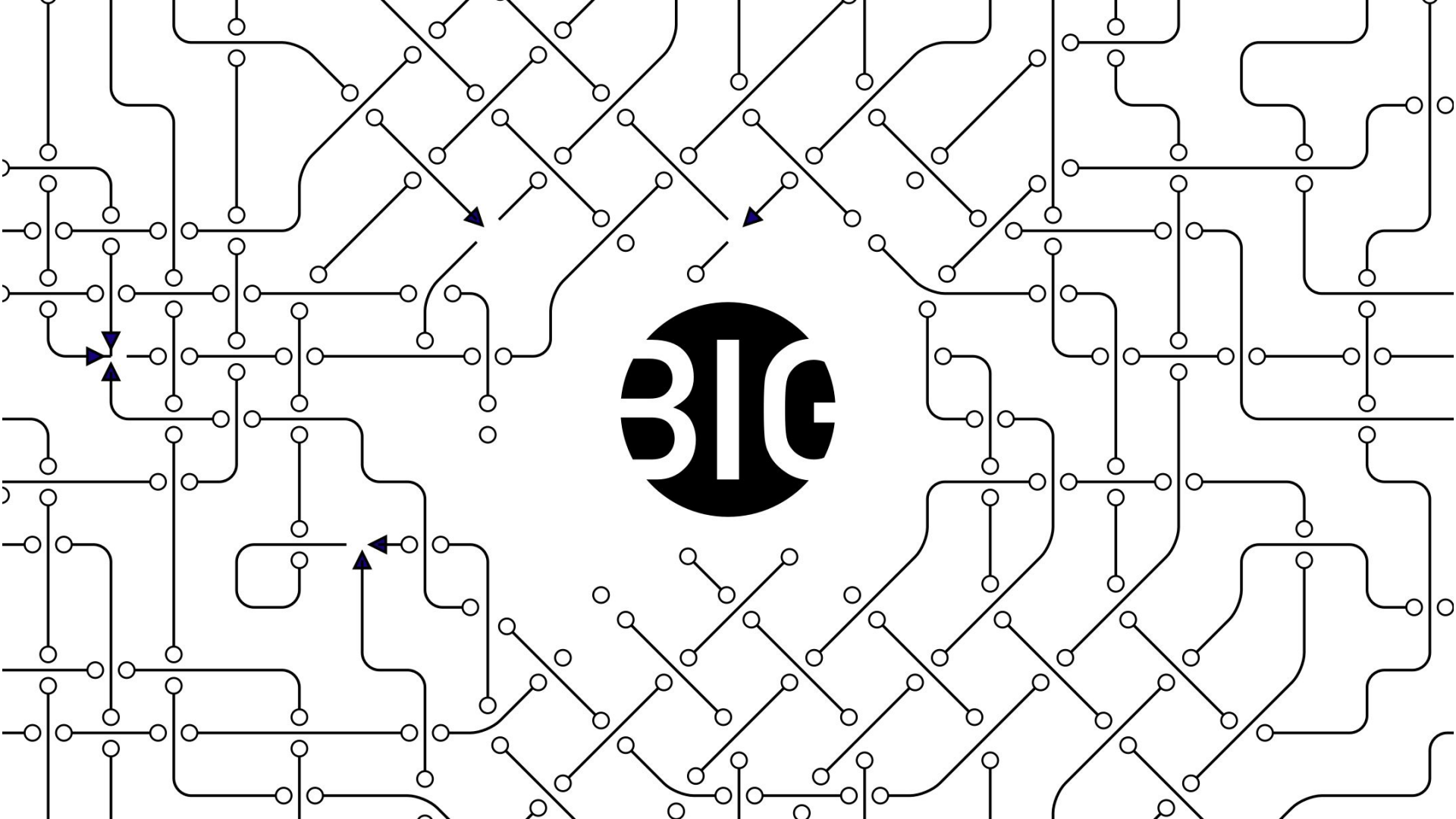
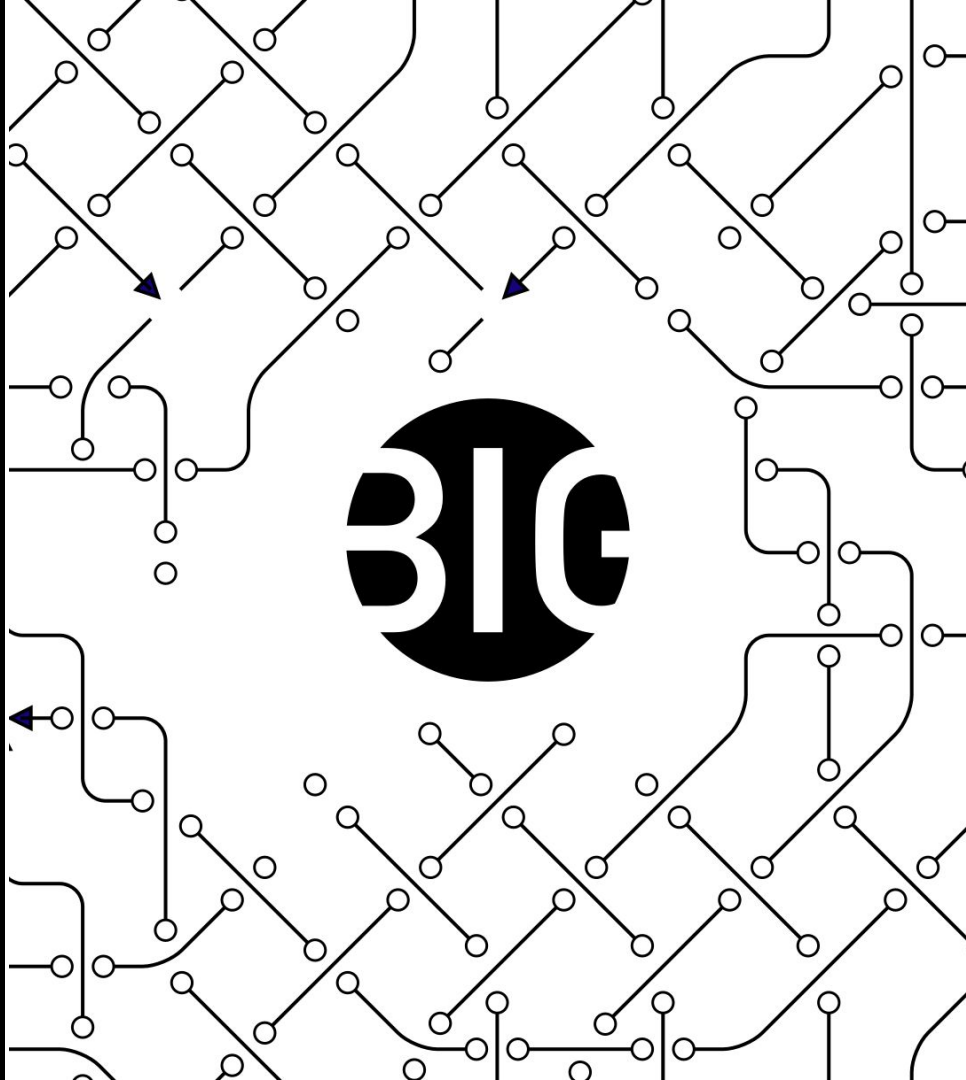

