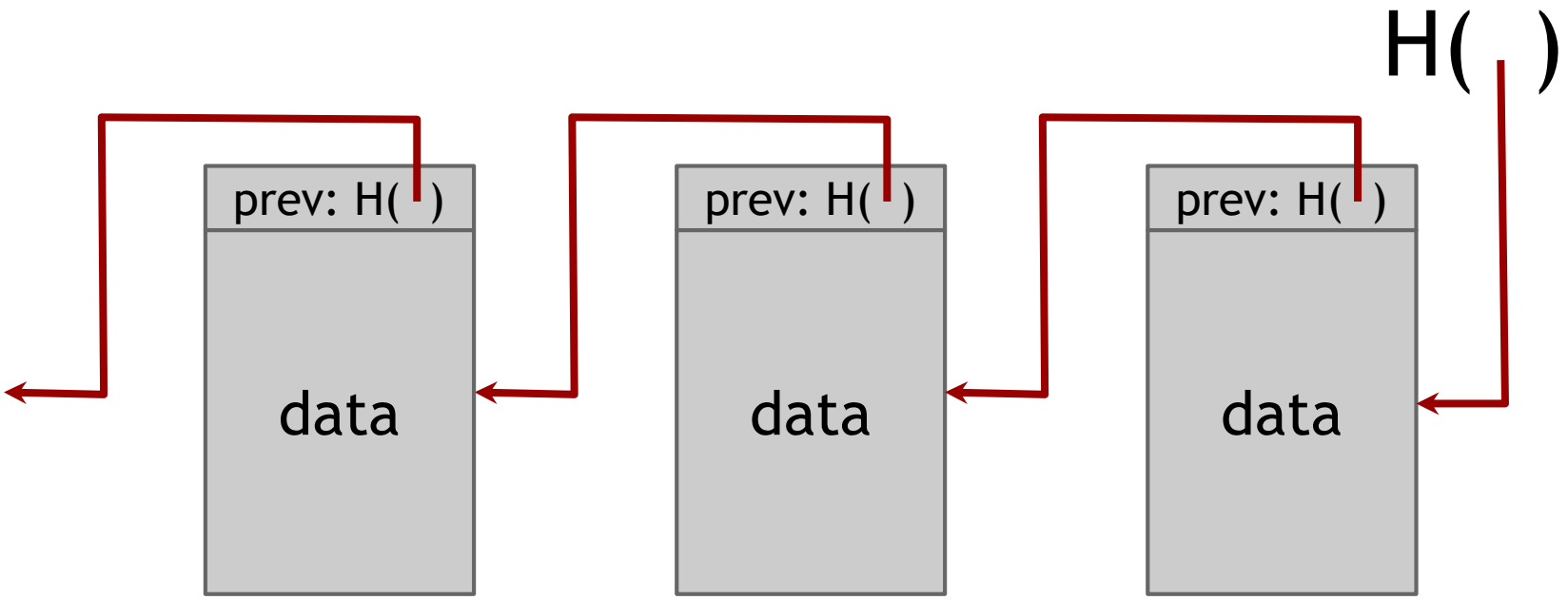
Intro to Blockchain and Cryptocurrencies

