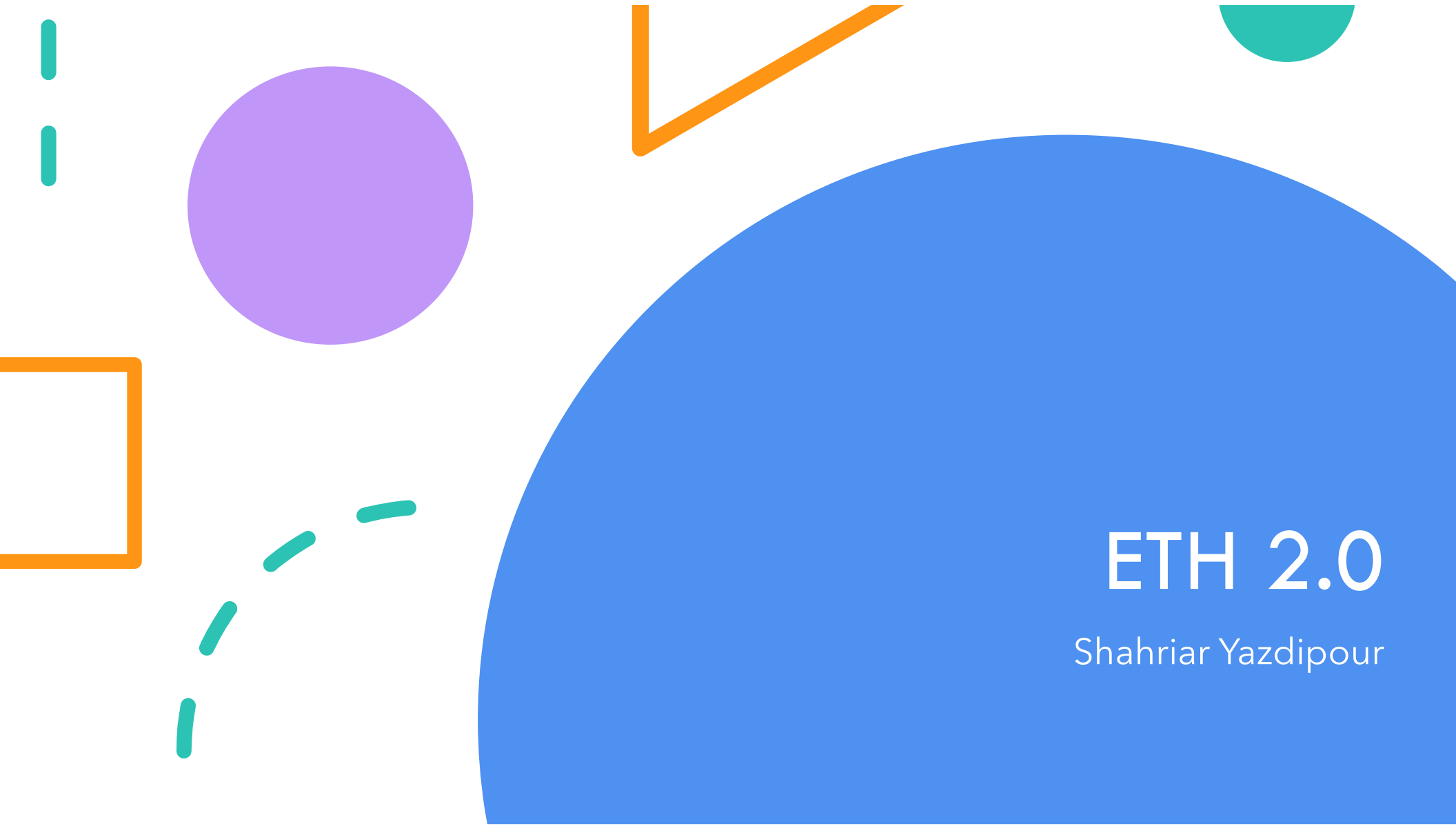

ETH 2.0
Shahriar Yazdipour

About Me

- Shahriar (Sha) Yazdipour

- Masters in CS from TUI
- Software Engineer at TomTom

- hi@yazdipour.com
- https://yazdipour.com

Introduction to Ethereum

- The network was launched in 2015.
- The second-largest cryptocurrency and the blockchain network.
- The largest developer ecosystem.
- Different from Bitcoin: it can store and execute smart contracts, which are software programs that can be used as applications on the network.

