NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Sandip Chakraborty

Department of Computer Science & Engineering
Indian Institute of Technology Kharagpur

Lecture 38: Consensus Scalability

CONCEPTS COVERED

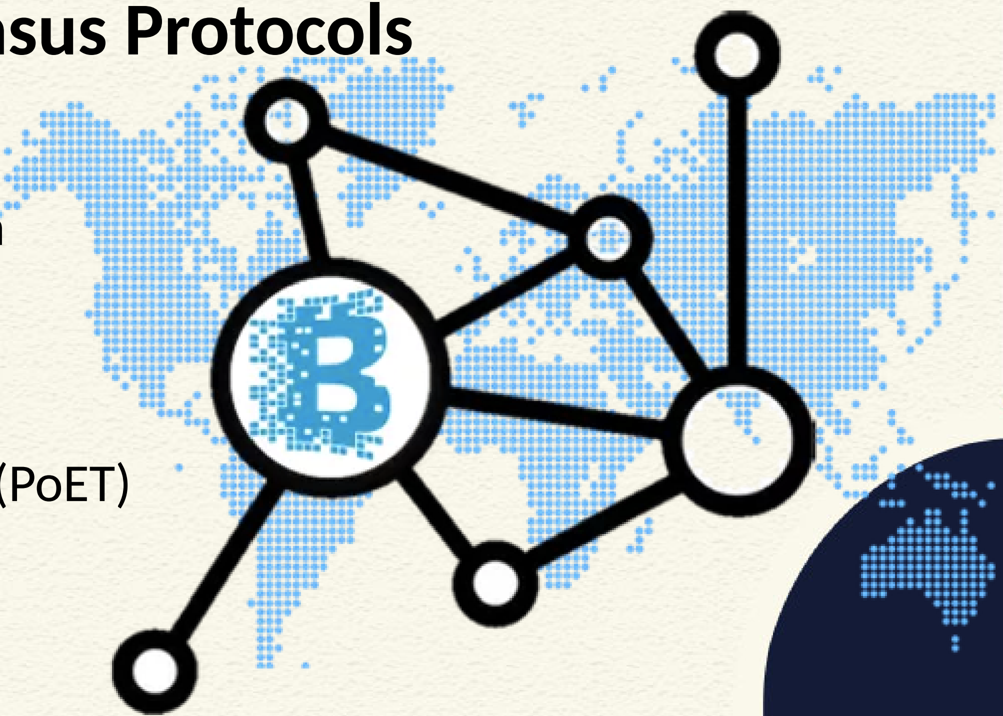
- **Blockchain Scalability**

KEYWORDS

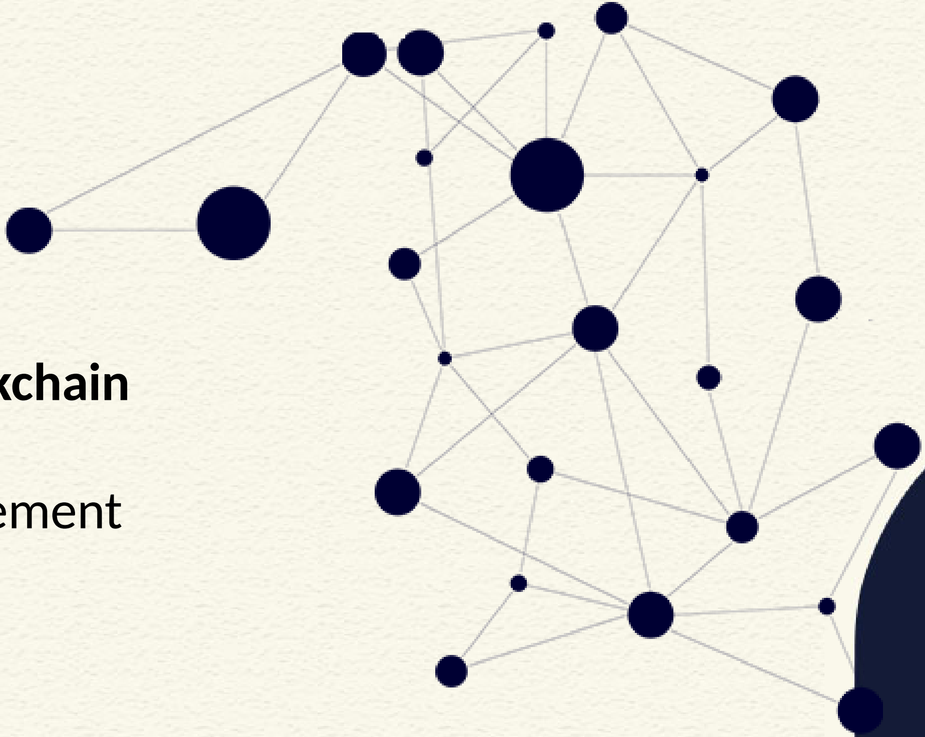
- PoW vs PBFT
- Scalability
- Consensus Finality

