Bitcoin-NG: A Scalable Blockchain Protocol

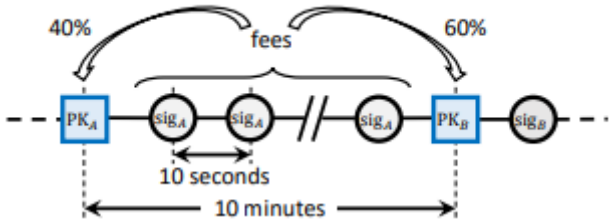
Scalability barrier: time and size of block. Bitcoin NG latency is limited only by propagation network. Decoupling: leader election and transaction serialization.

The protocol divides time into epoch – single leader. Two types of block: key for leader election and microblocks ledger entries. Key blocks – solve nonce (PoW). Micro – predefined size and time (10 sec). Fork of microblocks os pruned. You can get reward only after key 100 blocks and spend it (maturity period). Double spending by forking is prevented using poison transaction (header transaction, before rewards spend, cheater loses rewards and founder gets 5% of it).

He can try to mine on secret block, but that is not beneficial.

If leaders publishes no microblocks, you can wait your transaction to be included afer abour 4/3 key blocks.

Metrics: consensus delay – odds that how many nodes will agree on time, fairness, mining power utilization, subjective time to prune, time to win. Interesting about experimental setup: block propogation time grows linearly with block size. Evaluation: BincoinNG beats Bitcoin in all metrics without security leakages. In experiments key blocks is 10 seconds to reduce forks. Frequency increasy does not lead to worse other metrics (Figure 8). Bitcoing NG also scales in case of block size(only in transaction frquency same Figure 9)



Fairness principle example:

🧪 **Example:**

💻 Mining Power Distribution:

- **Miner A** (largest): 40%
- **Other miners**: 60%

📦 Blockchain Transitions (i.e. who added the blocks):

- **Miner A** produced 70% of the blocks
- **Other miners**: only 30%

🔢 **Plug into the formula:**

- Fraction of transitions **not by Miner A**: 30% = **0.3**
- Fraction of mining power **not held by Miner A**: 60% = **0.6**

$$\text{Fairness} = \frac{0.3}{0.6} = 0.5$$

Scalable and Probabilistic Leaderless BFT Consensus through Metastability

Snow family – leaderless BFT consensus protocols. No centralized leader, Consensus by sampling, Probabilistic safety, No energy consumption required , low overhead. Example: avalanche system (3400 tps, low confirmation latency)

Safety is better, can hold til 33% of failure nodes. The protocol degrades smoothly after 1/3. Formal properties: P1- safety (almost no conflict decision), P2 – liveness (within some rounds), P3- liveness If the number of bad nodes is ≤ O(√n),this system will almost certainly reach consensus quickly,- implemented in O(log n) voting rounds. Gossip distribution protocol. No sybil attack resistance (has PoS or other on top), flooding protection (charge of fee).

Protocol design : Slush- consensus between colors (Red and blue), Snowflake (adds counter) – Basic BFT upgrade , SnowBall (confidence history). Slush – purely probabilistic(no guarantee), no BFT, Once a color has even a small lead ($\delta > 0$), probability of reversing decreases exponentially. Multivalue consensus – multiple snowball instances or directly few colors.

Avalanche: p2p payment system on top of snowball. Byzantine users can stale. Interfere DAG structure (efiicency, security). Conflict set- just one accepted(more children), tie breaking – first seen. Runs multiple Snowball instances. Each transaction or conflict – one instance. Transaction is accepted only if all ancestors solved conflict sets. Mutiple UTXO – transaction accepted if all inputs are accepted. Messages = O (k n), k – how many neighbors. "Do you support T? And her parents too?" (1 chit). Evaluations – 7000tps with batch size 40 (40 txs in voting). Latency 1.35 sec. Leaderless design. Signature verification is the current performance bottleneck (without it 2.6 times faster). Tolerance to Byzantian nodes.

Deconstructing Blockchains: A Comprehensive Survey on Consensus, Membership and Structure

PoW- work (cryptopuzzles). First found – member, sybil attack resistance. PoW CPU (Bitcoin), Memory Bound PoW(egalitarian). PoR (Proof of Reputation)-membership is based on long-term contribution.

PoS – stake coins. Different types of PoS (Deposit-Based PoS : Proof of Lock, Proof of Deposit; Balance-Based PoS: Proof-of-coin-age, Proof-of-activity(Combines PoW and PoS), Algorands VRF, Ouroboros(coinflip, random leader election); Delegated PoS(DPoS – fixed numbers of delegates who produces blocks); Proof of Burn (Burn))

Proof of Authority (trusted nodes produces block, manually chosen). Implementations : Aura (Round-based PoA), Clique (Epoch based)

Proof of Capacity – prove validity by demo storage space usage. Challenge based on hash in plot file (find solution in stored). To propose a block, a node must retrieve data from its storage to prove it holds the necessary space. Proof-of-Retrievability – nodes prove it has access or Proof-of-Space – use storage space to generate a proof

TEE-Based (Trusted Execution Environment)- code is running inside trusted hardware. Proof-of-Elapsed-Time (PoET): Nodes sleep for a random time inside the TEE; the first to wake create the

block. Proof-of-Luck: All nodes generate a random number securely inside the TEE; the node with the “luckiest” (lowest) number wins.

Proof-of-Location - geographic location as part of consensus or transaction validation.