Delegated Proof-of-Stake Consensus

A robust and flexible consensus protocol

Delegated Proof of Stake (DPOS) is the fastest, most efficient, most decentralized, and most flexible consensus model available. DPOS leverages the power of stakeholder approval voting to resolve consensus issues in a fair and democratic way. All network parameters, from fee schedules to block intervals and transaction sizes, can be tuned via elected delegates. Deterministic selection of block producers allows transactions to be confirmed in an average of just 1 second. Perhaps most importantly, the consensus protocol is designed to protect all participants against unwanted regulatory interference.

BitShares is first and foremost a globally distributed database that is used as a ledger to track ownership of digital assets. All updates to the ledger must be validated and applied in the proper order to allow the database to remain consistent and universally agreed upon. Reaching a consensus about the order in which updates should be applied is the purpose of Delegated Proof of Stake (DPOS).

Overview

The questions that must be answered by any consensus process include, but are not limited to:

1. Who should produce the next block of updates to apply to the database?
2. When should the next block be produced?
3. What transactions should be included in the block?
4. How are changes to the protocol applied?
5. How should competing transaction histories be resolved?

The goal is to find answers to these questions that ensure the consensus process is robust against an attacker who wishes to gain control over the network. In practice, gaining control means acquiring the ability to unilaterally censor transactions. The process should also be robust against an attacker wishing to take advantage of a temporary inconsistency in the database state on different computers.

Block Production by Elected Witnesses

The term witness was chosen because it is a legally neutral word that is free from regulation. Traditional contracts often have a place for witnesses to sign. For extremely important contracts, a public notary is sometimes used. Neither witnesses nor notaries are party to the contract, but they serve a very important role of certifying that the contract was signed by the specified individuals at the specified time. In BitShares, witnesses serve a similar role of validating signatures and timestamping transactions by including them in blocks.

Under DPOS, the stakeholders can elect any number of witnesses to generate blocks. A block is a group of transactions which update the state of the database. Each account is allowed one vote per share per witness, a process known asapproval voting. The top N witnesses by total approval are selected. The number (N) of witnesses is defined such that at least 50% of voting stakeholders believe there is sufficient decentralization. When stakeholders expresses their desired number of witnesses, they must also vote for at least that many witnesses. A stakeholder cannot vote for more decentralization than witnesses for which they actually cast votes.

Each time witnesses produce a block, they are paid for their services. Their pay rate is set by the stakeholders via their elected delegates (to be discussed later). If a witness fails to produce a block, then they are not paid, and may be voted out in the future.

The slate of active witnesses is updated once every maintenance interval (1 day) when the votes are tallied. The witnesses are then shuffled, and each witness is given a turn to produce a block at a fixed schedule of one block every 2 seconds. After all witnesses have had a turn, they are shuffled again. If a witness does not produce a block in their time slot, then that time slot is skipped, and the next witness produces the next block.

Anyone can monitor network health by observing the witness participation rate. Historically, BitShares has maintained 99% witness participation. Any time witness participation falls below a certain level, users of the network can allow more time for transactions to confirm, and be extra vigilant about their network connectivity. This property gives BitShares the unique advantage of being able to alert users of potential problems less than 1 minute after the trouble arises.

Parameter Changes by Elected Delegates

Delegates are elected in a manner similar to witnesses. A delegate becomes a co-signer on a special account that has the privilege of proposing changes to the network parameters. This account is known as the genesis account. These parameters include everything from transaction fees, to block sizes, witness pay, and block intervals. After the majority of delegates have approved a proposed change, the stakeholders are granted a 2 week review period during which they may vote out delegates and nullify the proposed changes.

This design was chosen to ensure that delegates technically have no direct power and that all changes to the network parameters are ultimately approved by the stakeholders. This is done to protect the delegates against regulations that may apply to managers or administrators of cryptocurrencies. Under DPOS, we can truly say that the administrative authority rests in the hands of the users, rather than either the delegates or witnesses.

