Image Source:
https://steemit.com/blockchain/@tariq3njr/what-is-blockchain-technology

Research Aspects - I
Consensus Scalability

Outline of talk

- In this lecture, we will look in to different use cases, which are there in the development of the BC platform and how you can participate in this research procedure
- What are different open research challenges that researchers are still facing.
- What are the different scopes to do research in this BCT area.

Blockchain Consenus Protocols

- Permissionless Blockchain
  - Proof of Work (PoW)
  - Proof of State (PoS)
  - Proof of Burn (PoB)
  - Proof of Elapsed Time (PoET)

Uses Challenge response mechanism

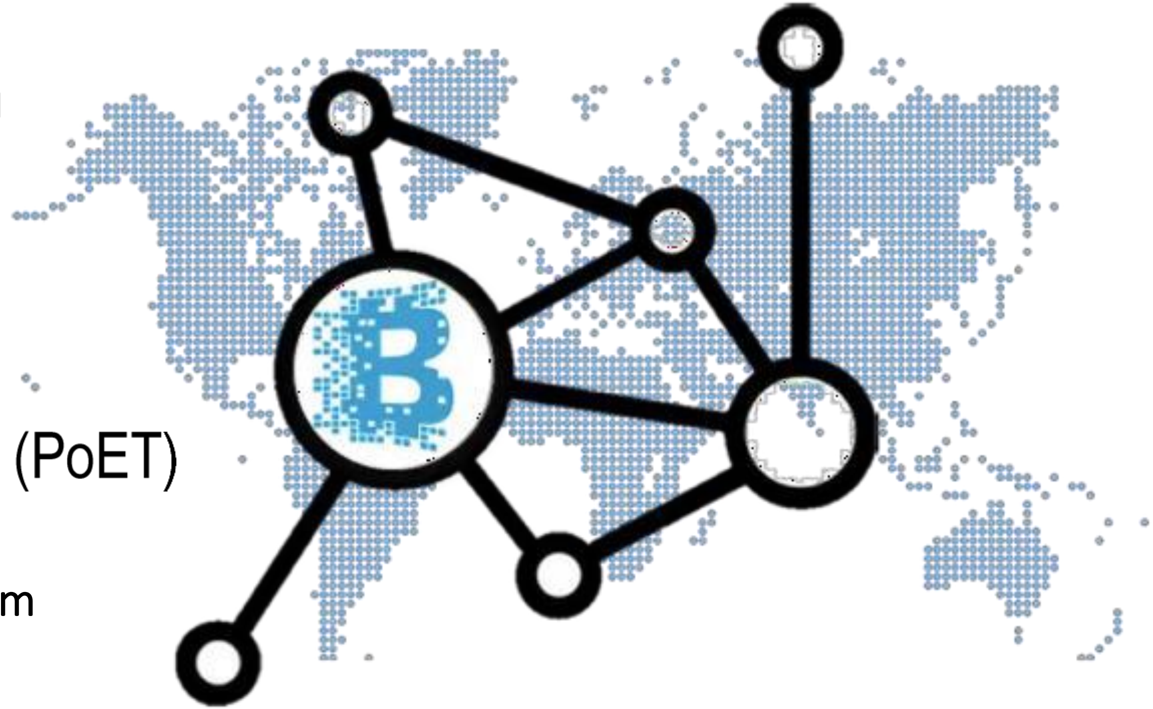


Image Source: https://www.ictworks.org/eight-practical-blockchain-use-cases/

Blockchain Consenus Protocols

- Permissioned Blockchain
  - BFT
  - PBFT
  - RBFT

Uses BFT classes of Algorithm

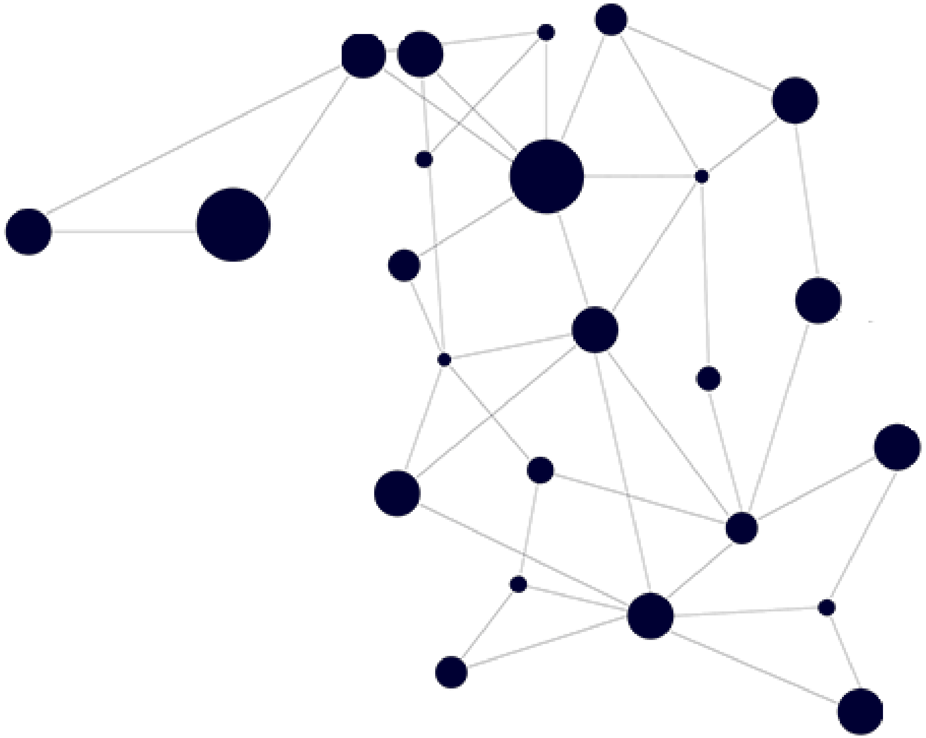


Image Source: https://www.challenge.org/demo/blockchain-challenge-2/

