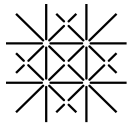


University of Basel

Center for Innovative Finance

Bitcoin, Blockchain and Cryptoassets

Alternative Consensus Protocols

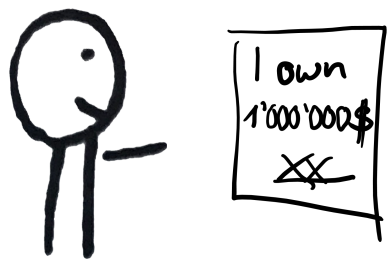
Prof. Dr. Fabian Schär
University of Basel

Release Ver.: (Local Release)
Version Hash: (None)
Version Date: (None)

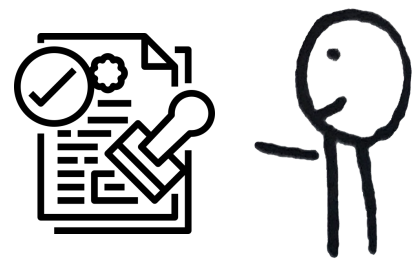
Why Consensus Matters

Blockchain as chain of transactions and states whose compliance with an explicit rule set is attested by a reliable network of record keeping nodes.

Account statement example:



vs.



$\Rightarrow$ Value of the chain content depends on the network attesting it.

Measures Supporting Consensus

Explicit and unambiguous rule set for legitimate changes to the ledger and block sequence.

$\Rightarrow$ Invalid blocks are detected easily and unambiguously.

Decision mechanism for consensus over different, legitimate extensions of the ledger.

$\Rightarrow$ Swiftly resolving situations of uncertainty.

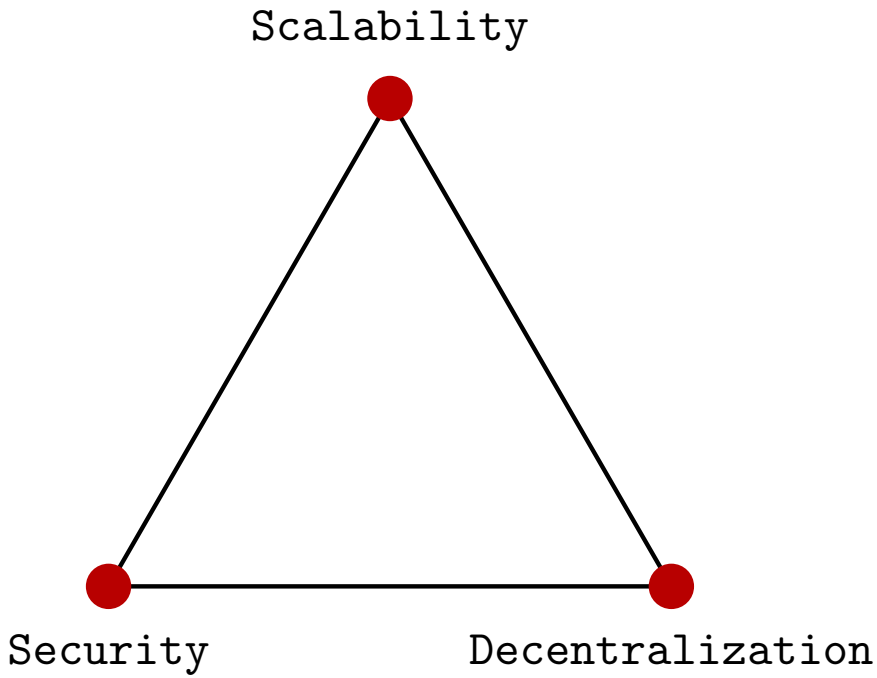
Incentive system that rewards compliant behaviour and / or penalizes manipulation attempts.

$\Rightarrow$ Typically in native protocol asset, tying the participant's interest to the sustainable value of the network.

What Makes a Good Consensus Mechanism?

Suitability of a consensus mechanism depends on the purpose and usecase of a blockchain.

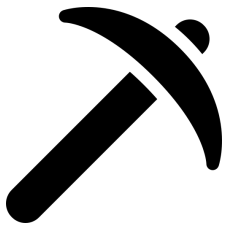
The Trilemma:



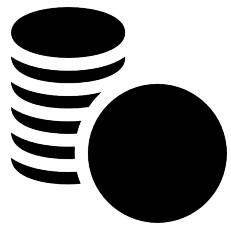
Generalized Rule: Subject to tade-offs, i.e., not possible to achieve all three goals.

