NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications
Prof. Sandip Chakraborty

Department of Computer Science & Engineering
Indian Institute of Technology Kharagpur

Lecture 39: Bitcoin-NG

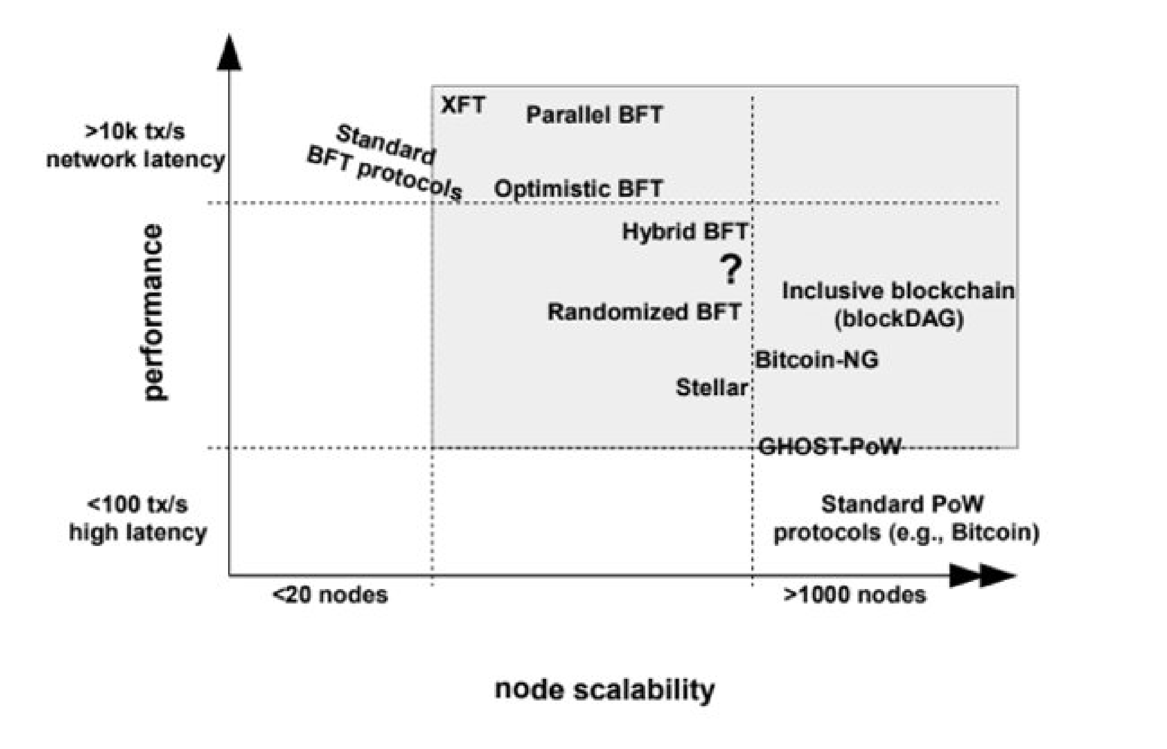
CONCEPTS COVERED

- Issues with Bitcoin – Revisit
- Bitcoin-NG

KEYWORDS

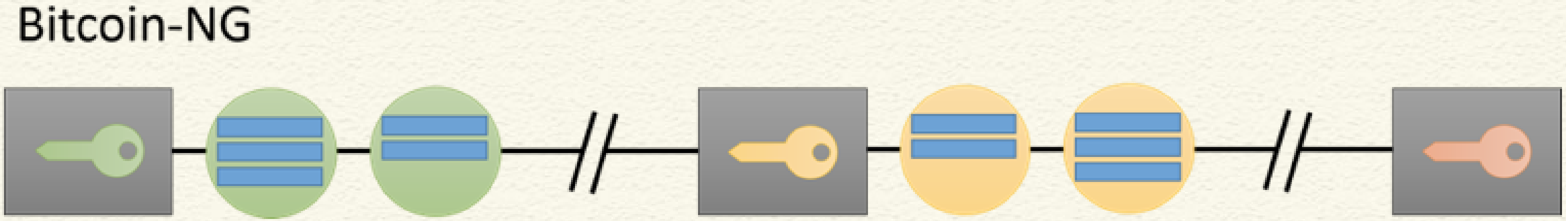
- **Transaction Serializability**
- **Key-blocks and Microblocks**

