



BLOCKCHAINS

ARCHITECTURE, DESIGN AND USE CASES

SANDIP CHAKRABORTY
COMPUTER SCIENCE AND ENGINEERING,
IIT KHARAGPUR

PRAVEEN JAYACHANDRAN
IBM RESEARCH,
INDIA



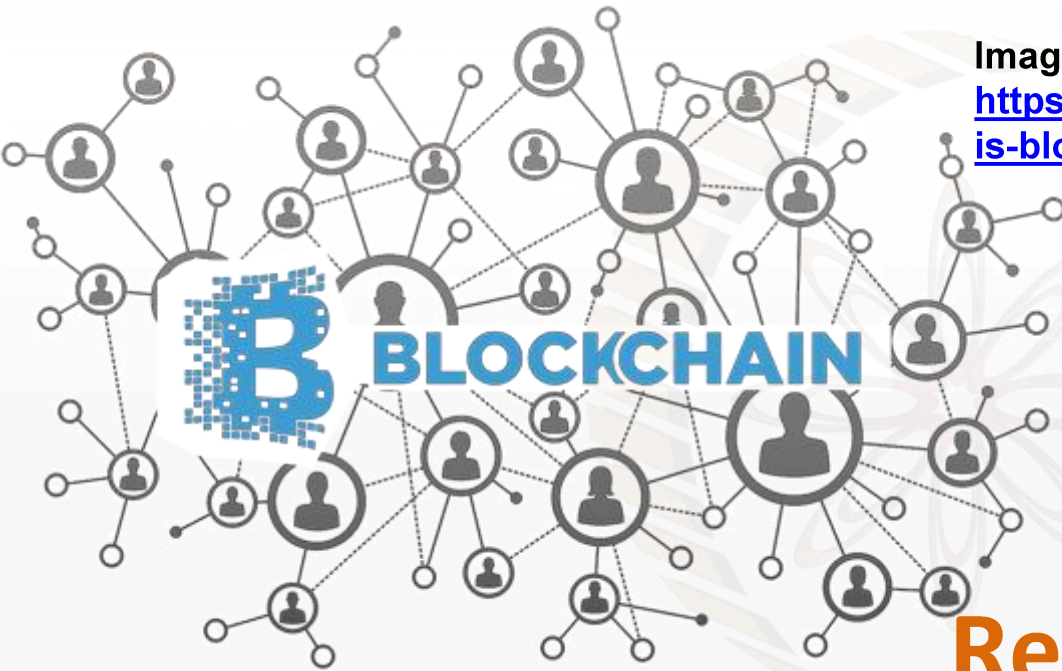


Image Source:

<https://steemit.com/blockchain/@tariq3njr/what-is-blockchain-technology>

Research Aspects - II

Bitcoin NG



IIT KHARAGPUR

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.



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



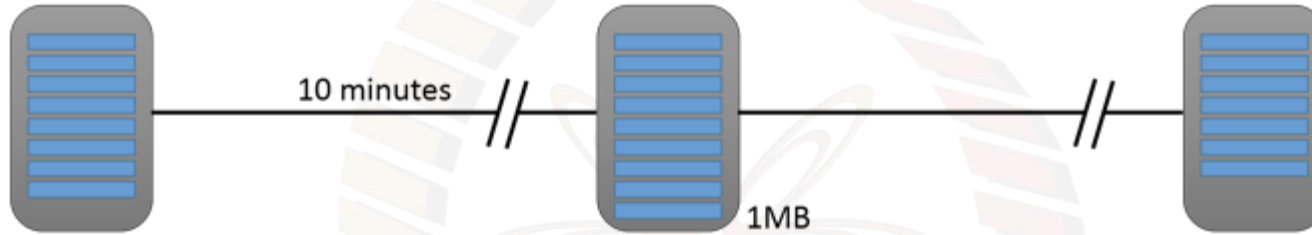
Bitcoin-NG: A Scalable PoW Protocol

- 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

Bitcoin



Bitcoin-NG



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



IIT KHARAGPUR

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



Bitcoin-NG: Key Blocks

- For a key block to be valid, the cryptographic hash of its header must be smaller than the target value.
- The key block also contains a public key (so the name, key block)
 - Used in subsequent microblocks



