

Parity

The world's fastest and lightest Ethereum client

Proof-of-Authority Chains

- Parity supports a Proof-of-Authority consensus engine to be used with EVM based chains
 - Secure
 - Green
 - Performant
 - Predictable

Proof of Work

- Proof of work is a requirement to define an **expensive computer calculation** that needs to be performed in order to create **a new group of trustless transactions** on a distributed ledger.
 - To verify the legitimacy of a transaction, or avoiding the so-called double-spending
 - To create new digital currencies by rewarding miners for performing the task

Proof of Stake

- Proof of stake is a greener and cheaper way to validate transactions based and achieve the distributed consensus.
 - Miners may potentially own none of the digital currency they are mining.
 - The creator of a new block is chosen **in a deterministic way**, depending on its wealth, also defined as stake.

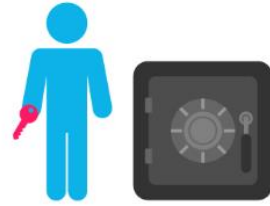
Proof of Work

vs

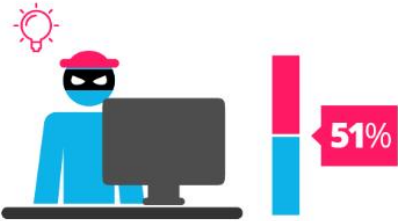
Proof of Stake



proof of work is a requirement to define an expensive computer calculation, also called mining



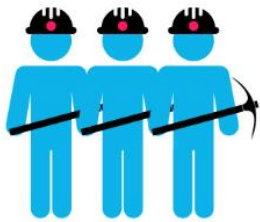
Proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake.



A reward is given to the first miner who solves each blocks problem.



The PoS system there is no block reward, so, the miners take the transaction fees.

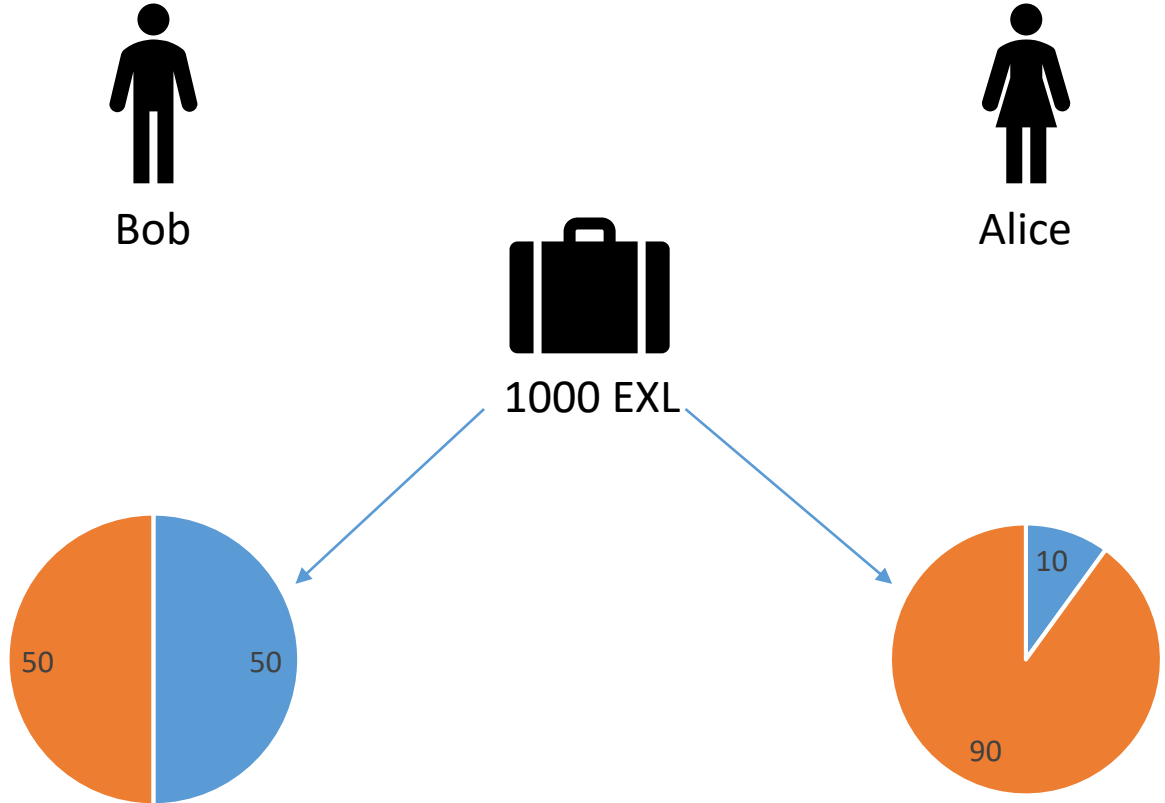


Network miners compete to be the first to find a solution for the mathematical problem



Proof of Stake currencies can be several thousand times more cost effective.

