SHARIYAH
REVIEW BUREAU

CRYPTO STAKING: NODES, REWARDS AND SHARIA COMPLIANCE

September 2022

BLOCKCHAIN AND CONSENSUS MECHANISMS

Blockchain is a special distributed database whose main purpose is to record information so that users can write and read the information. This data is structured in a decentralised way such that a "digital ledger" can be shared across a network of computers around the world without a need for a central authority. At the centre of this digital ledger is a consensus mechanism that ensures no single party tampers with the records, and everyone is kept honest.

A distributed database is not new to the market, but what makes blockchain different is that it has no database admin (decentralised network). Anyone can set up a server and join the blockchain to become a node of the network. Every node is equal, and all nodes are synced in a blockchain. Bitcoin leverages the blockchain technology as a public digital ledger to record transactions of when Bitcoins are moved from one address to another address (e.g. digital payments). All of these transaction records are public so that you can easily verify if the payer has enough Bitcoins to make the payment.

The key to the blockchain operation is the maintenance of the consensus of the information recorded on the blockchain within the network. It also impacts the financial parameters and security of the operation[1].

In simpler terms, consensus is a dynamic way of reaching agreement in a group. While voting just settles for a majority rule without any thought for the feelings and well-being of the minority, a consensus on the other hand makes sure that an agreement is reached which could benefit the entire group as a whole.

Most blockchain projects use one of the three currently most common consensus algorithms: Proof of Work (PoW), Proof of Stake (PoS) or Delegated Proof of Stake (DPoS). All these mechanisms aim at ensuring that all participants dispose of identical copies of the distributed database files[2].

1 Gong, C. (2018). 5 Types of Blockchain Consensus Mechanisms. Available at:
   https://www.logicsolutions.com/5-types-blockchain-consensus-mechanisms/
2 Nick, A. and Hoenig, L. (2020), Consensus Mechanisms in Blockchain Technology. Available at:
   https://www.lexology.com/library/detail.aspx?g=e30e7d54-3c7f-4ca0-8a22-478227a9b5ec

Proof of Work (PoW)

In contrast to other consensus mechanisms, the proof-of-work mechanism requires a lot of energy and computer power to reach a consensus and is thereby a very expensive option. The underlying idea is that so-called "miners" in a network must prove that they have made a certain effort. Miners provide the computing power needed to maintain the blockchain and to verify transactions. At the same time, miners ensure the network's immunity against hackers. They compete against each other in order to chain together a group of transactions, so-called "blocks" ("blockchain"). The blockchain contains all verified transactions which are accessible to all network participants. Miners use so-called hash functions, i.e. mathematical functions. In simple terms, hashing means taking an input string of any length and giving out an output of a fixed length. The actual challenge lies in the fact that by solving mathematical puzzles a result with certain characteristics must be obtained, which are derived from the hash function. By solving the mathematical puzzles, it can be proven that the transactions (i.e. the calculation path) have been executed without errors. If the block is then mined correctly, it gets attached to the blockchain and the first miner to solve the mathematical puzzle gets rewarded. The best known crypto-asset using the proof-of-work mechanism is Bitcoin.

Proof-of-Stake (PoS)

The idea of Proof of Stake (PoS) is to divide the voting power of a miner from its computing power, i.e. PoS gives mining power based on the percentage of tokens held by a miner. The larger his or her share of the total amount of tokens, the more likely this miner is to be selected to mine the next block. Nevertheless, the proof-of-stake-mechanism uses a random algorithm for consensus building. Though the amount of tokens held ("stake") is relevant (as the proportion of tokens held affects the probability that a miner will be allowed or selected to mine the next block), several other factors play a part in selecting the next miner.

The main objective of the PoS is to ensure that the miners support the blockchain project in the long term. Projects that use the PoS-mechanism include Dash and Neo.

A major way Proof of Stake reduces costs is by not requiring all those miners to churn through math problems, which is an energy-intensive process. Instead, transactions are validated by people who are literally invested in the blockchain via staking. Staking serves a similar function to mining, in that it's the process by which a network participant gets selected to add the latest batch of transactions to the blockchain and earn some crypto in exchange.

Delegated Proof-of-Stake (DPoS)

The DPoS-mechanism can be considered a more democratic development of the PoS-mechanism. In DPoS, it is not those with the highest number of tokens that are authorised to confirm or validate transactions, instead, all token owners select a group of delegates to perform this task. The mechanism remains decentralised as all users in the network are authorized to select the group of miners that confirm transactions. On the other hand, the advantage of the centralized aspect of DPoS over the PoS-mechanism consists in the higher speed of verification and transactions, which results in high scalability. The EOS project uses the DPoS-mechanism.

THE USE OF THE WORD STAKING IN THE CRYPTO MARKETS

THE WORD 'STAKING' SEEMS TO BE USED IN THREE WAYS IN THE CRYPTO MARKETS:

01.

Firstly, staking can be understood as "locking up" a digital asset to function as a validator in a decentralized crypto network, safeguarding its integrity, security, and sustainability.

02.

Secondly, the word 'staking' is used for yield farming. It's beneficial for token holders who possess a significant amount of a particular token they aren't using. In this case, the owner can stake their coins in the DeFi protocol, so that other ecosystem users will be able to choose this particular protocol among the options of the staking pool, borrow it and pay commissions to the owner.

03.

Thirdly, 'staking' is used for hold-incentive staking, which suggests lending or staking coins on a platform in return for interest or bonuses[3].

3   https://stobox.io/blog/what-is-cryptocurrency-staking

WHAT IS STAKING?

