futureskills prime
A MeitY - NASSCOM Digital Skilling Initiative

Introduction to Blockchain Technology & Benefits

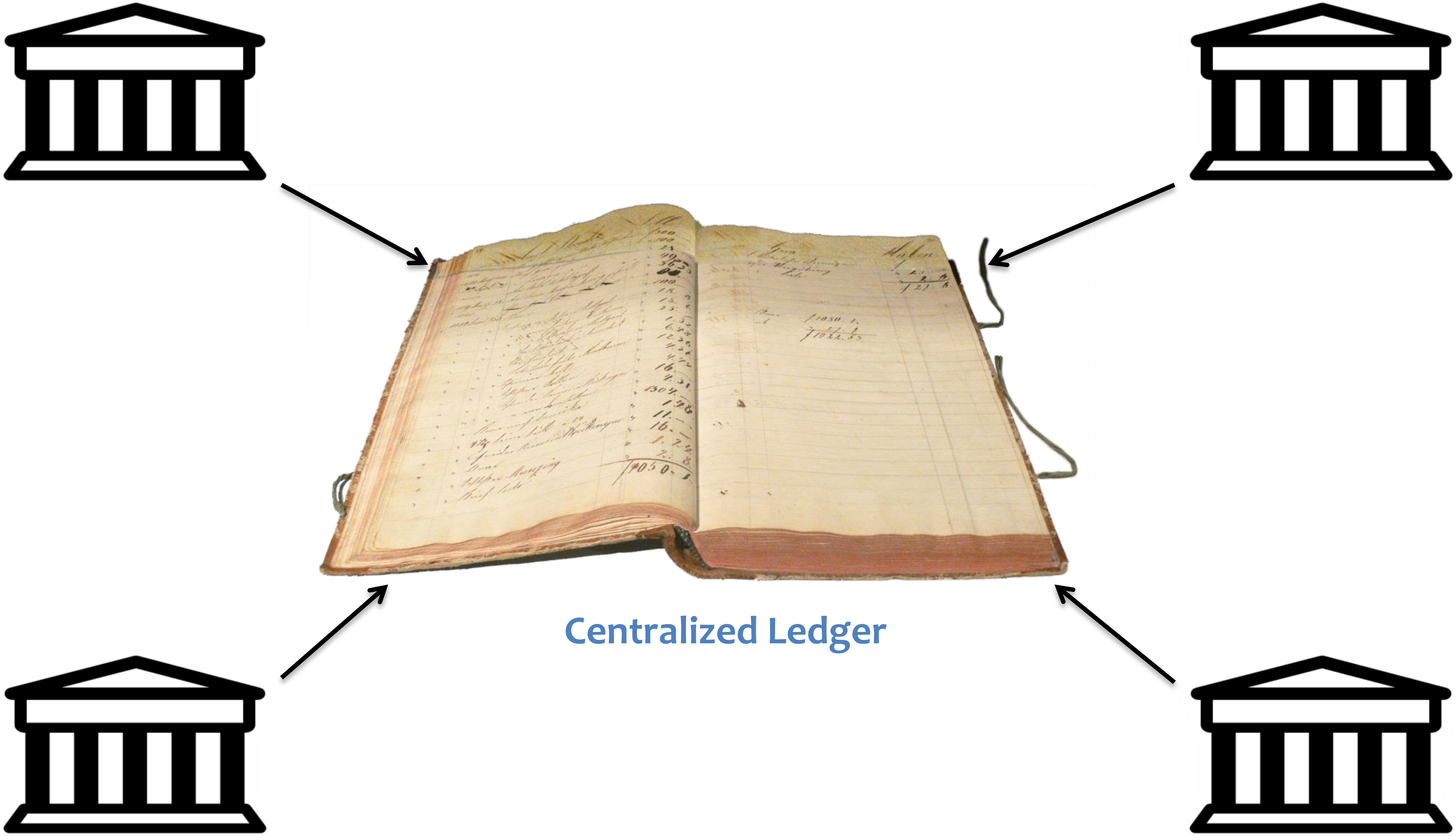
By
Ravi Kishore K,
C-DAC, Hyderabad.

What is Not a Blockchain

- Blockchain is **NOT a cryptocurrency**
- Blockchain is **NOT a programming language**
- Blockchain is **NOT a cryptographic codification**.

"Blockchain is the technology. Bitcoin is merely the first mainstream manifestation of its potential" — Marc Kenigsberg.