Why not Proof of Stake?



Proof of Authority

- Instead of stake with the monetary value, a validator's **identity** performs the role of stake.



Proof of Authority:

Consensus model with
Identity at Stake

PoS vs PoA

- Similarity
 - identity as a form of stake is also scarce.
- Difference
 - PoA only has one identity per person.
 - It is much harder to get your stake (identity) back in PoA.

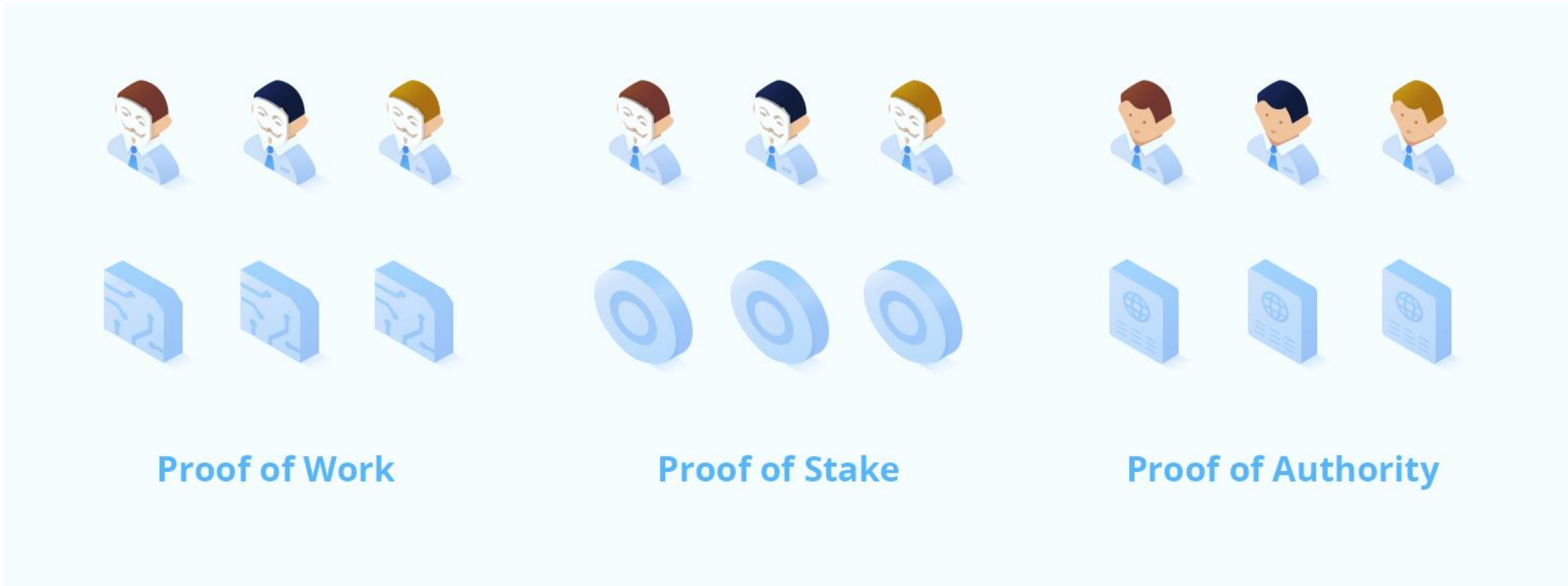
Conditions

- Identity must be true.
- Eligibility for staking identity should be difficult to obtain.
- The procedure of establishing the authority needs to be the same for all validators.

Approaches

- The notaries would go through the formal on-chain identity verification via the POA Network DApps.
- Candidates for validators have to overcome the hurdle of passing notary exams.
- The first approach makes the procedure of gaining the reputation/authority explicit and unified.

Conclusions



Thank you!