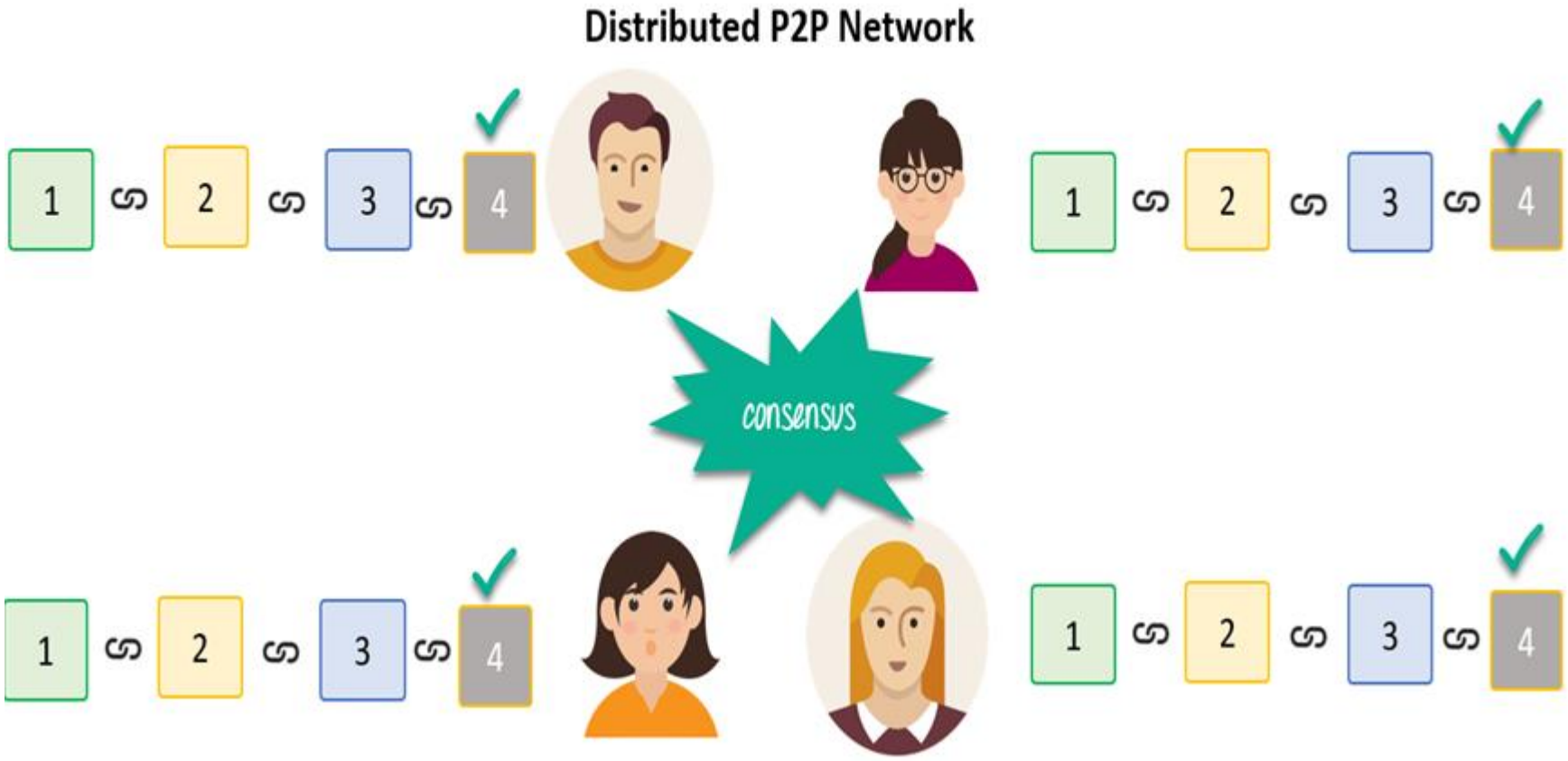
Slides by Arvind Narayanan et al.

linked list with hash pointers = “block chain”



use case: tamper-evident log

How to achieve consistency?