Legacy Ledgers

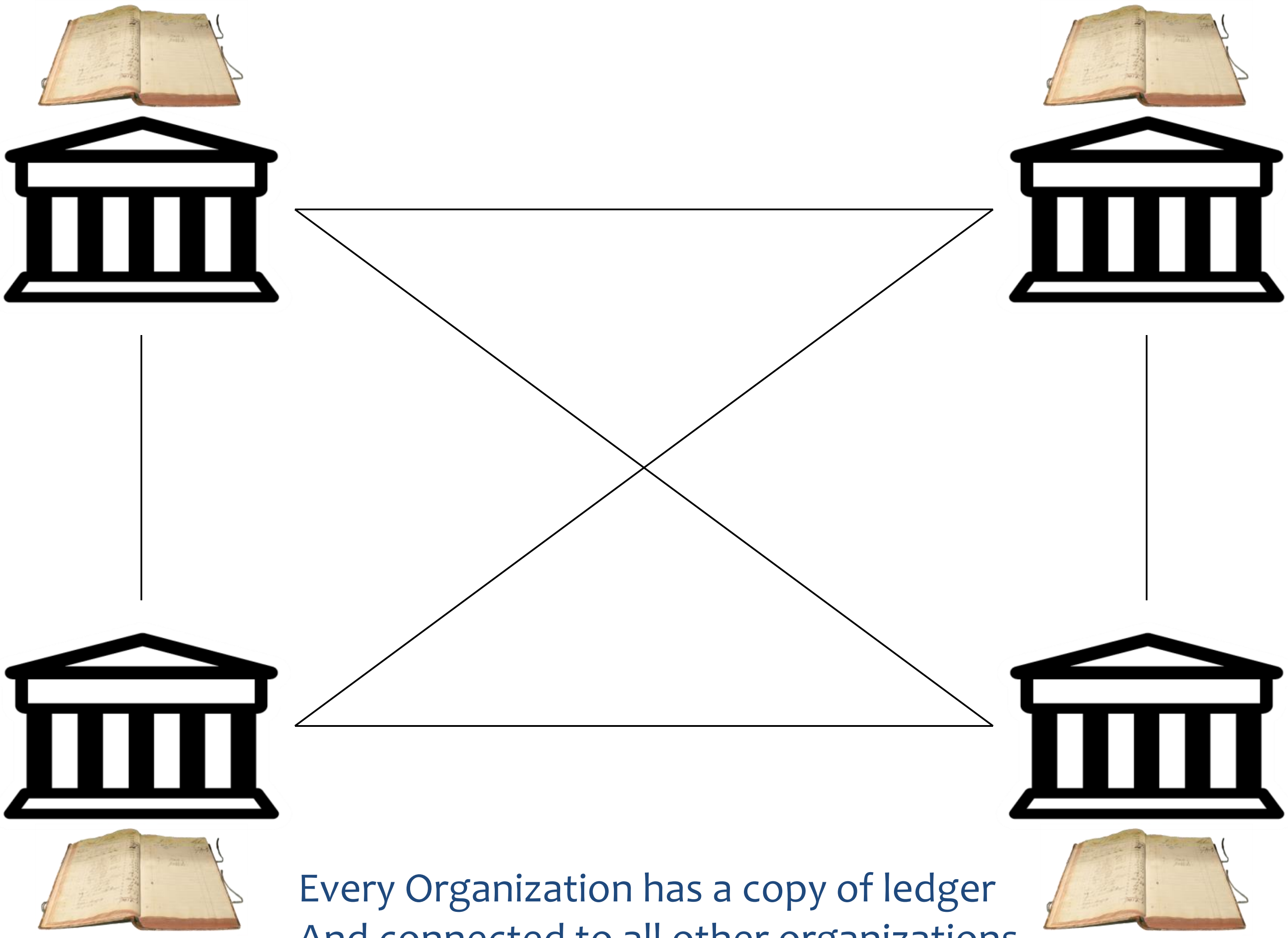


Centralized Ledger

Problems with current business ledgers

- Subject to misuse
- Tamperable
- Lack of transparency
- Inefficient

Distributed Ledger



Every Organization has a copy of ledger
And connected to all other organizations

Distributed Ledger Example

PUBLIC LEDGER

DR GULATI
Rs 1000/-

PUBLIC LEDGER

BUSINESS MAN
Rs 1000/-

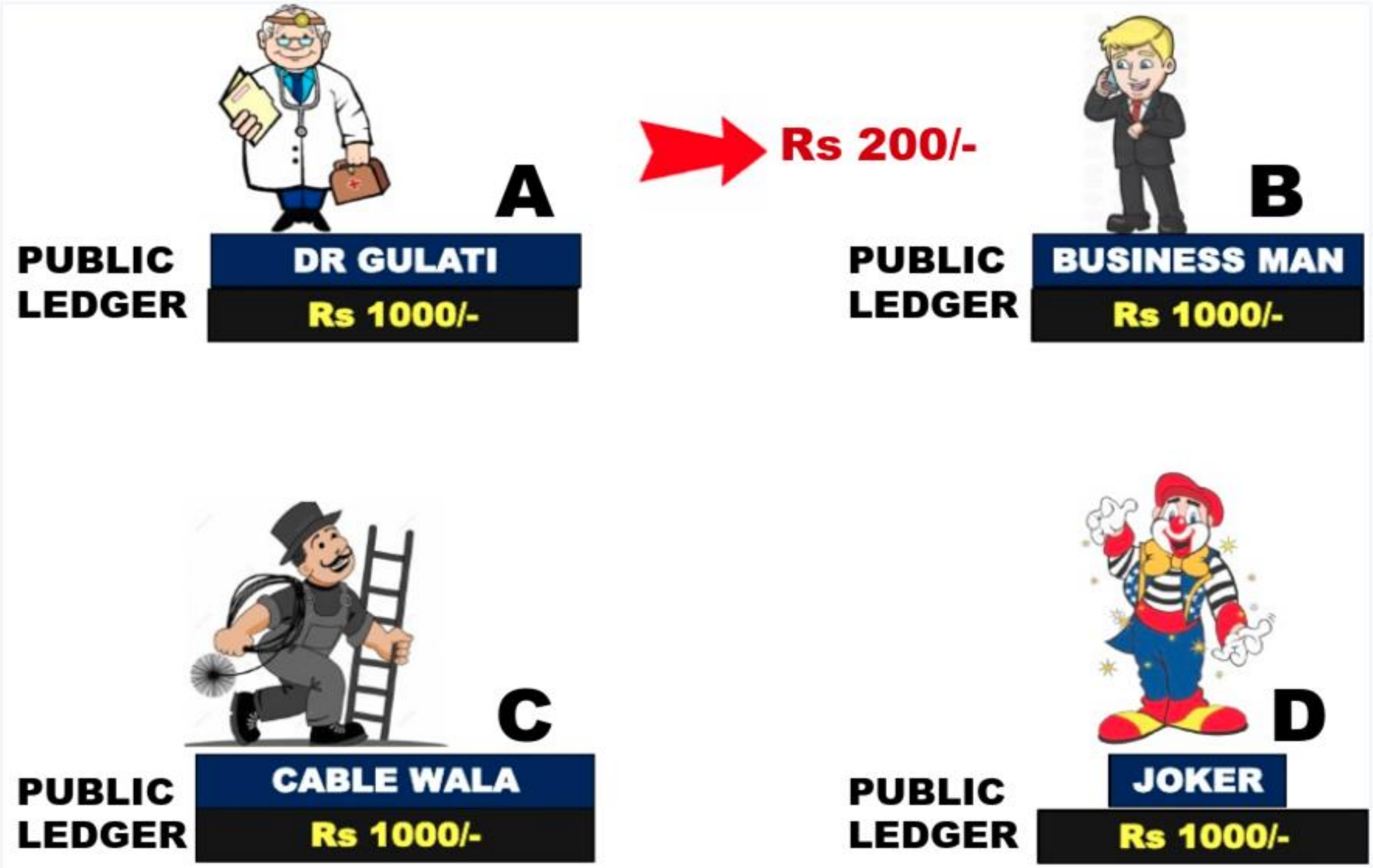
PUBLIC LEDGER

CABLE WALA
Rs 1000/-

PUBLIC LEDGER

JOKER