PoW vs PBFT

- PoW
  - Open environment, works over a large number of nodes
  - Scalable in terms of number of nodes
  - Transaction throughput is low

- PBFT
  - Closed, not scalable in terms od number of nodes
  - High transaction throughput

PoW Scalability

Always a research question how to improve the Tx scalability of PoW based system ?

- Two magic numbers in PoW
  - **Block frequency** - 10 minutes
  - **Block size** - 1 MB

But with these two parameters, we can achieve:

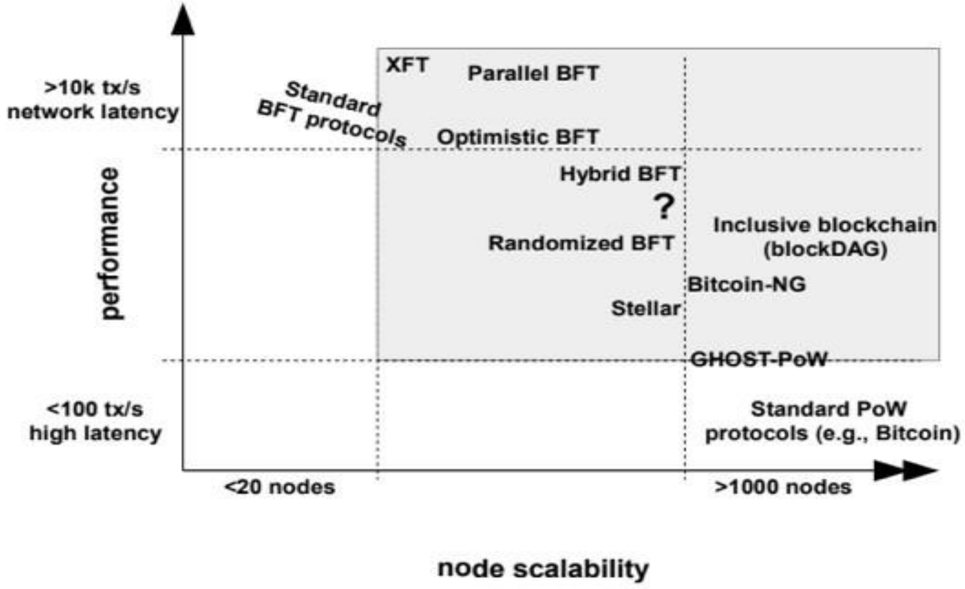
- Transaction throughput - 7 transactions per second (with 200-250 bytes transactions)

7 Txs per ses is very is very low for PoW type based Algorithms. E.g) In Visa and master card there are more than 40 million Txs per sec (which is a real number in this scenario)

Block Frequency: indicates at what frequency you generate the blocks, which is controlled by the mining difficulty. After every 10 min a new block is generated.