Considering the first use-case of the word staking described above, staking is an umbrella term used to denote the act of pledging your crypto-assets to a cryptocurrency protocol to earn rewards in exchange. Staking allows users to participate in securing the network by locking up tokens. Consequently, users are rewarded for securing the network in the form of native tokens. The higher the amount of crypto-assets you pledge, the higher the rewards you receive. The rewards are distributed on-chain, which means the process of earning these rewards is completely automatic. All you have to do is to stake them.

Staking is often thought of as a less resource-intensive alternative to mining. Stakers (validators) are paid with freshly minted cryptocurrency as an incentive for helping to protect the ecosystem. Staking in this understanding, to put it simply, is the act of securing crypto in order to collect bonuses, and it wouldn't be wrong to call it the way of making a passive income - in its mechanics, this process can be compared to the loyalty program, as the user receives bonuses for being loyal to the company, which is expressed in holding its tokens for a long-term perspective. Within this case, staking's purpose is to secure the network and contribute to a more sustainable way of producing the newest coins - you can read more about this in the next chapter. In this case, the user is rewarded for serving a blockchain validator, while tokens are only used to participate in the validation process. At the same time, being a blockchain node takes a lot of your computer resources. On a very practical level, staking just means keeping funds in a suitable wallet. This enables essentially anyone to perform various network functions in return for staking rewards. According to research on staking, crypto-assets are still in one's possession when staked. One is essentially putting them to work, and one is free to unstake them later. The unstaking process may not be immediate, and, with some cryptocurrencies, you're required to stake coins for a minimum amount of time[4].

4   https://www.fool.com/investing/stock-market/market-sectors/financials/cryptocurrency-stocks/what-is-staking/
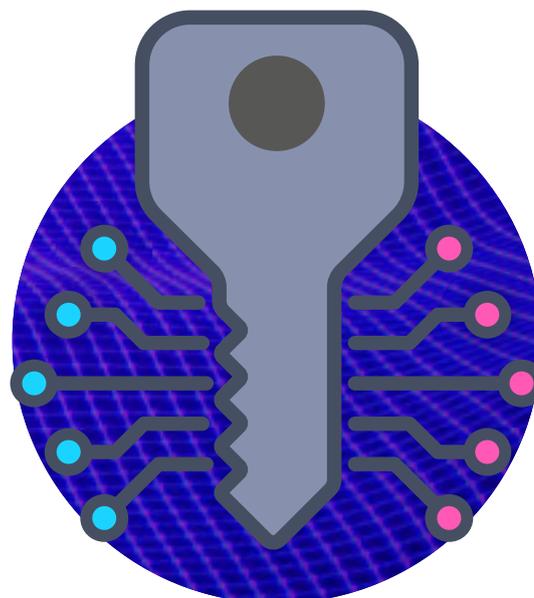
Staking tokens typically involves locking up a portion of coins, tokens, or other digital assets in a smart contract. The coins are set aside for an important role of becoming a validator node. A validator is a critical piece of a Proof-of-Stake network that works to actively secure a network and validate transactions[5].

Staking involves holding funds in a wallet to support the security and operations of a blockchain network[6]. Every time a block is validated new tokens of that currency are minted and distributed as staking rewards Proof-of-stake (PoS) assets like Solana, Tezos, etc let you earn rewards on your staked assets.

Staked tokens act as a guarantee of the legitimacy of any new transaction they add to the blockchain. The network chooses validators based on the size of their stake and the length of time they've held it. So the most invested participants are rewarded. If transactions in a new block are discovered to be invalid, users can have a certain amount of their stake burned by the network, in what is known as a slashing event.

Networks view a stake as a commitment to the network. Those that financially stake are incentivised to behave properly and maintain the integrity of the network, because bad actors could diminish the value of their stake[7].

5   https://primexbt.com/for-traders/what-is-staking-in-crypto/
6   https://academy.binance.com/en/articles/what-is-staking
7   https://community.trustwallet.com/t/introduction-to-staking-and-earning-crypto/33814
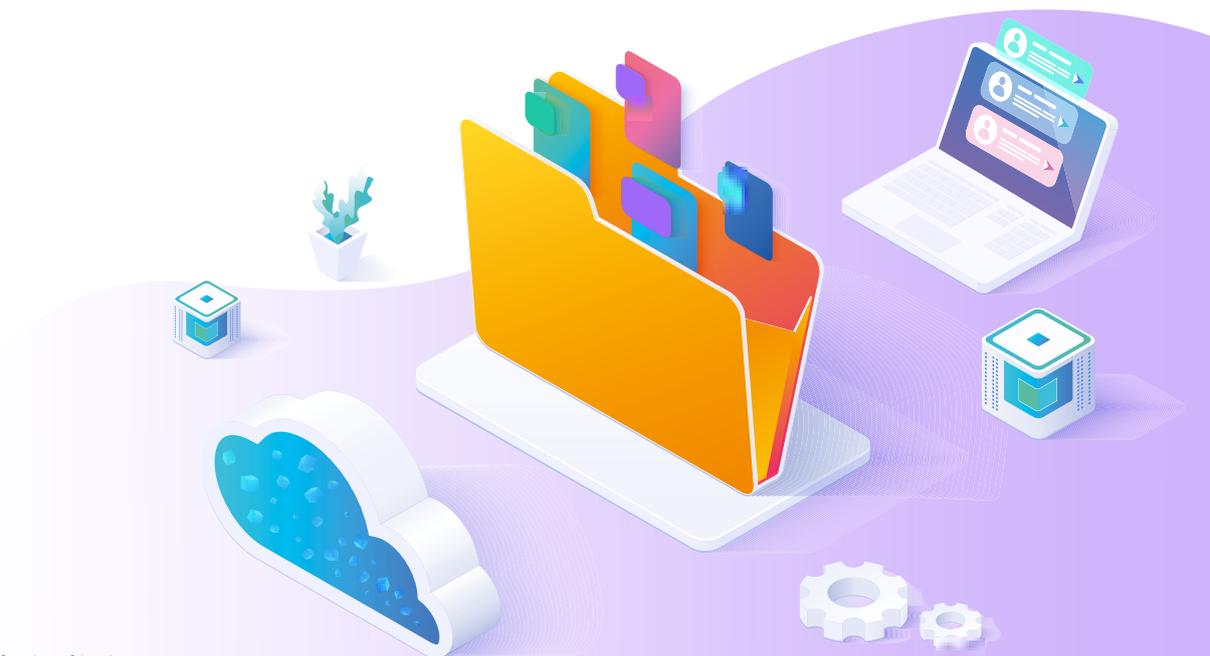
STAKING REWARDS