Blockchain Consensus Protocols

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



Blockchain Consensus Protocols



- **Permissioned Blockchain**
  - Byzantine Agreement
  - PBFT

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 of number of nodes
  - High transaction throughput

PoW Scalability

- Two magic numbers in PoW
  - **Block frequency** - 10 minutes
  - **Block size** - 1 MB / 8MB

- For Bitcoin:
  - Let's assume, block size = 1 MB.
  - Average transaction size = 380.04 bytes
  - Number of transactions per block = 1048576/380.04

    = 2,759.12

PoW Scalability

- Two magic numbers in PoW
  - **Block frequency** - 10 minutes
  - **Block size** - 1 MB / 8MB

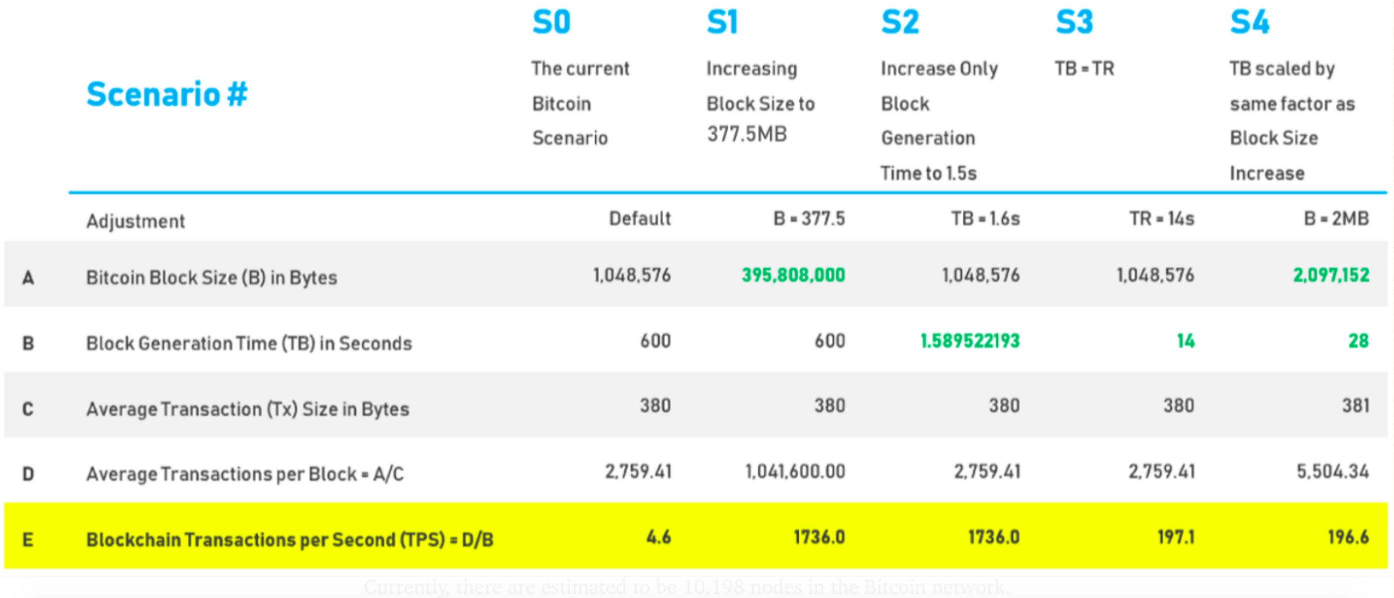
- For Bitcoin:
  - With 10 minutes (600 seconds) as block mining time,
    - 2759.12 transactions in 600 seconds
    - 4.6 transactions per second