Rs 1000/-

Distributed Ledger Example



A

Rs 200/-

B

PUBLIC LEDGER

DR GULATI

Rs 1000/-

PUBLIC LEDGER

BUSINESS MAN

Rs 1000/-

C

D

PUBLIC LEDGER

CABLE WALA

Rs 1000/-

PUBLIC LEDGER

JOKER

Rs 1000/-

Distributed Ledger Example

PUBLIC LEDGER

DR GULATI

Rs 1000/-

A>B Rs 200

PUBLIC LEDGER

BUSINESS MAN

Rs 1000/-

A>B Rs 200

PUBLIC LEDGER

CABLE WALA

Rs 1000/-

A>B Rs 200

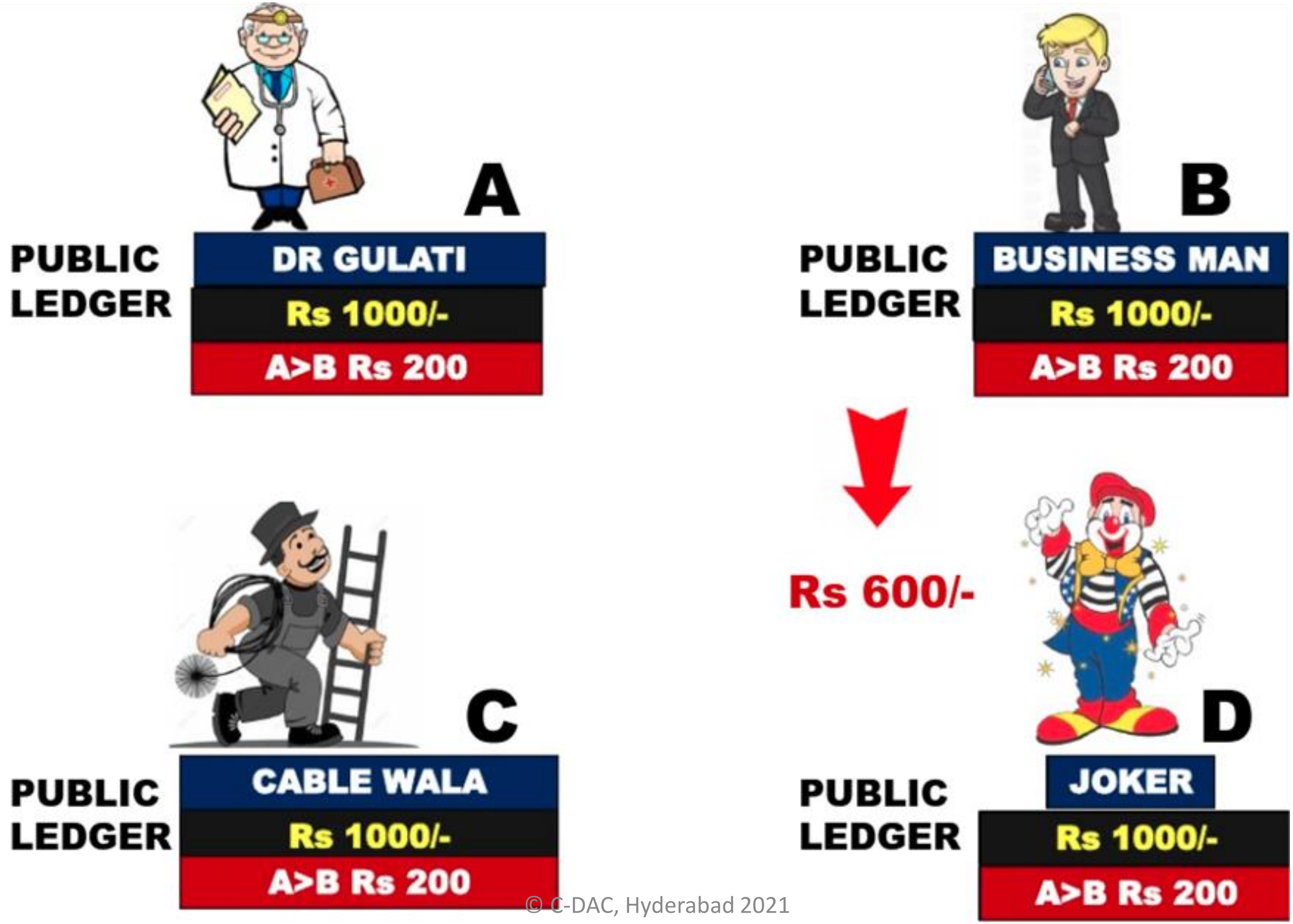
PUBLIC LEDGER

JOKER

Rs 1000/-

A>B Rs 200