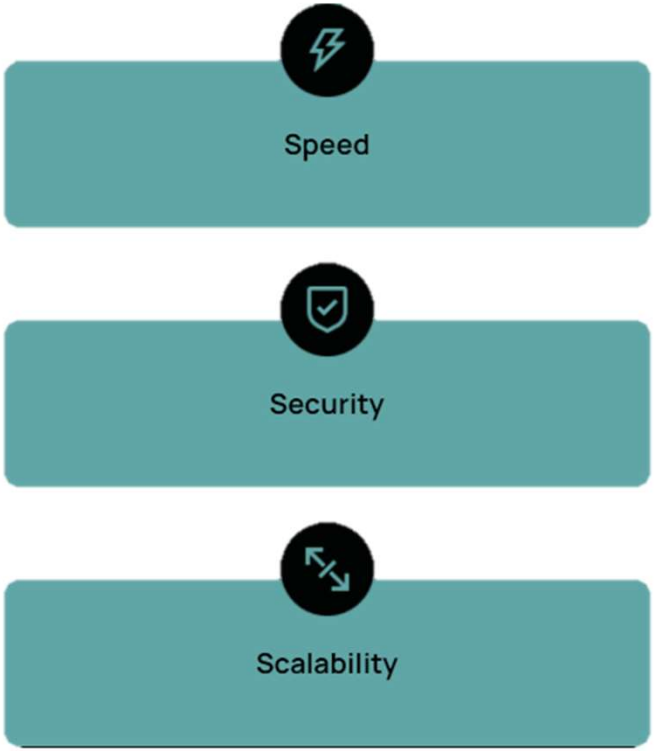
ETH 2.0

Serenity

- First announced in 2018.
- The most ambitious and radical change to be implemented on the network.
- Implementation of Proof of Stake consensus algorithm and moving the network away from PoW architecture.

Why the upgrade?

3S Vision



Why the upgrade?

- Scalability is the main reason
- In ETH1.0, the network can only support around 30 transactions per second which causes delay & congestion.
- Ethereum 2.0 promises up to 100,000 tps.

Why the upgrade?

- To make ETH more Secure.
- Most PoS networks have a small set of validators, making a more centralized system and decreased network security.
- Since PoW suffers from scalability and accessibility issues. PoS replaces it with validators and stake.
- Features: Sharding and Staking and DeFi

ETH2.0 Upgrade Stages

1

The Beacon Chain

Launched in December 2020.

Launch of Beacon Chain.

2

Sharding

In 2021, the first iteration of 64 shards will be launched.

