters (stakeholders) based on how many coins one used to vote relative to the coins used by other voters who voted for the same delegate.

5. After each maintenance interval the stakeholders perform delegate election. Thus, if a delegate fails to produce a block after being elected, he may be voted out in future elections. Additionally, users do not need to worry about the dishonest delegate because he could be voted out easily.

DPoS Evaluation from Shariah Perspective

The DPoS consensus algorithm is evaluated from Shariah perspective by considering its three main issues, which are: delegates rewards, stakeholders rewards, using stakeholders' stake to vote for delegates selection.

1. Regarding the delegates rewards, each elected delegate gets a turn in producing a block and getting the reward. The reward is guaranteed to be received after achieving a certain task and there is no chance that the delegate is wasting resources without a reward. Thus, delegates reward has none of the three prohibited financial activities (i.e. interest, uncertainty, and gambling).

2. The stakeholder reward is received from the delegates that they elected. Each delegate shares his reward with the stakeholders that elected him based on the weights of the votes that each stakeholder gave to him. Thus, a stakeholder with large size stake has high voting weight and receives more rewards than a stakeholder with a small size stake. In addition, a stakeholder receives a variable amount of rewards from more than one delegate. As a result, the reward that a stakeholder receives is not a fixed ratio of the stake size. Moreover, the stakeholder does not lose the staked money unless he commits a dishonest or malicious act that deserves the punishment of losing the stake. Therefore, the stakeholder reward is considered Shariah compliant as it does not involve any forbidden interest (*riba*), uncertainty, or gambling.

3. The third issue of DPoS is using stakeholders stake size to vote for delegates selection. As mentioned previously, stakeholders with large stakes are highly unlikely to act dishonestly or be involved in producing invalid blocks. This is because in such a situation the stakeholder will lose his stake. Therefore, using the stakeholder stake size as a weight of their votes is to give different trust levels for the votes received from stakeholders. In this context, stakeholders with large stakes are more trusted. In addition, using the stakeholder stake cannot be considered as betting because the stakeholder is not going to lose the staked money anyway. Thus, there is no risk of losing the staked money in this process. In conclusion, DPoS is Shariah compliant.

Practical Byzantine Fault Tolerance (PBFT) Consensus Algorithm

Hyperledger Fabric utilizes the PBFT as its consensus algorithm. PBFT works only on a permissioned blockchain (private or consortium), because it requires that all nodes must know each other and there's no anonymity (Jenks, 2018). There is no hashing procedure in PBFT (Zheng et al., 2016). In PBFT, each node in the consensus group has to query every other node, which makes PBFT inefficient for a large network due to its underlying communication overhead (Zilliqa, 2017). A new block is determined every round. In each round, all the nodes within a consensus group are ordered in a sequence, and one primary node (a leader) is selected based on certain rules. The other nodes are referred to as backup nodes. Every round of PBFT is divided into three phases: pre-prepared, prepared and committed. In each phase, a node would enter the next phase if it has received votes from over 2/3 of all nodes. The following points explain PBFT phases (Zheng et al., 2016; Zilliqa, 2017):

1. Pre-prepare phase: In this phase, the leader announces the new block that the group should agree on. This is done by sending a "pre-prepare" message.

2. Prepare phase: Upon receiving the pre-prepare message, every node validates the correctness and validity of the block and multicasts a "prepare" message to all the other nodes.

3. Commit phase: Upon receiving the prepared messages from a super majority, each node multicasts a commit message to the group. Finally, each node waits for commit messages from a super majority to ensure that a sufficient number of nodes have agreed on the announced block.

In fact, at the end of the three phases, all honest nodes either accept the block or reject it. The original PBFT algorithm does not involve any incentives as it was first proposed for distributed systems. However, to use PBFT in blockchain it has been suggested that an incentive layer should be added in order to incentivize all participating nodes (Zilliqa, 2017).

PBFT Evaluation from Shariah Perspective

In PBFT the participants are not required to deposit or pay any amount of money. All participants are rewarded for their participation in the consensus algorithm. The amount of reward depends on the private or consortium blockchain owner regulations. Thus, the PBFT participants work as hired employees to validate the blocks and they receive a payment (rewards) for this job.

Accordingly, the PBFT consensus algorithm is considered Shariah compliant as it does not involve any prohibited financial activity.

