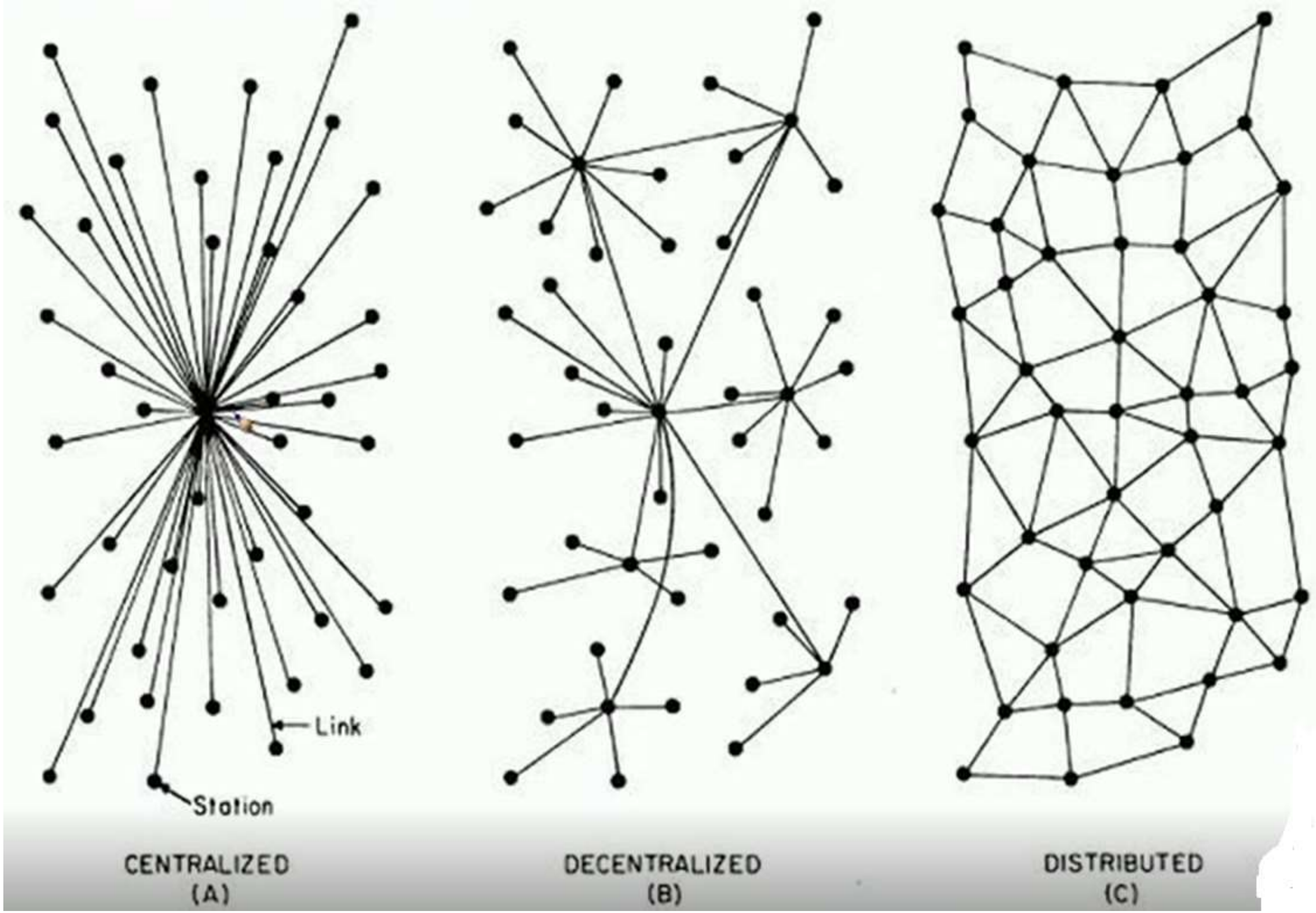
Introduction and Basics of Blockchain

Outline

- What is a blockchain?
- Differences among centralized, decentralized, and distributed systems
- Distributed Ledger

- **Blockchain** is a distributed and immutable ledger, shared among multiple parties **who do not trust** each other, to cooperate, coordinate, and collaborate in a business process.
- The ledger contains number of blocks.
- One block is chained with next block by hash value.
- Existing blocks can not be modified.
- New blocks can be added if it is valid and accepted by a majority voting.
- Every node can check the validity of a new block, so they may agree or disagree to add it.
- If a majority of nodes agrees then the new block can be added.



- **Centralized**- complete reliance on a single point, not safe
- **Decentralized** - Multiple points of coordination
- **Distributed**- Everyone collectively execute the job

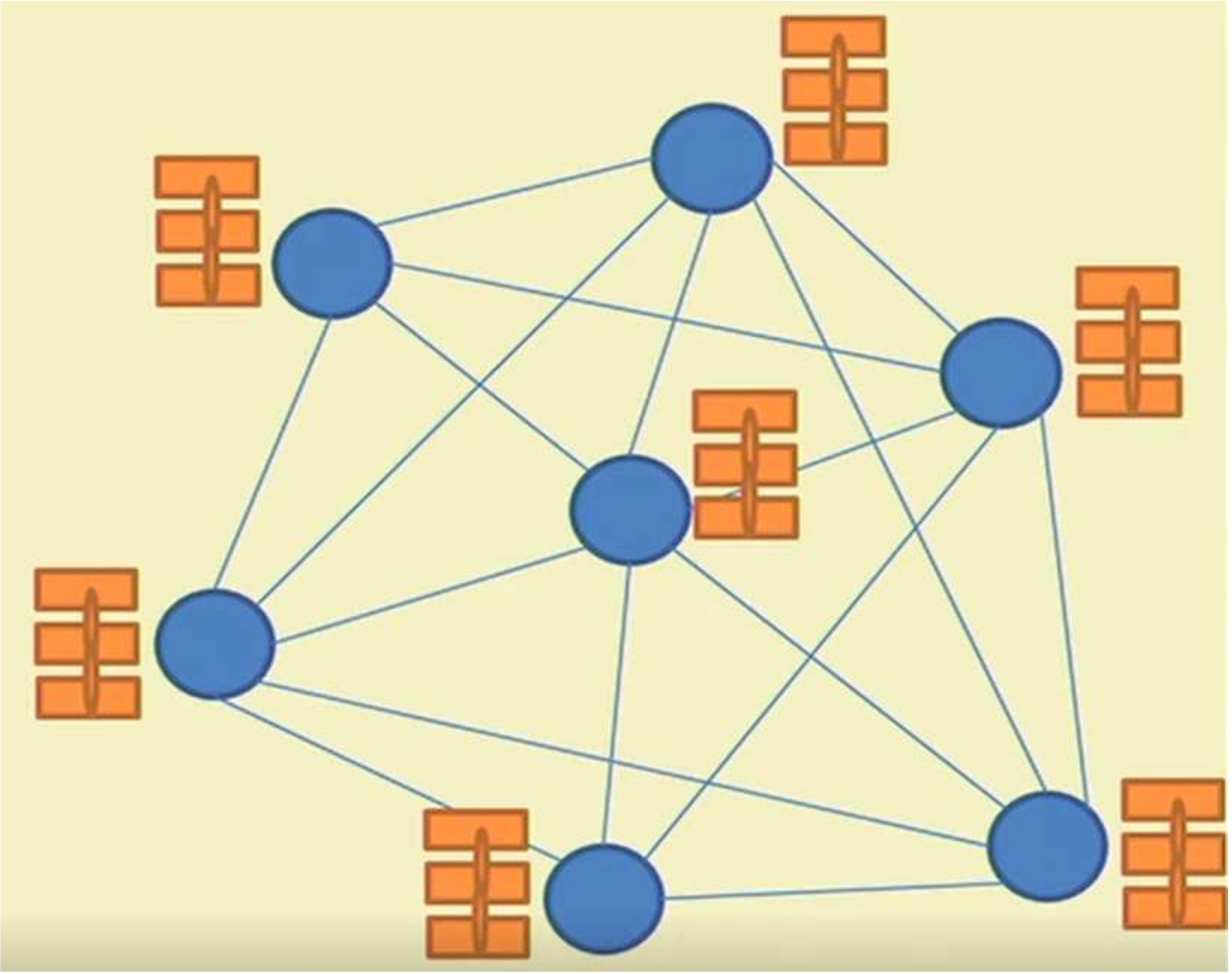
Blockchain

- Every node maintains a local copy of the global data sheet.

- The local copies are identical.

- The local copies are always updated based on global information.

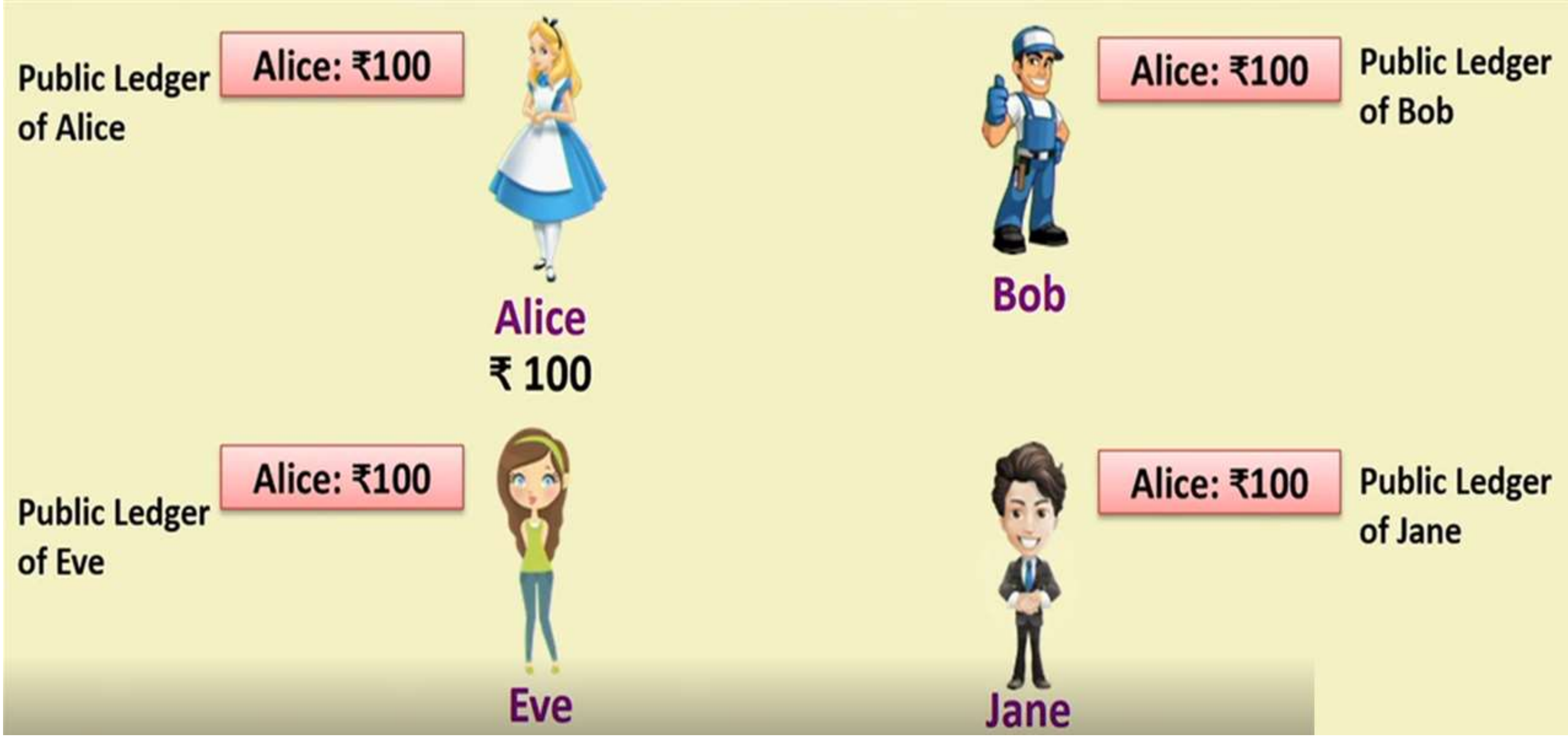
- But the local copies can not be modified.