There are generally two types of rewards that get distributed:

01. Staking rewards/inflationary rewards

02. Transaction fees

1. Stake Tokens

2. Participate in consensus

3. Receive rewards

Decentralized Network

1. Staking rewards

This will be the rewards upon successful validation. If one stakes crypto-assets with a PoS node (a server running the protocol) to validate a block of transactions, then the staker receives rewards upon validation. If the node you have delegated to successfully signs or attests to blocks, you receive staking rewards — thereby increasing your net crypto-assets. In case your node is unresponsive or malign (double-signing), a portion of the node's assets, and hence your assets, can get slashed or destroyed.

The staking rewards are, thus, an incentive for these nodes to perform the process of ordering the transactions, verifying them, collecting them in a block, and subsequently validating the block. When these rewards are freshly minted, they get the name inflationary rewards. Every time a block is validated new tokens are minted and distributed as staking rewards. The reason your crypto earns rewards while staked is because the blockchain puts it to work by ensuring that all transactions are verified and secured without a bank or payment processor in the middle. One's crypto, if staked, becomes part of that process[8].

2. Transaction Fee

In addition to the staking rewards, each transaction carries with itself a small fee making it easier for the node to prioritize the selection of transactions to be entered into the block. The accumulated fees from the underlying transactions also go to the node.

Transactions are what makes up a crypto-asset. For different protocols, these transactions could mean different things. They vary from token transfers to smart contract executions. Despite the dissimilarity in transaction types, the common thread is that these transactions always get ordered and clubbed into a new block so that all nodes in a network can agree on the state of the network.

For some other networks, staking rewards are determined as a fixed percentage. These rewards are distributed to validators as a sort of compensation for inflation. Inflation encourages users to spend their coins instead of holding them, which may increase their usage as cryptocurrency. But with this model, validators can calculate exactly what staking reward they can expect.

8   https://www.coinbase.com/learn/crypto-basics/what-is-staking

A predictable reward schedule rather than a probabilistic chance of receiving a block reward may look favourable to some. And since this is public information, it might incentivize more participants to get involved in staking.

TRANSACTIONS   BLOCK

Tx Hash: 0x6303cb909a7f250cd876b7b9225e7b

Sender
Address   ●●   Receiver
                              Address

Tx Hash: 0x05b31728a78b3bc2dff0845b3d54f9

Sender
Address   ●●   Receiver
                              Address

Tx Hash: 0x72016570e80be80e0f462b9ea9d784

Sender
Address   ●●   Receiver
   Address
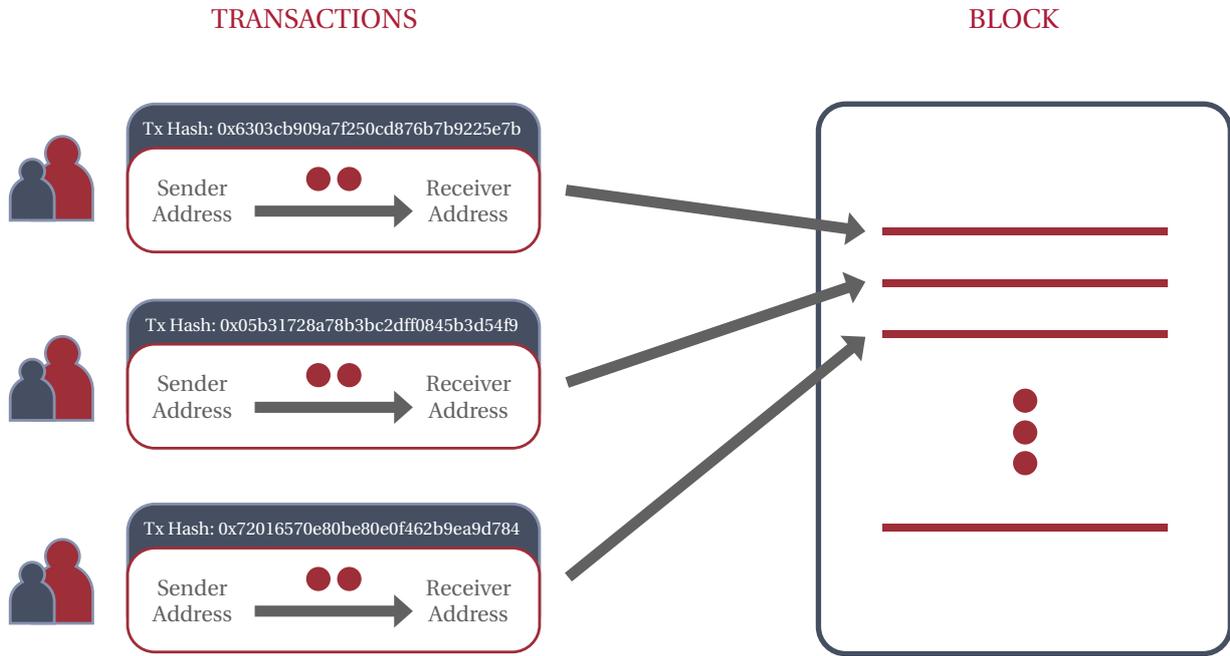
In a centralised institution like a bank, every transaction can be verified by the central authority (bank's central server). However, the lack of centralised authority in the crypto world requires the verification and subsequent validating of these blocks by the decentralized nodes of the network. These nodes are known by a variety of names — validators, bakers, etc. Their counterparts in the proof-of-work networks are called miners..