Unlike witnesses, delegates are not paid positions. However, these parameters are not expected to change often.

The *genesis account* can technically perform any action that any other account can perform, which means it is possible to send funds to the *genesis account* or specify the *genesis account* as an escrow agent. The *genesis account* can also be used to issue new assets. There are untold number of applications where elected delegates can aid the stakeholders in performing tasks that demand a high degree of trust and accountability.

Changing the Rules (aka Hard Forks)

From time to time, it is necessary to upgrade a network to add new features. Under DPOS, all changes must be triggered by active stakeholder approval. While it is technically possible for the witnesses to collude and change their software unilaterally, it is not in their interest to do so. Witnesses are selected based upon their commitment to remain neutral to blockchain policy. Remaining neutral protects witnesses against allegations that they are the administrators/managers/owners/operators of the network. A witness is merely an employee of the stakeholders.

Developers may implement whatever changes they deem appropriate, so long as those changes are contingent upon stakeholder approval. This policy protects the developers as much as it protects the stakeholders and ensures that no individual has unilateral control over the direction of the network.

The threshold for changing the rules is the same as replacing 51% of the elected witnesses. The more stakeholder participation in electing witnesses, the harder it becomes to change the rules.

Ultimately, changing the rules depends upon everyone on the network to upgrade their software, and no blockchain level protocol can enforce how rules are changed. This means that hard-forking “bug fixes” can be rolled out without requiring a vote of the stakeholders, so long as they remain true to the universally expected behavior of the code.

In practice, only security critical hard-forks should be implemented in such a manner. The developers and witnesses should wait for the stakeholders to approve even the most minor changes.

Double Spend Attack

A double spend can occur anytime a blockchain reorganization excludes a transaction previously included. This means that the witnesses had a communication breakdown caused by disruptions in the infrastructure of the Internet. With DPOS, the probability of a communication breakdown enabling a double spend attack is very low.

The network is able to monitor its own health and can immediately detect any loss in communication which shows up as witnesses failing to produce blocks on schedule. When this occurs, it may be necessary for users to wait until half of the witnesses have confirmed their transactions, which could be up to a minute or two.

Transactions as Proof of Stake

Each transaction on the network may optionally include the hash of a recent block. If this is done, the signer of the transaction can be confident that their transaction may not be applied to any blockchain that does not include that block. A side effect of this process is that, over time, all stakeholders end up directly certifying the long-term integrity of the transaction history.

Blockchain Reorganizations

Because all witnesses are elected, highly accountable, and granted dedicated time slots to produce blocks, there is rarely any situation where two competing chains can exist. From time to time, network latency will prevent one witness from receiving the prior block in time. If this happens, the next witness will resolve the issue by building on whichever block they received first. With 99% witness participation, a transaction has a 99% chance of being confirmed after a single witness.

While the system is robust against *natural* chain reorganization events, there is still some potential for software bugs, network interruptions, or incompetent or malicious witnesses to create multiple competing histories that are longer than a block or two. The software always selects the blockchain with the highest witness participation rate. A witness operating on their own can only produce one block per round and will always have a lower participation rate than the majority. There is nothing that any witness (or minority group of witnesses) can do to produce a blockchain with a higher participation rate. The participation rate is calculated by comparing the expected number of blocks produced vs the actual number of blocks produced.

Maximally Decentralized

Under DPOS, every stakeholder has influence that is directly proportional to their stake, and no stakeholders are excluded from exercising this influence. Every other consensus system on the market excludes the vast majority of stakeholders from participating. There are many different ways that alternatives exclude stakeholders. Some alternatives use invite-only systems. Others exclude participation by making it cost more to participate than they earn. Still other systems technically allow everyone to participate, but they can be safely ignored by a few large players who produce the vast majority of all blocks. Only DPOS ensures that block production is evenly distributed among the most people and that everyone has an economically viable way to influence who those people are.