Stellar Consensus Protocol (SCP)

SCP follows the federated byzantine fault tolerance algorithm and it utilizes the concept of quorum slices (Sankar et al., 2017). In the SCP network, nodes (participants) do not need to trust the entire network nodes but, rather, have the ability to choose which nodes they trust. This group of nodes which trust each other is referred to as a "quorum slice". An individual node can appear on multiple quorum slices (Baliga, 2017). A "quorum" is a set of nodes sufficient to reach an agreement, whereas a quorum slice is a subset of a quorum which convinces one particular node of agreement (Bach et al., 2018). SCP consists of nomination protocol and ballot protocol (Sankar et al., 2017; Bach et al., 2018). The following steps explain SCP work-flow (Mazieres, 2015):

1. Initially the nomination protocol is executed. During this, new candidate values for agreement are proposed (i.e. transaction records).

Each node receives these values votes for a single value among these, which eventually results in one value winning the majority vote.

2. After successful execution of nomination protocol, the nodes execute the ballot protocol. This involves the federated voting to either commit or abort the values resulted from nomination protocol. This results in externalizing the ballot for the current slot. The aborted ballots are now declared irrelevant. But there can be stuck states where nodes cannot reach a conclusion, whether to abort or commit a value. This situation is avoided by moving it to a higher valued ballot, considering it in a new ballot protocol execution.

Unlike participating in other consensus algorithms, Stellar participants do not directly gain rewards or incentives. In fact, transaction fees are recycled back into the network and added on top of the network's built-in inflation process. The Stellar distributed network has a built-in, fixed, nominal inflation mechanism. New lumens (the Stellar cryptocurrency) are added to the network at the rate of 1% each year. Each week, the protocol distributes these lumens to any account that gets over 0.05% of the "votes" from other accounts in the network. Basically, every participant selects another participant as its inflation destination, or nominee to receive the votes. Voting is weighted according to the number of lumens the voting participant holds. For example, if participant A has 120 lumens and sets its inflation destination to B, the network counts 120 votes for B. Each time inflation distribution is conducted, the lumens used to pay transaction fees since the last voting round are also included in the total lumens' distribution (Morgan, 2018; Stellar Developers, 2015).

SCP Evaluation from Shariah Perspective

In SCP the rewards that participants receive are obtained from two sources: the 1% annual inflation and the transaction fees. Although the 1% annual inflation is similar to interest (*riba*) as it is a predetermined return on deposit, the rewards also include the transaction fees which are variable amounts of money. This leads to generating variable rewards that depends on the Stellar network usage. Each participant needs to receive at least 0.05% of the total votes in the network to receive the reward. Thus, only participants that can collect the minimum percentage of votes will receive rewards the other participants cannot receive any rewards. In this case, there is uncertainty of rewards for individuals working in a Stellar network as the participant may or may not receive rewards. In addition, votes are received by setting inflation destinations among participants and it is not clear under which condition a participant is chosen as the inflation destination. Due to the condition of reward distribution which involves uncertainty and ambiguity the SCP protocol cannot be considered as Shariah compliant.

Ripple Consensus Algorithm

Ripple consensus algorithm utilizes collectively-trusted subnetworks within the larger network. Participants in the consensus process are called servers. Each Ripple server has a Unique Node List (UNL) to query. When determining whether to put a transaction into the ledger, the server would query the nodes in UNL (Schwartz et al., 2014). The following points elaborate the consensus work-flow (Bach et al., 2018; Baliga, 2017):

1. Each server takes all valid transactions it has seen prior to a new consensus round and puts them into a list called the "candidate list", and then, it broadcasts its candidate list to other nodes in its UNL.

2. Each server from UNL validates the transactions, votes on them and broadcasts the votes in a series of one or multiple rounds.

3. All transactions that meet a minimum of 80% "yes" votes in the final round are written to the public ledger (blockchain). Consensus in the entire network is reached when each individual sub- network reaches consensus.

4. Next round of consensus is started with newer transactions and pending transactions that did not make it into the last round of consensus.