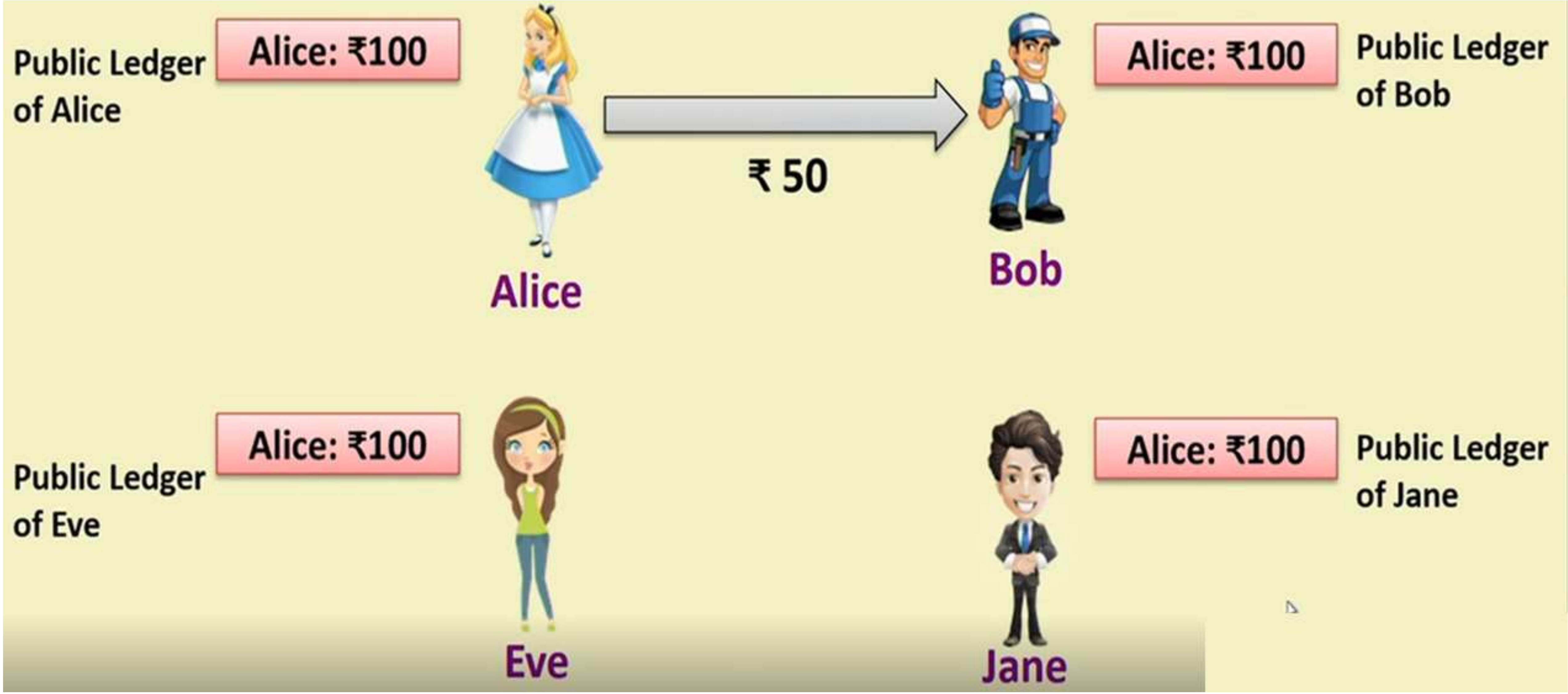
Blockchain Basics

- This local copy is called as **public ledger.**
- It is a database with historical information available to everyone.
- Old information is used to validate the new information
- In traditional system the ledger is with the bank and bank validates any new transaction based on the ledger.
- In decentralized system any new transaction is validated against the old transactions present in the public ledger.

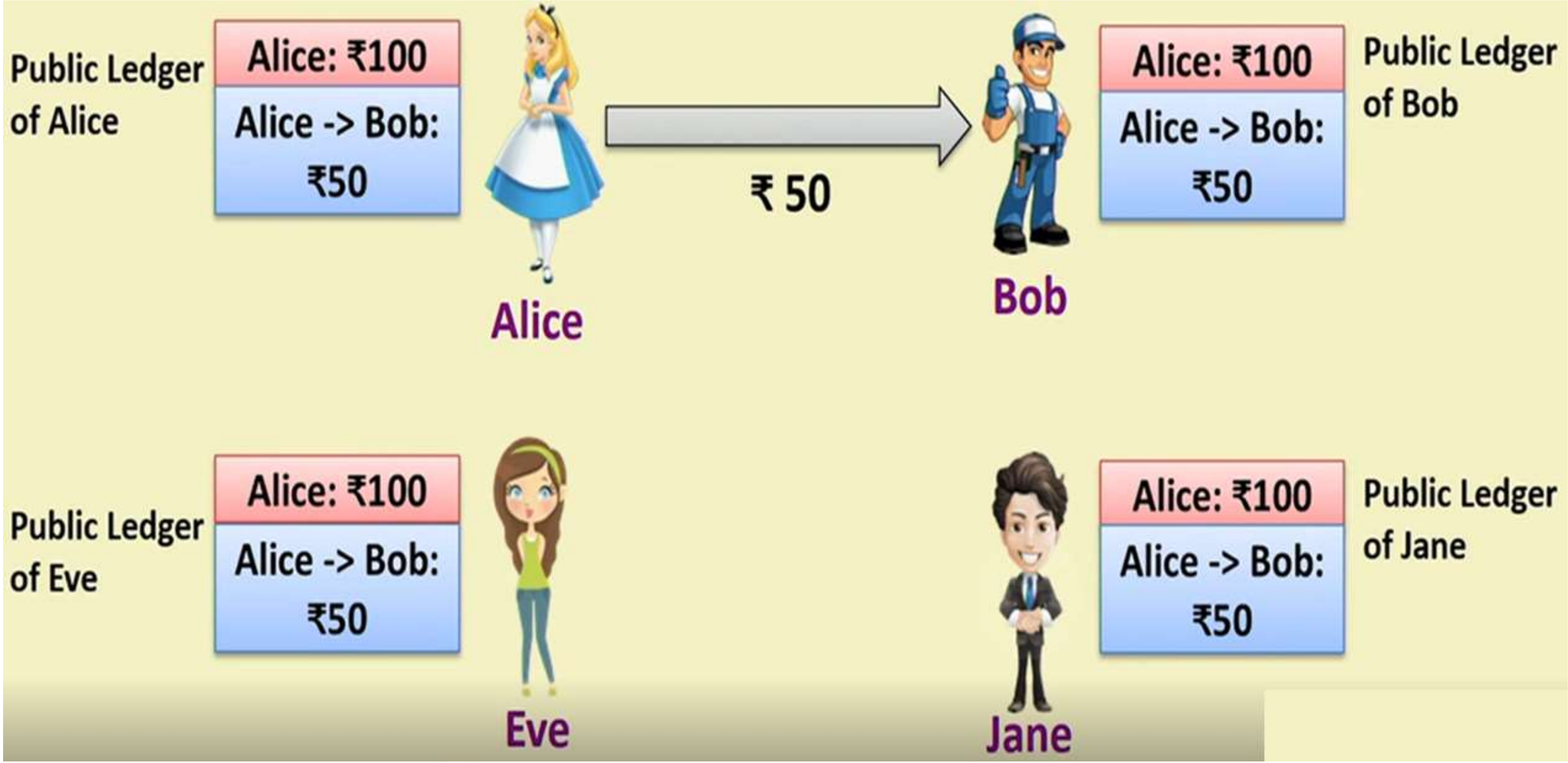
An Example of Public Ledger from Banking Sector