Popular Consensus Mechanisms

We will briefly compare the following consensus mechanisms:



Proof of Work



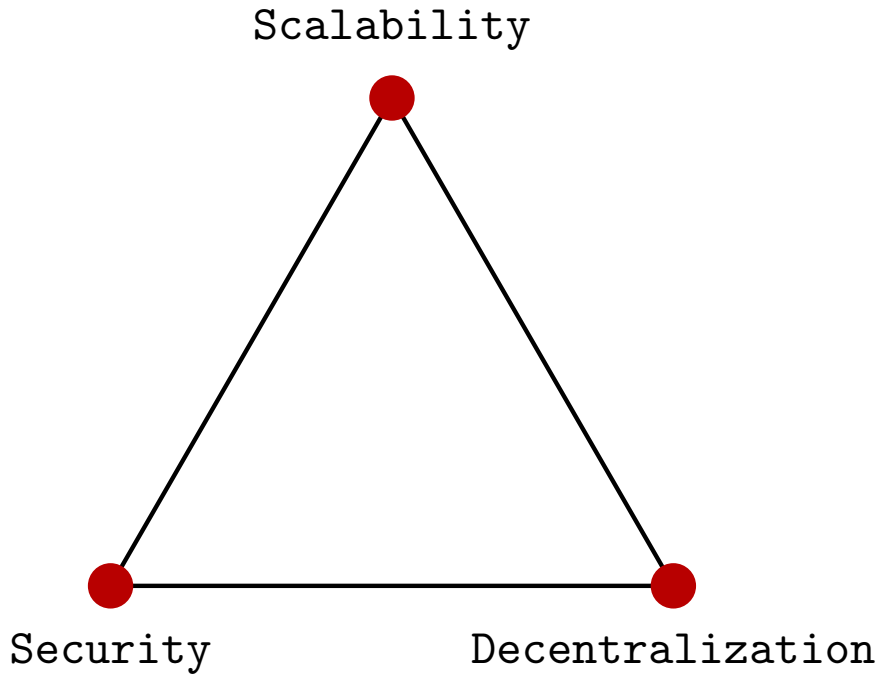
Proof of Stake

Proof of Authority

Openness of the set of consensus-relevant nodes and resources:

	Nodes	Resources
Proof of Work	Open	Open
Proof of Stake	Open	Closed
Proof of Authority	Closed	Closed

Proof of Work Trilemma



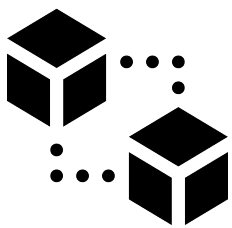
Scalability Every full node needs to process every transaction. Block creation is very resource intensive.

Decentralization Open network with many participants. Mining pools compromise decentralization.

Security Secured by ressource allocation. Simplicity increases security.

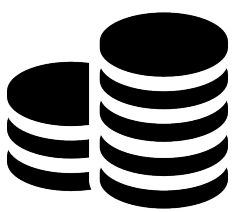
Proof of Stake

To participate in the consensus network, each node - called a validator - needs to deposit and lock native protocol assets. This is called staking.



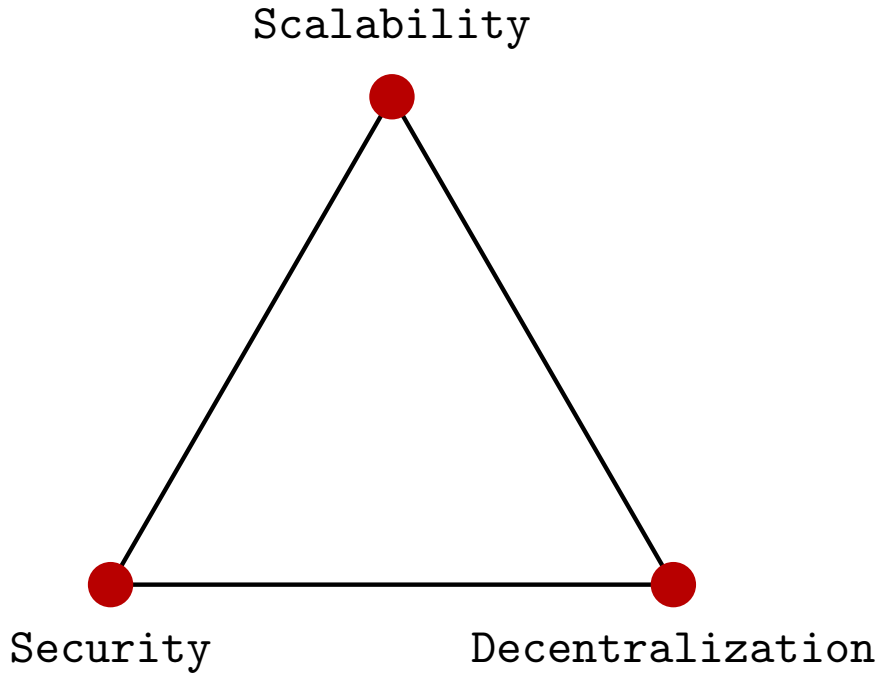
Block creation and transaction validation
Block creators are selected at random in proportion to their stake. A subset of other validators will then attest to the validity of the created blocks.