Distributed Ledger Example



A

PUBLIC LEDGER

DR GULATI

Rs 1000/-

A>B Rs 200

B

PUBLIC LEDGER

BUSINESS MAN

Rs 1000/-

A>B Rs 200

Rs 600/-

C

PUBLIC LEDGER

CABLE WALA

Rs 1000/-

A>B Rs 200

D

PUBLIC LEDGER

JOKER

Rs 1000/-

A>B Rs 200

Distributed Ledger Example

A

PUBLIC LEDGER

DR GULATI
Rs 1000/-
A>B Rs 200
B>D Rs 600

B

PUBLIC LEDGER

BUSINESS MAN
Rs 1000/-
A>B Rs 200
B>D Rs 600

C

PUBLIC LEDGER

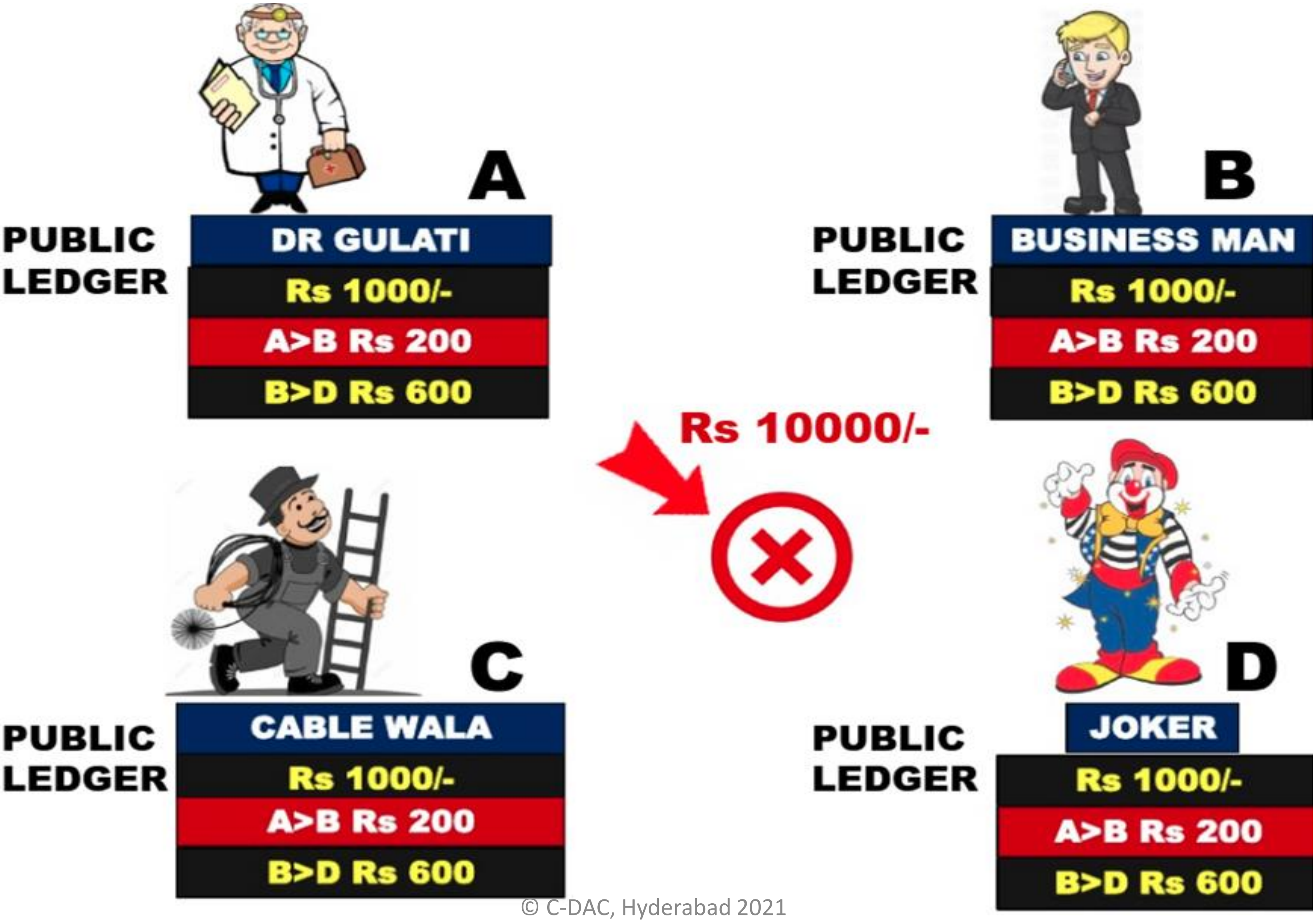
CABLE WALA
Rs 1000/-
A>B Rs 200
B>D Rs 600

D

PUBLIC LEDGER

JOKER
Rs 1000/-
A>B Rs 200
B>D Rs 600

Distributed Ledger Example



A

PUBLIC LEDGER

DR GULATI

Rs 1000/-

A>B Rs 200

B>D Rs 600

B

PUBLIC LEDGER

BUSINESS MAN

Rs 1000/-

A>B Rs 200

B>D Rs 600

Rs 10000/-

C

PUBLIC LEDGER

CABLE WALA

Rs 1000/-

A>B Rs 200

B>D Rs 600

D

PUBLIC LEDGER

JOKER

Rs 1000/-

A>B Rs 200

B>D Rs 600

Blockchain is a
Distributed **Ledger,**
has a network of replicated databases,
Synchronized via Internet,
visible to all network participants