3

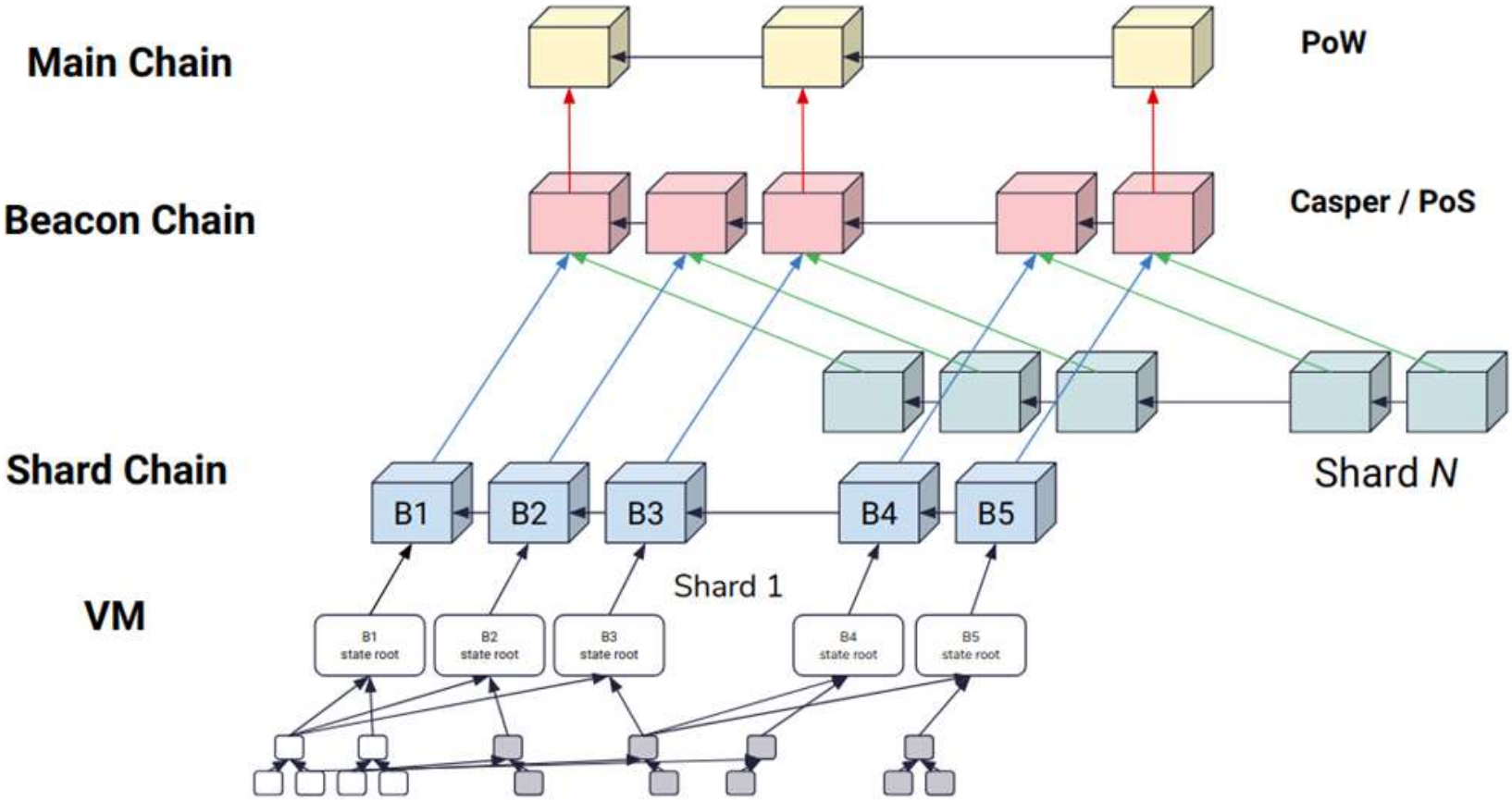
The Docking

The merge is when the current ETH 1.0 chain becomes an ETH2.0 shard.

Planned for June 2022.

4

It will be an upgrade where the 64 shards will be fully functional with smart contract compatibility and other added features.



Source: Hsiao-Wei Wang

Staking

- This concept provides a new opportunity to participate and receive rewards for maintaining the network.

- For those who wish to run their own validators with 32 ETH, use a third-party provider to stake their 32 ETH, or pool their funds with others.

Sharding

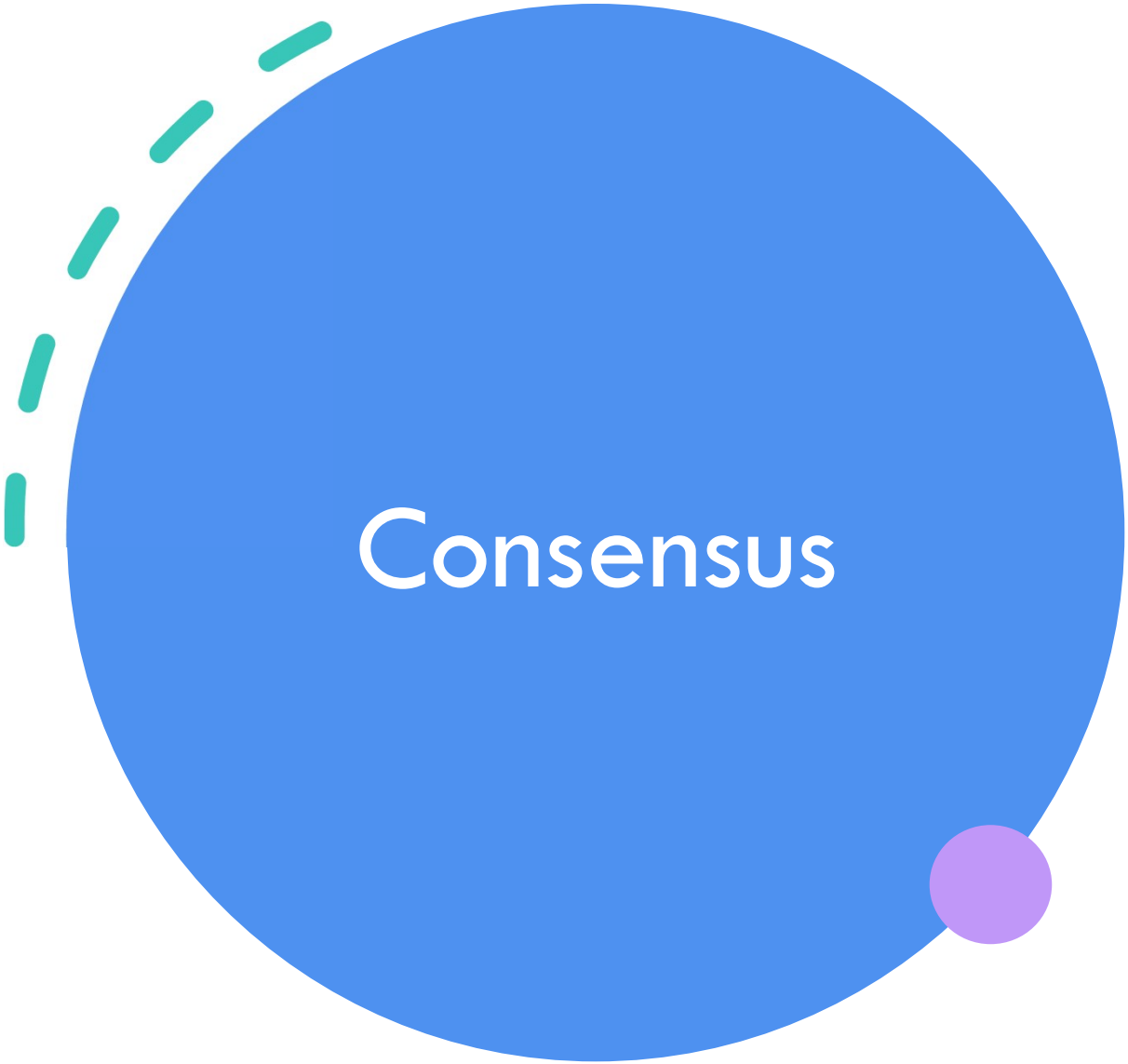
- is a solution to bring about scalability.
- breaks the blockchain into a set of parallel chains.
- The ability to process transactions on different shards in parallel will allow Ethereum to process a larger number of transactions.
- Each shard stores the state for a subset of all Ethereum accounts.
- A very important shard will be the one for today's Ethereum mainnet. This will occupy one of the 64 shards. Thus, all the accounts and smart contracts running on ETH1.0, will continue to be neighbors on the same shard.