BIG

18th

Monthly Meetup

Thursday, August 24 | UST Global, Trivandrum



Show of Hands

Should I skip the intro?

History of Bitcoin

- 2009
- Satoshi Nakamoto
- Bitcoin
- Cryptocurrency
- Blockchain

Blockchain: Definition

A datastore that is:

- **Tamper-proof**
- **Decentralized**
- **Uncensorable**
- **Slow**

Who?

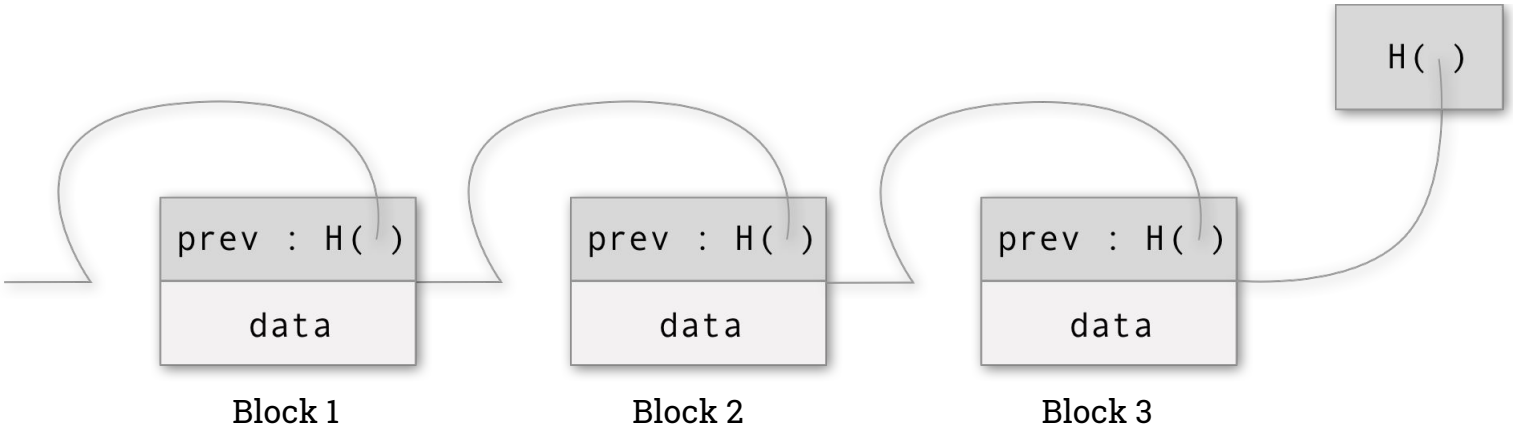
- **Rakesh BS**
- Co-founder of **Qucentis** & **BIGOrg**
- Currently building a Blockchain based product