Block Size: it is restricted up to 1MB as per the original Bitcoin proposal by Nakamoto but later on increased up to 8MB

Performance vs Scalability for PoW and BFT



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.

Node scalability: means how many number of nodes this particular TX/consensus protocol can support
Performance: means Tx throughput

- PoW protocol has good scalability in terms of number of nodes that an be supported but the scalability is very less in terms of Tx /sec that can be supported
- BFT can supports good Tx scalability (more than 10k Tx/sec) but the number of nodes supported by BFT is typically less than 20 nodes
- So to find the scalable way to move in BC environment is an open research area

PoW vs PBFT – Consensus Finality

- *If a correct node p appends block b to its copy of blockchain before appending block b', then no correct node q appends block b' before b to its copy of the blockchain* (Vukolic, 2015)

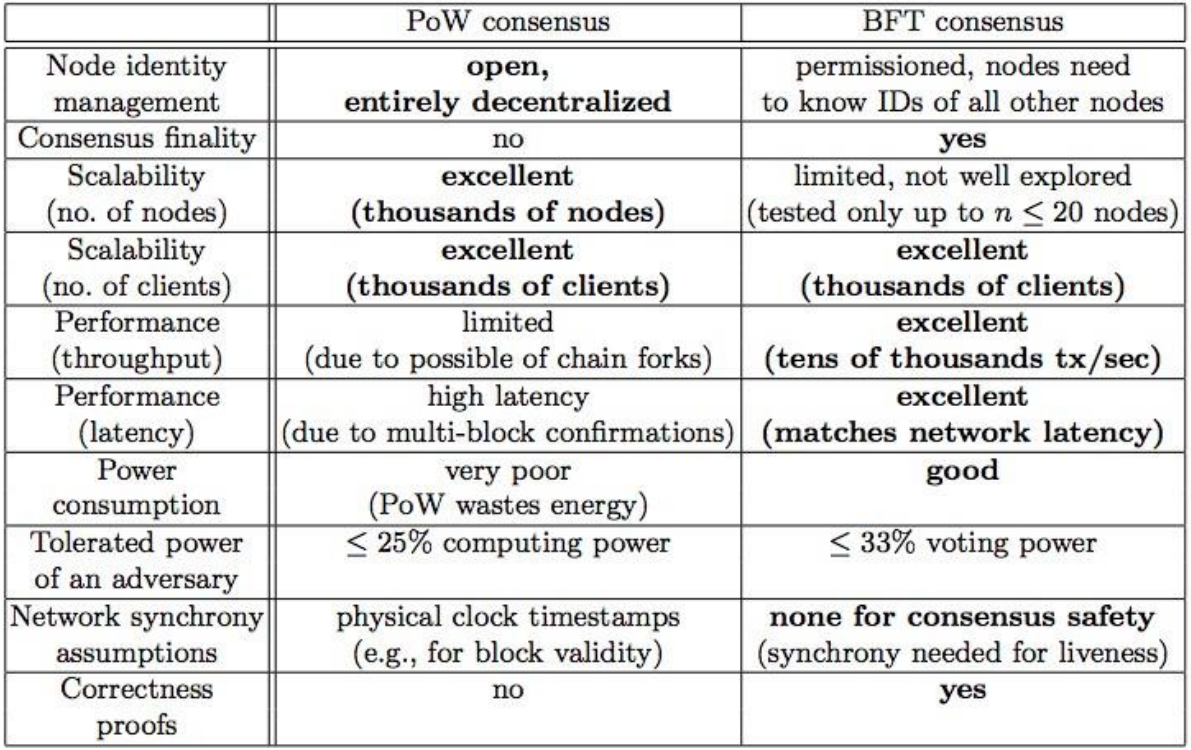
E.g) if we have two blocks B10 and B11 then every correct node in the n/w will append B11 after B10. It ensures that there is always a **"total ordering"** among the blocks

- PoW is a randomized protocol - does not ensure consensus finality
  - Remember the forks in Bitcoin blockchain

Because In PoW, the challenge is thrown by the system that you have to generate certain hash value based on constrains like merkle root, find out nonce.