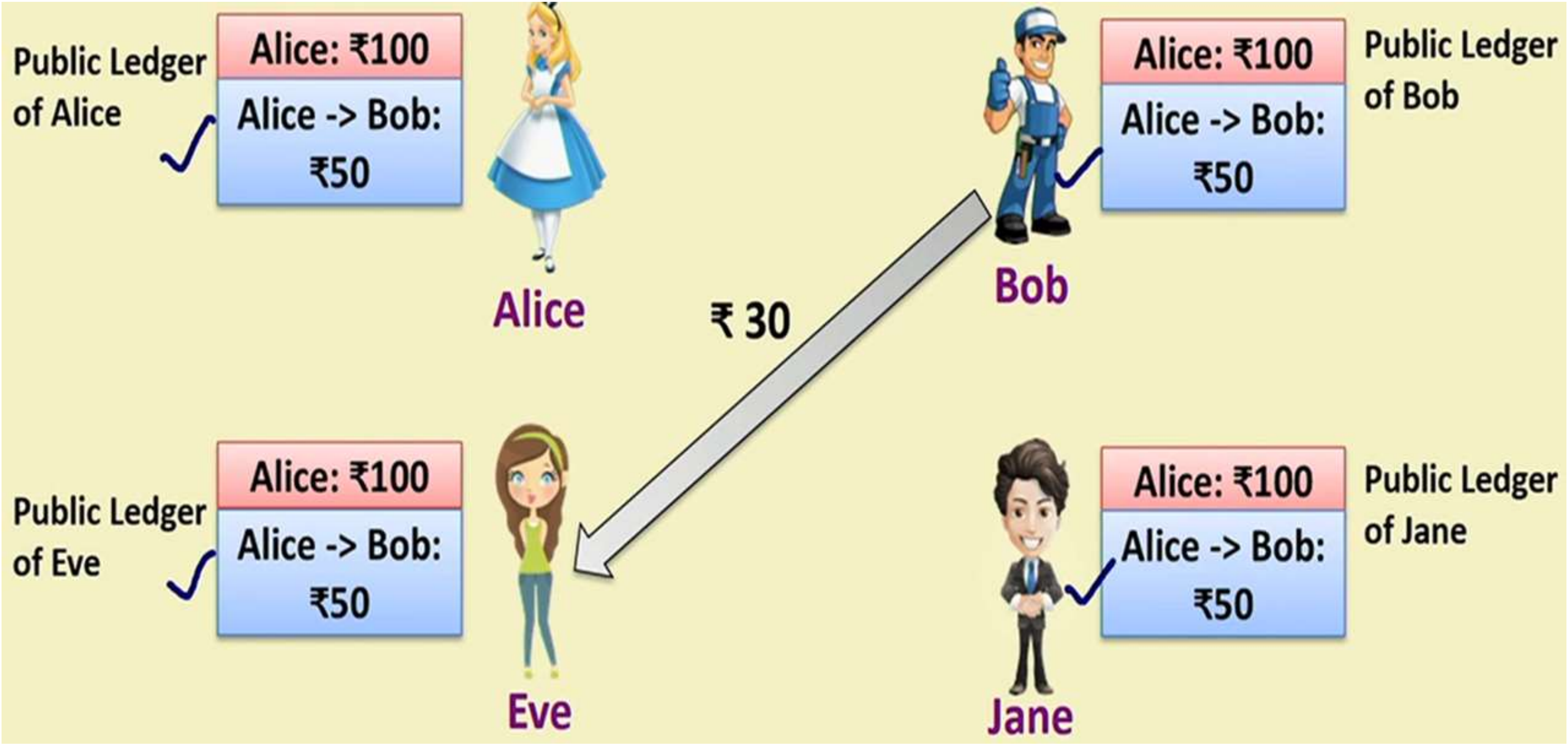
An Example of Public Ledger from Banking Sector



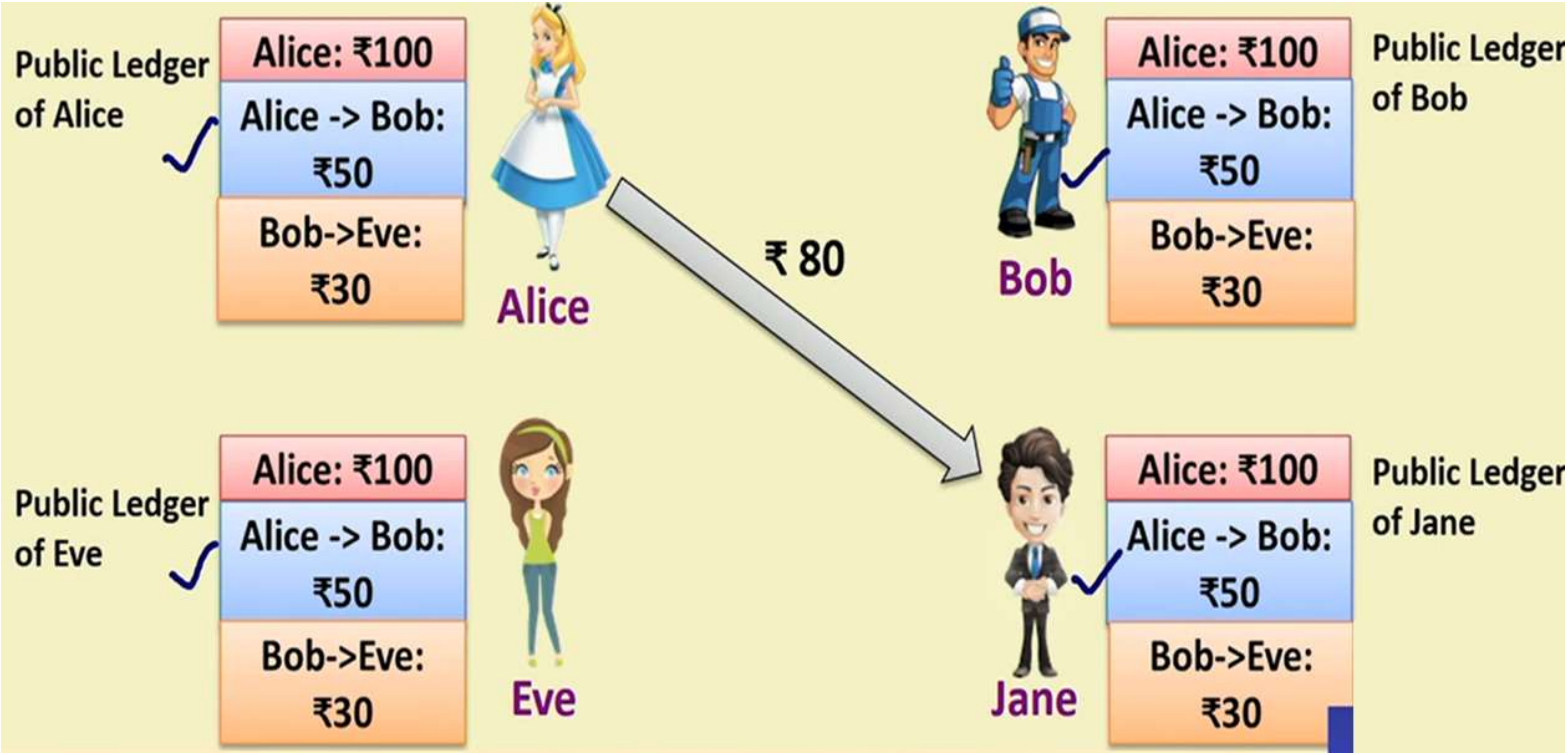
An Example of Public Ledger from Banking Sector



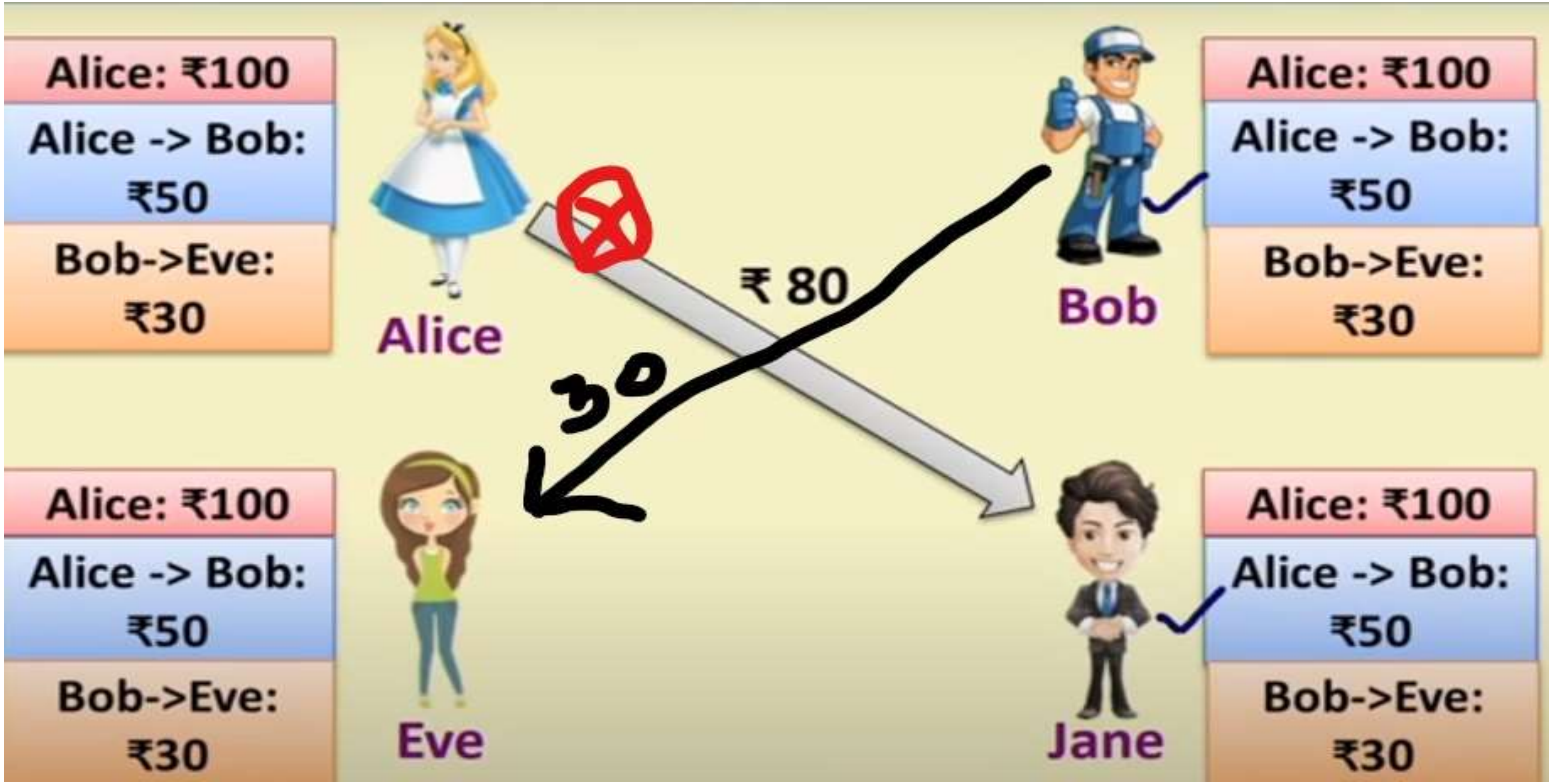
An Example of Public Ledger from Banking Sector