Shard Chain

- Shard Chains store and process transactions.
- ETH2.0 will support 1024 Ethereum shard chains, each will be secured by a committee size of 128 validators.
- Transactions are only executed and validated within a shard, and that state is only stored at the shard level.
- These beacon chains to make sure every shard has the most up-to-date data with the help of validators who communicate the state of shard chains to the beacon chain.

Beacon Chain

- It is a new blockchain that will serve as the Ethereum 2.0 backbone
- Bringing together all the shards.
- It provides a crucial coordination point by recording the status of validators, recording attestations (the verification of blocks) and recording links to shards.


Consensus

Consensus mechanism

- the way peers reach a common agreement about the present state of the distributed ledger.
- A consensus mechanism in a cryptoeconomic system also helps prevent certain kinds of economic attacks.
- In theory, an attacker can compromise consensus by controlling 51% of the network.
- Consensus mechanisms are designed to make this "51% attack" unfeasible.

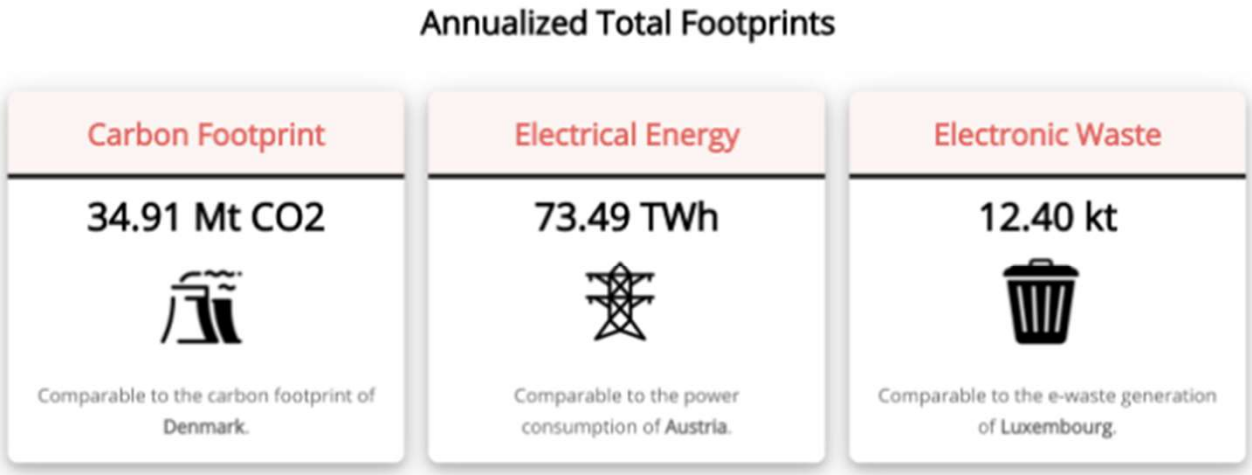
Proof-of-Work

- Block creation is done by miners.

