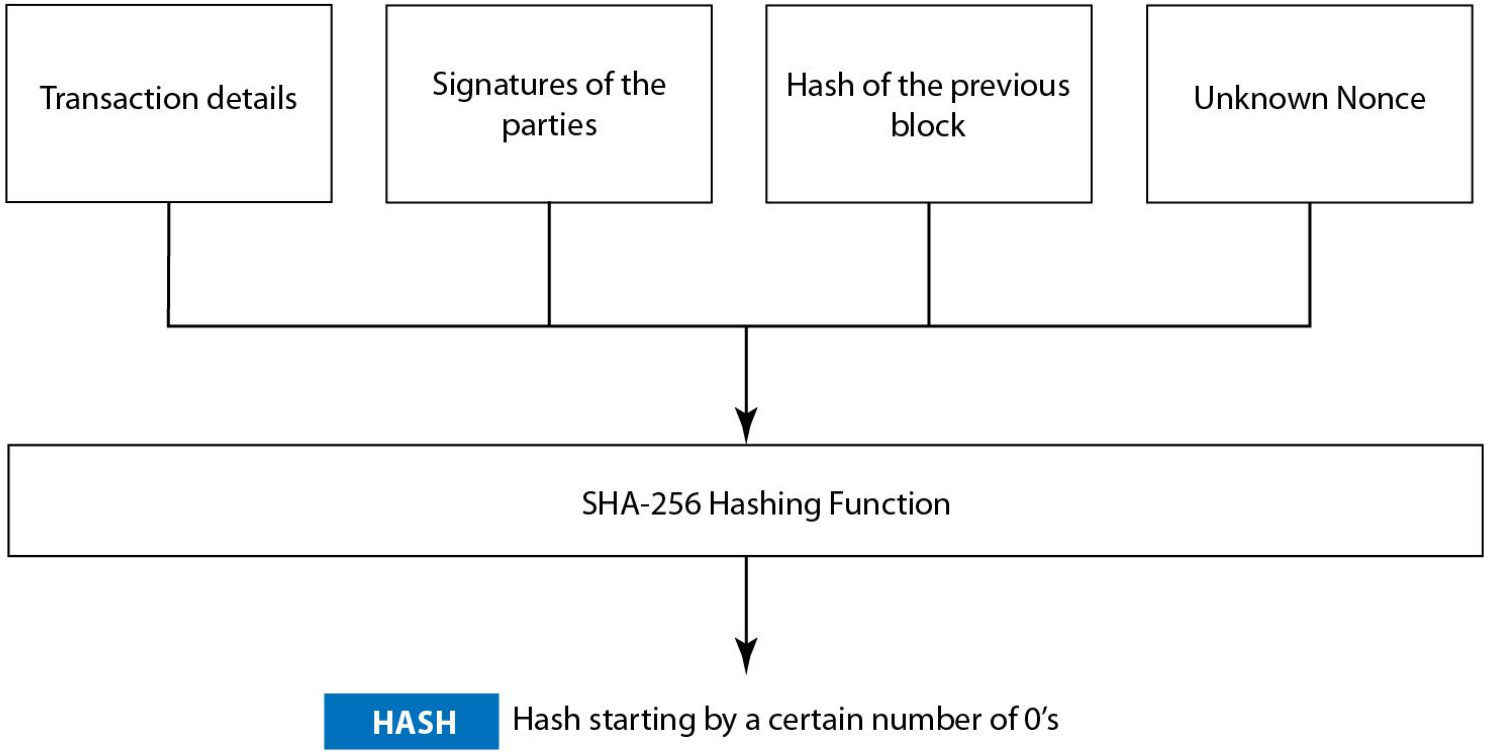
Professional Blockchain Course

Top 5 Consensus Mechanisms

Proof of Work

- Proof of Work is the consensus algorithm where miners compete to solve a difficult mathematical problem based on a cryptographic hash algorithm. This proof proves that a miner spends a lot of time and resources to solve the problem. When a block is 'solved,' the transactions contained are considered confirmed.
- By Mathematical problem we mean:
  - Hash function - how to find the input knowing the output.
  - Integer factorization - how to present a number as a multiplication of two other numbers.
  - Guided tour puzzle protocol - If the server suspects a DoS attack, it requires a calculation of hash functions, for some nodes in a defined order. In this case, it’s a ‘how to find a chain of hash function values’ problem.
- Miners receive a reward when they solve the complex mathematical problem.
- For example in Bitcoin miners receive 12.5 bitcoins for solving the puzzle.
- Miners can also receive transaction fees in addition to rewards.