An Example of Public Ledger from Banking Sector



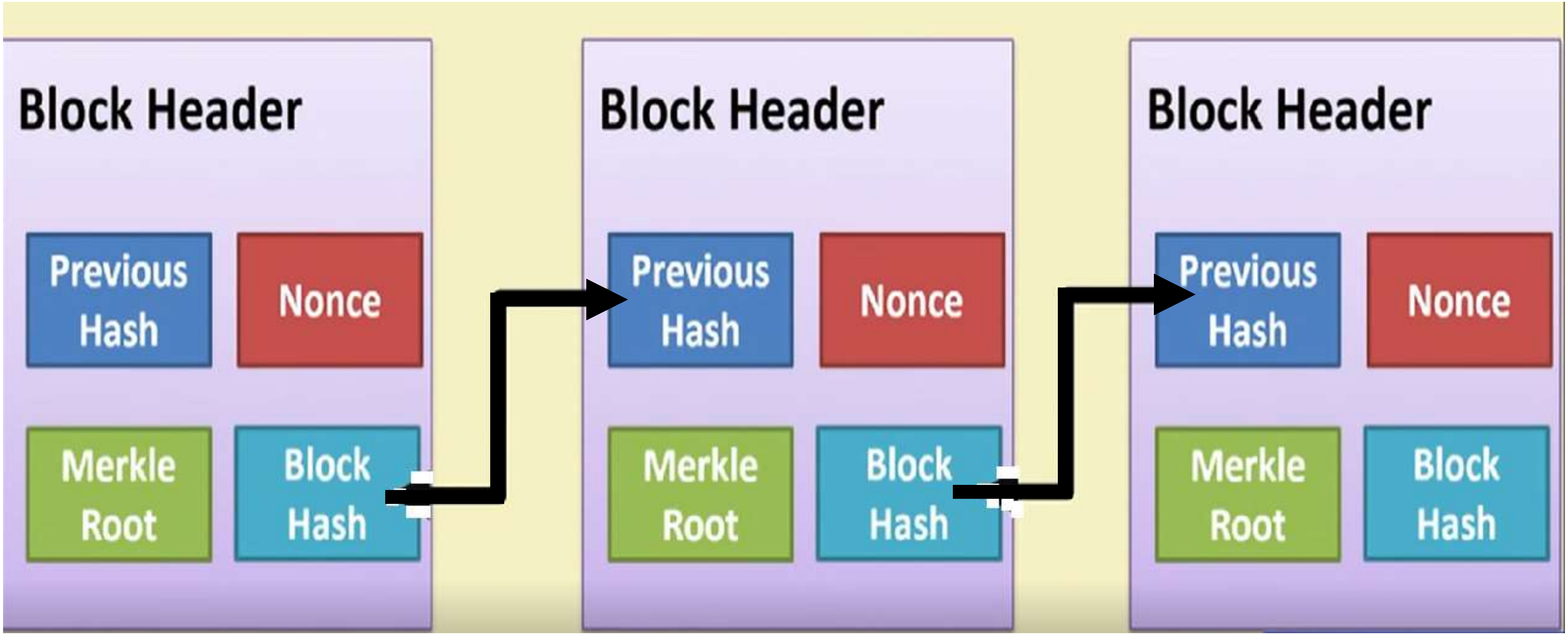
An Example of Public Ledger from Banking Sector



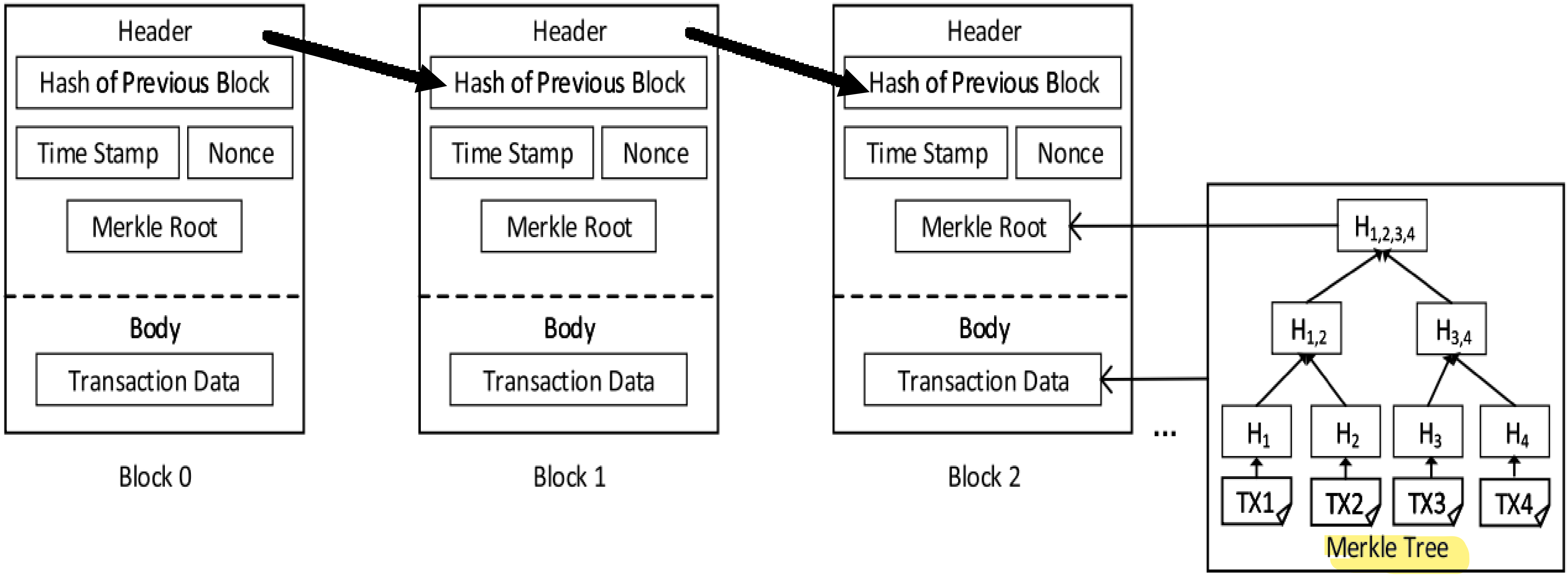
Blockchain and Public Ledgers

- Blockchain work like a public ledger
- Need to ensure different aspects:
  - **Protocols for commitment:** Ensure that every valid transaction from the clients are committed and included in the blockchain within the finite time.
  - **Consensus:** Ensures that local copies are updated and consistent
  - **Security:** The data needs to be temper proof. Note that the client may act malicious or compromised.
  - **Privacy and Authenticity:** The data / transaction belongs to various clients So, privacy and authenticity need to be ensured.