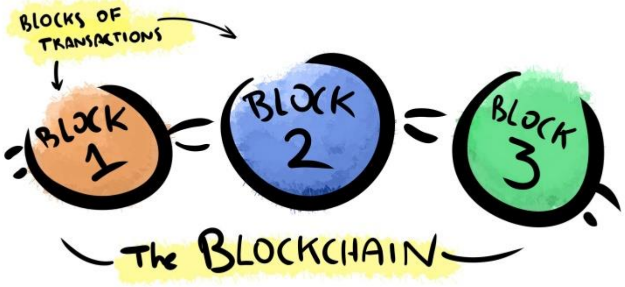
Blockchain in a nutshell

- Many computers are connected in a network without any hierarchy (peer to peer network)

- These computers verify all transactions one by one

- A set of Verified transactions over a time period are added in a “Block (similar to a page in ledger book)” of information

- All the Blocks are chained cryptographically and downloaded onto each computer



How to Sync distributed copies of Ledgers ???

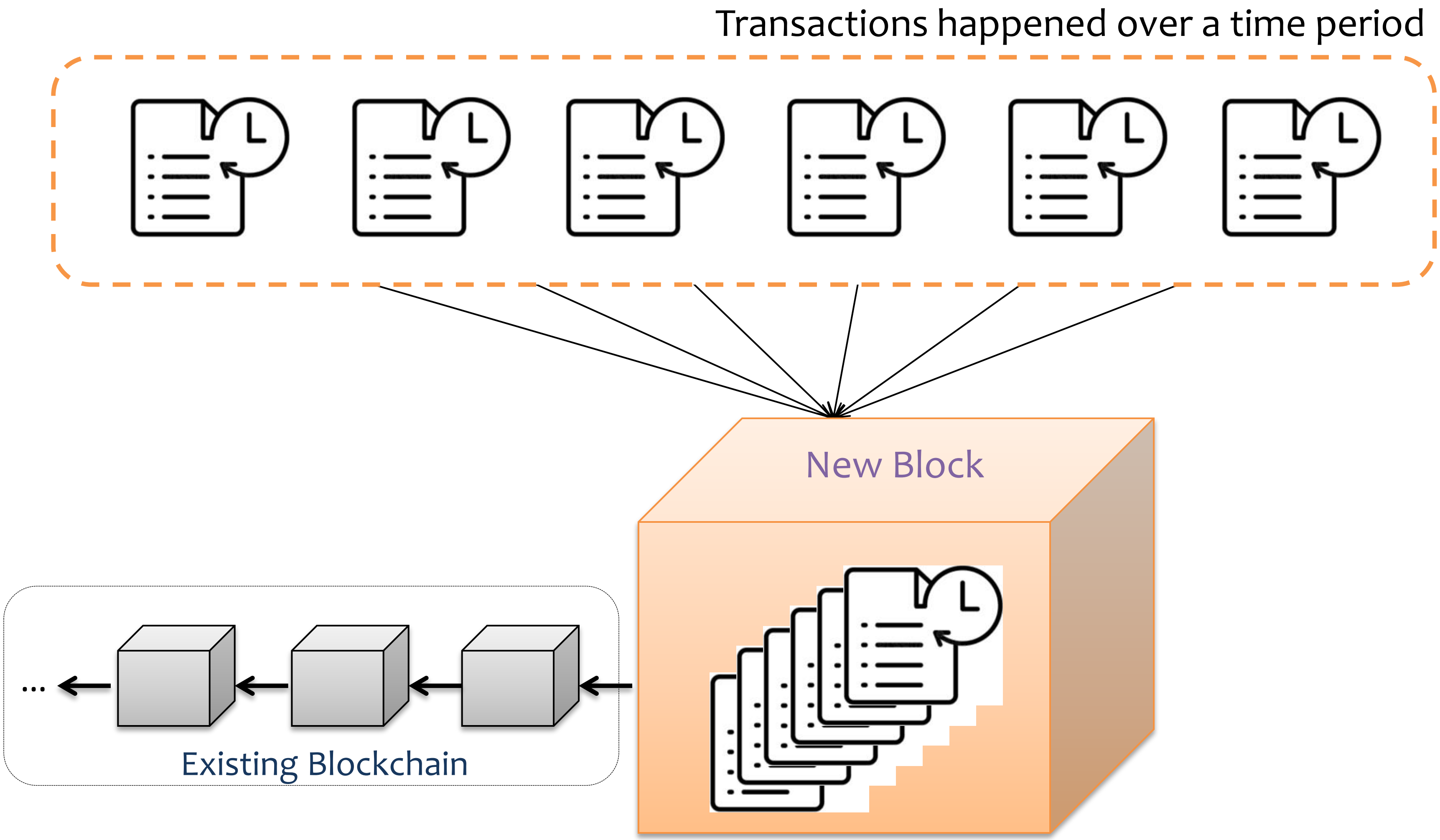
Consensus

- Instead of relying on a third party to mediate transactions, members in the Blockchain network uses a **consensus protocol** to agree on ledger content

- **Consensus** ensures that the shared ledgers are exact copies in all the nodes of distributed systems

- For updating the distributed ledger, consensus is required among the participants of the network
    - Ensures No Malicious Transactions nor Changes can be made on the distributed network

How Blockchain Creates a New Block?



