

# CONSENSUS AND THE CONSORTIA

## KNOW-HOWS

**ARUN S M**

Senior Software Engineer, Walmart  
Hyperledger TSC Member  
Co-Lead Hyperledger India Chapter

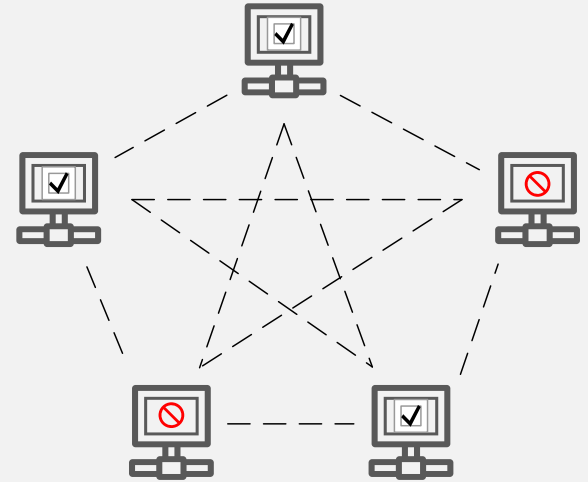


# AGENDA

- Learn and un-learn consensus
- Consensus in consortium
- Deciding on the consensus algorithm

# CONSENSUS ALGORITHMS

Consensus algorithms are a decision-making process to get an agreement on a single data point among distributed systems.



Fully Connected Network of 5 nodes

# GUARANTEED AVAILABILITY

## **Crash Fault Tolerance**

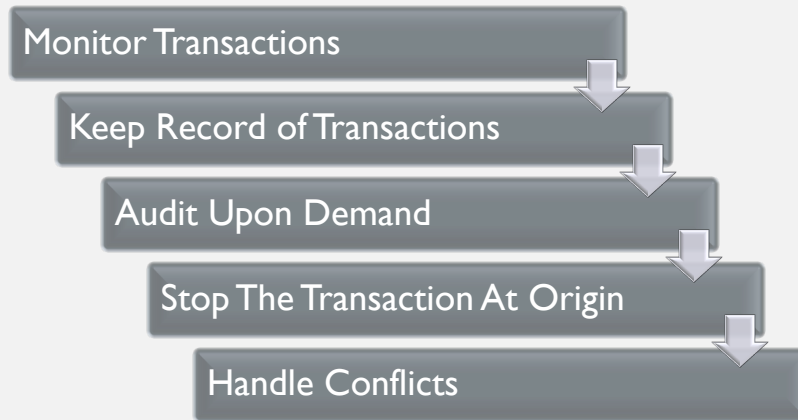
If a subset of nodes go down, the system is still working.

## **Byzantine Fault Tolerance**

If a subset of nodes behave wrong, the system still functions normally.

# WHAT IS BLOCKCHAIN?

**Distributed, Decentralized, Immutable Ledger Of Records**



# CONSENSUS IN BLOCKCHAIN

Define set of rules for

- Proposing a block with possible state transition
- Validating a block and agreeing upon it
- Commit a block



# NAKAMOTO STYLE CONSENSUS ALGORITHMS

## **Proof of Work**

- Proof based on the work done.

## **Proof of Stake**

- Proof with a stake for BFT behaviour.

## **Proof of Elapsed Time**

- Proof based on the random timer and waiting for the period of the timer value.

\* Other variants of Proof of XYZ algorithms are available.

## **What makes them unique?**

- Can scale to larger networks easily
- Susceptible to 51% attack, but such attacks are unrealistic in larger networks

## **Common Challenges**

- Slow commit rate because of forks, solution to address them
  - Example: Agree for all the blocks prior to 50 blocks
  - Get signature from subgroup of nodes, chosen randomly
- What if a node signs two blocks

# FAST-FINALITY CONSENSUS ALGORITHMS

## Practical Byzantine Fault Tolerance (PBFT)

- Proposal and voting for both leader election and the content commit operation.
- Breaks if minimum 2/3rd are non-Byzantine.

## Raft

- One node is leader and other nodes follow the instructions.

\* Other options are available to consume for advanced use cases.

## What makes them unique?

- Faster, when consensus is expected in short interval

## Common Challenges

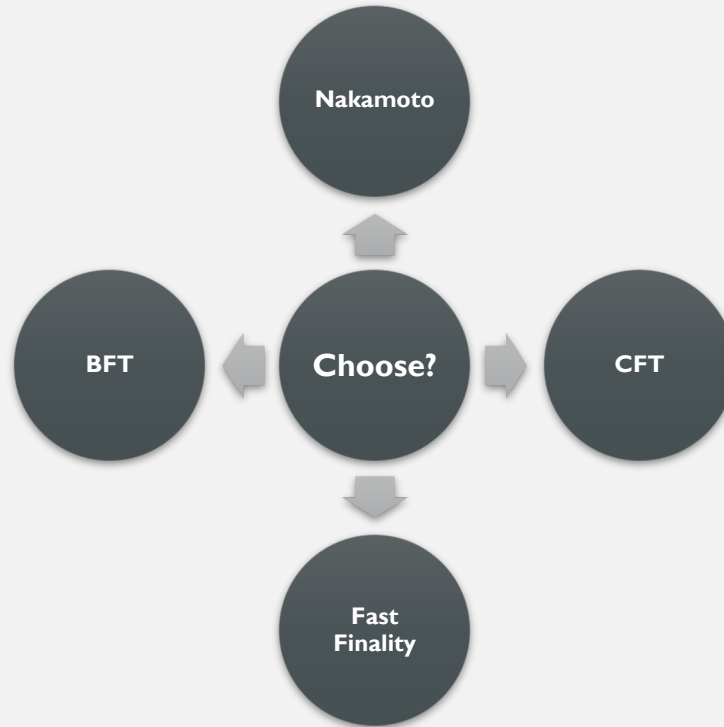
- Requires a fully connected network of nodes
- Cannot be used in larger networks
- Number of messages exchanged between the nodes increase as the size grows



# CONSORTIUM

An association of two or more organizations with the objective of participating in a common activity or pooling their resources for achieving a common goal.

# DECISION MATRIX



## AGREEMENT IN HYPERLEDGER FABRIC

### Step 1

- Client receives the transactions
- Client asks the network to endorse the transaction

### Step 2

- Client sends the endorsements to the ordering service cluster
- Ordering service cluster runs the consensus to order the transactions

### Step 3

- Ordered transaction block is sent for commitment

## CONSENSUS AVAILABLE IN HYPERLEDGER PROJECTS

PoET, RAFT, PBFT, RBFT, Mir-BFT ..

Pluggable & Bring Your Own Consensus

## QUESTIONS TO ANSWER

- Privacy of the data
- Size of the network
- Degree of decentralization
- Performance & throughput

The background is a vibrant collage of overlapping squares in various colors including orange, light blue, yellow, green, red, and purple. Each square features a large, bold, black question mark. A dark grey horizontal bar with a thin white border is centered across the image, containing the title text in white.

# DECIDING ON THE CONSENSUS ALGORITHM

**QUESTIONS?**