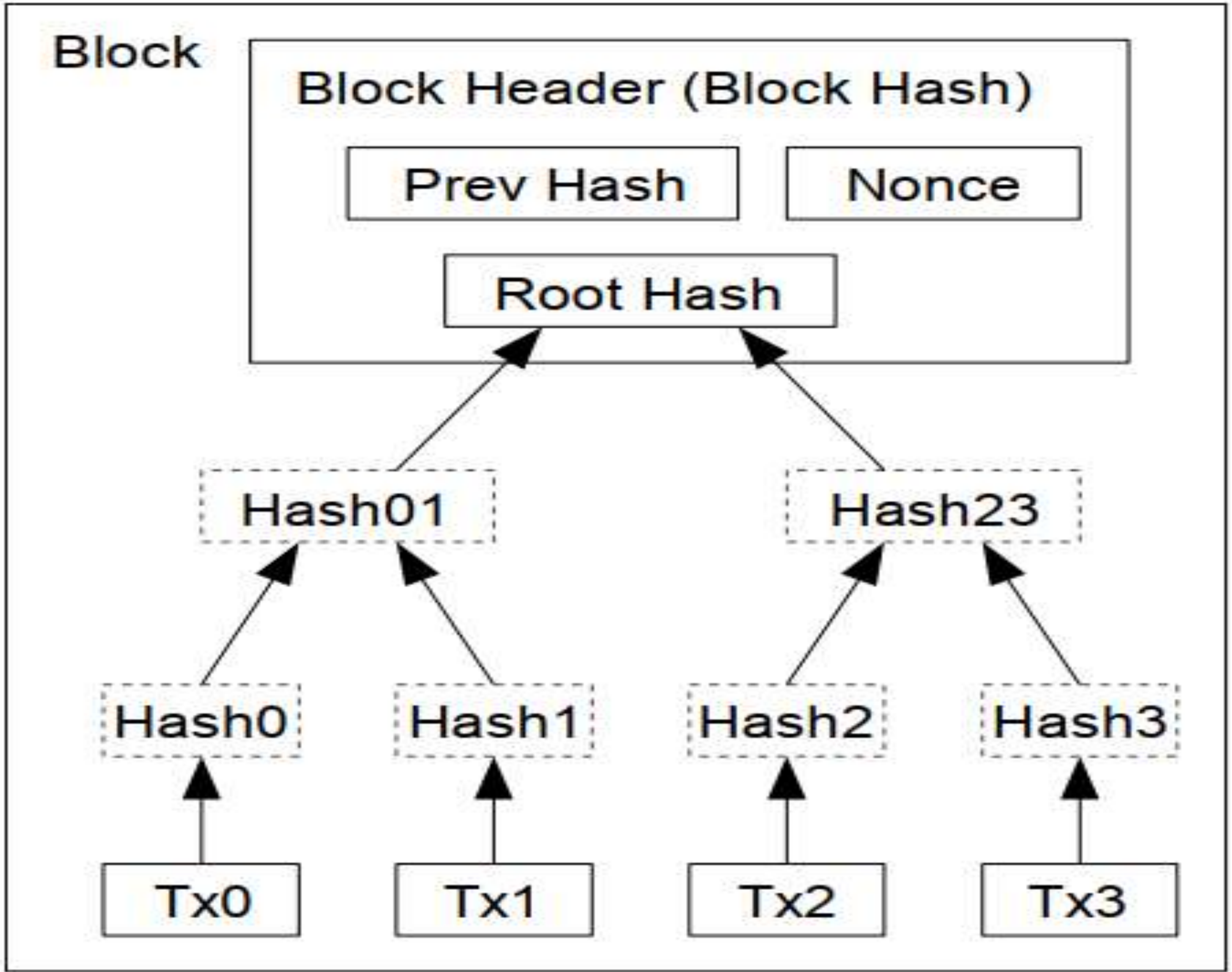
Blockchain Structure as Hash Chain



Blockchain Structure



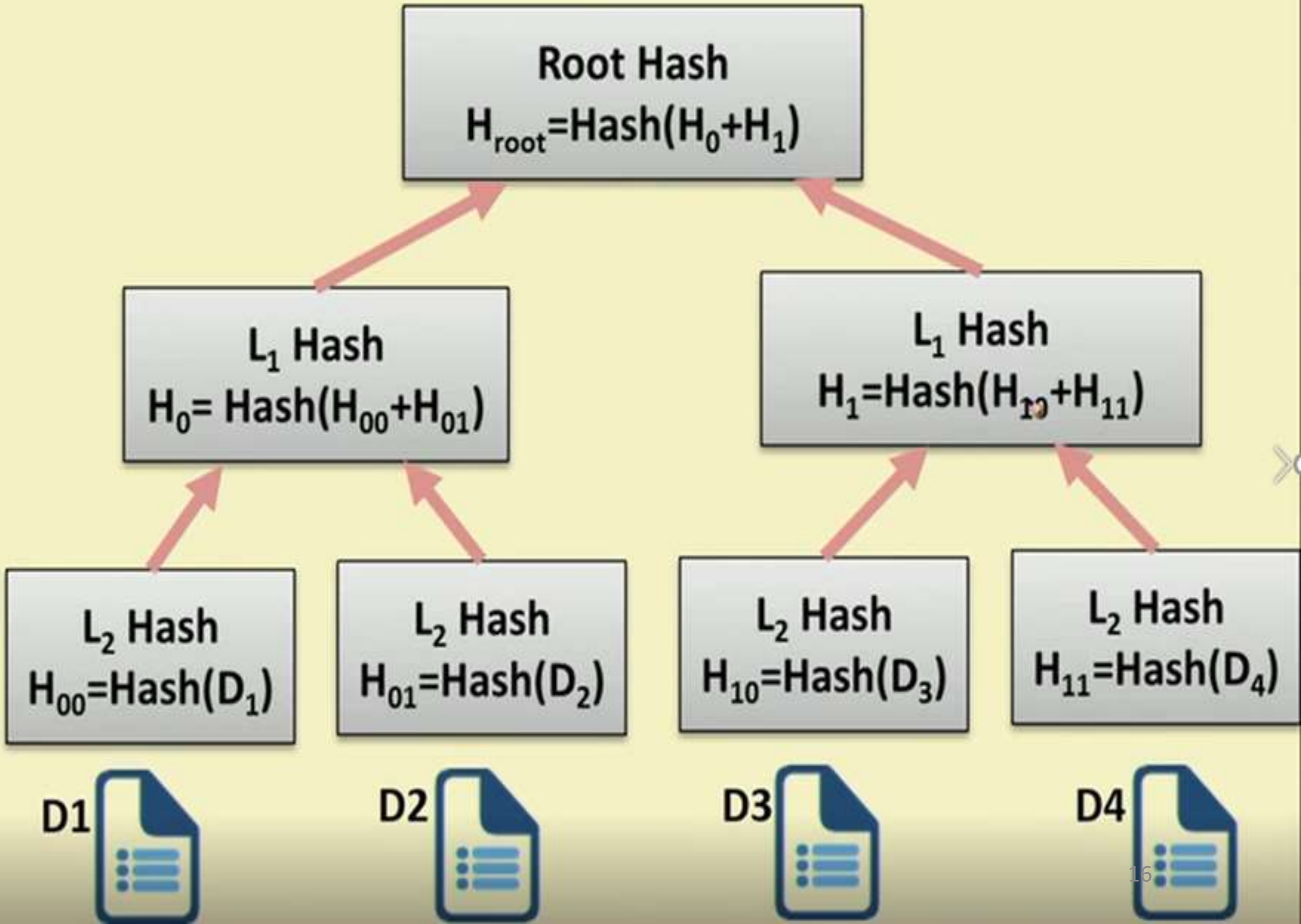
Merkele Tree



Merkle Trees (Ralph Merkle, 1979)

Also known as **hash tree**

- *every leaf node* is labelled with the hash of a data block
- ***every non-leaf node*** is labelled with the cryptographic hash of the labels of its child nodes



Root Hash

H_{root}=Hash(H_0+H_1)

L_1 Hash

H_0= Hash(H_{00}+H_{01})

L_1 Hash

H_1=Hash(H_{10}+H_{11})

L_2 Hash

H_{00}=Hash(D_1)

L_2 Hash

H_{01}=Hash(D_2)

L_2 Hash

H_{10}=Hash(D_3)

L_2 Hash

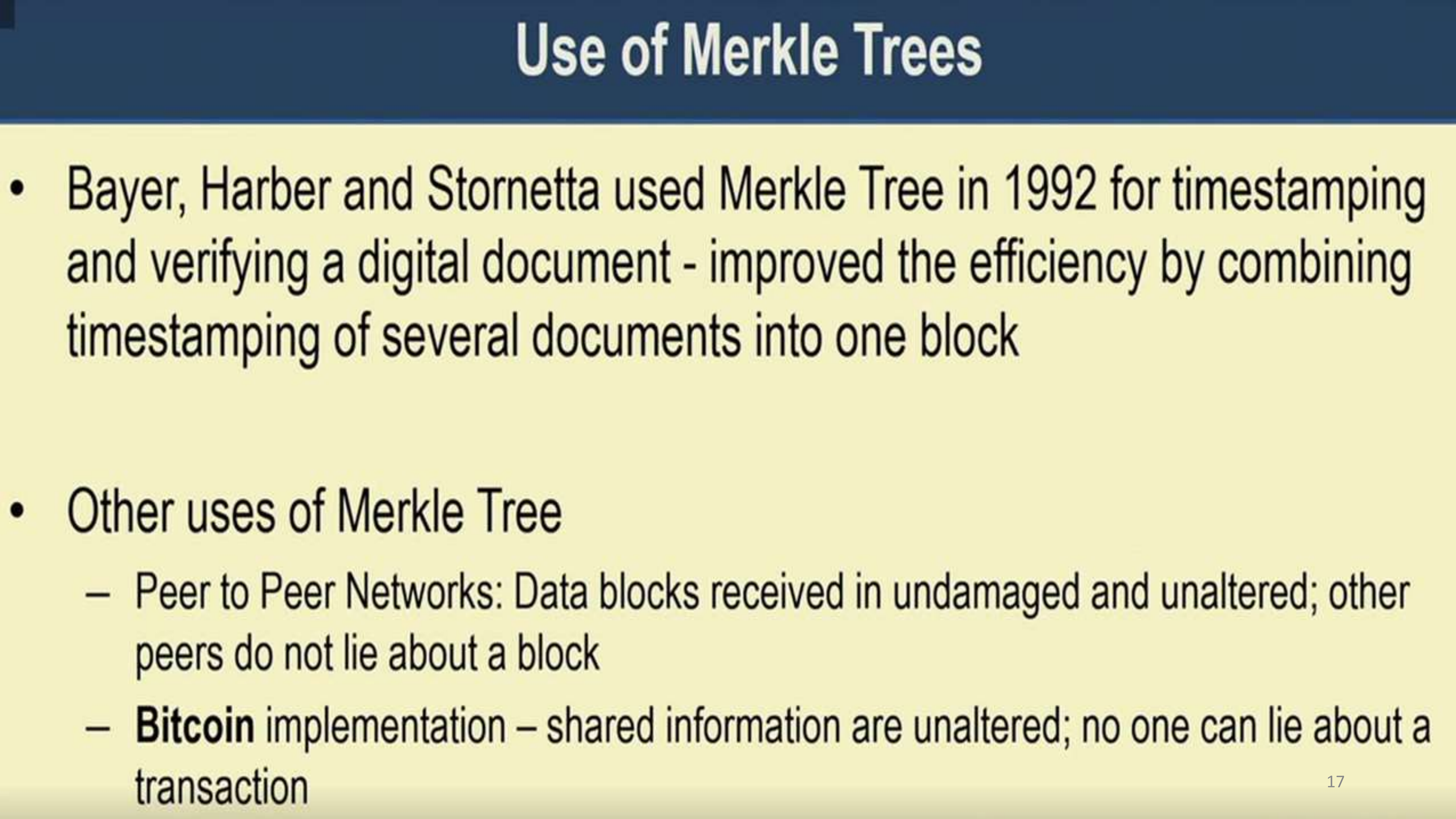
H_{11}=Hash(D_4)

D1

D2

D3

D4



Use of Merkle Trees

- Bayer, Harber and Stornetta used Merkle Tree in 1992 for timestamping and verifying a digital document - improved the efficiency by combining timestamping of several documents into one block

- Other uses of Merkle Tree
  - Peer to Peer Networks: Data blocks received in undamaged and unaltered; other peers do not lie about a block
  - **Bitcoin** implementation – shared information are unaltered; no one can lie about a transaction

- Is Bitcoin same as Blockchain
- Similarity ??
- Difference ??

Modes of Blockchain

- Permissionless Blockchain (Open Environment):
  - Suitable for open control-free financial applications e.g. Cryptocurrencies (BitCoin, Ethereum, Ripple, LightCoin etc.)