Performance vs Scalability



Vukolić, Marko. "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication." *International Workshop on Open Problems in Network Security*. Springer, Cham, 2015.

Towards a Scalable Consensus



Eyal, I., Gencer, A. E., Sirer, E. G., & Van Renesse, R. (2016, March). **Bitcoin-NG: A Scalable Blockchain Protocol**. in *NSDI 2016*

Issues with Nakamoto Consensus

- **Transaction scalability**
  - Block frequency of 10 minutes and block size of 1 MB during mining reduces the transactions supported per second

Issues with Nakamoto Consensus

- **Transaction scalability**
  - Block frequency of 10 minutes and block size of 1 MB during mining reduces the transactions supported per second

- **Issues with Forks**
  - Prevents consensus finality
  - Makes the system unfair - a miner with poor connectivity has always in a disadvantageous position

Bitcoin-NG: Decouple Leader Election

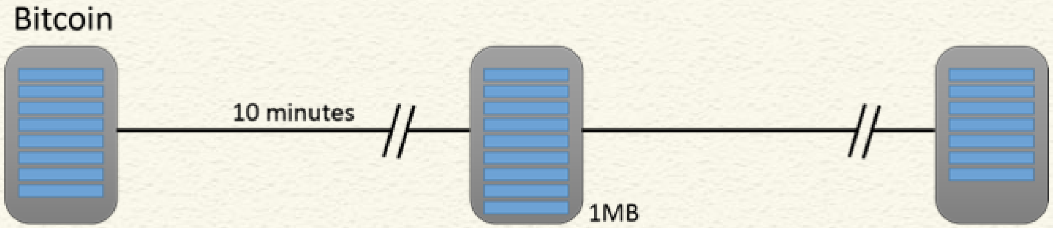
- Bitcoin - think of the winning miner as the **leader** - the leader serializes the transactions and include a new block in the blockchain

Bitcoin-NG: Decouple Leader Election

- Bitcoin - think of the winning miner as the **leader** - the leader serializes the transactions and include a new block in the blockchain

- Decouple Bitcoin's blockchain operations into two planes
  - **Leader election**: Use PoW to randomly select a leader (an infrequent operation)
  - **Transaction Serialization**: The leader serializes the transaction until a new leader is elected