An Example of Public Ledger from Banking Sectors

Public Ledger of Alice

Alice: ₹100

Alice
₹ 100

Bob

Alice: ₹100

Public Ledger of Bob

Public Ledger of Eve

Alice: ₹100

Eve

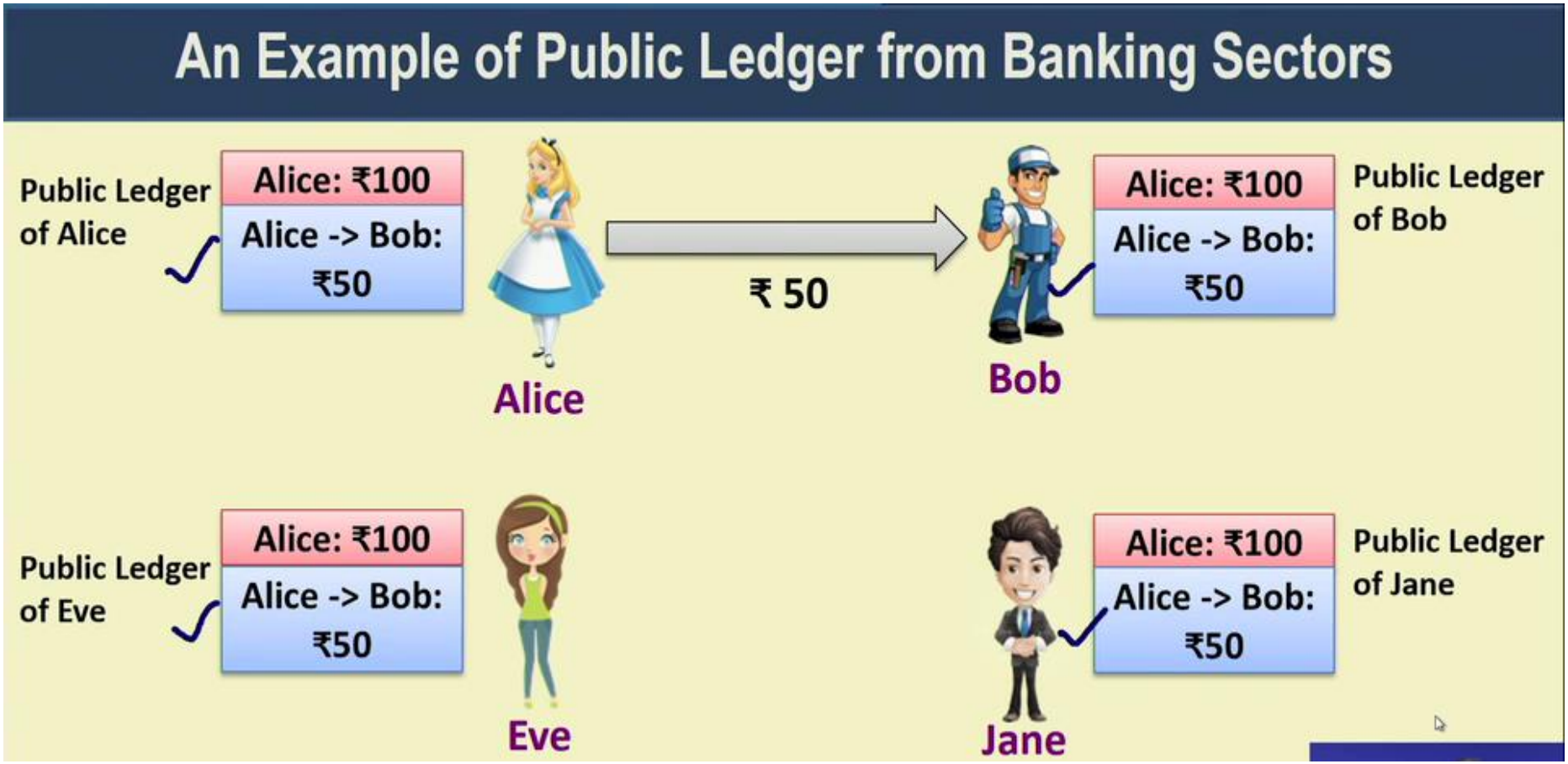
Jane

Alice: ₹100

Public Ledger of Jane

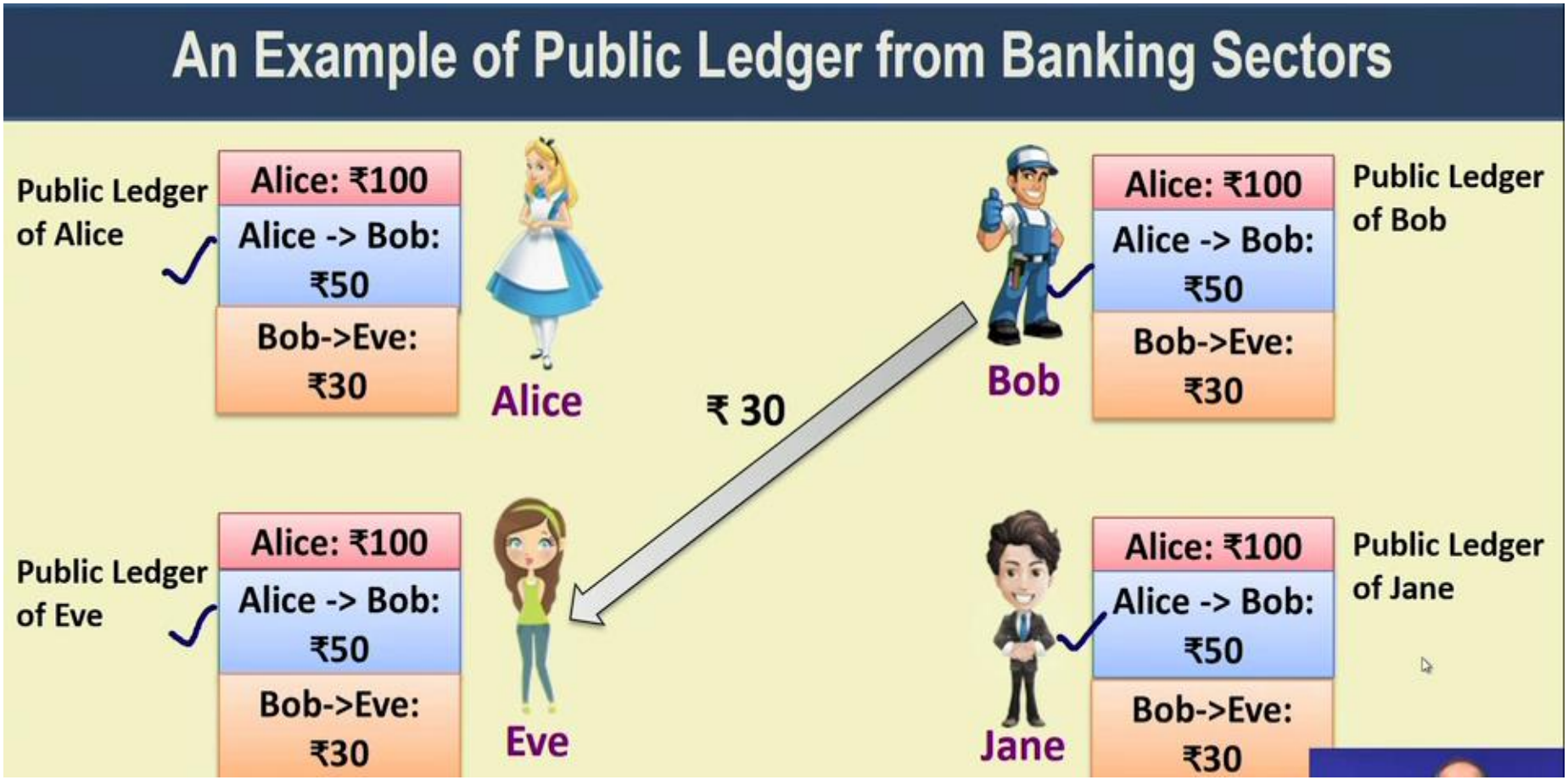
Courtesy: Lectures by Dr. Sandip Chakraborty