One can perform two roles when participating in staking:

01. Validation

02. Delegation
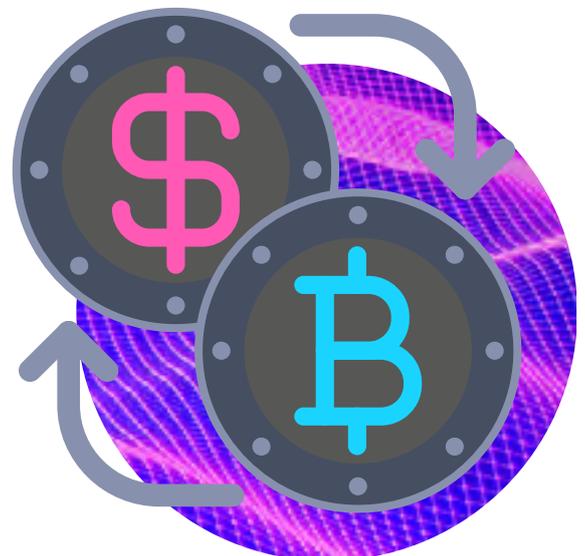
VALIDATORS IN A POS

Quite simply, to become a validator node in such a network crypto-asset holders are required to stake their tokens as collateral, instead of spending electricity as is the case with Bitcoin nodes. Additionally, validators are selected randomly to create the block. The probability of a validator's selection is directly proportional to the volume of crypto-assets staked. This means that PoS is a system where the value at stake is the main determinant of which blocks are added to the blockchain.

Participants in a Proof-of-Stake network essentially vote with their assets on blocks of transactions that they deem valid. They get rewarded if the majority of the network agrees and risks losing their stake (deposited tokens) if they try to cheat, e.g. by voting on two different blocks of transactions at the same time. The former encourages a rise in the number of nodes and the latter discourages malicious behaviour.

To become a validator some of the hurdles one can possibly face:

- Stake a minimum amount of tokens - For example in Ethereum 2.0 one would need to stake 32 ETH.
- Set up secure and performant infrastructure that should ideally be online 24x7
- Build a team of skilled engineers to run and continuously upgrade the infrastructure in accordance with the protocol.

These are just a few of the hurdles to become a validator. Not all of them apply to every network but most networks demand steep requirements that an individual may find difficult to fulfill.

A person is selected based on several factors including:

- how many coins the validator is staking
- how long the validator has been actively staking
- how many coins are staked on the network in total
- the inflation rate
- other factors

DELEGATION

Most PoS protocols foresee the impracticality of everyone becoming a validator, and incorporate ways to enable asset holders to stake their tokens with a validator that they do not run themselves.

The process of staking your assets with a validator without actually sending them your tokens is commonly called delegation. Delegating your assets means letting them count towards the stake of a validator in return for a share of the reward received. In practice, a delegator deposits tokens in a smart contract specifying the validator whose influence in the network she wants to increase.

As a result, the rewards earned in the validation process increase, but instead of only the validator receiving compensation, the rewards are automatically split between the validator and the delegator, usually by applying a simple commission rate as pictured below.
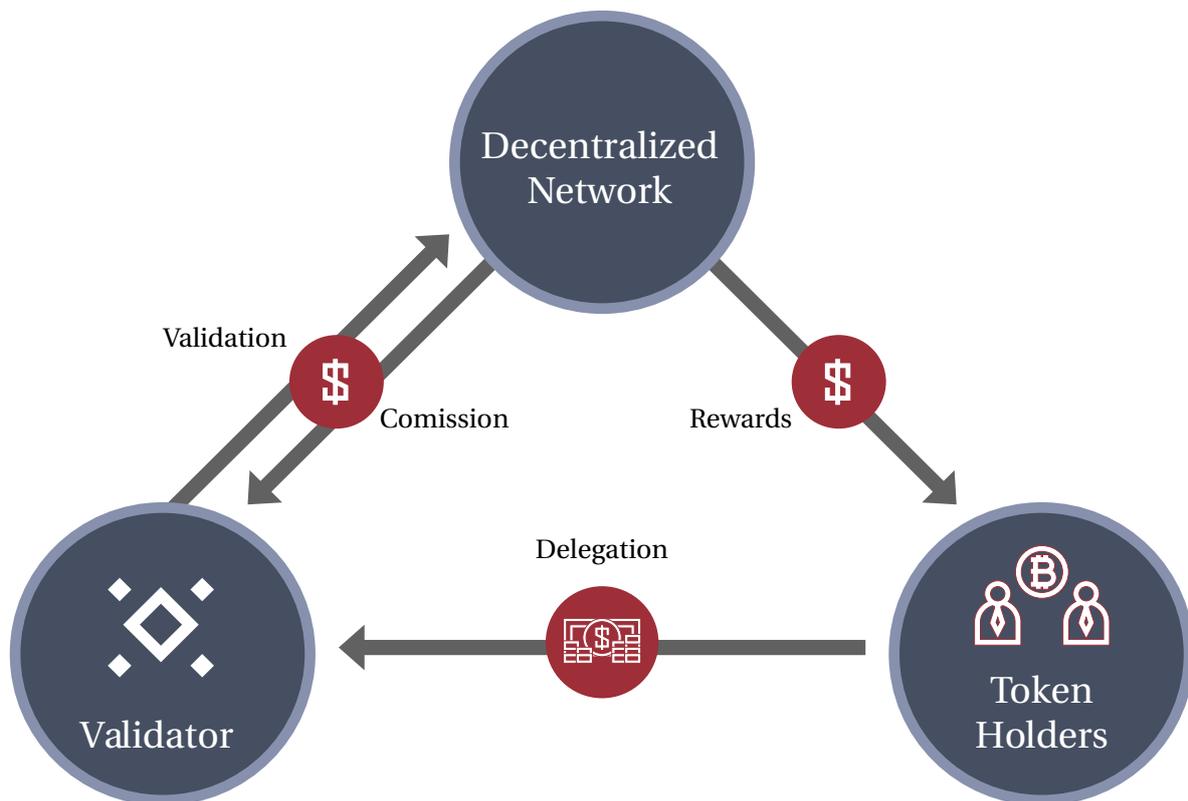
WHAT IS A STAKING POOL?