Transaction details
Signatures of the parties
Hash of the previous block
Unknown Nonce
SHA-256 Hashing Function
HASH
Hash starting by a certain number of 0's

Proof of Work Example

Example Bitcoin:

In Bitcoin, a block is being mined every 10 minutes. The difficulty is adjusted such that it never deviates much from this limit. If the difficulty stays the same, while the computer power increases gradually, it will take less and less time to mine a block.

To make sure this doesn't happen over blockchain, the Proof of Work target is a dynamic parameter. In the Bitcoin blockchain, the target gets adjusted every 2016 blocks. Computing the amount of time it took to mine 2016 blocks. It should take 20160 minutes (2016 * 10 minutes = 14 days). The difficulty is adjusted depending on the time it took to mine those blocks.

Proof of Stake

- Proof-of-Stake is a different algorithm to validate transactions and achieve the distributed consensus.
- Proof-of-Work algorithm rewards miners who solve complex mathematical problems with the end goal of validating transactions and creating new blocks. On the other hand, in the Proof-of-Stake algorithm, the creator of a new block is chosen in a deterministic way, depending on its wealth/stake in the blockchain.
- No block reward
- All the digital currencies are created at the start of the chain, and their number never changes. Miners only take the transaction fees. That is why in the PoS system miners are also called forgers.

1 Anyone who holds the native currency can become a validator.

2 The chance of mining and earning rewards are based on how much of the stake they have in the blockchain.

3 The chosen validator is rewarded by a part or the whole of the transaction fee.

Proof of Stake Example

Example Neo:

NEO is a smart contract development platform often referred to as “China’s Ethereum.” The network aims to be the center of a creative economy where digital assets can be securely traded with little overhead.

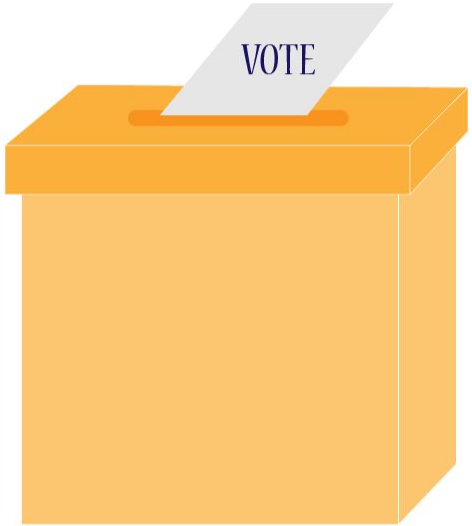
Staking NEO lets, you generate GAS, the platform’s internal currency. The more NEO you have staked, the more GAS you’ll earn with each payment. NEO rewards stakeholders with an annual return of 4-6%.

Delegated Proof of Stake

- People in a particular blockchain ecosystem vote for Witnesses to safeguard their computer network.
- Let's imagine a reward system where only the top 100 Witnesses are paid for their service, and only top 20 earn a regular salary. As it creates a healthy competition, many wants become a Witness thus providing hundreds of backup Witnesses.
- The vote strength of a person is determined by how many tokens they hold. People who have more tokens will influence the network more than people who have less tokens.
- If a Witness starts acting like a schmuck or stops doing a quality work in securing the network, people in the blockchain community can remove their votes, essentially firing the lousy actor. Voting is always ongoing.
- Delegates are elected as witnesses. A delegate becomes a co-signer on an individual account that has the privilege of proposing certain 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.

1 Anyone who holds the blockchain base currency can vote for a validator.

2 The validator with the most votes gets to become a delegate, validating transactions and collecting the rewards for doing so