Immutability

- Blockchain data structure
- Consensus protocol

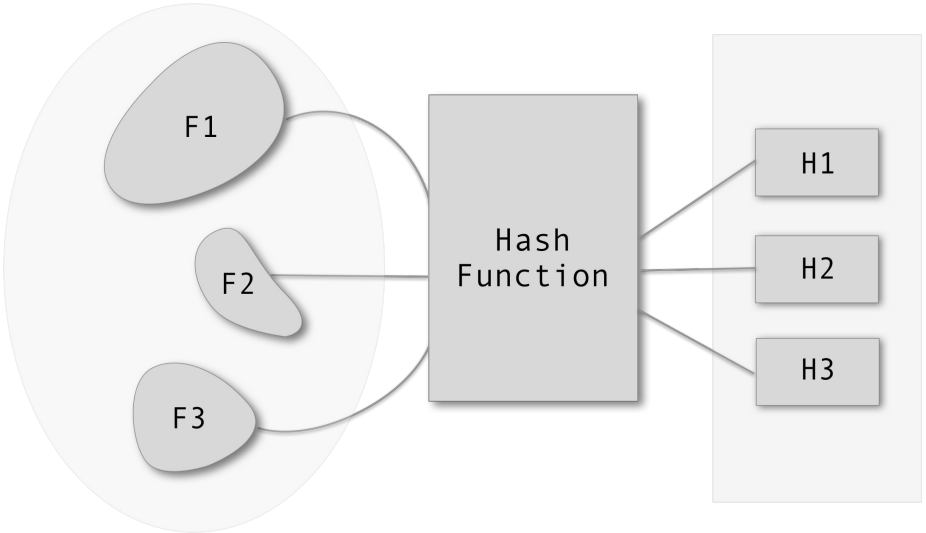
Blockchain

- **Linked list of hash pointers**
- **Tamper-proof**



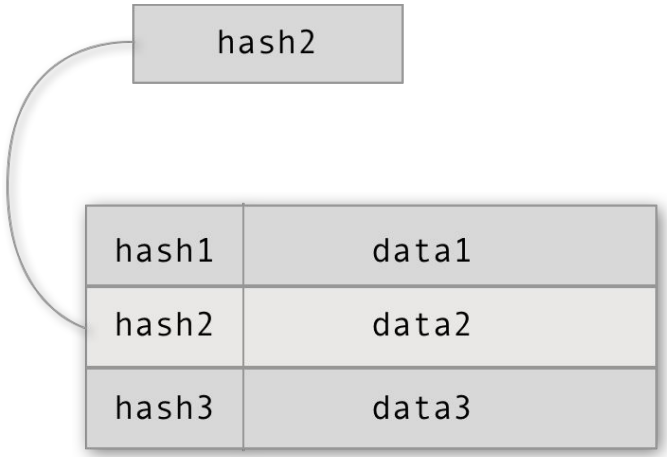
Cryptographic Hash Functions

- **Collision resistant**
- **Non-reversible**
- **Efficient**
- **Variable** length input
- **Fixed** length output