An Example of Public Ledger from Banking Sectors



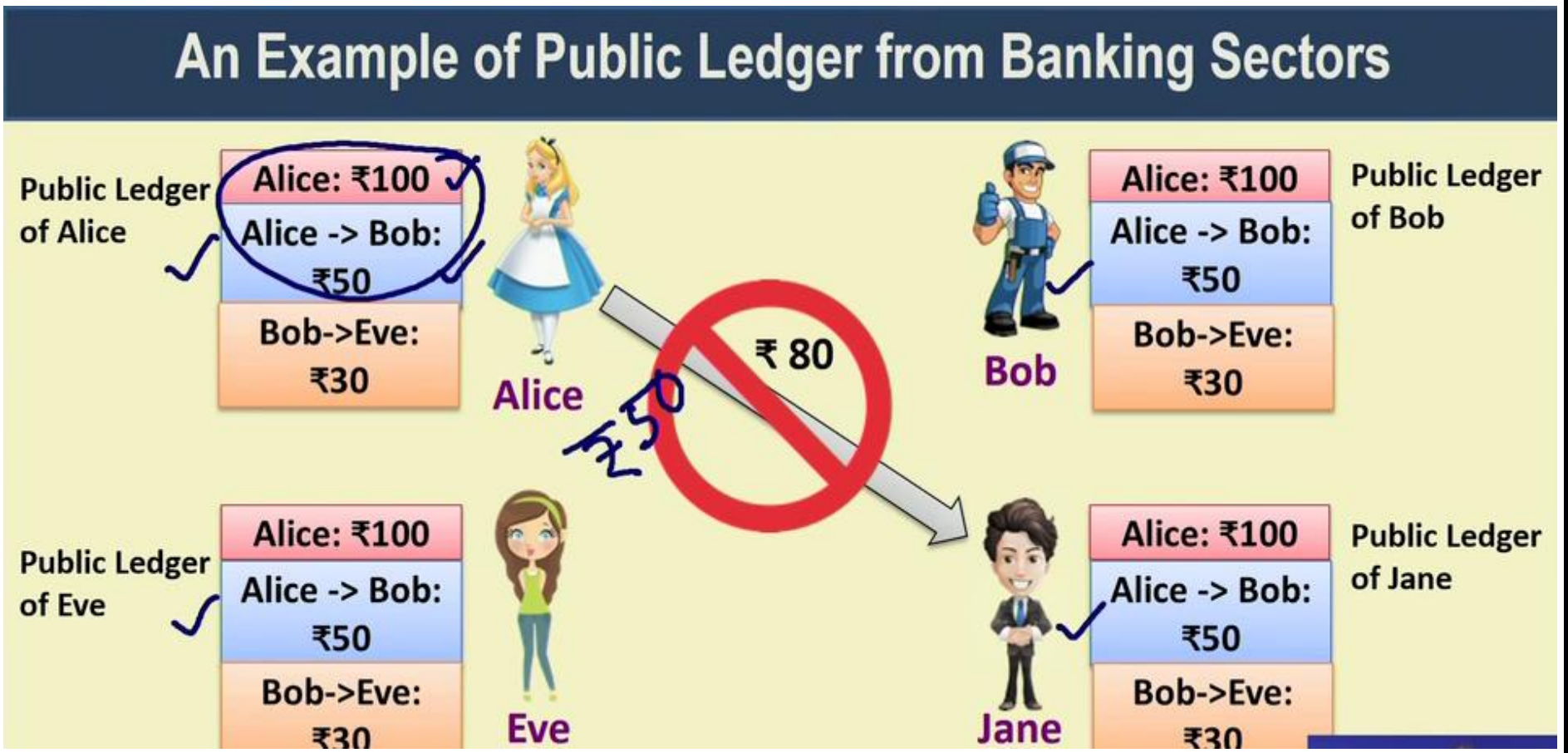
Courtesy: Lectures by Dr. Sandip Chakraborty

An Example of Public Ledger from Banking Sectors



Courtesy: Lectures by Dr. Sandip Chakraborty

An Example of Public Ledger from Banking Sectors



Courtesy: Lectures by Dr. Sandip Chakraborty

The path to decentralization

- technology & incentive design

All Participants

Who maintains the ledger of transactions? (and how?)

Consensus

All Participants

Who determines the validity of transactions to be included in the ledger?