- Permissioned Blockchain (Close Environment):
  - Suitable for business applications e.g. Smart contracts

The Permission-less Model

- Works in an open environment and over a large network of participants

- The users do not need to know the identity of the peers, and hence the users do not need to reveal their identity to others

- Good for financial applications like banking using cryptocurrency

Privacy and Security

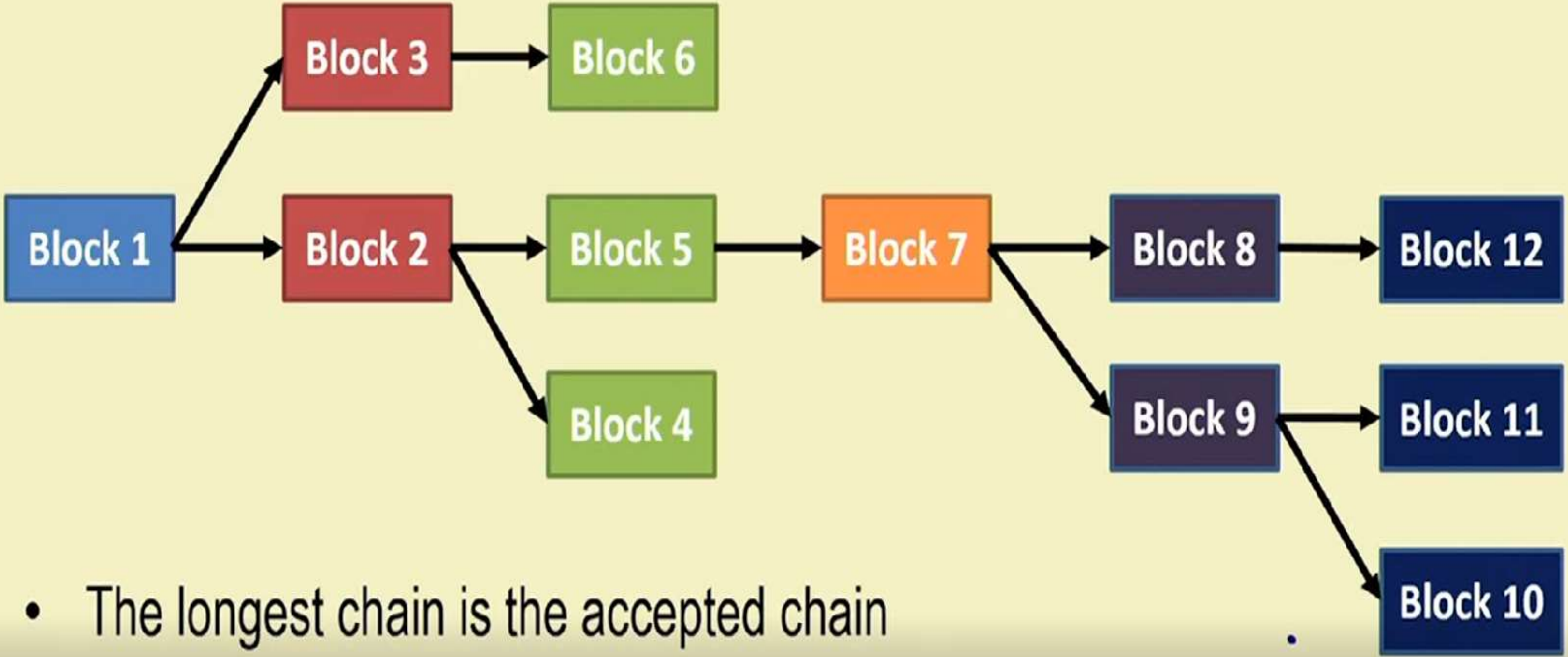
- **Tamper proof:** Extremely hard to change in blockchain
  - Becomes harder as chain grows

- Transactions are pseudo anonymous
  - Transactions sent to public key address (OR)
  - Cryptographically generated address (OR)
  - Computed by wallet applications

Privacy and Security

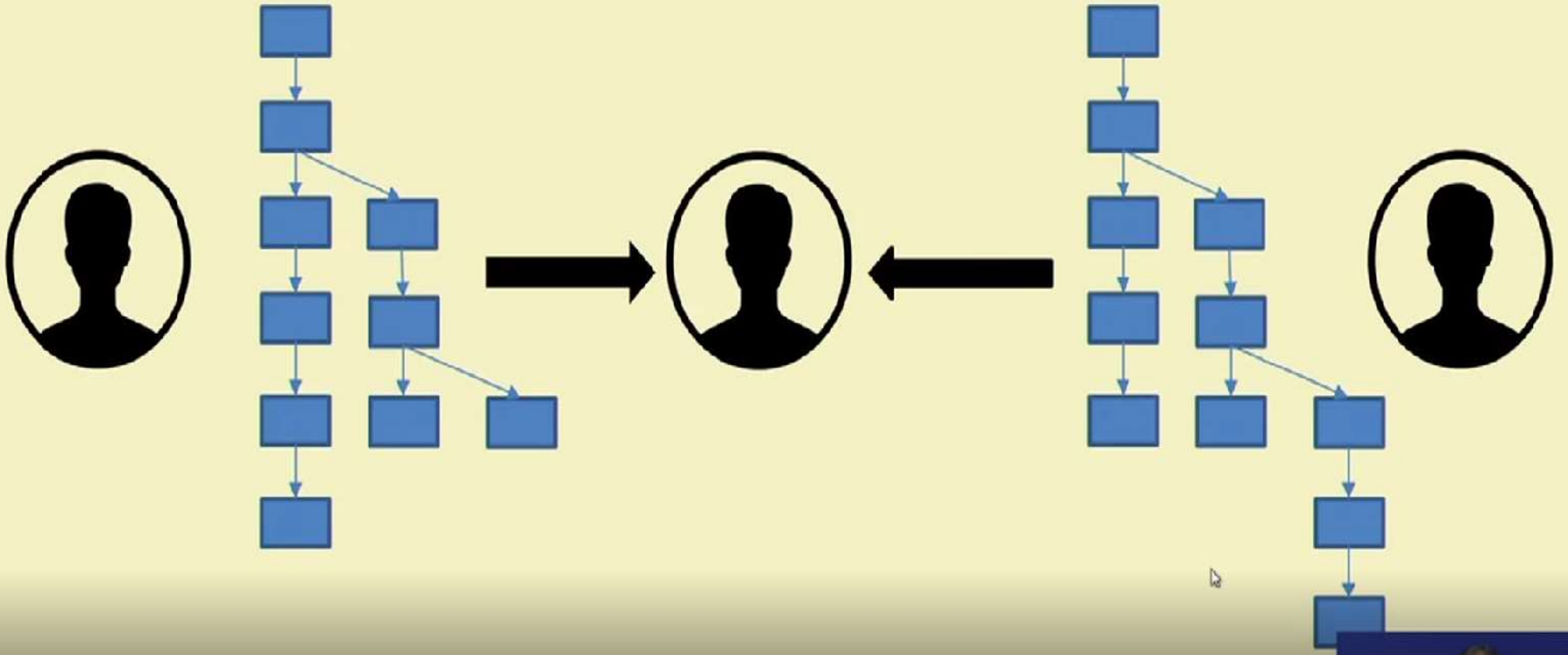
- **Peer Address:** Similar to bank account number
  - Becomes harder as chain grows
- Wallet listens for transactions specified by address
  - Encrypts the transaction by public key of target address
  - Only target node can decrypt and accept
- Actual transaction amount is open to all for validation
  - Anyone can validate