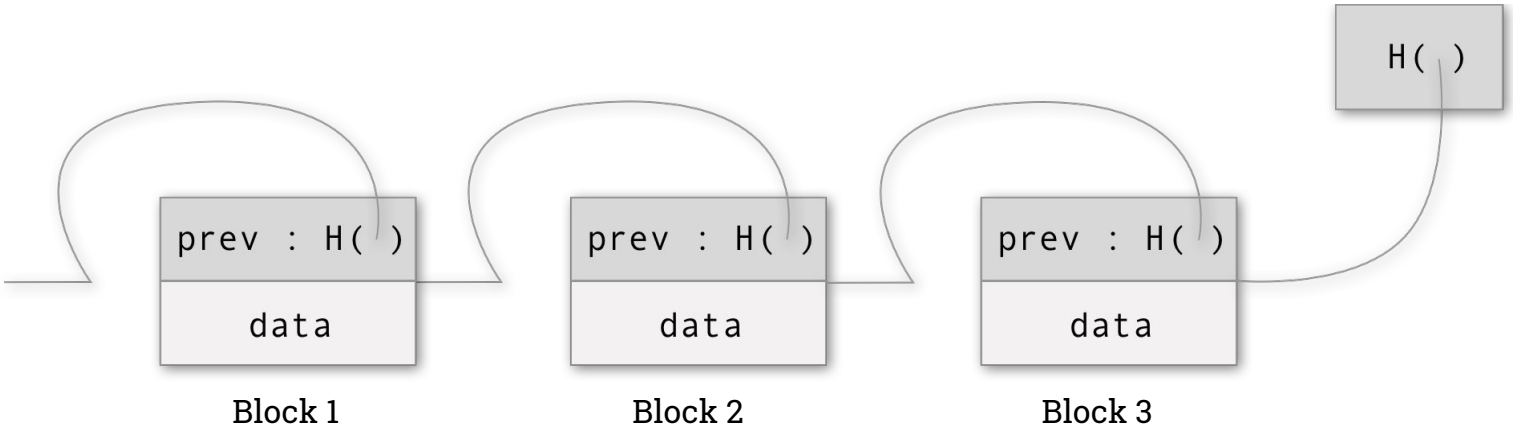
Hash Pointers

- Hash used as **reference** to data
- Ensures data is **tamper-proof**



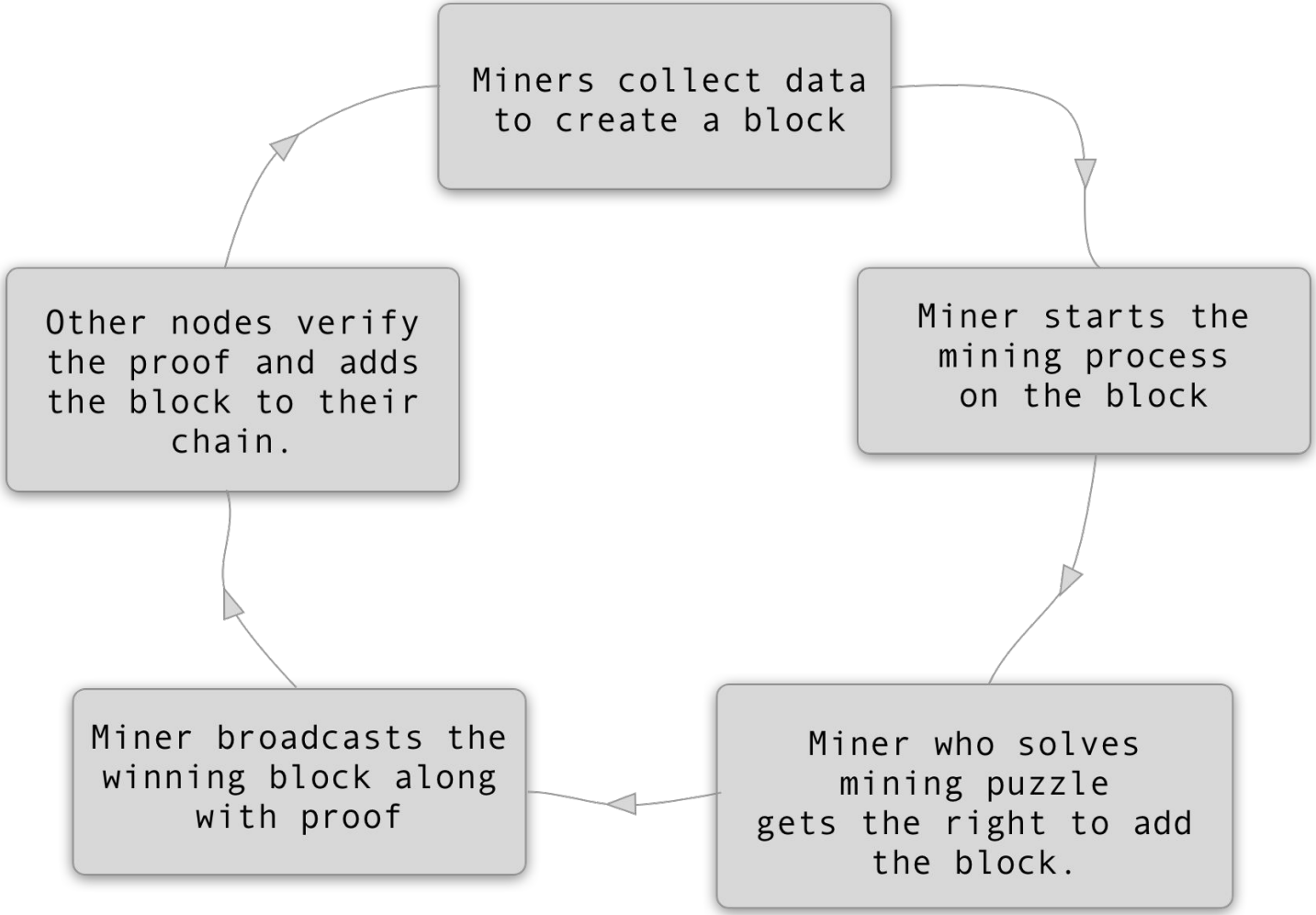
Blockchain

- **Linked list of hash pointers**
- **Tamper-proof**



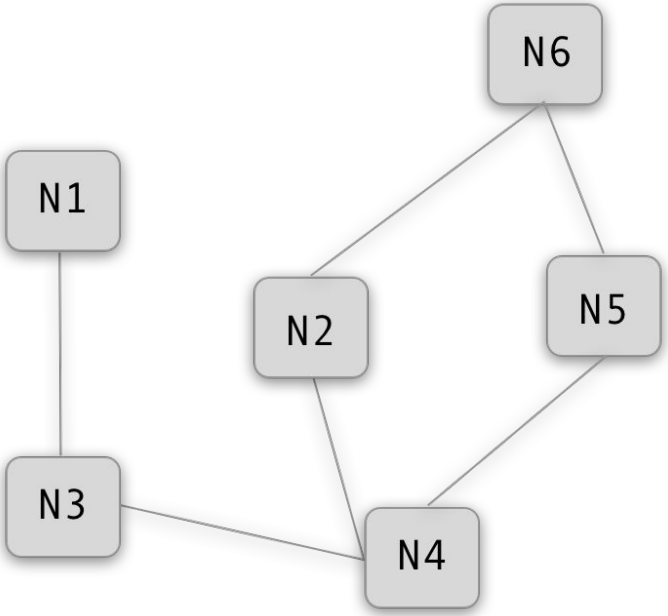
Consensus Protocol (Bitcoin)

- **Mining** - Process of adding new blocks
- Every node solves a **puzzle** and submits **Proof-of-Work**
- **Winner** gets the right to add a new block
- **Winner** gets the **block reward**