Bitcoin Script

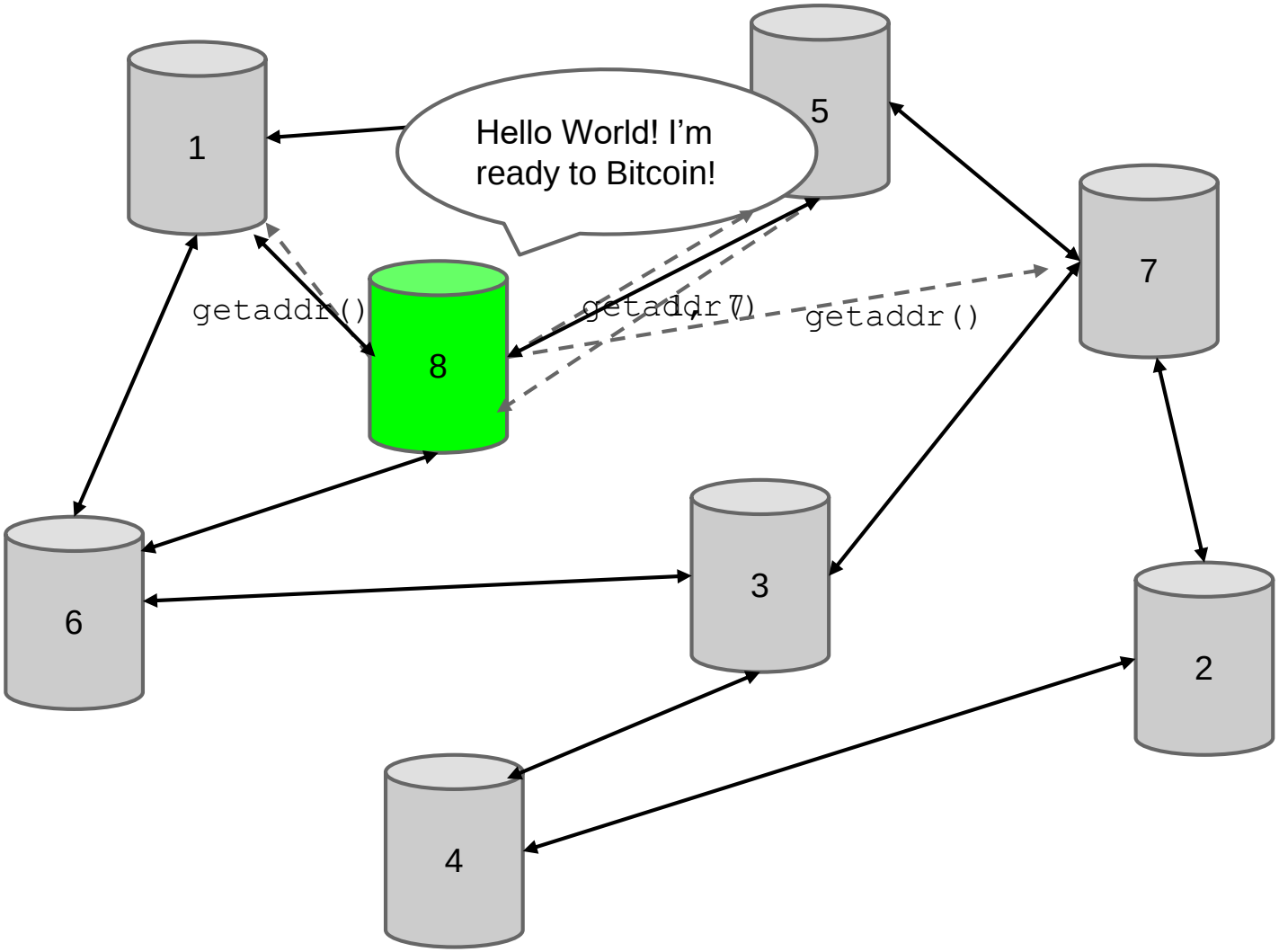
Who creates new Bitcoins?

Reward for Mining

Bitcoin P2P network

- Ad-hoc protocol (runs on TCP port 8333)
- Ad-hoc network with random topology
- All nodes are equal
- New nodes can join at any time
  - Network Changes over time - dynamic
- No explict way to leave network
  - Forget non-responding nodes after 3 hr