Blockchain (at Permission-less Model) as a Tree

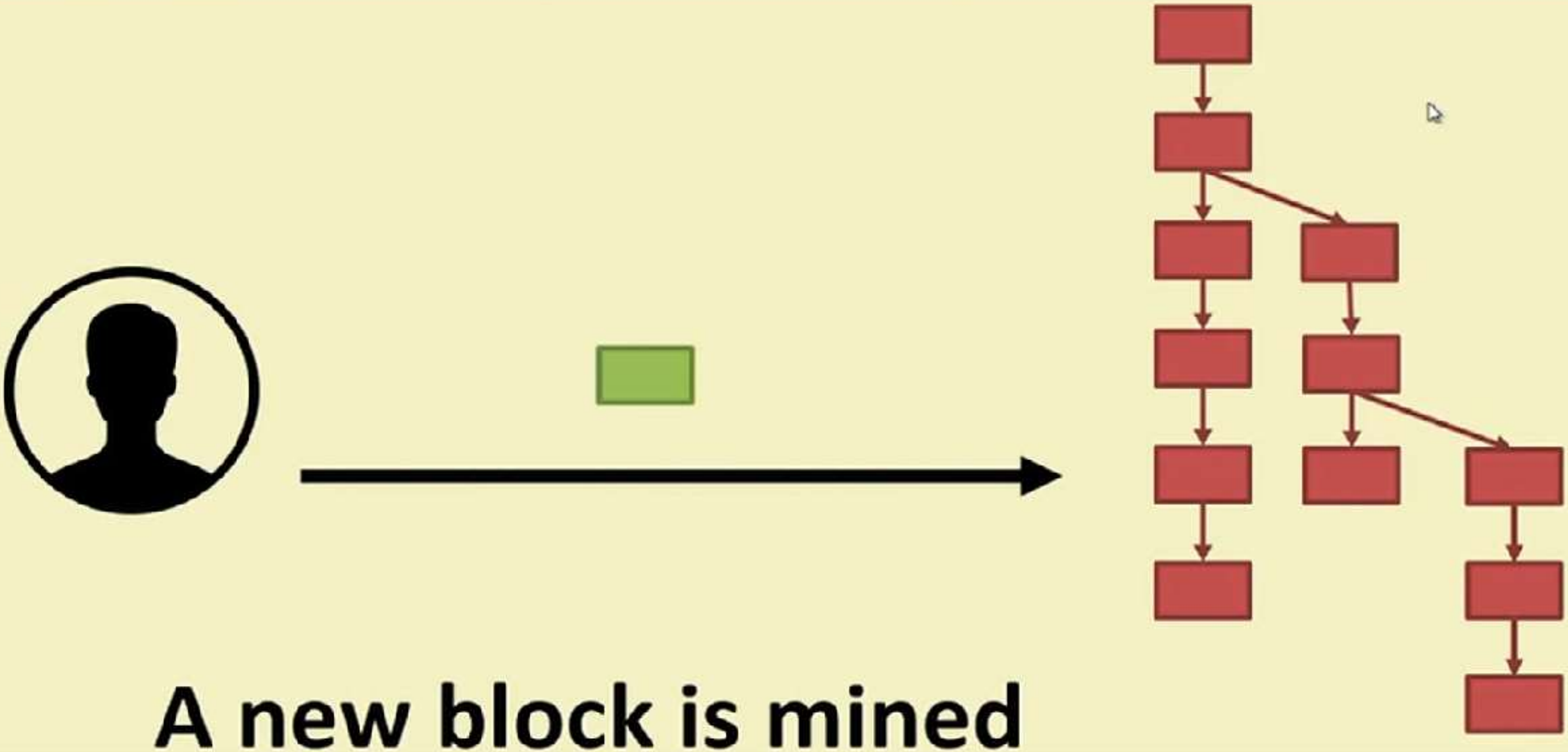


- The longest chain is the accepted chain

Accepting the Longest Chain

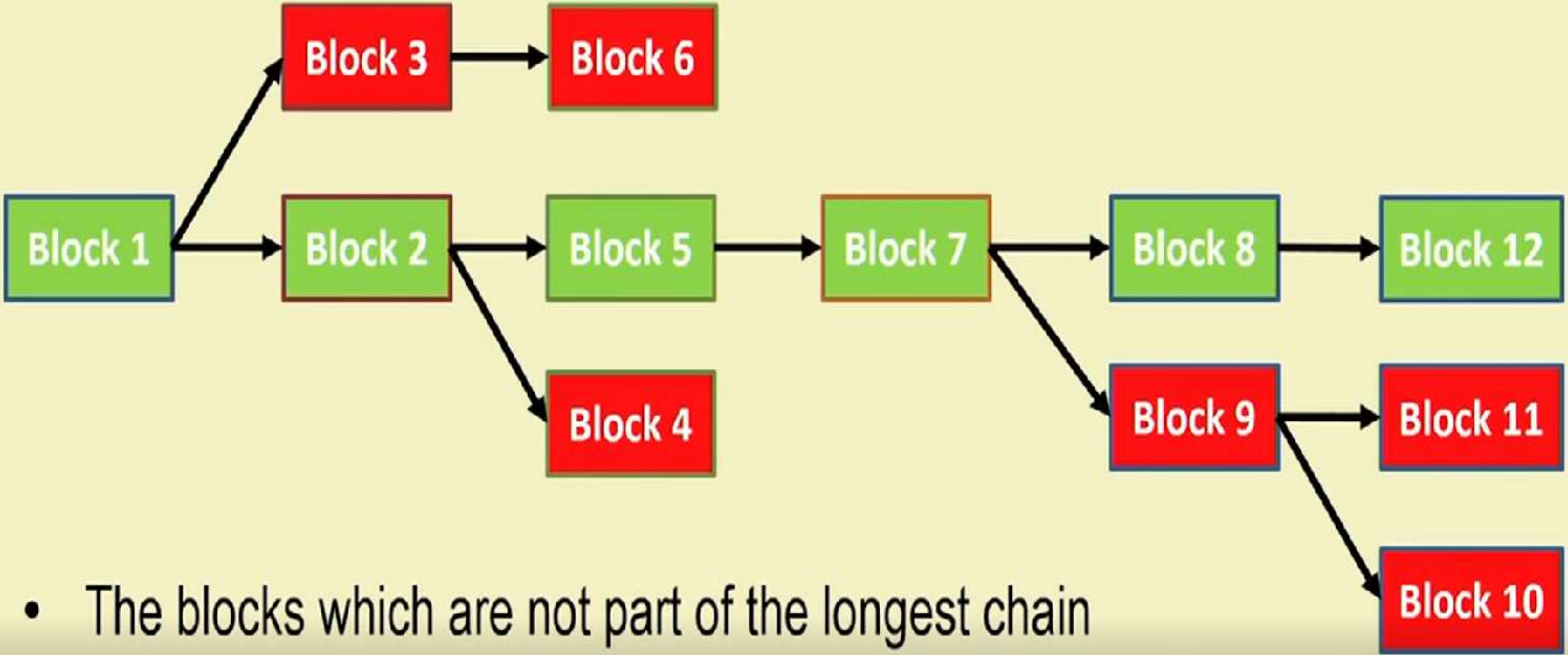


Accepting the Longest Chain



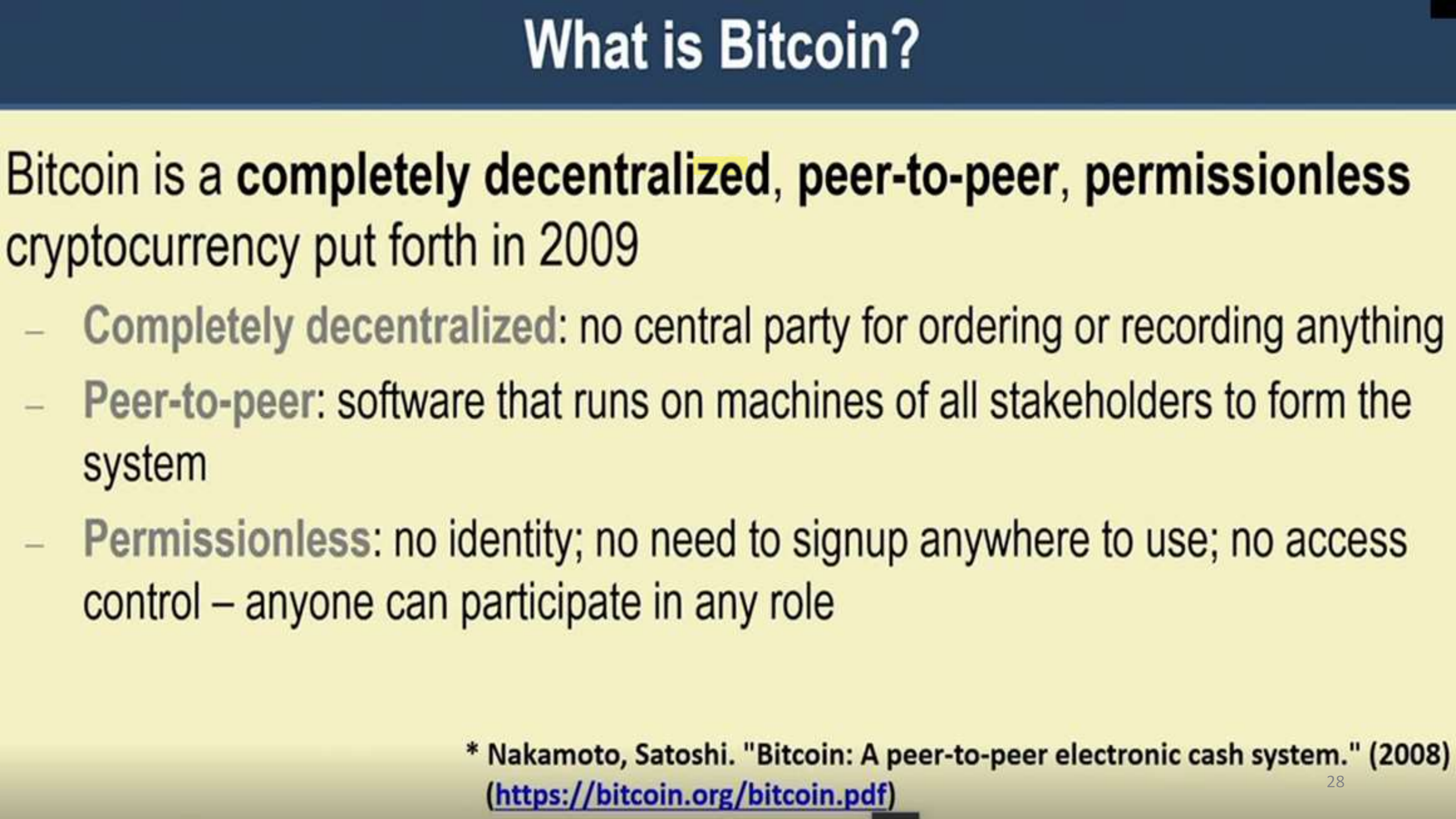
A new block is mined

Orphaned Blocks



- The blocks which are not part of the longest chain

- Is Bitcoin same as Blockchain
- Similarity ??
- Difference ??



What is Bitcoin?

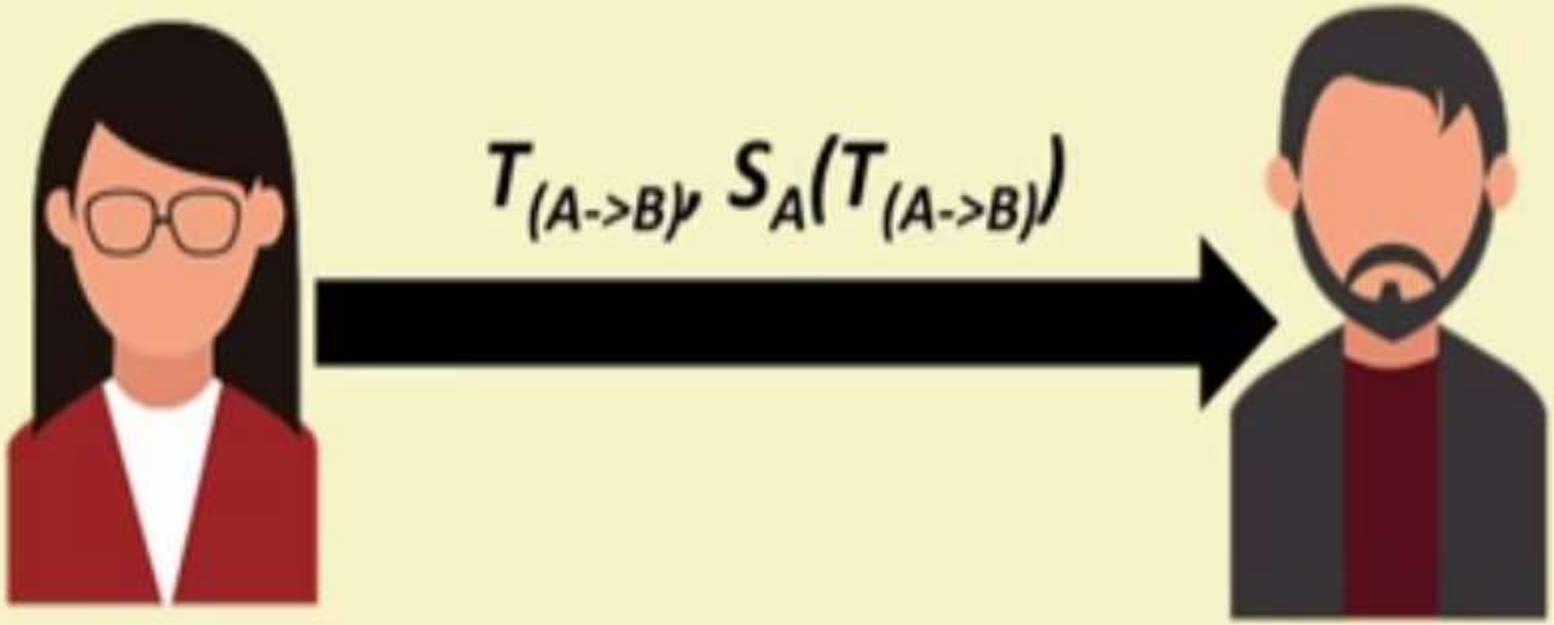
Bitcoin is a **completely decentralized**, **peer-to-peer**, **permissionless** cryptocurrency put forth in 2009

- **Completely decentralized**: no central party for ordering or recording anything
- **Peer-to-peer**: software that runs on machines of all stakeholders to form the system
- **Permissionless**: no identity; no need to signup anywhere to use; no access control – anyone can participate in any role