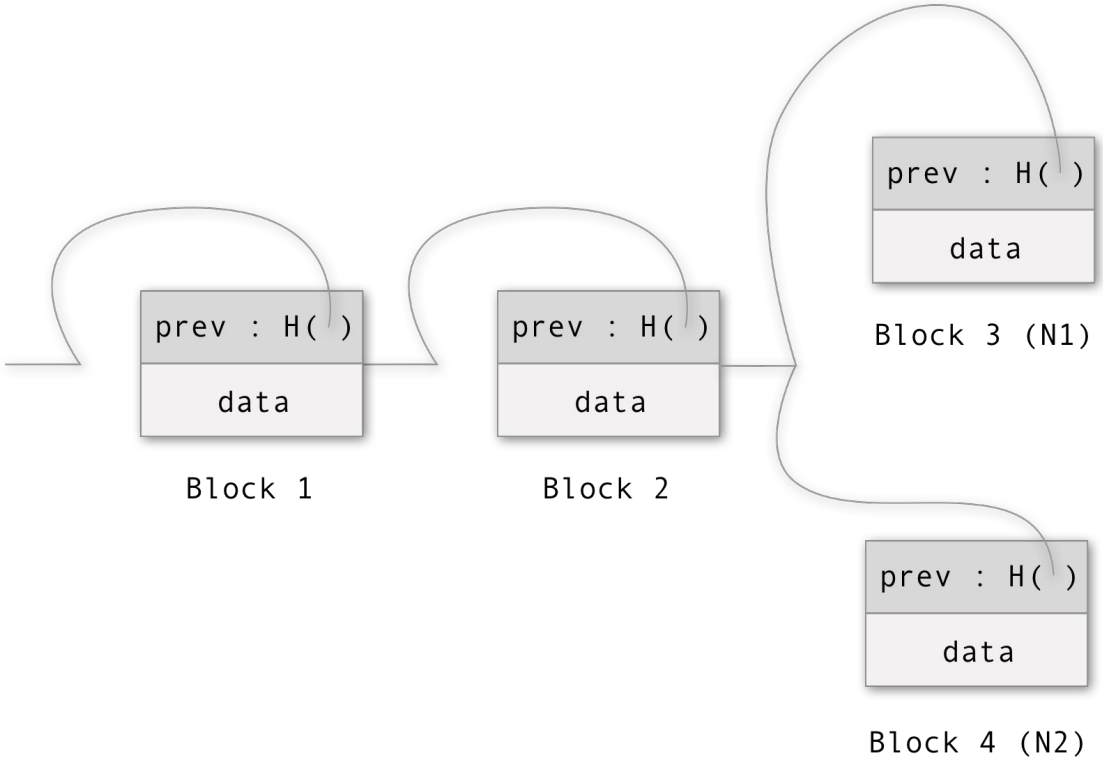

Miners collect data to create a block
Miner starts the mining process on the block
Miner who solves mining puzzle gets the right to add the block.
Miner broadcasts the winning block along with proof
Other nodes verify the proof and adds the block to their chain.

A Fork in the Chain

- Two nodes can produce blocks around the **same time**
- For a few block intervals, there might be **two** versions of the blockchain
- **Mining** is a **random process**
- All nodes follow the **longest chain** — the chain with the **largest amount of work** done
- Wait **7** blocks for **confirmation**