A staking pool is a group of token holders merging their resources to increase their chances of validating blocks and receiving rewards. They combine their staking power and share the rewards proportionally to their contributions to the pool.

Setting up and maintaining a staking pool often requires a lot of time and expertise. Staking pools tend to be the most effective on networks where the barrier of entry (technical or financial) is relatively high. As such, many pool providers charge a fee from the staking rewards that are distributed to participants[9].

9 *https://academy.binance.com/en/articles/what-is-staking*

HOW DOES STAKING WORK?

The process of staking starts by buying a certain number of tokens in the network. It is important to note that staking can only be done in a network that supports a PoS protocol. After the purchase is completed, the user now has to lock the holdings by following the procedure indicated by the developers of each particular network. In most cases, a staking transaction can be performed in a few minutes by following the wallet's instructions.

On the other hand, cryptocurrency exchanges have facilitated the process of staking tokens by introducing features such as staking pools. These aim to increase the compensation obtained from staking the tokens of a certain network by upping the number of coins staked at a given point in time.

In most cases, the higher the number of staked coins, the higher the number of transactions a given node will be assigned to validate. Nodes are ranked, in most cases, based on the number of tokens they hold. As a result, the nodes that hold the largest number of tokens will often receive higher compensation, which is the reason why staking pools have become so popular these days.

On the other hand, a user can stake tokens for a certain period – known as fixed staking. Some providers are also offering the possibility of entering a more flexible scheme in which the user can withdraw their tokens at any given point – known as flexible staking[10].

When a token is staked, they will be set to a locked state. During this time, the tokens cannot be moved or traded. This is true in most cases, like with Tron and Cosmos. While some tokens does not require you to lock your tokens, they have certain ways to check your balance on a wallet. A periodic snapshot is being done to monitor and calculate the rewards given. Some examples are with Tezos, VeChain and Algorand.

The key here is for the blockchain operation to validate the transaction. This helps with securing transactions and protects against double spending. It is what makes the entire system maintain itself. This task is done by nodes. A node is technically a computer or other electronic device running software. Nodes maintain either a full or partial copy of the blockchain and employ their computing power to confirm transactions. They confirm transactions through a consensus protocol, which involves nodes relaying information to one another.

A question may arise as to how does a node get selected to validate the block?

The blockchain uses special software designed for this function with huge computing power. To make them selected for this task, they need to "vote". That voting is done by staking and locking up tokens. Not all nodes have huge numbers of tokens, so they ask people to stake with them to vote. Token holders stake by locking their tokens (note, these are not lent to the node and cannot be used by the node). Thereafter, if the node is selected and validates, the node shares the rewards with everyone.

STAKING IN EXCHANGE NODE

Some exchanges run their node as a validator and allow the users to stake their coins on the exchange. This will help exchange to stake more coins and increase the chances of being selected as a next block validator. The more blocks verified by an exchange node, the more rewards it will receive. The exchange took some commission from the rewards, and the rest rewards circulated among all the stakers. This is how both users and exchanges benefit from staking.

In such an instance, a person can participate in the staking process through third-party wallets or exchanges that offer staking services. A Person does not need to run a node for verification or coin minting purposes. This is mainly for those who don't have the technical knowledge or internet support to carry out the process. In short, by just holding coins in the wallet, a person can stake. Only some crypto-assets support staking, which are built on top of PoS protocol. The process is as follows:

- When the minimum balance is met, an exchange node deposits that amount of cryptocurrency into the network as a stake (similar to a security deposit).

- The chances of the exchange node being chosen to forge the next block is proportional to the size of a stake done by nodes.

- Suppose the node successfully creates a new block. In that case, the validator node receives a reward and distributes it among all the stakers who staked in this node.

- Validators would lose part of their stake or be charged a penalty if they double-sign.

With Proof of Stake, there is still a requirement of hardware to run the nodes, as well as a number of tokens that has to be submitted to be considered a full fledged validator. Basically, there are operational costs, and these cost are being taken from the rewards gained thru staking. Validators are those responsible for governance and their active participation in the network is required. In turn, users select their desired validators in terms of their reliability as well as the percentage of the rewards allocated to the users.

The validators may set the percentage of the commission at any time without the consent of the users. It is the users responsibility to be always monitoring these changes and adjust their stakes if needed[11].

11 https://community.trustwallet.com/t/the-risks-of-staking/672

CASE STUDIES

Some of the crypto-assets that can be staked are as follows:

• Ethereum (CRYPTO:ETH) was the first cryptocurrency with a programmable blockchain that developers can use to create apps. Ethereum started out using proof of work, but it's transitioning to a proof-of-stake model.

• Cardano (CRYPTO:ADA) is an eco-friendly cryptocurrency. It was founded on peer-reviewed research and developed through evidence-based methods.

• Polkadot (CRYPTO:DOT) is a protocol that allows different blockchains to connect and work with one another.