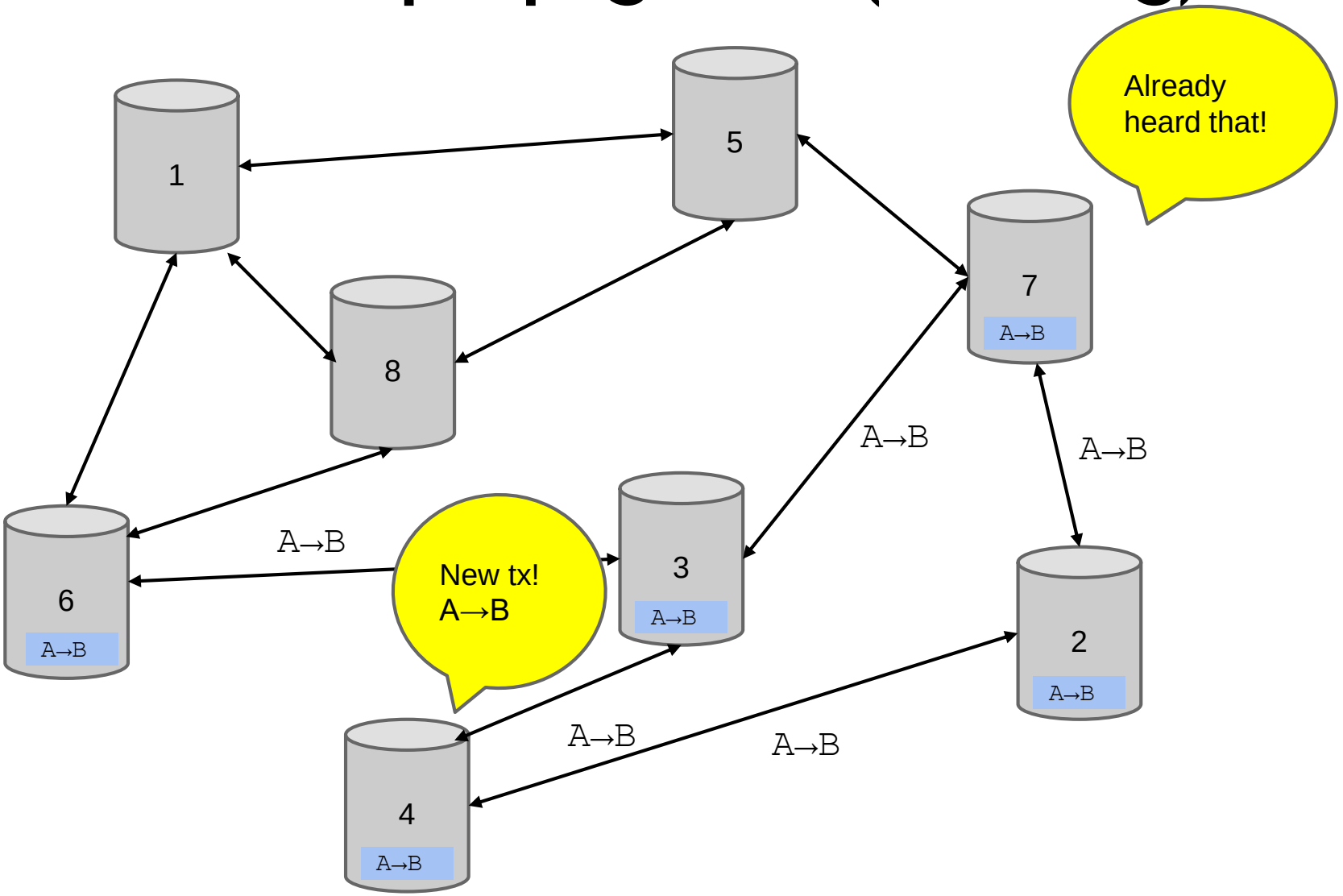
Joining the Bitcoin P2P network



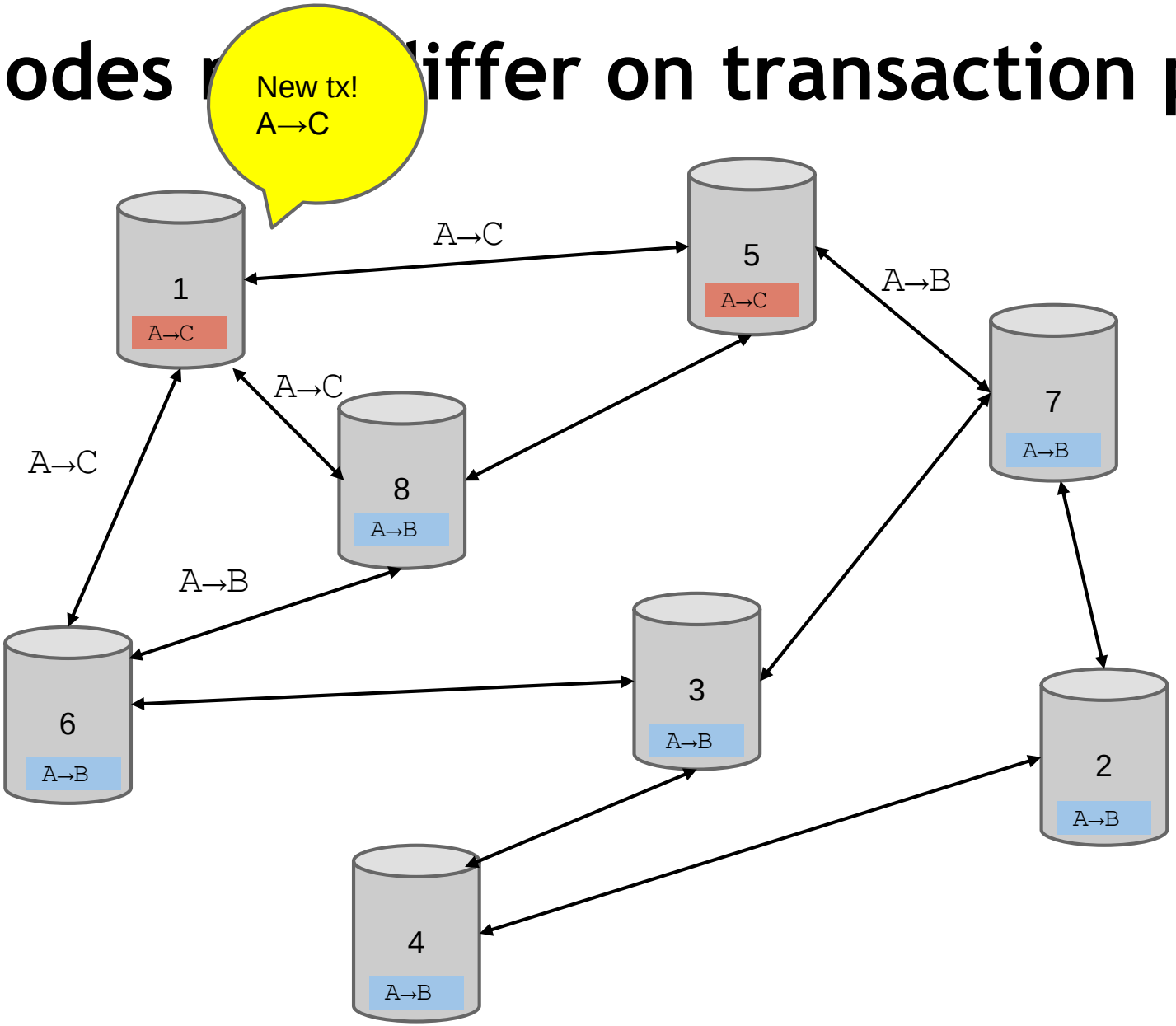
BLOCKCHAIN WORKING PRINCIPLE

HOW THE BLOCKCHAIN WORKS?

Transaction propagation (flooding)