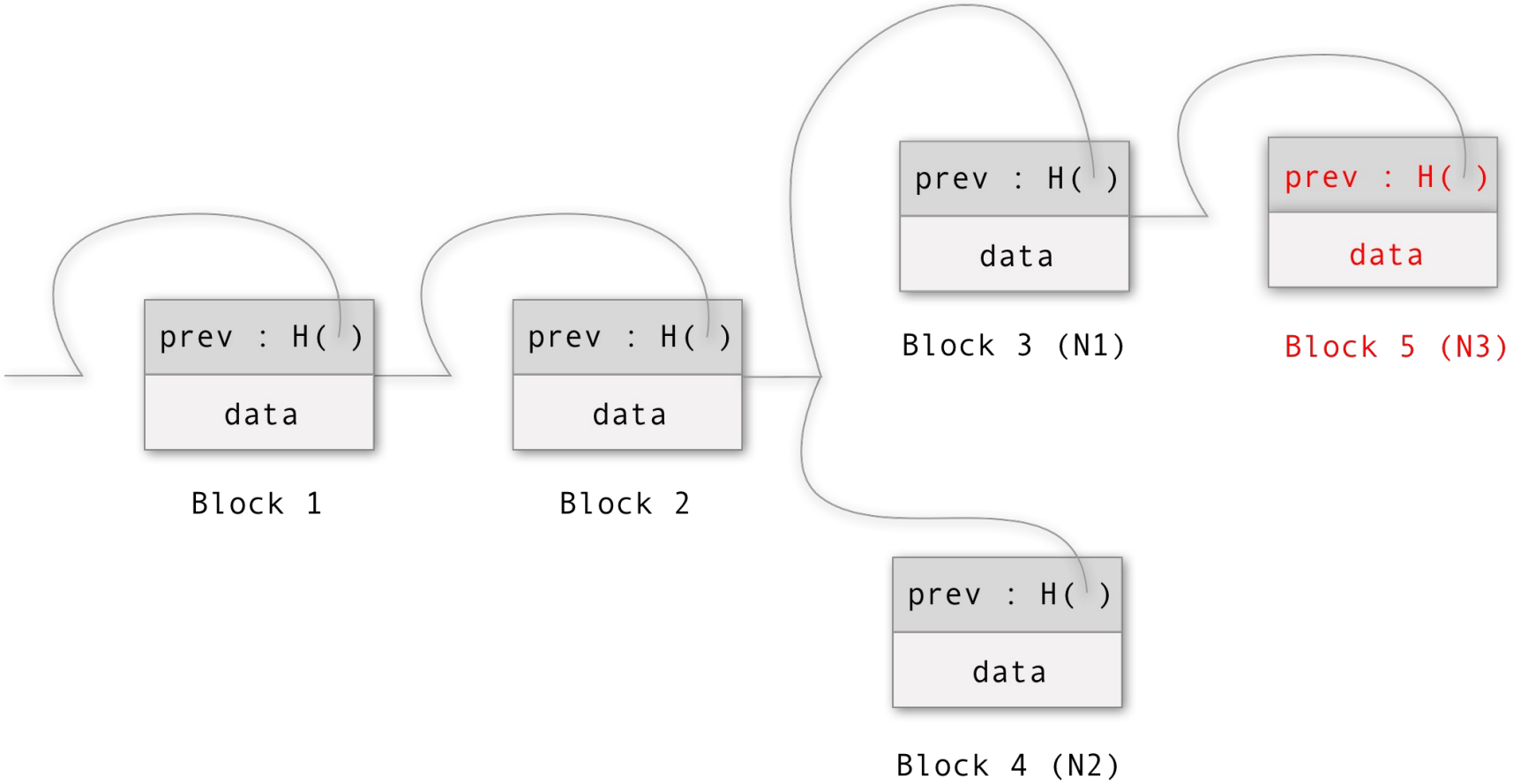


A Sample Network



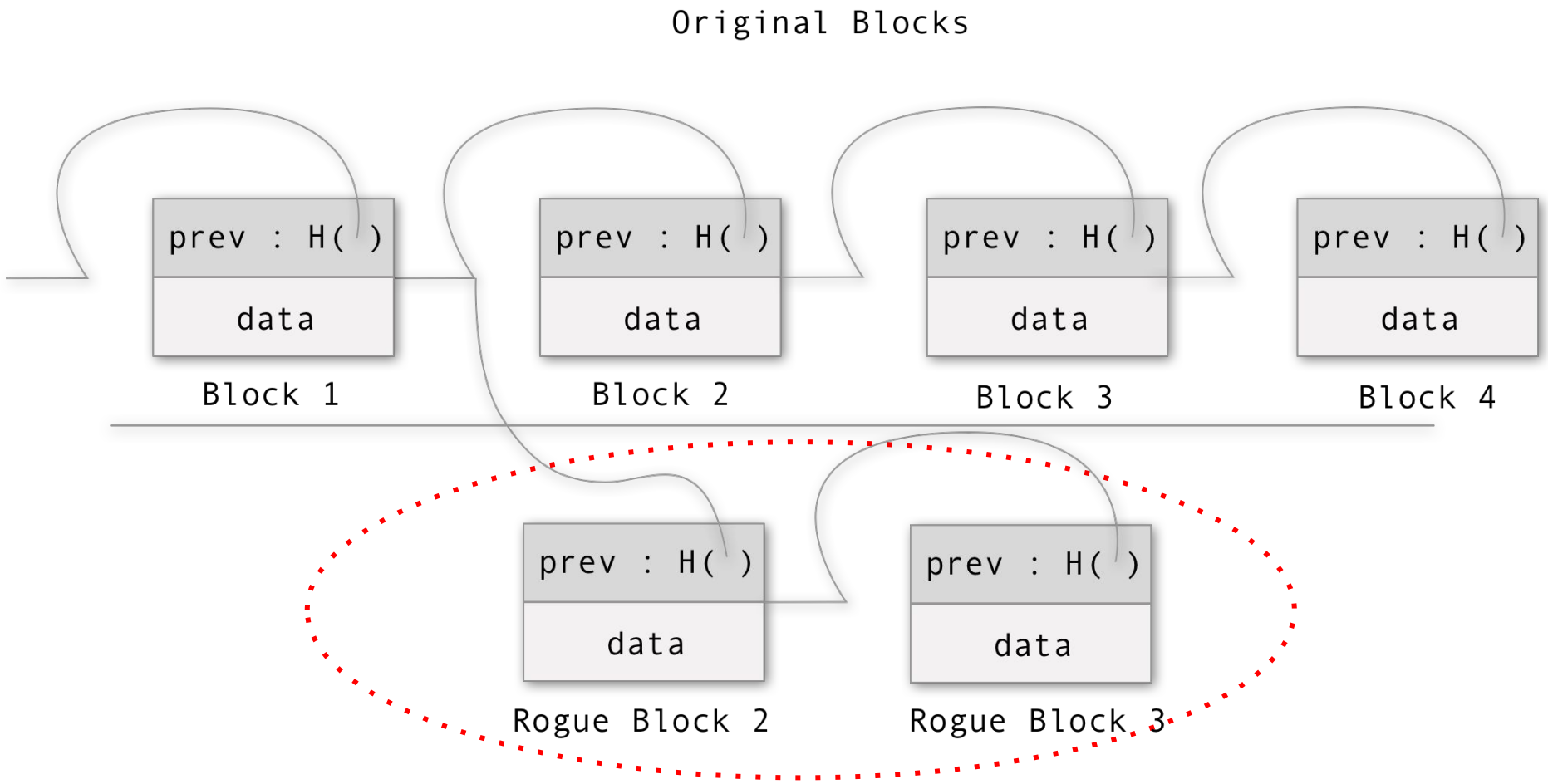
Fork in the Chain

Resolution of the Fork



An Attack Scenario

- A rogue node tries to replace a block
- All nodes follow the **longest chain**
- The **collective computing power** of the network will always be much higher than a single rogue node
- Hence have to redo all work done after the block