Ripple Evaluation from Shariah Perspective

Since 2012, Ripple Labs have been working with financial institutions to build one of the largest payment networks in the ecosystem (Schuster, 2017). In this network, banks and other financial institutions are represented by the Ripple servers. In particular, Ripple was not designed to allow individual participants to be involved in the consensus process. Although Ripple does not introduce rewards or incentives, banks still have a strong motivation to use Ripple as it makes the transactions between banks easier and faster. Nevertheless, from the Shariah perspective, Ripple is just a payment network between banks to support inter-bank and global transactions without introducing interest (*riba*) in its transactions. Therefore, based on the aforementioned Ripple consensus work-flow, it can be considered as Shariah compliant as it does not involve interest, uncertainty, or gambling.

DISCUSSION AND REMARKS

Besides cryptocurrencies, the number of applications that are built on blockchain platforms is increasing rapidly. However, it is not sufficient to only evaluate the application from the Shariah perspective, but also the blockchain platform needs to be evaluated. As consensus algorithms are the core of blockchain platforms, the workflow and the rewarding method of the most used consensus algorithms in blockchain platforms are analyzed in this study. Afterwards, the algorithms are evaluated from the Shariah perspective to reveal whether or not each algorithm involves any of the financial activities that are prohibited by Shariah. Table 1 shows the blockchain type (permission/permissionless) and the blockchain application example as well as the Shariah compliant evaluation of the considered consensus algorithms.

Table 1: Comparison of the most used blockchain consensus algorithms

Consensus algorithm	Blockchain type	Blockchain application	Evaluation from Shariah perspective			
			Interest (*Riba*)	**Uncertainty (*Gharar*)**	**Gambling (*Maisir*)**	**Shariah compliant**
PoW	Permissionless	Bitcoin, Ethereum (currently)	No	Yes	Yes	No
PoS	Permissionless	Ethereum (future), Peercoin	No	No	No	Yes
DPoS	Permissionless	Onegram	No	No	No	Yes
PBFT	Permissioned	Hyperledger Fabric	No	No	No	Yes
SCP	Permissioned	Stellar network	No	Yes	No	No
Ripple	Permissioned	Ripple Network	No	No	No	Yes

In fact, permissionless consensus algorithms provide significantly better support for network scalability at the cost of slower processing. As pointed out by Vukolić (2015), permissioned consensus algorithms can be employed in a semi-centralized consensus framework. Although permissioned consensus generates high messaging overhead to provide immediate consensus finality, it has high transaction processing throughput. In contrast, permissionless consensus algorithms are more suitable for large scale blockchain networks that have less control over the nodes behaviour.

Based on the evaluation results, the PoW and SCP consensus algorithms are considered not compliant with Shariah rules. This is because PoW has uncertainty (*gharar*) and gambling (*maisir*) in its rewarding method, and SCP has some uncertainty in the rewarding process that makes the gaining of rewards subjective to the number of received votes. From the Shariah perspective it is necessary to build blockchain applications on a Shariah compliant blockchain platform. Since the consensus algorithms control the performance of blockchain platforms, it is crucial to use or design a Shariah compliant consensus algorithm in order to create a Shariah compliant blockchain platform.

CONCLUSION

This study focused on evaluating the consensus algorithms used by many blockchain platforms from the Shariah perspective. The evaluation considered the three prohibited financial activities in Shariah, which are: interest (*riba*), uncertainty (*gharar*) and gambling (*maisir*). Based on the comparative analysis conducted in this study, it can be concluded that some famous blockchain platforms (e.g. Bitcoin, Ethereum, Stellar) are not Shariah compliant as they use consensus algorithms that are not Shariah compliant. For our future work this research will be extended by considering more evaluation parameters and more consensus algorithms.

ACKNOWLEDGEMENTS

This research is funded by OK Blockchain Center Sdn. Bhd. and OKWAVE Co. Limited, and conducted in collaboration with Universiti Teknologi

Malaysia (UTM). UTM Research Management Centre (RMC) VOT NUMBER 4C209.

REFERENCES

Bach, L. M., Mihaljevic, B., & Zagar, M. (2018). Comparative analysis of blockchain consensus algorithms. *In 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO).* pp. 1545-1550.

Baliga, A. (2017). Understanding blockchain consensus models. *Persistent*, *4*, 1-14.

Biswas, K., & Muthukkumarasamy, V. (2016). Securing smart cities using blockchain technology. In *2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS)* (pp. 1392-1393). IEEE.

Blockgeeks. (2017). Proof of Work vs Proof of Stake: Basic Mining Guide. https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/. Accessed 03 Jan 2019.

