Bitcoin-Next Generation (NG) wants to solve the scalability issues of Bitcoin like blockchains that are limited by block size and block interval. The issues arise when tweaking these parameters:
increasing the block size results in higher throughput but slower propagation, and a reduced block interval means reduced latency but with more instability as the system is in disagreement and the blockchain is subject to reorganization.

Bitcoin-NG's latency is just limited by the propagation delay of the network. Its bandwidth is limited only by the processing capacity of the individual nodes. This performance is achieved through decoupling Bitcoin's blockchain operation into two planes: leader election and transaction serialization. Time is divided into epochs with a single leader that is entitled to serialize transactions until a new leader is chosen. This approach maintains Bitcoin's security despite departing from Bitcoin's operation. How is it different?
Bitcoin-NG is forward looking and ensures the system can continually process transactions. This contrasts with Bitcoin's 'choice of leader' operation where it's the leader's responsibility to serialize the entire history and proposing a block.
Furthermore, Bitcoin-NG improves latency and throughput while avoiding fairness and mining power utilization problems.

There are two block types in Bitcoin-NG: key blocks and microblocks.
Key blocks are used for leader election, and microblocks with ledger entries.
A key block contains a public key that will be used in subsequent microblocks to sign the header and make sure its transactions are valid. Since microblocks do not require mining, they can be generated cheaply and quickly by the leader.
However, this behavior allows the leader to publish different replicated-state-machine states to different machines. This allows double spending. In order to demotivate such behavior, a dedicated ledger entry is used: a poison transaction that contains the header of the first block in the pruned branch as a proof of fraud. If such proof of fraud is published on the blockchain by the next miner of the following key block within the maturity window of the misbehaving leader, he will be reprimanded of rewards.

Blockene: a scalable, resource-light, blockchain that can run on smartphones.
https://www.youtube.com/watch?v=pPDkk1amNzw

Proof of Capacity utilizes hardware storage which is used to maintain the blockchain.
A node needs to prove validity through storing and retrieving shards of a single file.
Problem: anyone can purchase a vast amount of cloud storage to overcome the network.
Solution: nodes can only have local storage.
Also known as: **proof of retrievability**, **proof of space**.

Trusted Execution Environment (TEE)-based allows trust to be placed on the hardware running on a node, allowing algorithms that use randomness and waiting time to be utilized. This places stronger assumptions on the system, but allows for a range of different techniques to improve performance. It requires the users to trust the manufacturers of the trusted hardware components…
Techniques include **Proof of Elapsed Time** and **Proof of Luck**.
PoEt: each node "sleeps" a random amount. The first who wakes up is the leader..
P-o-L: all nodes generate a random number that is being compared with all the other numbers. This comparison (however it is implemented) decides the leader..

Proof of Location uses mobile devices dynamic locations to create and verify proofs of a given device's location. It relies heavily on close peers to validate the location of another.
There is a reward for acting honestly, and a punishment for falsifying / spoofing your location.