- BFT protocols ensure total ordering of transactions - ensures consensus finality

PoW Consensus vs BFT Consensus



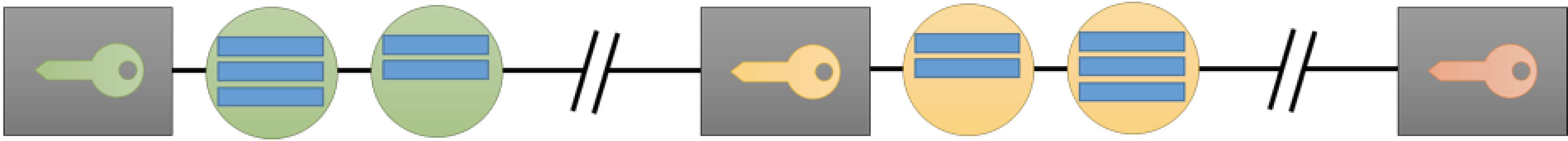
	PoW consensus	BFT consensus
Node identity management	**open, entirely decentralized**	permissioned, nodes need to know IDs of all other nodes
Consensus finality	no	**yes**
Scalability (no. of nodes)	**excellent (thousands of nodes)**	limited, not well explored (tested only up to $n \leq 20$ nodes)
Scalability (no. of clients)	**excellent (thousands of clients)**	**excellent (thousands of clients)**
Performance (throughput)	limited (due to possible of chain forks)	**excellent (tens of thousands tx/sec)**
Performance (latency)	high latency (due to multi-block confirmations)	**excellent (matches network latency)**
Power consumption	very poor (PoW wastes energy)	**good**
Tolerated power of an adversary	$\leq 25\%$ computing power	$\leq 33\%$ voting power
Network synchrony assumptions	physical clock timestamps (e.g., for block validity)	**none for consensus safety** (synchrony needed for liveness)
Correctness proofs	no	**yes**

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.**

Outline of talk

- In this lecture, we will discuss about Bitcoin NG protocol, which is successor of standard Bitocoin protocol by replacing the PoW scalability with more sophisticated work (Bitcoin NG)

Bitcoin-NG



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

Bitcoin-NG

Issues with Nakamoto Consensus (PoW)