Delegated Proof of Stake Example

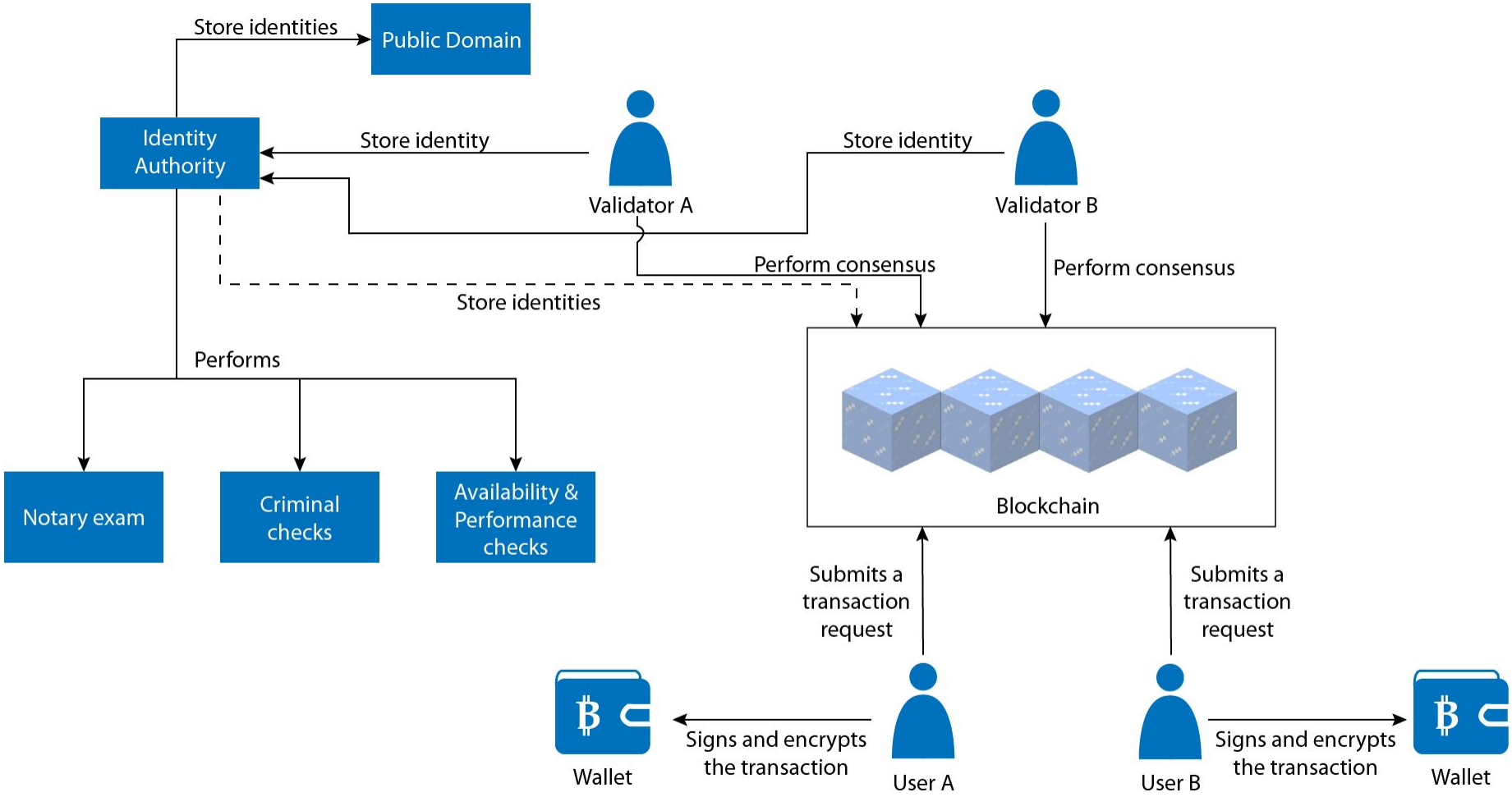
Example Lisk:

Lisk is a decentralized network similar to Bitcoin, Ethereum, or BitShares. Lisk uses a simplified implementation of the Delegated Proof of Stake consensus algorithm.

Lisk token holders can vote for mainchain delegates who secure the network. There is a maximum of 101 active mainchain delegates whosoever got the most votes on the whole network, and they can earn block generation rewards. Every other delegate is on standby waiting to be elected, or securing a Lisk sidechain.

Proof of Authority

- The proof-of-authority consensus is essentially an optimized Proof of Stake model that leverages identity as the form of stake rather than staking tokens.
- The group of validators is usually supposed to remain relatively small (~25 or less) to ensure efficiency and manageable security of the network.
- Individuals under PoA earns the right to become a validator, that's why there is no incentive to retain the position that they hold.
- Validators are required to formally verify identity either on the chain or some public domain.
- The eligibility to become a validator is difficult to obtain, and the individuals need to go through many steps to become a validator.


Store identities
Public Domain
Identity Authority
Store identity
Validator A
Store identity
Validator B
Perform consensus
Perform consensus
Store identities
Performs
Notary exam
Criminal checks
Availability & Performance checks
Blockchain
Submits a transaction request
Submits a transaction request
Wallet
Signs and encrypts the transaction
User A
User B
Signs and encrypts the transaction
Wallet