• Solana (CRYPTO:SOL) is a blockchain designed for scalability since it offers fast transactions with low fees.

There are many exchanges that offer staking solutions. Rewards are received automatically when tokens are kept in the exchange wallet. Most exchanges that offer this service charge a small percentage from the profits. By staking on an exchange you become a member of a very large staking pool. The following exchanges are some that offer staking[12]:

• BINANCE
• BLOCKFI
• CRYPTO.COM
• CHANGENOW
• COINBASE

---
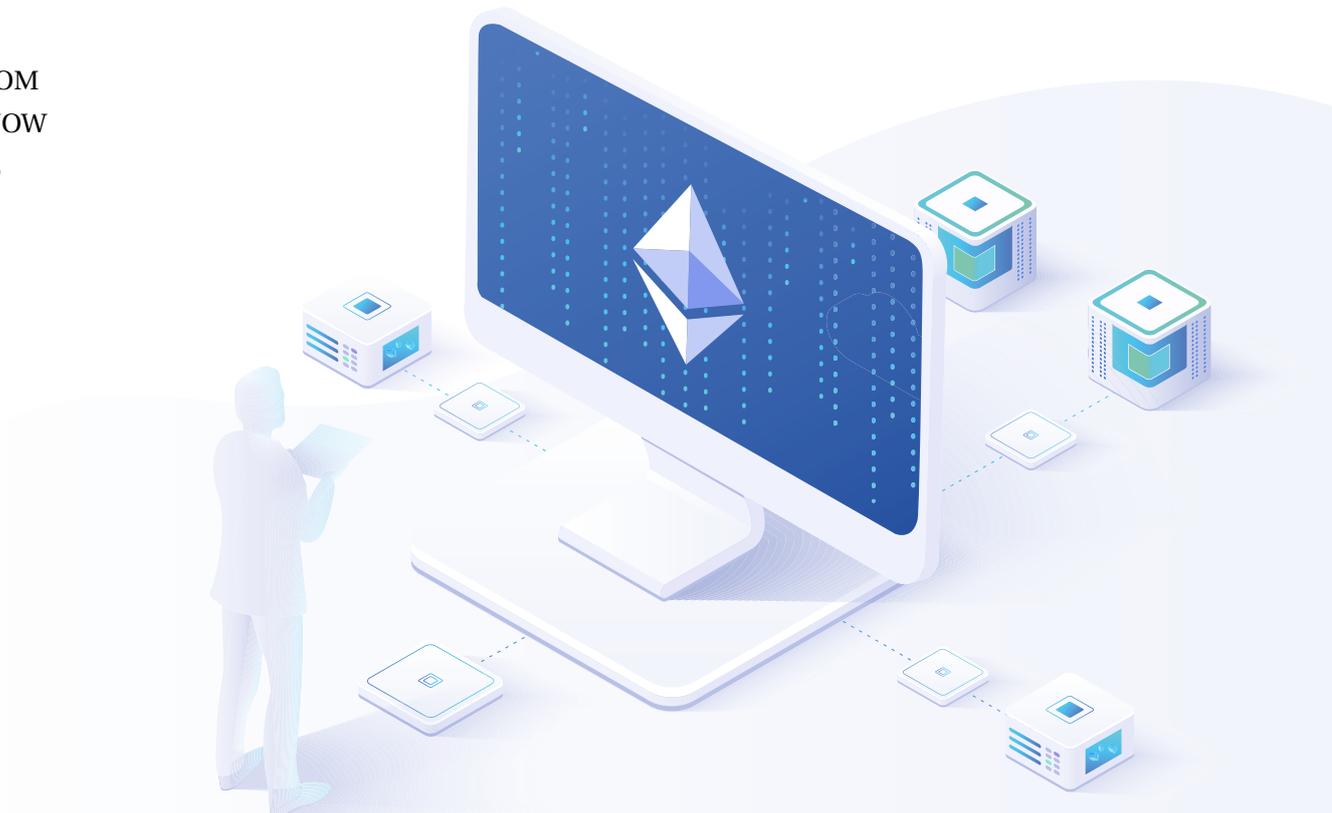
12   https://cryptotips.eu/en/knowledge-base/what-is-cryptocurrency-staking/#How_does_cryptocurrency_staking_work

SHARIAH ANALYSIS OF STAKING

The Shariah discussion on staking is all on the presumption that the crypto itself is Shariah compliant. Before entering any staking operation and benefiting from staking, a crypto-asset must be screened. Since there are various types of crypto-assets, screening crypto-assets for Shari'ah compliance before investing is absolutely essential. The following screenings should take place for crypto-assets:

01.

Legitimacy screening – ensuring that the crypto-asset is a genuine project and not a scam.

02.

Project screening – ensuring that the project is Shariah compliant.

03.

Financials screening – ensuring that it meets the financial criteria for Shariah compliance if it is an equity-based token.

04.

Token screening – understanding the Shariah compliance of the token.

If after the above screening a crypto-asset is deemed Shariah compliant, then the staking operation must be reviewed.

Staking operations

There are four potential scenarios that can be thought of today and in the future of staking. We will address each scenario and their potential Shariah ruling.

Note, each Shariah ruling is open to debate and the views of scholars differ on the interpretations.

Further, the analysis below is of an academic nature, and cannot be applied to any particular staking without the staking being reviewed by a Shariah advisor.

SHARIAH ANALYSIS OF STAKING

1. Tokens locked in your wallet, and you do validation work

In the scenario where Shariah compliant tokens are locked in one's e-wallet and not used by anybody, and a person does the validation work, in this scenario, a potential suggestion for the Shariah model and the Shariah interpretation of the staking operation could be Ju'alah.