- **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

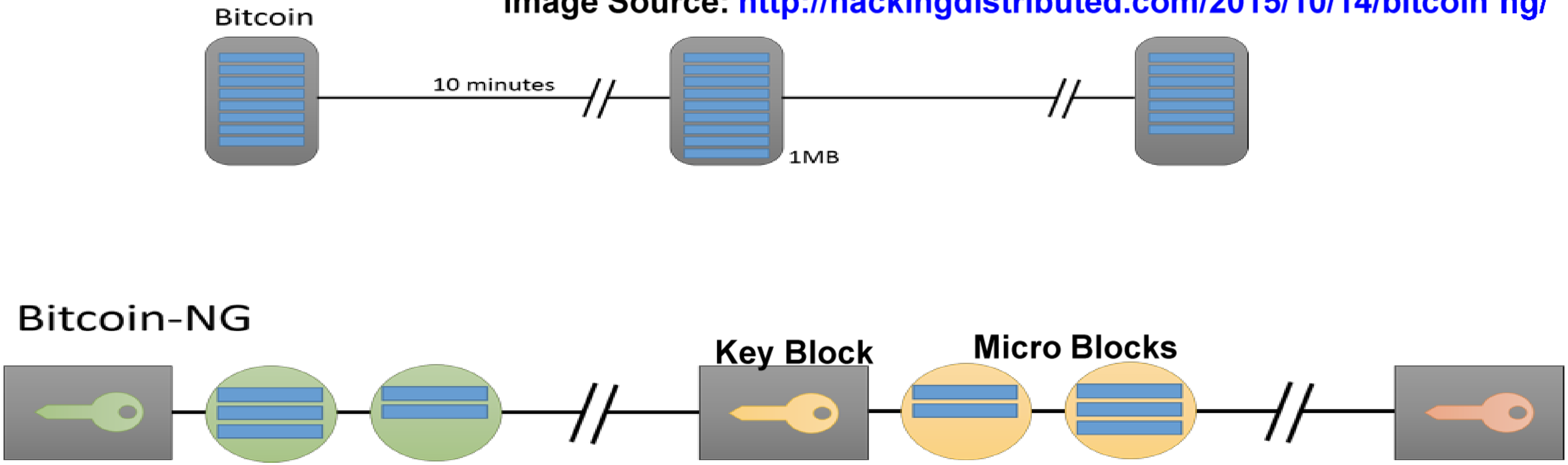
Bitcoin-NG : A Scalable PoW Protocol

- 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

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



In Bitcoin n/w, after every 10 min you elect a new leader (miner who solved the puzzle) whose task is to add the new block in the system.

In Bitcoin NG, we have 2 types of block; key block: which are generated by the PoW based Mechanism. In every PoW round you generate one keyblock, which contains the public key of the miner who has been able to solve the challenge. Then, that miner will generate multiple micoblocks, which contains the set of Txs inside. Leader will encrypt all microblock with his/her private key and other have public key which can be used for verification purpose.

Bitcoin-NG : Key Blocks

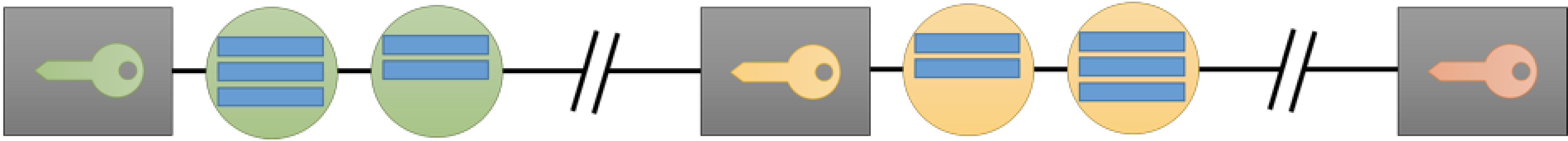
- Key blocks are used to choose a leader (similar to Bitcoin)

- A key block contains Similar to std. block in the Bitcoin
  - The reference to the previous block
  - The current Unix time Just a time stamp
  - A coinbase transaction to pay of the reward
  - A target hash value
  - A nonce field

Bitcoin-NG: Key Blocks

- For a key block to be valid, the cryptographic hash of its header must be smaller than the target value. Similar to PoW in Bitcoin

- The key block also contains a public key (so the name, key block)
  - Used in subsequent microblocks



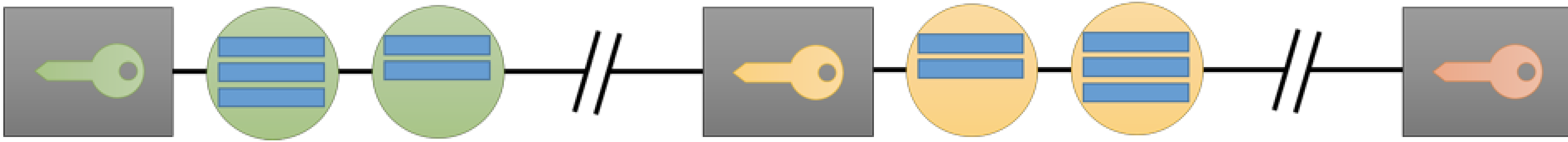
Pub key is used in the subsequent microblocks to validate that these microblocks have been generated by the respective miner.