Malicious and unresponsive validators
Malicious behavior is punished by slashing the staked assets of the offenders. Failure to participate forfeits any rewards and might lead to further punishments.



Rewards and incentive system
Validators receive returns on their stake by performing their duties. These rewards are funded by transaction costs and/or newly generated assets.

Proof of Stake Trilemma



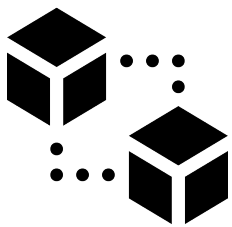
Scalability Only a subset of validators need to process each transaction. Proposers are randomly selected.

Decentralization Open network with many participants. Potential crowding out over time.

Security Pro: Attacker must acquire protocol asset. Con: Complex design may introduce new attack vectors.

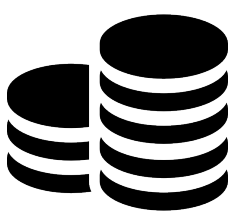
Proof of Authority

The consensus network consists of a small set of approved nodes - called validators. They are identified and therefore have their reputation at stake.



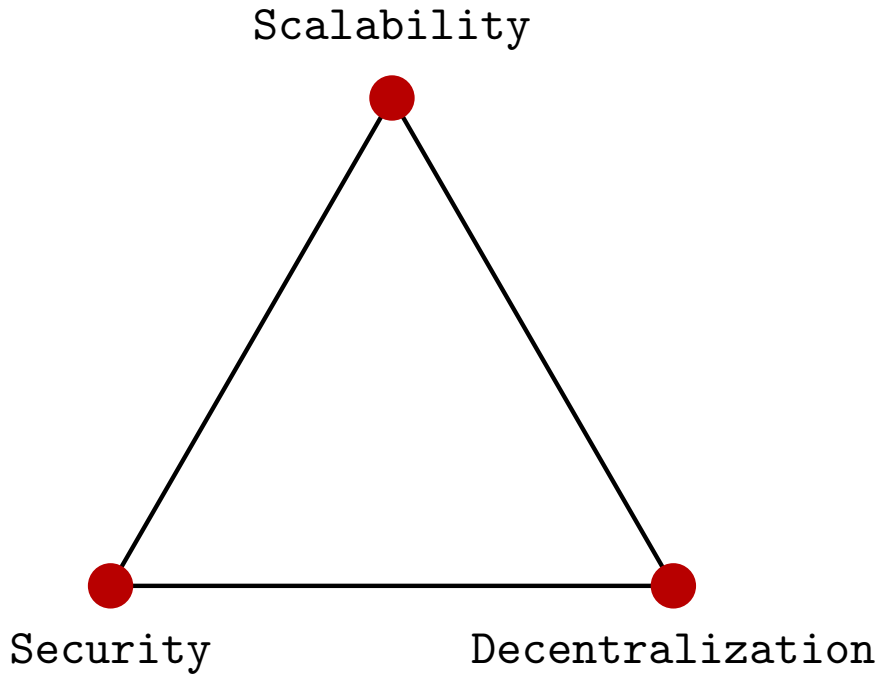
Block creation and transaction validation
Validators (alternating or random selection) create and validate blocks. Other validators will attest to the validity of the created blocks.

Malicious and unresponsive validators
Malicious or unresponsive behavior is punished by exclusion, tarnished reputation and potential legal actions.



Rewards and incentive system
Block rewards are usually limited to the transaction costs. Validators often have external incentives to run their nodes.

Proof of Authority Trilemma



Scalability Very small set of validators and simple mechanism. Higher ceiling for validator performance (hardware).

Decentralization Closed network with risk of collusion. In many cases: heavily centralized.

Security Not immutable (with all pros and cons). In many cases: Just your average database.

Key Takeaways

1. All consensus algorithms have their pros and cons.
2. Immutability and transparency is not just given, because you call your project "Blockchain" – it depends on the architecture, and in particular, on the choice of the consensus mechanism.
3. It is possible for a blockchain to change its consensus mechanism via a hard fork.
4. These are just a few high level examples to give you an overview. There are hundreds of variations and other consensus mechanisms.