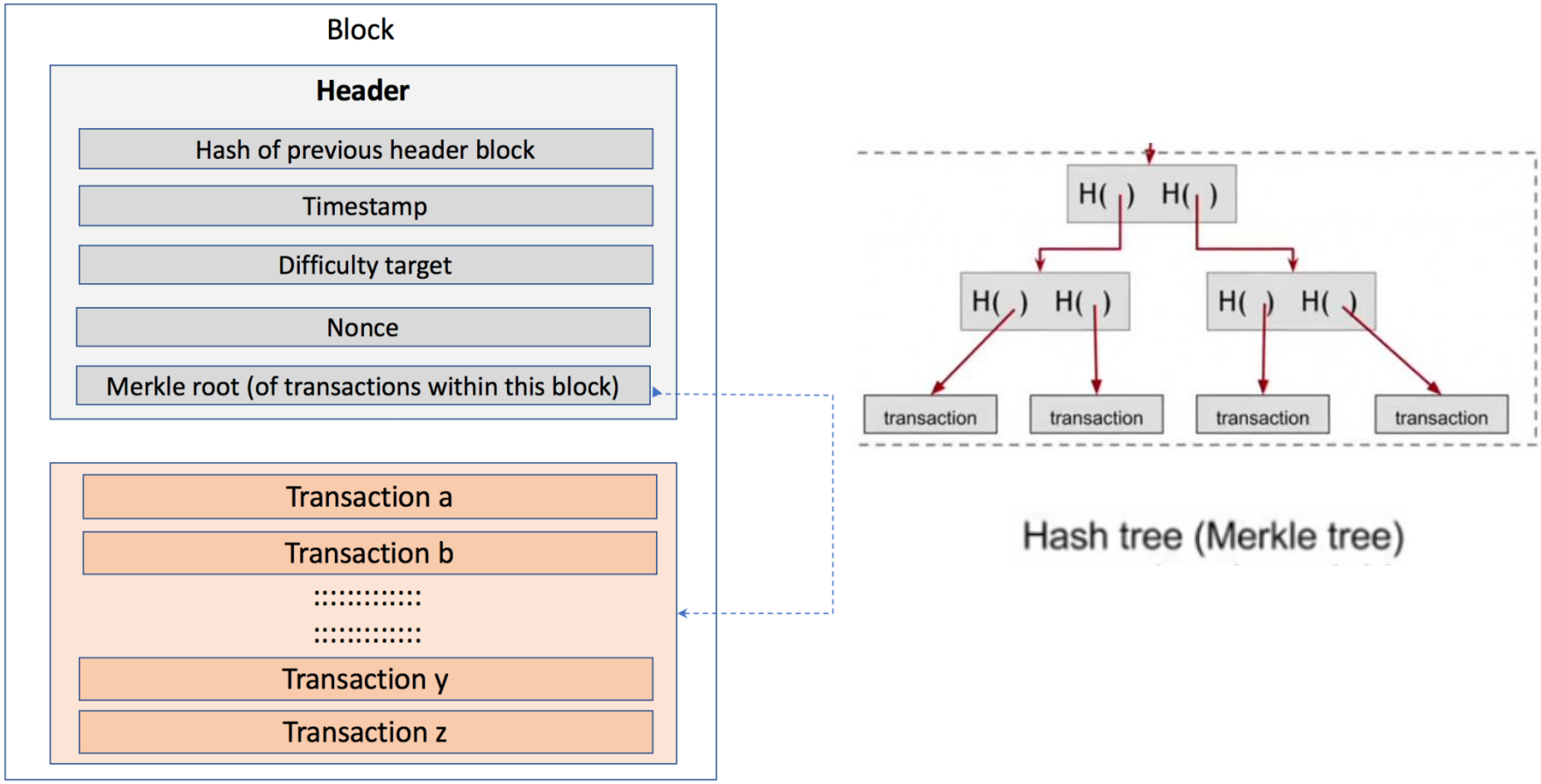
Nodes may differ on transaction pool



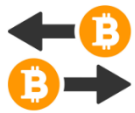
BLOCKCHAIN WORKING PRINCIPLE

HOW THE BLOCKCHAIN WORKS?