In next round again the challenge is given to be solved by the miners

Bitcoin-NG: 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**

- As a leader, the node is allowed to generate microblocks
  - Microblocks are generates at a set rate smaller than a predefined maximum
  - The rate is much higher than the key block generation rate

For example, If you generate a key block at every 10 minutes then it is like that after every 1 min you generate a microblock (Means within 1 min whatever Txs have been received to that particular miner, which is working as a leader of this round, so the miner can generate a new microblock with the serialized TXs and added to the existing BC)
Because of this you will be able to generate more microblocks in the system and ultimately added more TXs, which will help you to increase the Scalability of the entire system

Bitcoin-NG: Microblocks

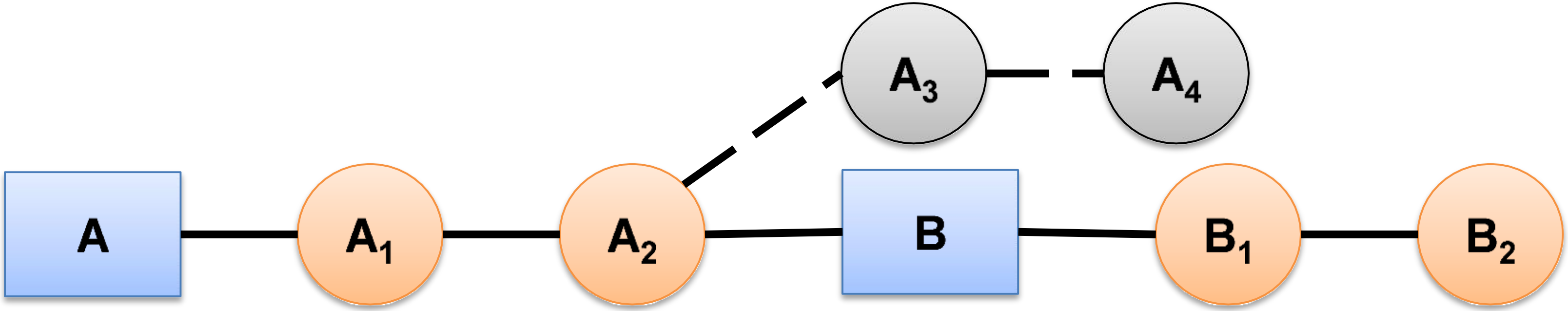
- A microblock contains
  - Ledger entries
  - Header
    - Reference to the previous block
    - The current Unix time
    - A cryptographic hash of the ledger entries (Markle root)
    - A cryptographic signature of the header
- The signature uses private key corresponding to the key block public key

This keyblock contains the public key and all the microblocks, ultimately the microblock header, which contains the signature (generated from std. digital signature mechanisms using private key corresponds to public key.)

Now verify whether the signature is coming from the respective miner who has generated this particular keyblock

Bitcoin-NG: Confirmation Time

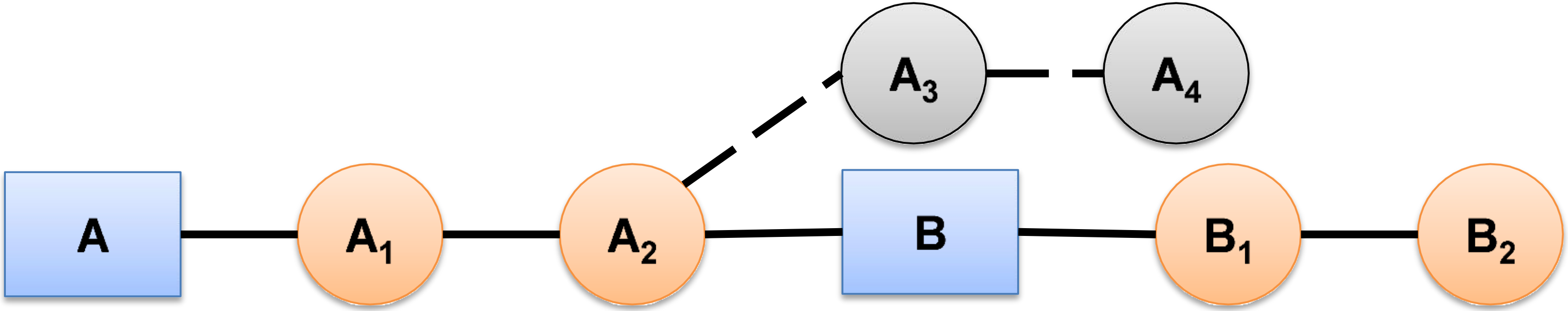
- When a miner generates a key block, he may not have heard of all microblocks generated by the previous leader
  - Common if microblock generation is frequent
  - May result in microblock fork



For example, Say A was a miner who has generated this keyblock and at some time instance another miner B has generated keyblock. Now it may happen that when B has generated the key block during this time, it has not heard about all the microblocks which has been generated by node A. Then, A3 and A4 becomes a fork.