Bitcoin vs Bitcoin-NG



Bitcoin vs Bitcoin-NG

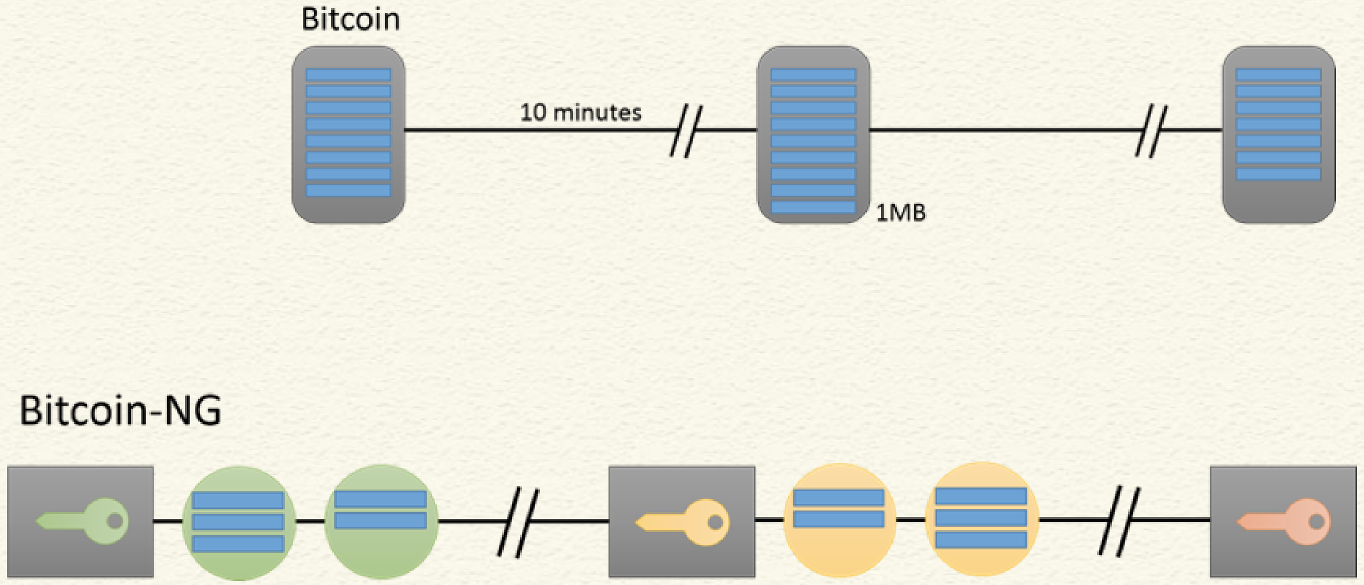


Image Source: http://hackingdistributed.com/2015/10/14/bitcoin-ng/

Bitcoin-NG: Key Blocks

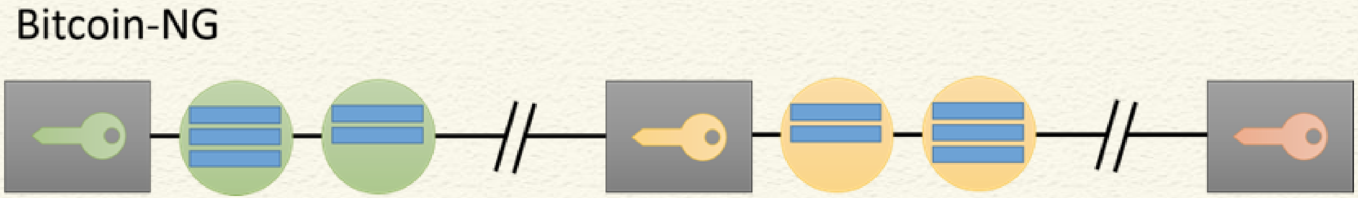
- Key blocks are used to choose a leader (similar to Bitcoin)

- A key block contains
  - The reference to the previous block
  - The current Unix time
  - A coinbase transaction to pay of the reward
  - A target hash value
  - A nonce field

Key Blocks

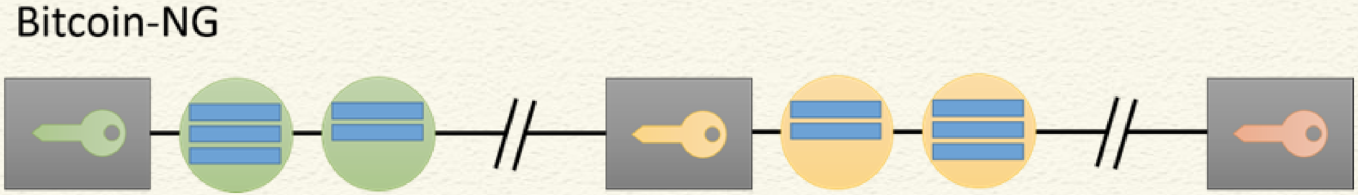
- Key blocks are generated based on regular Bitcoin mining procedure
    - Find out the nonce such that the block hash is less than the target value

- Key blocks are generated infrequently - the intervals between two key blocks is exponentially distributed