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 generated at a set rate smaller than a predefined maximum
 - The rate is much higher than the key block generation rate



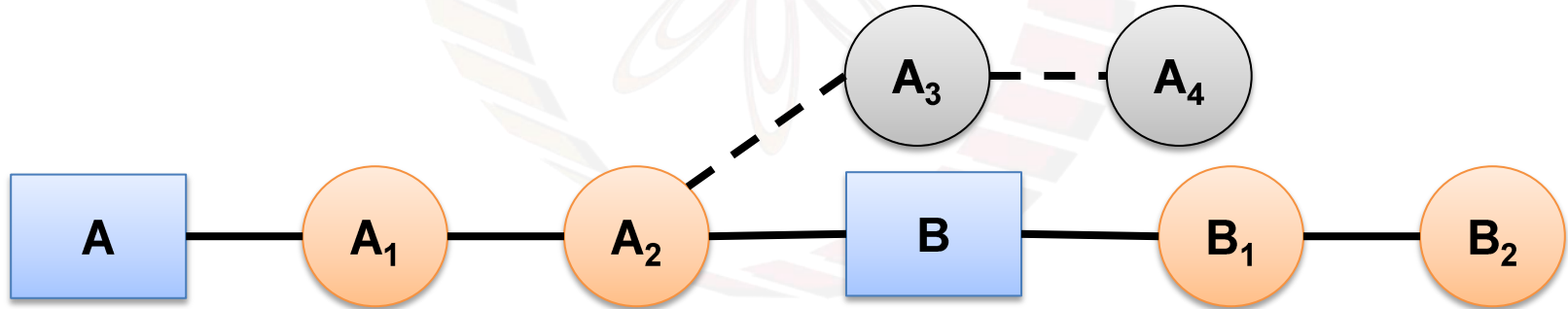
Bitcoin-NG: Microblocks

- 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
- The signature uses private key corresponding to the key block public key