Original Blocks
prev : H( )
data
Block 1
prev : H( )
data
Block 2
prev : H( )
data
Block 3
prev : H( )
data
Block 4
prev : H( )
data
Rogue Block 2
prev : H( )
data
Rogue Block 3

Who?

- **Nikhil Mohan**
- Co-founder, Lightrains

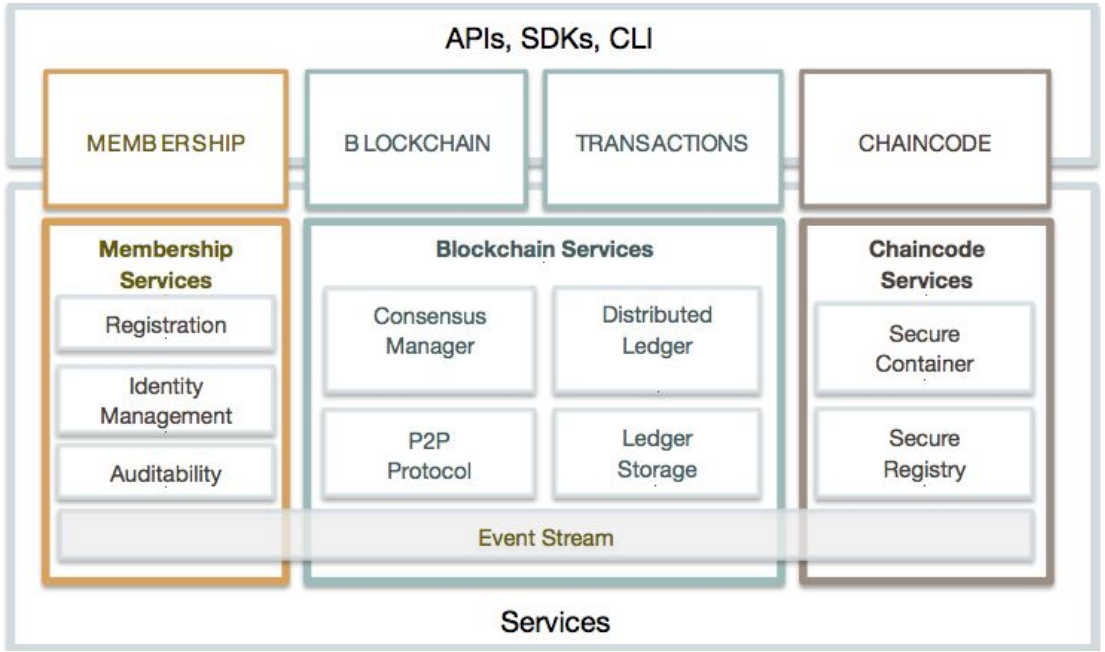
Hyperledger: A First Look

- Open source collaborative hosted by The Linux Foundation including leaders in:
  - Finance
  - Banking
  - Internet of Things
  - Supply chains
  - Manufacturing
  - Technology

3 Big Points

- Trust
- Data privacy
- Auditability

Architecture



Ethereum v/s Hyperledger

Characteristic	Ethereum	Hyperledger Fabric
Mode of operation	Permissionless, public or private	Permissioned, private
Consensus	• Mining based on proof-of-work (PoW) • Ledger level	• Broad understanding of consensus that allows multiple approaches • Transaction level
Smart contracts	Smart contract code (e.g., Solidity)	Smart contract code(e.g., Go, Java), known as chaincode
Currency	• Ether • Tokens via smart contract	• None • Currency and tokens via chaincode

A Use Case

Problem

- You own a **logistics** company
- You and I **are on a blockchain** with different entities markets, shippers etc.
- We make a deal at a **lower price** than the market norm
- **Everybody** sees

A Use Case

Solution: Hyperledger Fabric

- First send **transaction to peer**
- Peers generate a result - for transaction agreement **both peers** need to **generate the same** result
- Then send to **consensus crowd** for ordering
- The order crowd sends **transaction back to peers** and added to ledger
- The parties don’t need to know about our special price.

Blockchain Interest Group

Thank you for your attention