[*] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008) (https://bitcoin.org/bitcoin.pdf)

Bitcoin Basics – Sending Payments

- Alice wish to transfer some bitcoin to Bob.
  - Alice can sign a transaction with her private key
  - Anyone can validate the transaction with Alice's public key



$T_{(A\text{->}B)}, S_A(T_{(A\text{->}B)})$

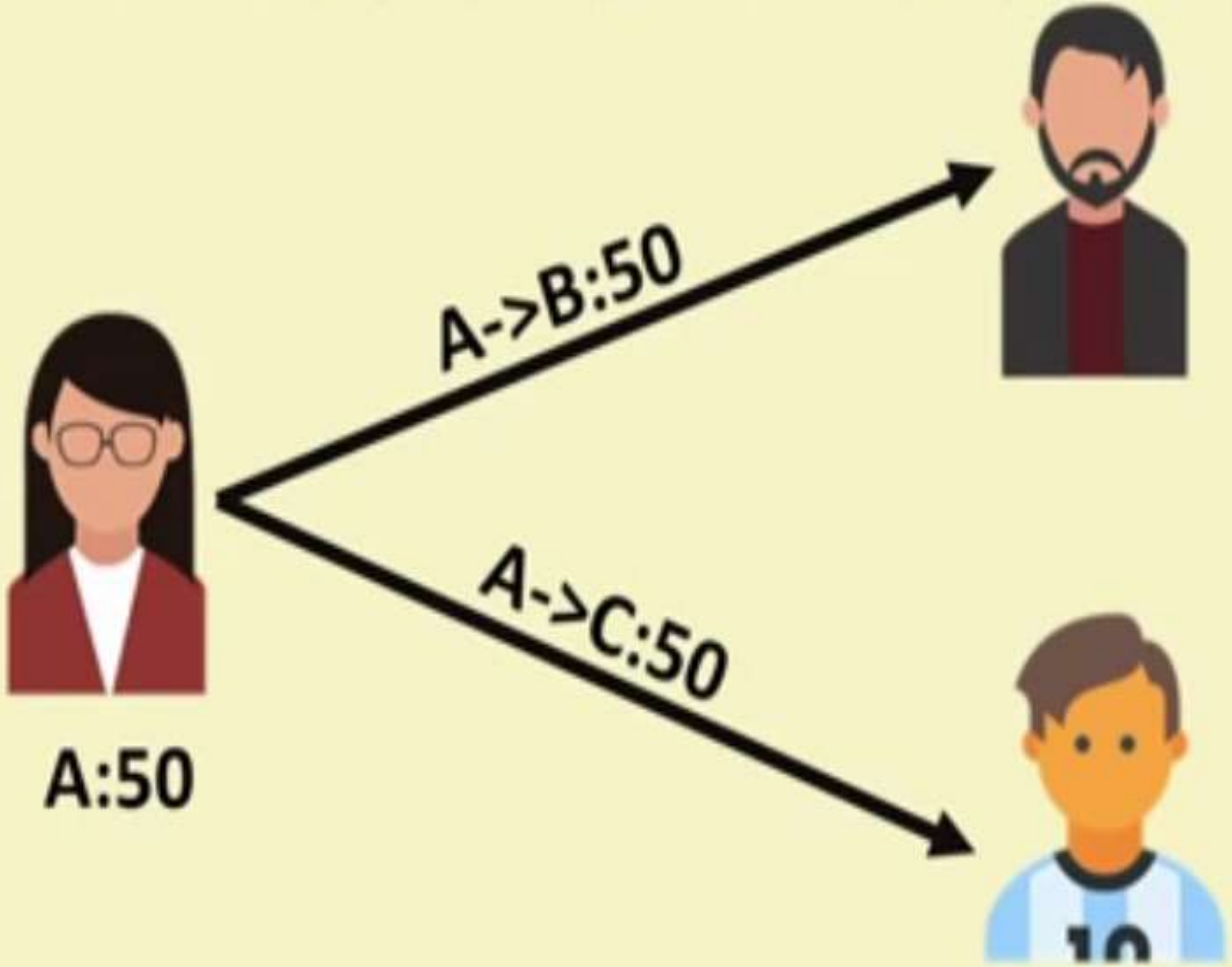
Bitcoin Basics – Sending Payments

- Alice wants to send bitcoin to Bob
  - Bob sends his address to Alice
  - Alice adds Bob's address and the amount of bitcoins to transfer in a "transaction" message
  - Alice signs the transaction with her private key, and announces her public key for signature verification
  - Alice broadcasts the transaction on the Bitcoin network for all to see

Information Source: https://en.bitcoin.it/wiki/

Double Spending

- Same bitcoin is used for more than one transactions



- In a centralized system, the bank prevents double spending
- **How can we prevent double spending in a decentralized network?**

Handle Double Spending using Blockchain

- Details about the transaction are sent and forwarded to all or as many other computers as possible

- Use **Blockchain** – a constantly growing chain of blocks that contain a record of all transactions

- The blockchain is maintained by all peers in the Bitcoin network – everyone has a copy of the blockchain

Information Source: https://en.bitcoin.it/wiki/

Handle Double Spending using Blockchain

- To be accepted in the chain, transaction blocks must be valid and must include **proof of work** – a computationally difficult hash generated by the mining procedure

- Blockchain ensures that, if any of the block is modified, all following blocks will have to be recomputed

Handle Double Spending using Blockchain

- To be accepted in the chain, transaction blocks must be valid and must include **proof of work** – a computationally difficult hash generated by the mining procedure

$$\leftarrow \underline{\underline{Y}} = H(\underline{\underline{X}} \,\|\, \underline{\underline{\text{Nonce}}})$$

- Blockchain ensures that, if any of the block is modified, all following blocks will have to be recomputed

$$Y \approx \underline{0000 \ldots 00F}1G2FD$$

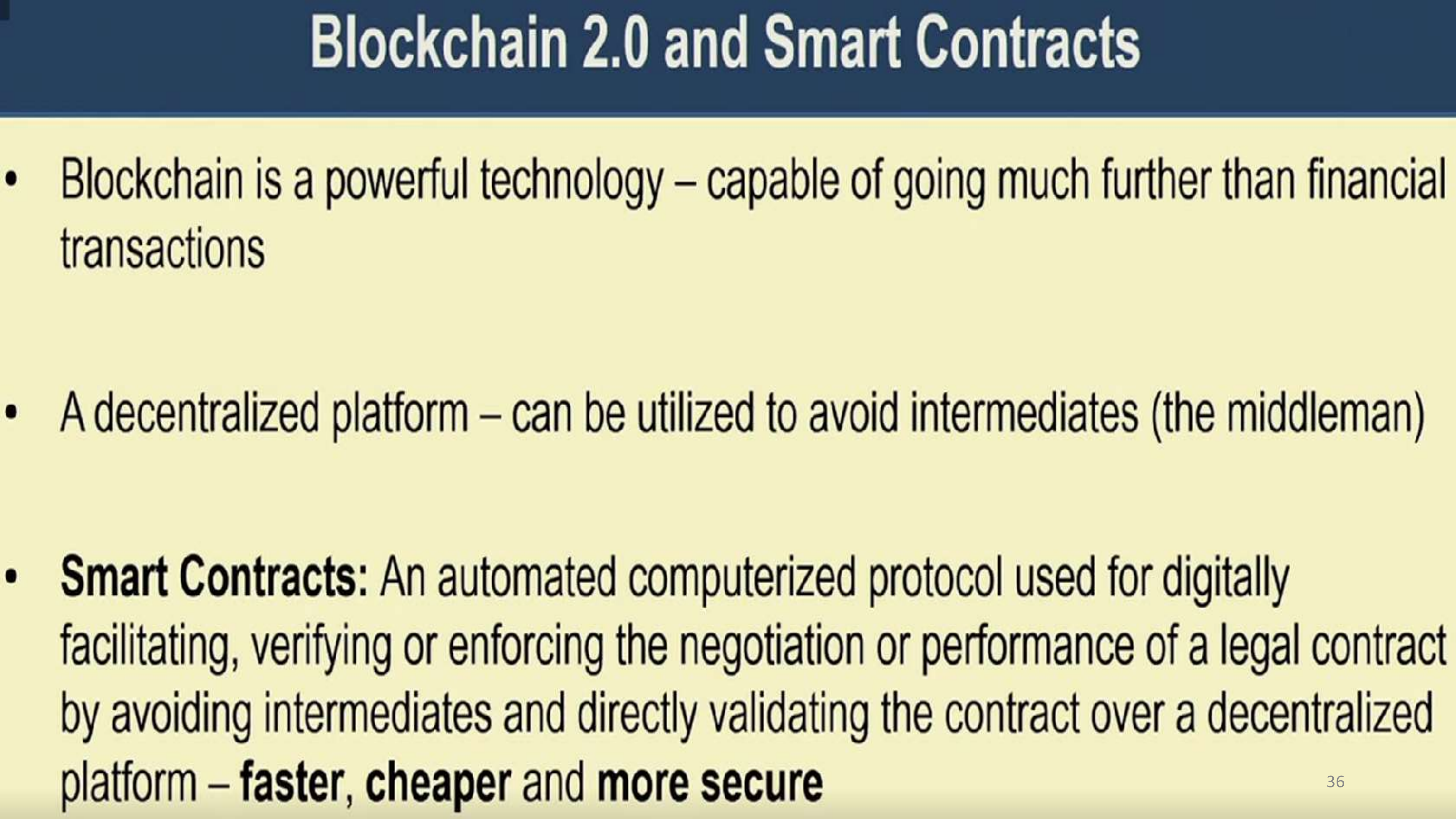
Handle Double Spending using Blockchain

- When multiple valid continuation to this chain appear, only the longest such branch is accepted and it is then extended further **(longest chain)**

- Once a transaction is committed in the blockchain, everyone in the network can validate all the transactions by using Alice's public address

- The validation prevents double spending in bitcoin

Information Source: https://en.bitcoin.it/wiki/



Blockchain 2.0 and Smart Contracts

- Blockchain is a powerful technology – capable of going much further than financial transactions
- A decentralized platform – can be utilized to avoid intermediates (the middleman)
- **Smart Contracts:** An automated computerized protocol used for digitally facilitating, verifying or enforcing the negotiation or performance of a legal contract by avoiding intermediates and directly validating the contract over a decentralized platform – **faster**, **cheaper** and **more secure**

Thank You!