PoW Scalability

- Two magic numbers in PoW
  - **Block frequency** - 10 minutes
  - **Block size** - 1 MB / 8MB

- Bitcoin Transaction throughput – 4.6 transactions per second
  - Visa supports around 1736 transactions per second

Tuning Bitcoin PoW Scalability

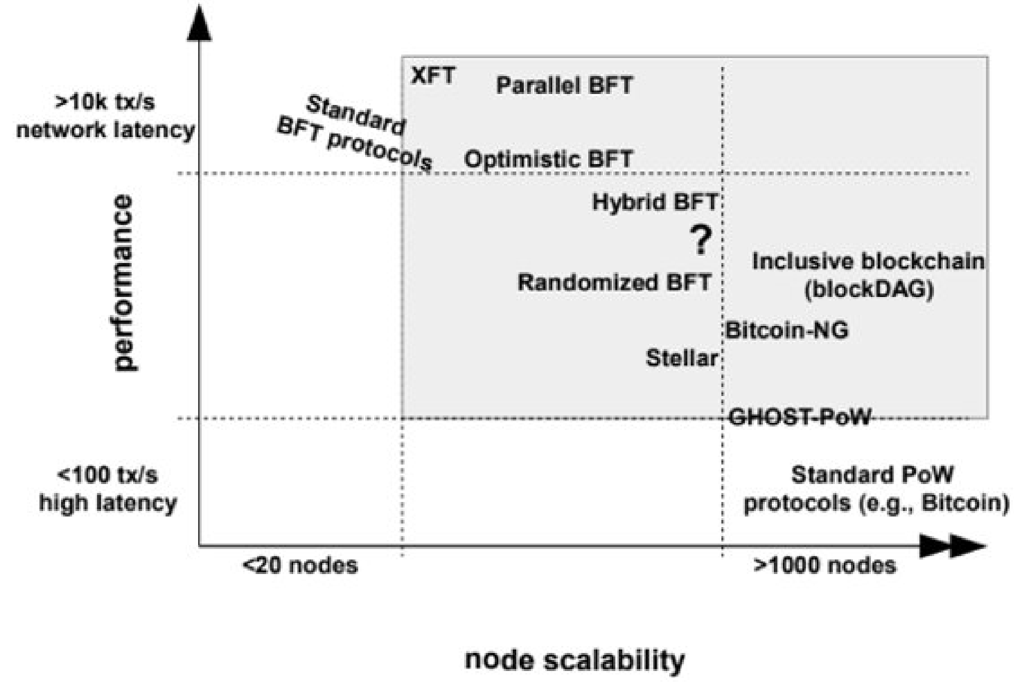


	Scenario #	S0 The current Bitcoin Scenario	S1 Increasing Block Size to 377.5MB	S2 Increase Only Block Generation Time to 1.5s	S3 TB = TR	S4 TB scaled by same factor as Block Size Increase
	Adjustment	Default	B = 377.5	TB = 1.6s	TR = 14s	B = 2MB
A	Bitcoin Block Size (B) in Bytes	1,048,576	395,808,000	1,048,576	1,048,576	2,097,152
B	Block Generation Time (TB) in Seconds	600	600	1.589522193	14	28
C	Average Transaction (Tx) Size in Bytes	380	380	380	380	381
D	Average Transactions per Block = A/C	2,759.41	1,041,600.00	2,759.41	2,759.41	5,504.34
E	**Blockchain Transactions per Second (TPS) = D/B**	**4.6**	**1736.0**	**1736.0**	**197.1**	**196.6**