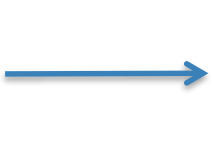
Block Structure



BLOCKCHAIN WORKING PRINCIPLE



Transactions



Miners

Block

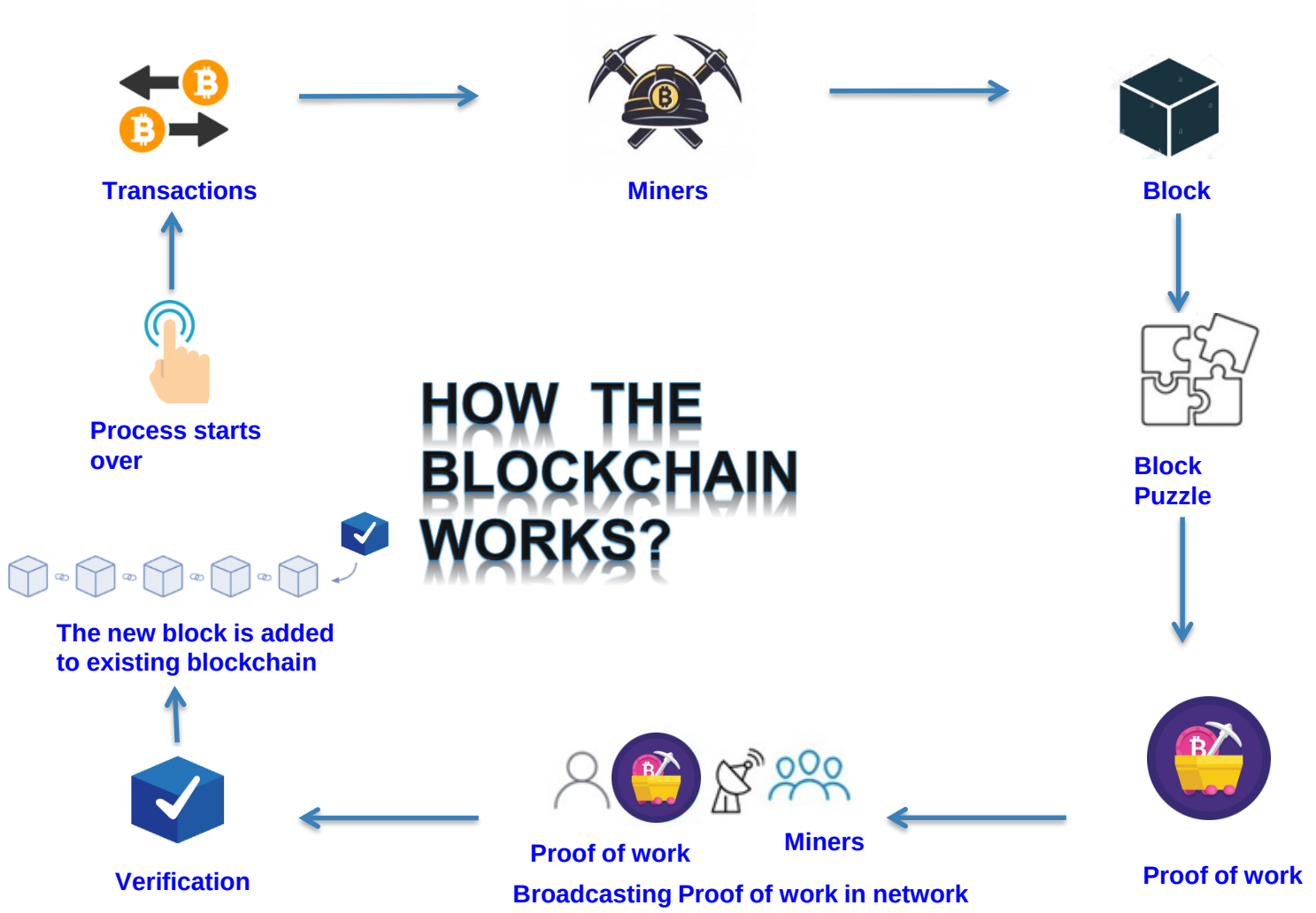
Block Puzzle

Proof of work

Process starts over

HOW THE BLOCKCHAIN WORKS?

BLOCKCHAIN WORKING PRINCIPLE



Mining Bitcoins in 6 easy steps

1. Join the network, listen for transactions
    a. Validate all proposed transactions
2. Miners will assemble them into new blocks and solve puzzle
3. On success, broadcast the new blocks
4. Listen for new blocks, maintain block chain
    a. When a new block is proposed, validate it
5. Find the nonce to make your block valid
6. Hope everybody accepts your new block
7. Profit!

Rewards and Transaction Fees!