Ju'alah is an arrangement whereby one party promises anyone a reward upon an outcome. The key thing in Ju'alah is that the process and who is doing the work need not be ascertained. Just the reward and outcome need to be known in advance. Ju'alah is permissible deeming the determination of the end result to be realised through it as sufficient, and it is not affected by the uncertainty that prevails with respect to the subject-matter of the contract, that is, the work to be done. It is for this reason that Ju'alah is suitable for activities for which Ijarah, which requires that the desired work be clearly specified, is not.

Hence, considering a Proof-of-Stake as a Ju'alah is plausible as the offer is there from the Blockchain protocol. One's response and acceptance is through staking the amount required to be part of the random selection. Thereafter, upon random selection, a person is selected to do the validation work and upon successful validation, earn a fee.

Some of the key principles which govern Ju'alah are as follows:

1. Ju'alah, in principle, is not a binding contract. The general offeror (Ja'il) or the worker ('Amil) are entitled to revoke it unilaterally, however, it becomes binding for the Ja'il when the worker commences work. If the worker undertakes not to revoke the contract during a specified period, it is binding on him to abide by the undertaking

2. The existence of legal capacity is a condition for both parties to the contract. It is not a condition that the worker be specified, therefore, Ju'alah is concluded by the issuance of an offer directed at the general public. Any person whom the offer reaches may undertake the work himself or with the help of another. If, however, the worker is specified, it is obligatory for him to undertake the work himself or with the express consent of the offeror through someone under his supervision and control.

3. The Ju'alah contract is concluded by an offer directed towards a specified worker or towards the general public, irrespective of such an offer being made verbally, in writing or through any other means that indicate an invitation to work and an obligation to pay the compensation. Acceptance of the offer is not stipulated as a condition.

4. The subject matter of the contract is the work that is agreed upon through Ju'alah as well as the compensation for the work.

5. It is permissible to stipulate that the job is done within a specified period so that the worker will not be entitled to compensation after this period, except when the period is over and the result is close to realisation, in which case the period will be automatically extended.

6. The Ju'alah contract is valid despite uncertainty as to the nature of the work, provided that the required result realised by the work is determined.

7. It is a condition that the work involves some type of effort.

8. It is a condition that the work should not be obligatory upon the worker.

9. The compensation should be known, valuable in the eyes of the Shari'ah, and deliverable. If the compensation is unknown, unlawful or not deliverable, payment of reasonable compensation becomes binding.

10. As a rule, entitlement to compensation is not established until the work is completed and delivered to the offeror.

11. It is permissible to stipulate that all or part of the compensation be paid in advance at the conclusion of the contract or thereafter, even though this is before the completion of the entire work, however, it is considered "subject to accounts" and the worker is not entitled to it without the realisation of the result, the offeror having the right to reclaim it if the work is not realised.

12. Ju'alah is distinguished from Ijarah on the following grounds:

- Ju'alah is valid despite uncertainty of work deeming the determination of the required result by the offeror as sufficient.

- Ju'alah does not require acceptance.

- Entitlement to compensation depends on completion of work and delivery of result.

- Ju'alah is valid even if the other party is not known.

- As a rule, Ju'alah is terminable, while Ijarah is binding.
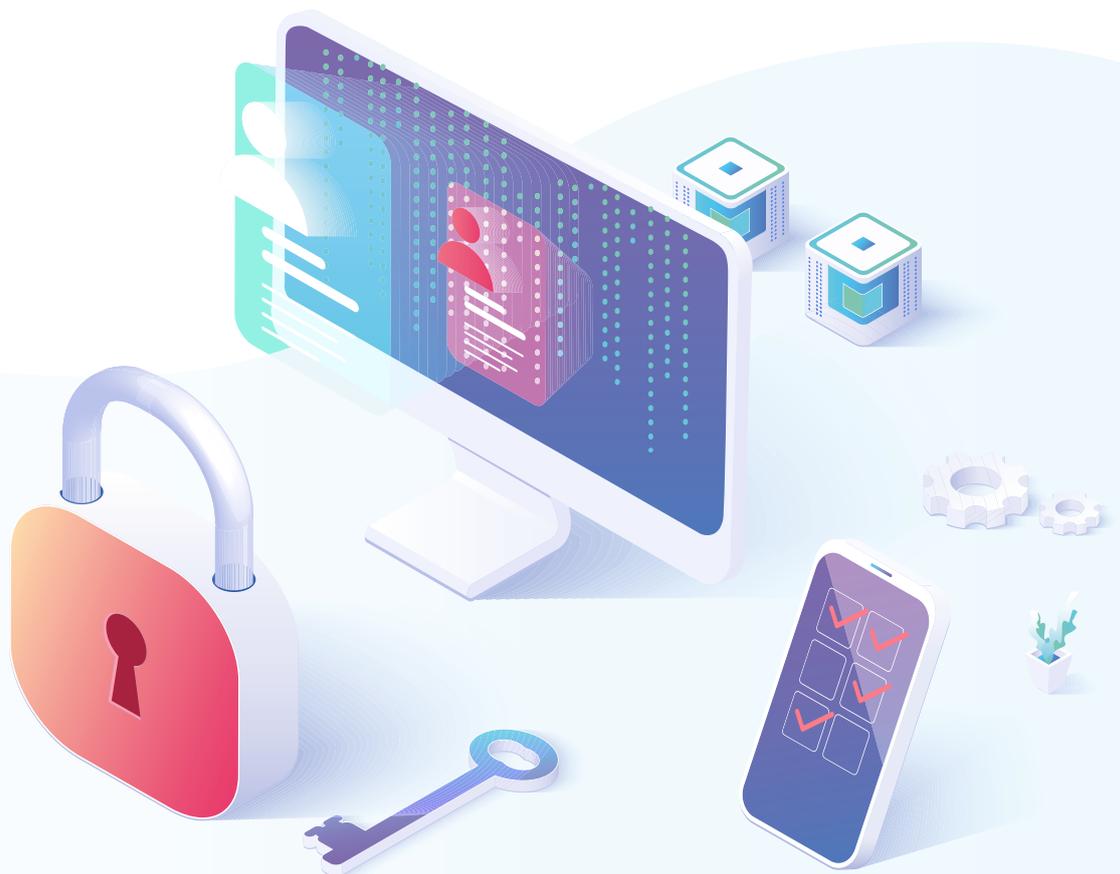
Fees gained from a valid Ju'alah agreement will be permissible and Halal for the stakers to receive.