Chong, B. S., & Liu, M. H. (2009). Islamic banking: interest-free or interest-based?. *Pacific-Basin finance journal*, *17*(1), 125-144.

Chuen, D. L. K. (Ed.). (2015). *Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data*. Academic Press.

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)* (pp. 618-623). IEEE.

Frankenfield, J. (2018). Proof of Stake (PoS). https://www.investopedia.com/terms/p/proof-stake-pos.asp Accessed 03 Jan 2019.

Hassan, M. K., & Aliyu, S. (2018). A contemporary survey of Islamic banking literature. *Journal of Financial Stability*, *34*, 12-43.

Hertig, A. (2016). How Ethereum Mining Work. https://www.coindesk.com/information/ethereum-mining-works. Accessed 03 Jan 2019.

Hess, Z., Malahov, Y., & Pettersson, J. (2017). Æternity blockchain. https://aeternity.com/aeternity-blockchainwhitepaper. Accessed 03 Jan 2019.

Huckle, S., Bhattacharya, R., White, M., & Beloff, N. (2016). Internet of things, blockchain and shared economy applications. *Procedia computer science*, *98*, 461-466.

Jenks, T. (2018). Pros and Cons of Different Blockchain Consensus Protocols. https://www.verypossible.com/blog/pros-and-cons-of-different-blockchain-consensus-protocols. Accessed 03 Jan 2019.

Kahf, M. (2014). *Riba* in Islamic economics and finance. In *Handbook on Islam and Economic Life*. Edward Elgar Publishing.

King, S., & Nadal, S. (2012). Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. *self-published paper, August*, *19*, 1.

Liu, P. T. S. (2016, November). Medical record system using blockchain, big data and tokenization. In *International conference on information and communications security* (pp. 254-261). Springer, Cham.

Mazieres, D. (2015). The stellar consensus protocol: A federated model for internet-level consensus. *Stellar Development Foundation*, *32*.

Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., & Qijun, C. (2017, October). A review on consensus algorithm of blockchain. In *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)* (pp. 2567-2572). IEEE.

Morgan, J.(2018). What is Stellar and how do you claim inflation? https://medium.com/blockchain-manchester/how-to-stellar-inflationary-rewards-3c7df9090c24. Accessed 03 Jan 2019.

Muhammad, A. (2007). *Understanding Islamic Finance*. England: Wiley.

Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf. Accessed 03 Jan 2019.

Rammeloo, G. (2017). The economics of the Proof of Stake consensus algorithm. https://medium.com/@gertrammeloo/the-economics-of-the-proof-of-stake-consensus-algorithm-e28adf63e9db. Accessed 03 Jan 2019.

Sankar, L. S., Sindhu, M., & Sethumadhavan, M. (2017, January). Survey of consensus protocols on blockchain applications. In *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)* (pp. 1-5). IEEE.

Schuster, B. (2017). The Ripple Currency Problem: Why Permissioned Blockchains Will Devalue XRP. https://hackernoon.com/the-ripple-currency-problem-why-permissioned-blockchains-will-devalue-xrp-d79aef84c074. Accessed 03 Jan 2019.

Schwartz, D., Youngs, N., & Britto, A. (2014). The ripple protocol consensus algorithm. *Ripple Labs Inc White Paper*, *5*(8).

Stellar Developers. (2015). Inflation. https://www.stellar.org/developers/guides/concepts/inflation.html. Accessed 03 Jan 2019.

Viriyasitavat, W., & Hoonsopon, D. (2019). Blockchain characteristics and consensus in modern business processes. *Journal of Industrial Information Integration*, *13*, 32-39.

Vukolić, M. (2015, October). The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In *International workshop on open problems in network security* (pp. 112-125). Springer, Cham.

Wood, G. (2014). Ethereum: A secure decentralized transaction ledger.

Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, A. B., & Chen, S. (2016, April). The blockchain as a software connector. In

2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA) (pp. 182-191). IEEE.

Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *Journal of medical systems*, *40*(10), 218.

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, *14*(4), 352-375.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)* (pp. 557-564). IEEE.

Zilliqa. (2017). The Zilliqa Design Story Piece by Piece: Part 2 (Consensus Protocol). https://blog.zilliqa.com/the-zilliqa-design-story-piece-by-piece-part-2-consensus-protocol-e38f6bf566e3. Accessed 03 Jan 2019.