Transactions

- The Blockchain records transactions and what gets transferred is the control of digital asset

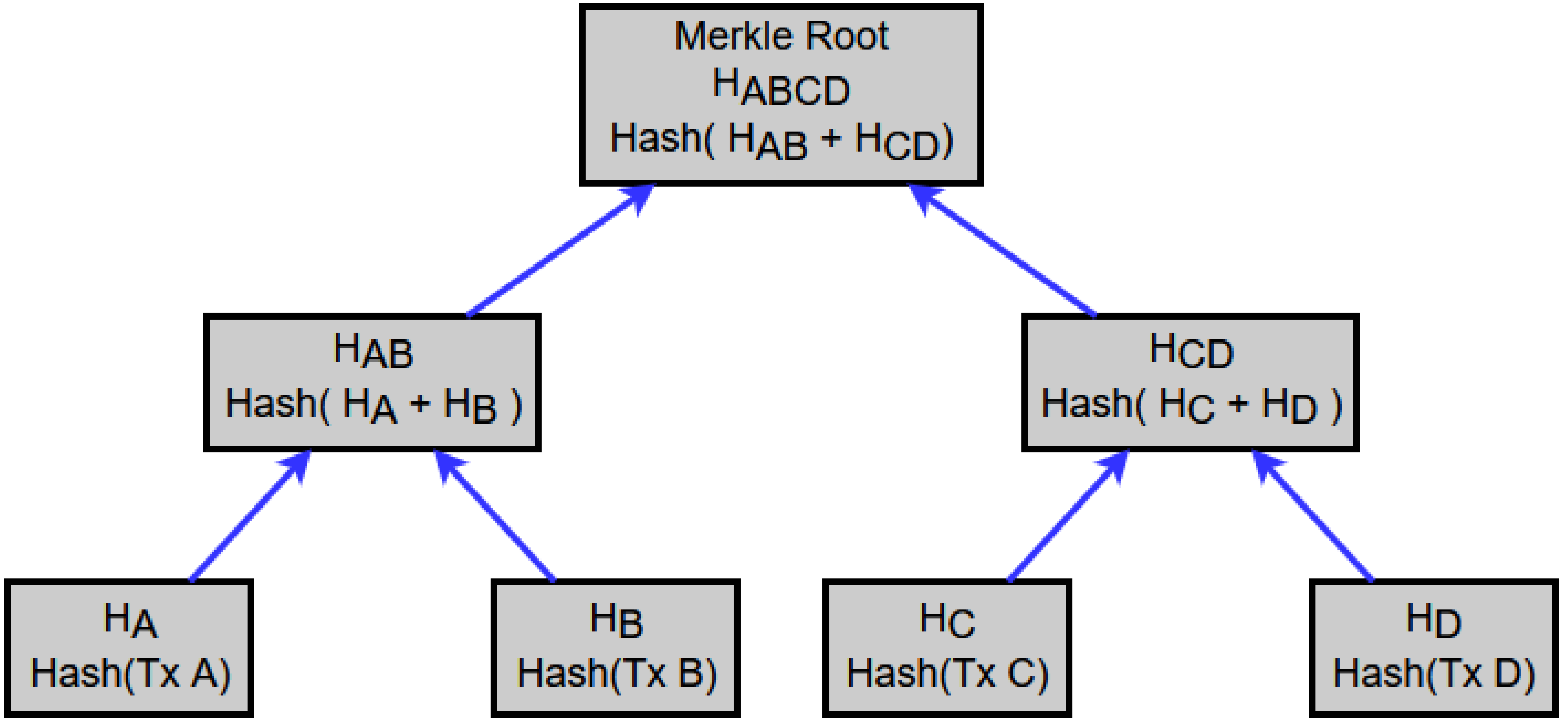
- This control comes through use of cryptography

- When a digital asset is exchanged, it is placed under the control of a specific public-private key pair

- If someone is able to prove that he has the private key matching the public key, the Blockchain network lets him control the digital asset

- If the private key is lost there is no recoverability!