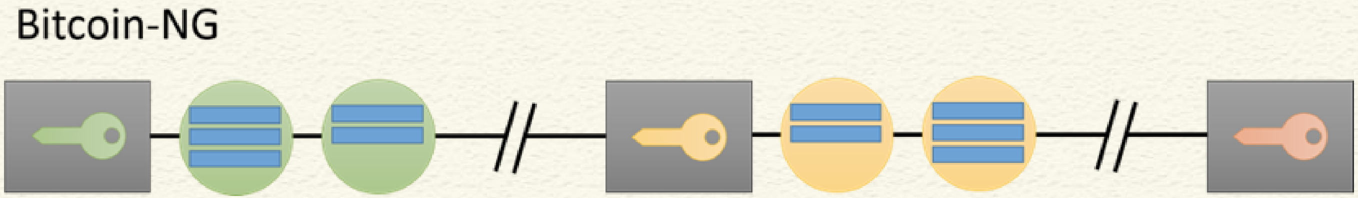
Bitcoin-NG: Microblocks

- Once a node generates a key block, it becomes the **leader** and generates further microblocks
  - Microblocks are generates at a set rate smaller than a predefined maximum
  - The rate is much higher than the key block generation rate



Bitcoin-NG: Microblocks

- A microblock contains
  - Ledger entries
  - Header
    - Reference to the previous block
    - The current Unix time
    - A cryptographic hash of the ledger entries (Markle root)
    - A cryptographic signature of the header (signature of the key block miner)



Microblock Fork

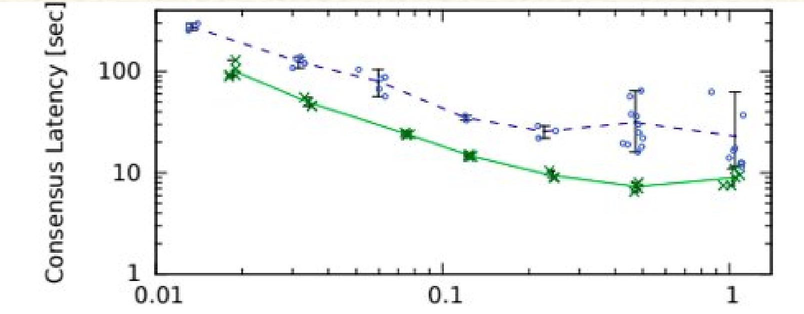
- When a miner generates a key block, he may not have heard of all microblocks generated by the previous leader
  - Common if microblock generation is frequent
  - May result in microblock fork

Microblock Fork

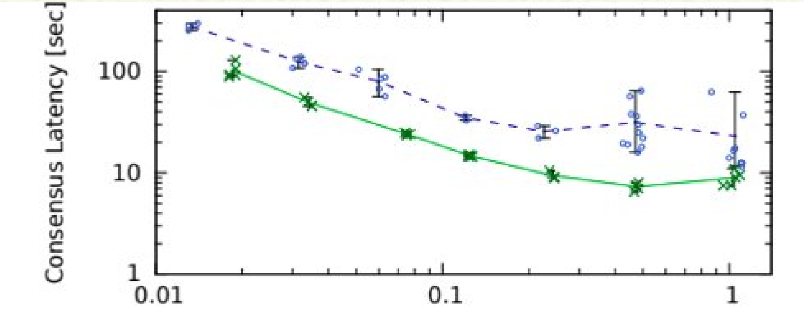
- When a miner generates a key block, he may not have heard of all microblocks generated by the previous leader
  - Common if microblock generation is frequent
  - May result in microblock fork