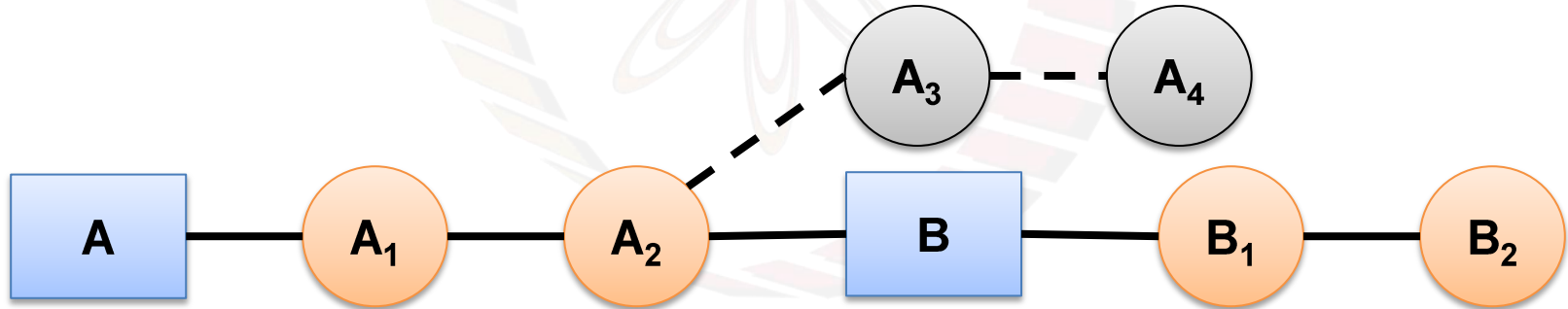
Bitcoin-NG: Confirmation Time

- 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

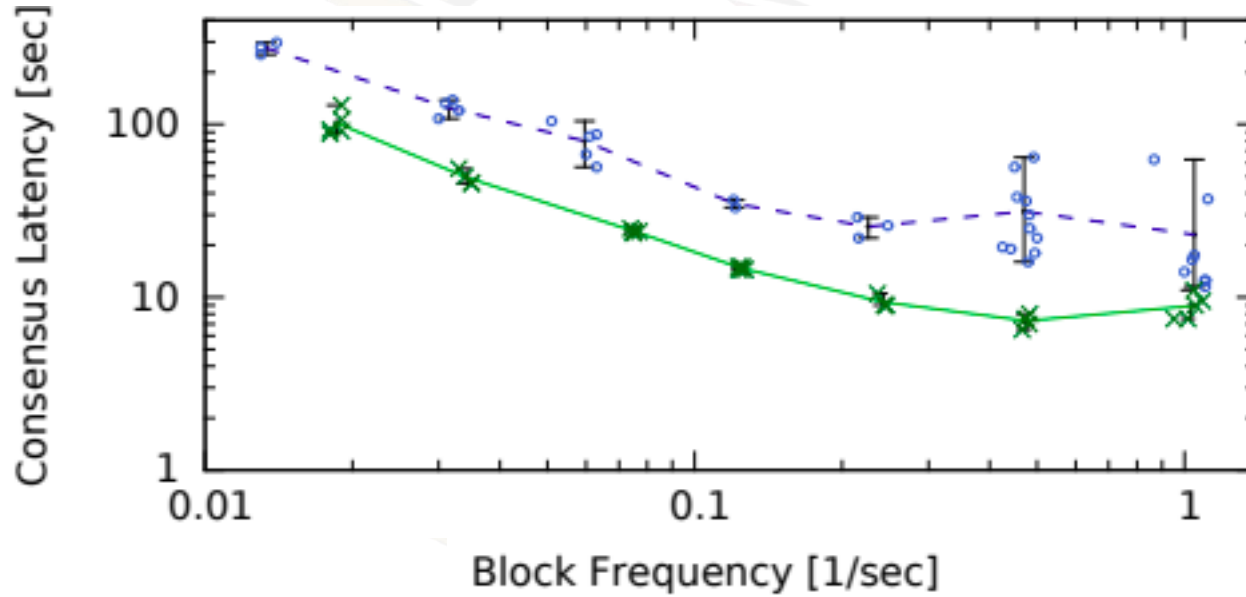


Bitcoin-NG: Confirmation Time

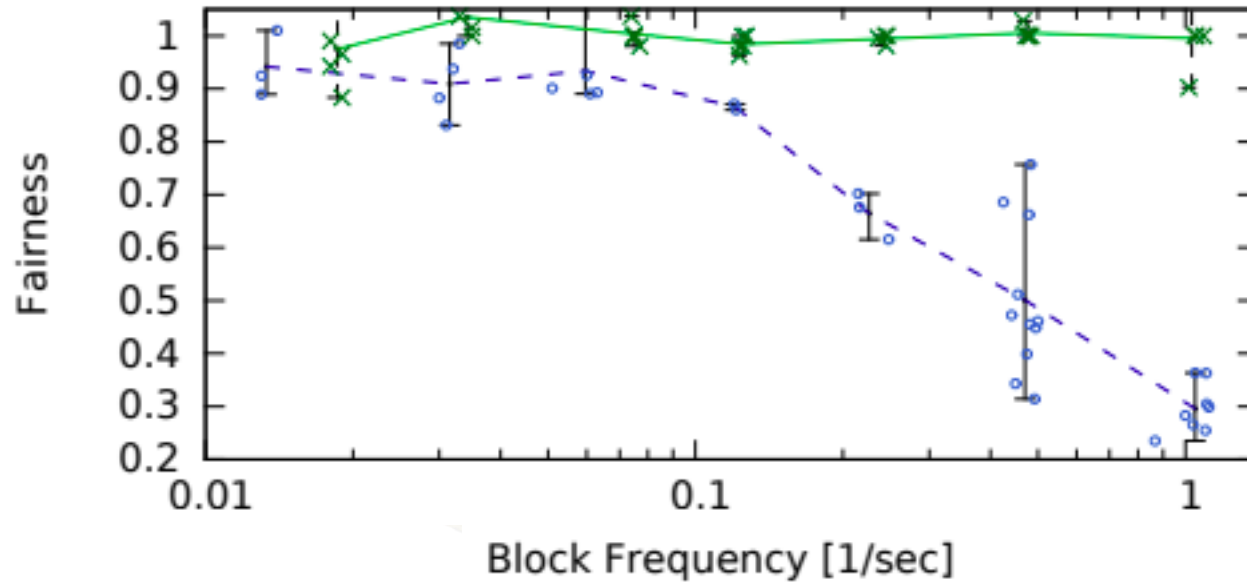
- A node may hear a forked microblock (A_3) but not the new key block (B)
 - This can be prevented by ensuring the reception of the key block
 - When a node sees a microblock, it waits for propagation time of the network, to make sure it is not pruned by a new key block