Currently, there are estimated to be 10,198 nodes in the Bitcoin network.

https://towardsdatascience.com/the-blockchain-scalability-problem-the-race-for-visa-like-transaction-speed-5cce48f9d44

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.

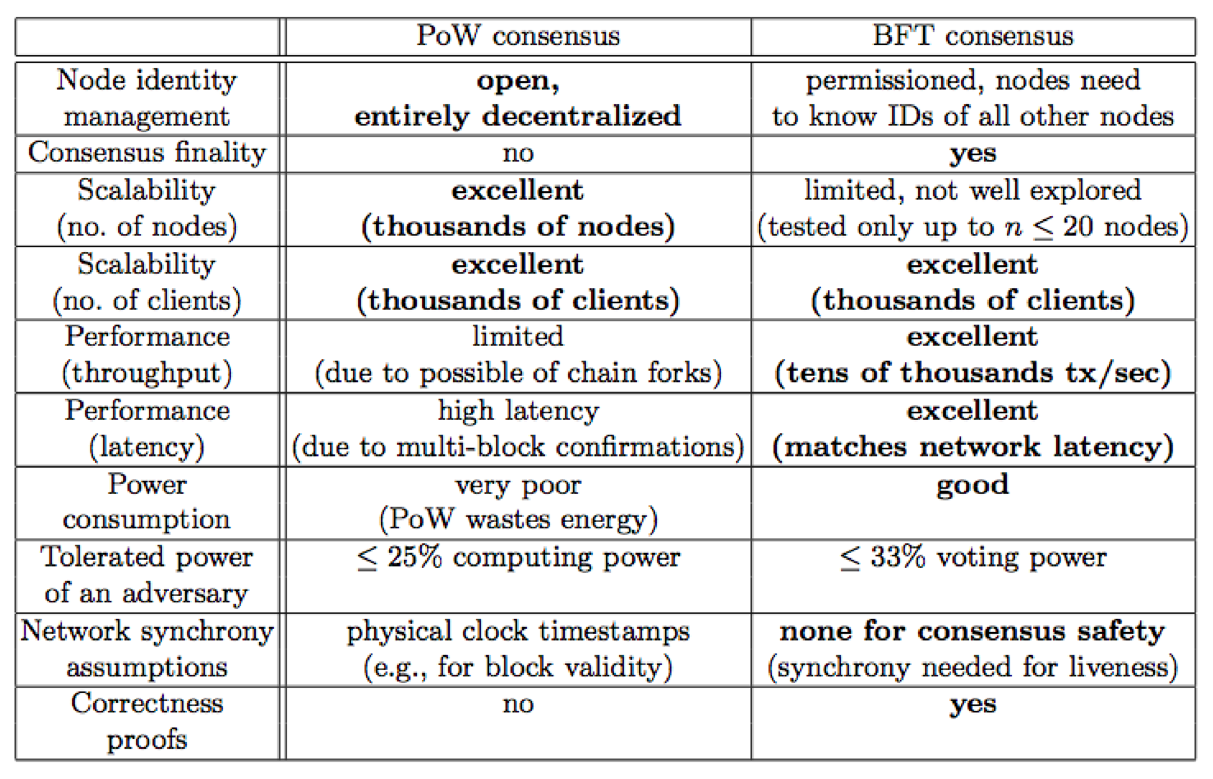
PoW vs PBFT – Consensus Finality

- *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)

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

- 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.**

Conclusion

- Scalability is a major issue in Blockchain consensus
- In the next lecture, we'll discuss different scalable blockchain protocols

Thank you