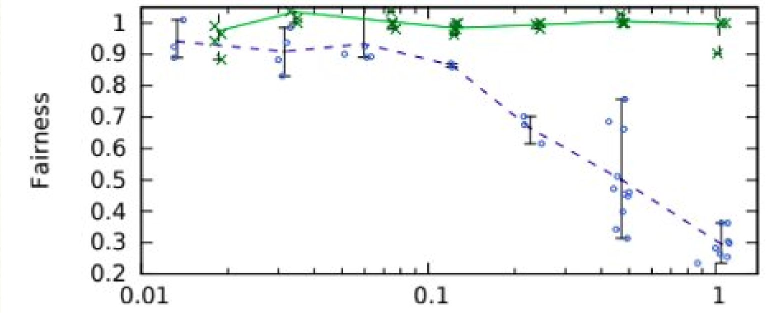
- A node may hear a forked microblock but not new key block
  - This can be prevented by ensuring the reception of the key block
  - When a node sees a microblock, it waits for propagation time of the network to make sure it is not pruned by a new key block

Bitcoin-NG Performance



Bitcoin-NG Performance



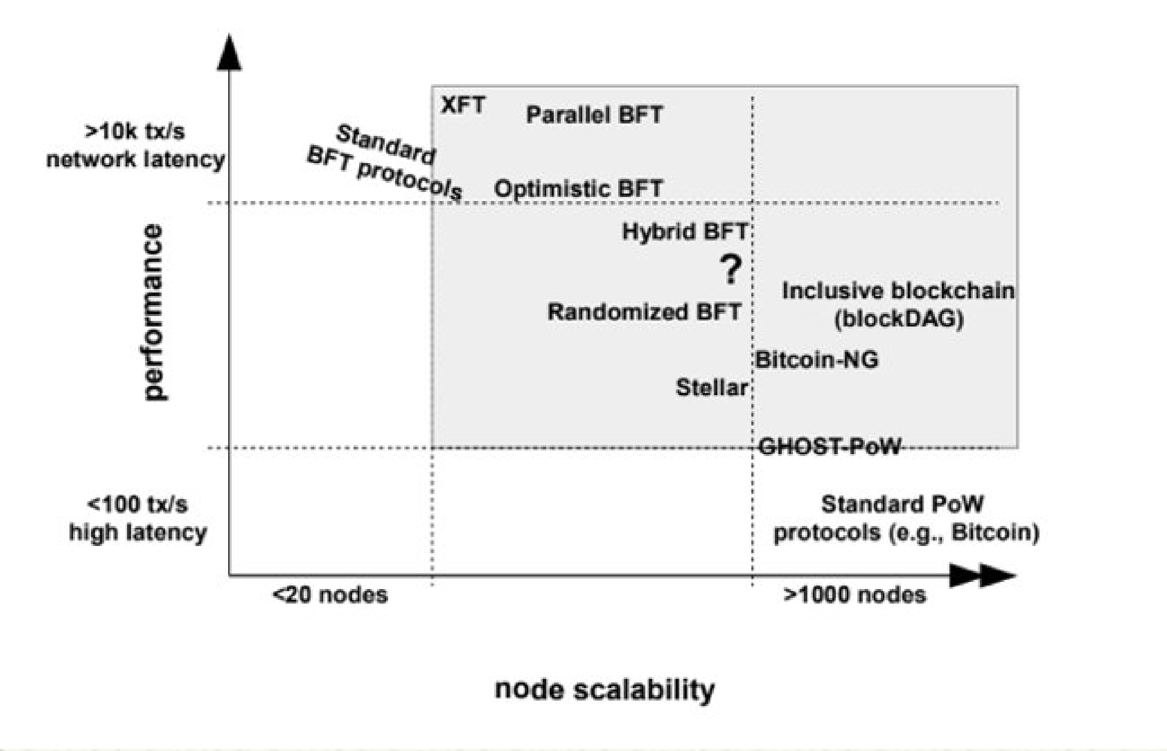


Conclusion

- A major source of latency in Bitcoin is that every block needs to be mined by different miners

- Bitcoin-NG decouples leader election from transaction serialization
  - Key blocks and Microblocks

Performance vs Scalability - Revisiting



Thank you