- The network is kept secure by the fact that you'd need 51% of the network's computing power to defraud the chain.
- This would require such huge investments in equipment and energy; you're likely to spend more than you'd gain.

Proof-of-Work

- Favors Computing Power
- Has an energy problem
- More computing power = more control



Bitcoin Energy Consumption — https://digiconomist.net/bitcoin-energy-consumption

Proof-of-Stake

- Block creation is done by validators who have staked ETH to participate in the system.

- You would need 51% of the total staked ETH to defraud the chain.
  And that your stake is slashed for malicious behavior.

Proof-of-Stake

Slashing conditions:

- Validators are split into block proposers and attesters who respectively create and validate new blocks.
- If they don't participate in the vote or if they validate incorrect blocks, their Ether stake will be either reduced or destroyed entirely.

Proof-of-Stake

- Favors Capital
- Larger stake = more power
- More Performant

Proof of Work

Pros		Cons	
Security:	Difficult and costly to attack	Energy efficiency:	Mining requires large amounts of computational power which results in high energy consumption and electricity costs
Decentralization:	highly decentralized, which only increases as more miners join the network	Transaction efficiency:	Networks cannot process large transaction volumes resulting in slow and expensive transactions.
Rewards:	Miners are rewarded for solving mathematical equations and creating new blocks	Risk of 51% attack:	Refers to when a miner obtains the majority of the mining power of a network allowing them to more easily tamper with transactions

Proof of Stake

Pros		Cons	
Transaction efficiency:	Allows for fast transactions and more scalability	Maturity:	PoS is yet to prove itself at scale compared to PoW
Energy efficiency:	Reportedly uses 99% less energy than PoW meaning it is far less damaging for the environment	Decentralization:	Leans more towards centralization as it favours users with high amounts of tokens
Staking:	Provides staking rewards for users who stake a balance of cryptocurrency		

Different PoS Variations

- Delegated Proof-of-Stake (DPoS)
- Liquid Proof-of-Stake (LPoS)
- Nominated Proof-of-Stake (NPoS)
- Hybrid Proof-of-Stake (HPoS)
- …

Attacks on the Ethereum POS Network

- Long-range attacks & weak subjectivity
- Nothing at stake

[2110.10086] Three Attacks on Proof-of-Stake Ethereum (arxiv.org) Oct 2021

Long-range attacks & weak subjectivity

- Attacker would use the current state of the blockchain at the genesis block, in combination with a significant stake of ETH, to create a malicious new chain that the attacker would trick network users to use.
- This new chain would then overtake the main chain and could theoretically rewrite transaction history.
- Long-range attacks exist due to weak subjectivity, which affects new nodes that are added to the network or those that come online after a significant amount of time offline.
- Creating up-to-date competing chains would take little effort in PoS as opposed to in PoW. Therefore, new nodes or nodes that have been a long time offline have to trust the information they receive from other nodes about which chain is the valid one, causing weak subjectivity.

Nothing at stake

- In a naive proof-of-stake implementation, the economically rational decision would be to put your stake on all forks so that you have a better chance of contributing to the winning fork.
- This makes sense since, unlike in PoW where you expend computational energy to contribute to block validation, in naive PoS you have nothing at risk (nothing at stake) when validating and helping to come to a consensus.
- This is an issue for consensus because if everyone has a chance to validate on all chains, coming to a consensus about the main chain would be tough.

Conclusion

- Does Ethereum 2.0 have these problems? Yes
- But ETH2.0 has protective measures.
- In the case of weak subjectivity, to ensure that the information about the valid chain is accurate, a node that is new or comes online after a significant period would have to get a recent block hash from a reputable source, such as a blockchain explorer, and insert that as a “checkpoint” into their blockchain client.
- A malicious attack would result in slashing, which is enough to make such an attempt too costly to be rationally implemented.
- With these measures in place, consequences of misbehavior would be equal to deposit + rewards, as opposed to just rewards in PoW systems.

Conclusion

- Will ETH2.0 replace ETH1.0? No.
- The present POW chain will run in parallel to the new POS shard chains.
- New Ether issuance will take place on the shard chains, and it will be possible to transfer ETH from the POW chain to a shard chain.

Any Questions?

hi@yazdipour.com | https://yazdipour.com