Proof of Authority Example

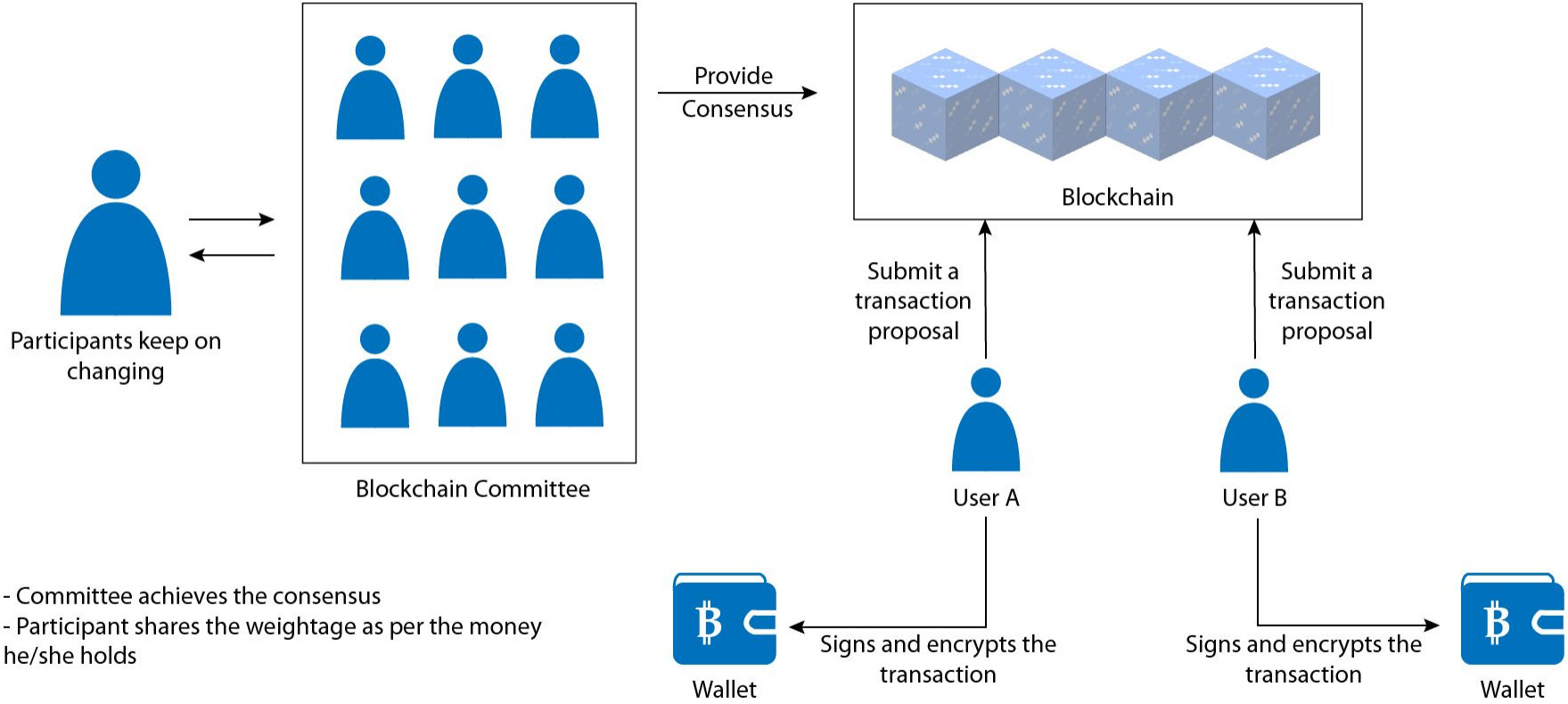
Example POA Network:

Proof of Authority Network (POA Network) is a blockchain platform founded on the core principle of implementing PoA consensus in their blockchain. POA Network is a public platform for smart contracts that exists as an Ethereum sidechain with their nodes consisting of independent validators.

To make eligibility for staking identity its very hard to obtain, candidates for validators have to overcome the hurdle of passing notary exams. Not only do the exams attest to no criminal records and good moral standing of a candidate, but they also filter out those who are not committed.

Proof of Weight

- Proof-of-Weight is a broad consensus classification based on the algorand algorithm which in turn specifies a new protocol known as Byzantine Agreement.
- BA* protocol is highly scalable and secure.
- PoW consensus model runs a committee where participants keep on changing, and the committee achieves the consensus for the network.
- Every user over the network has a weight attached to them which is determined by the money they hold in their account.



- Committee achieves the consensus
- Participant shares the weightage as per the money he/she holds

Proof of Weight Example

Example Filecoin:

Filecoin is using Proof-of-Spacetime as a weighted consensus on how much IPFS data you're storing. The weight is based on different parameters. If the overall weight fraction of honest users is higher than two-thirds of the total weight than the network will remain secure. This method also helps in protecting the network from double-spend attacks.

It is based on Algorand. While some may see similarities between Algorand and Proof-of-stake, they are not the same. In a PoS environment, the number of tokens held at any given time determines the amount of additional rewards users earn. Proof-of-weight uses an entirely different weighted value.

THANK YOU

For more information contact
info@we2blocks.com