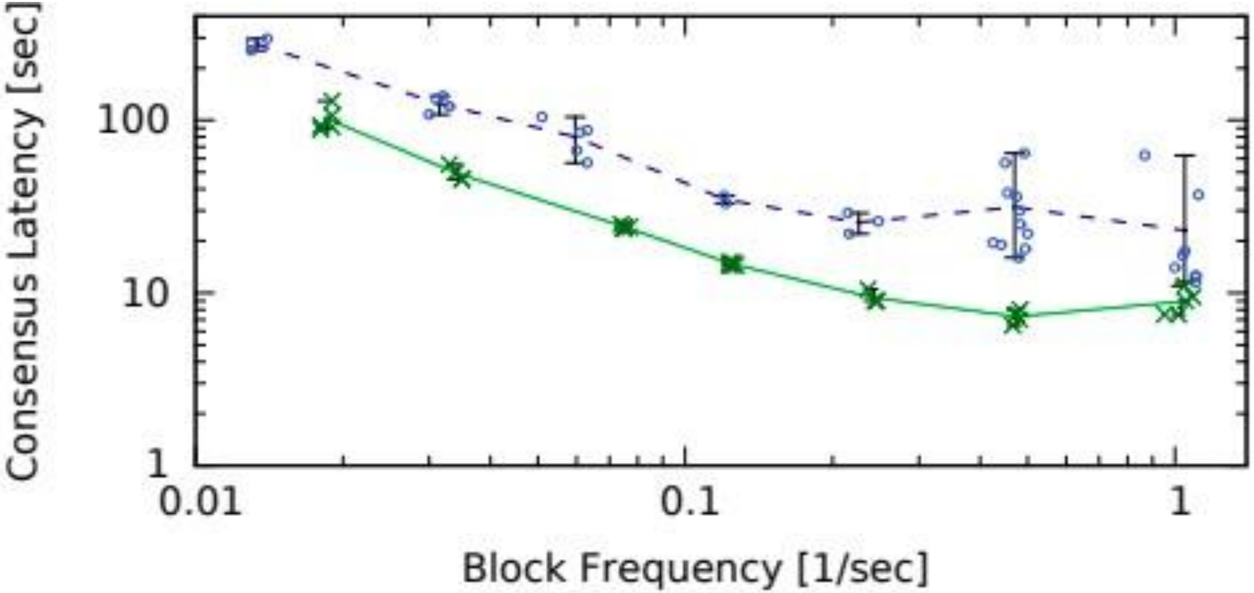
Bitcoin-NG: Confirmation Time

- A node may hear a forked microblock (A_3) but not the new key block (B)
  - 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