2. Tokens locked in your e-wallet as part of an exchange, and the staking pool or exchange does the validation

In this scenario, a potential suggestion for the Shariah interpretation is that the staking pool that is created among the participants is a Shirkat pool. The pool forms a Shrikat between the participants. Thereafter, there is a Shirkat al-A'mal relationship between the exchange and the pool of stakers. This is a service partnership where the partners will provide a service in lieu of payment. In a Shirkat al-A'mal, it is valid for one party to provide goods and assets which are not for trade, but to support the operations of the partnership. The AAOIFI Shariah Standard No.12 states:

If the service partnership requires capital goods (e.g., equipment or tools), then it is permissible for each party to provide the necessary goods that his services require, in which case each partner owns the goods he has provided. The partners may contribute funds to acquire the goods on the basis of a partnership in ownership. It is also permissible for a party to a Sharikah contract to provide the capital goods required by the partnership in consideration for fees that will be charged against the Sharikah operation as expenses.

If a third-party validator charges a fixed fee, then the suggested Sahriah interpretation is that it will not be a Shirkat al-A'mal between the validator and the staking pool, instead, this may be considered as a Wakalah between the third party validator and stake pool. The stake pool will be a Shirkat al-A'mal among themselves who have assigned the validator as an agent and pay a fixed fee as an expense. The remainder goes to the stake pool and they share the rewards proportionately.

3. Tokens transferred to another wallet but not used, only locked.

If tokens are ever transferred to another wallet and in another entity's possession as custodians, and that entity does not spend the tokens nor forms a service partnership, then the tokens will be held as a Wadi'ah (safekeeping deposit).

In such a staking scenario, the same principles in 1 and 2 above will apply depending on who is performing the validation requirements.

4. Tokens transferred to another wallet and used by the wallet owner with a liability upon them to return the same amount back.

If any staking operation ever operates in a manner where tokens are transferred or held in a wallet owned by another entity, who then use the tokens for their own purposes and have a liability to return the same amount on demand or after a fixed-term, then this will be a form of Qard (loan). Any gain or compensation in such a scenario will be a form Riba and will not be permissible.

CONCLUSION

Blockchain is a special distributed database whose main purpose is to record information so that users can write and read the information. The key to the blockchain operation is the maintenance of the consensus of the information recorded on the blockchain within the network. It also impacts the financial parameters and security of the operation. One such consensus mechanism is the Proof-of-Stake (PoS). Staking is an umbrella term used to denote the act of pledging your crypto-assets to a cryptocurrency protocol to earn rewards in exchange. Staking allows users to participate in securing the network by locking up tokens. Staking involves holding funds in a cryptocurrency wallet to support the security and operations of a blockchain network. Those who are selected to validate the transactions based on the selection of their stake will receive staking rewards and transaction fees. Before any staking operation is deemed Shariah compliant, it is necessary to screen the token itself to ensure it is Shariah compliant. This can be done through reviewing the legitimacy of a token, its project, the financials and the utility of the token. There are several suggested Shariah interpretations which all need further research.

Some proposed models for the Shariah scholars to further deliberate on is the suggestion of Ju'alah if one is doing the validation work. Another potential suggestion for Shariah scholars to review is that the staking operation be considered as a Shirkat al-A'mal if the staking is done with another entity doing the validation and stakers providing the staked tokens. However, if a stake is ever structured where tokens are borrowed by another entity, then any additional gain or reward in such an instance will not be Shariah compliant.

ABOUT OUR PEOPLE

Research Author
Mufti Faraz Adam
SHARIAH CONSULTANT AT SRB

- Completed his Islamic studies in the six-year Alimiyyah degree at Darul Uloom Leicester
- Specialised in Islamic law and graduated as a Mufti in South Africa at Darul Iftaa Mahmudiyyah, Durban.
- Accredited with: Masters of Arts in Islamic Theology with specialisation in Juristic verdicts (Iftaa) and a Diploma in Islamic Finance.
- Completed a Master's Degree in Islamic Finance, Banking and Management at Newman University in 2017.

Peer Reviewer
Shaikh Muhammad Ahmad Sultan
SHARIAH ADVISOR AT SRB

- Over 10 years of experience as a Shari'a consultant and academic in various parts of Islamic finance.
- Worked predominantly in the financial services along with retail and investment banking and has expertise in corporate advisory and real-estate funds.
- He procured his Masters (A'alamiyah) in Fiqh and Usool ul Fiqh from Jami'ah Ahsan Ul Uloom and procured Bachelors in Islamic sciences from Jamia Dar-ul-Uloom.

Peer Reviewer
Mufti Irshad Ahmad Aijaz
SHARIAH CONSULTANT AT SRB

- Completed his Takhassus in Iftaa in Jamia Dar-ul-Uloom
- Chairman, Shari'ah Advisory Committee, State Bank of Pakistan
- Chairman Shari'ah Supervisory Board, BankIslami Pakistan Limited & Summit Bank Limited
- Member, Shari'ah Board, Standard Chartered Bank Pakistan Limited
- Member, Subcommittee on legal and regulatory framework by Ministry of Finance, Government of Pakistan