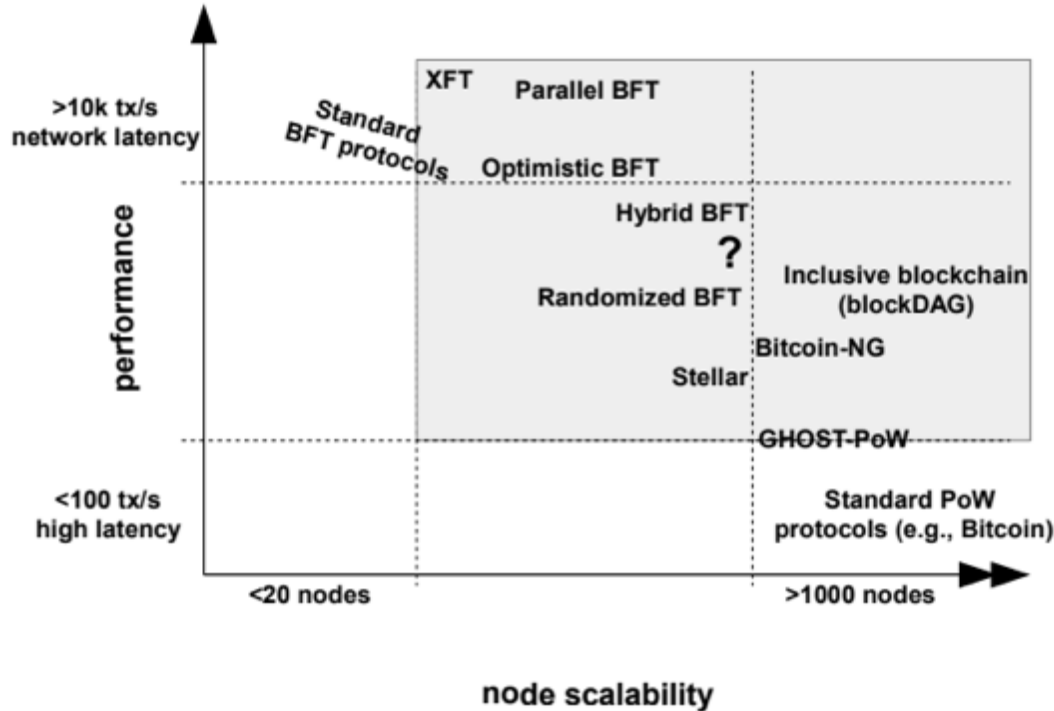
Bitcoin vs Bitcoin-NG



Bitcoin vs Bitcoin-NG



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.





thank you!