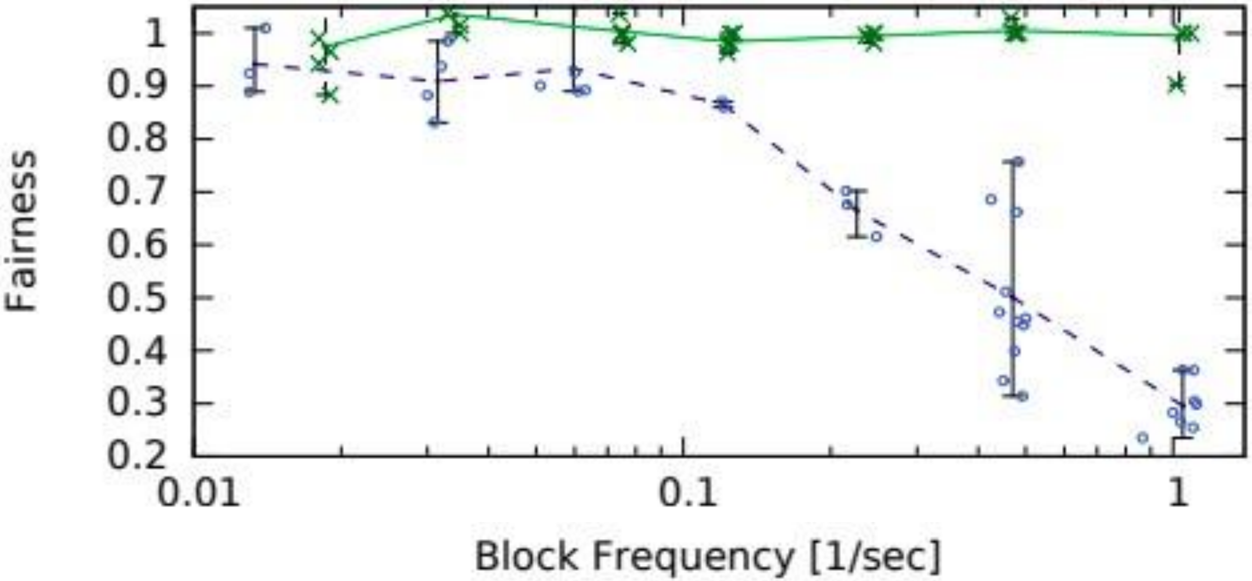
Means whenever you are hearing a new microblock then you wait for the maximum propagation time in the network

Bitcoin vs Bitcoin-NG



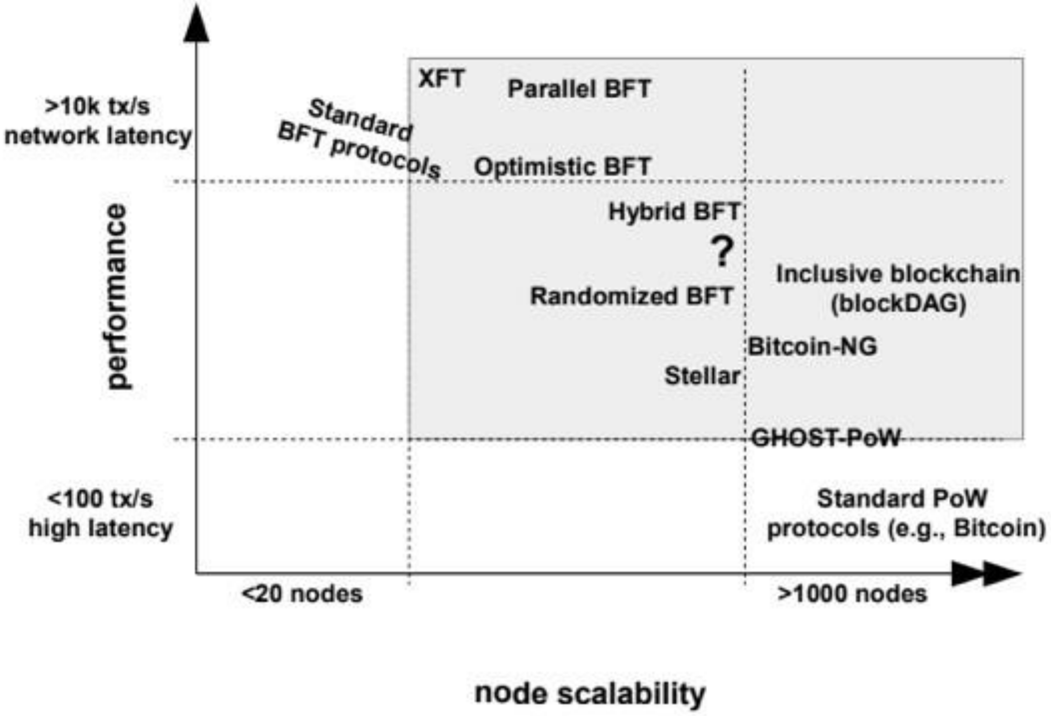
Blue line for Bitcoin, green for Bitcoin NG
Commitment latency for Bitcoin NG is significantly less than Bitcoin

Bitcoin vs Bitcoin-NG



Blue line for Bitcoin, green for Bitcoin NG
Fairness (because of fork in the system) for Bitcoin NG is significantly higher compared to Bitcoin

Performance vs Scalability for PoW and BFT



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.**