Merkle Tree



Merkle Root
H_{ABCD}
Hash(H_{AB} + H_{CD})

H_{AB}
Hash(H_A + H_B)

H_{CD}
Hash(H_C + H_D)

H_A
Hash(Tx A)

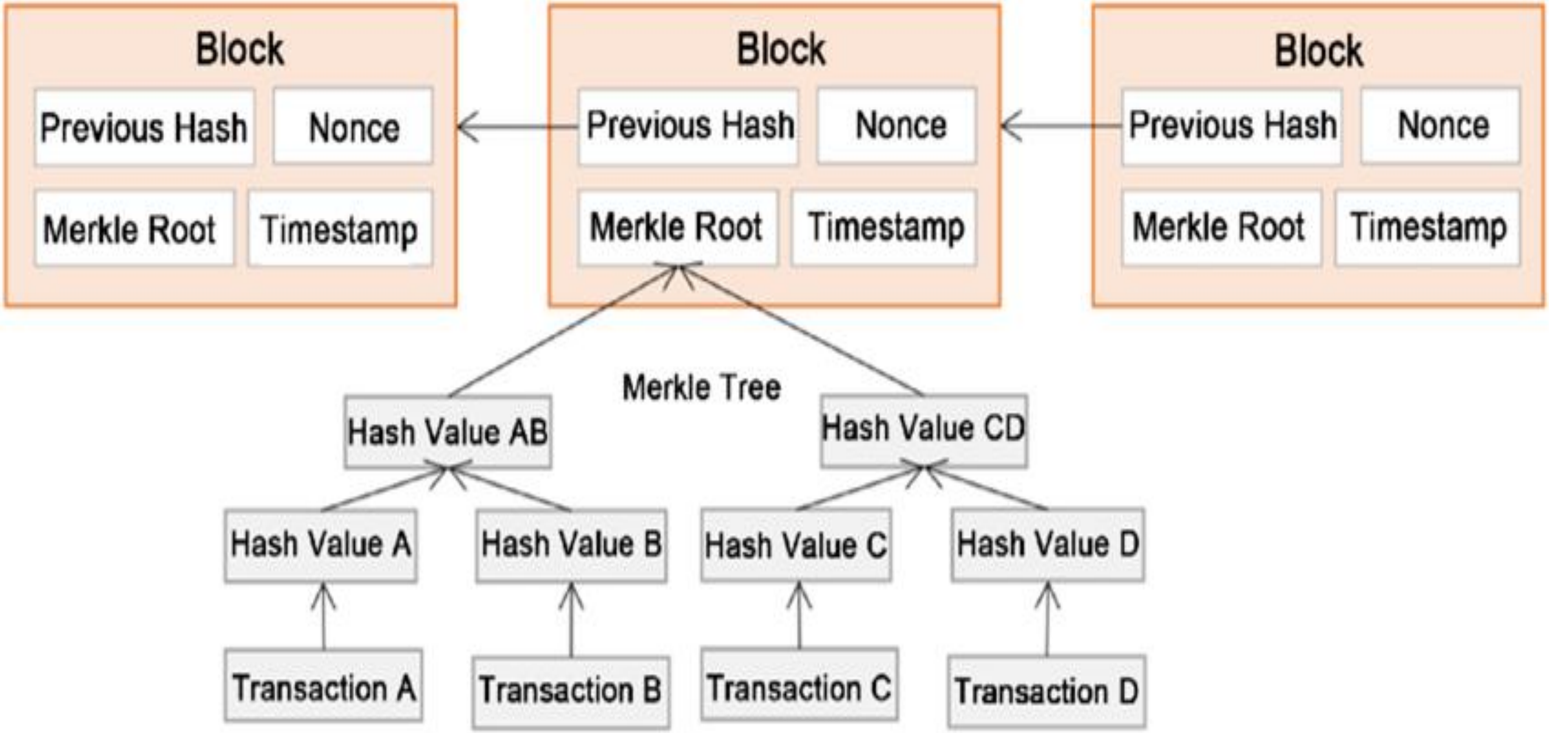
H_B
Hash(Tx B)

H_C
Hash(Tx C)

H_D
Hash(Tx D)

Each block in the Blockchain contains summary of all the transactions in the block using merkle tree

Merkle Tree in Blockchain

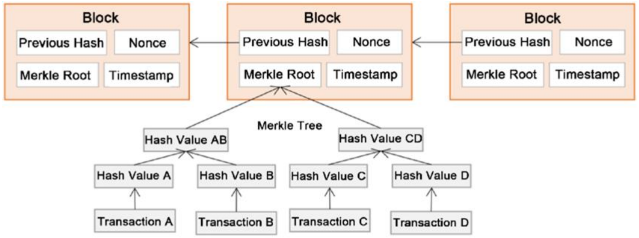


How it provides Security??

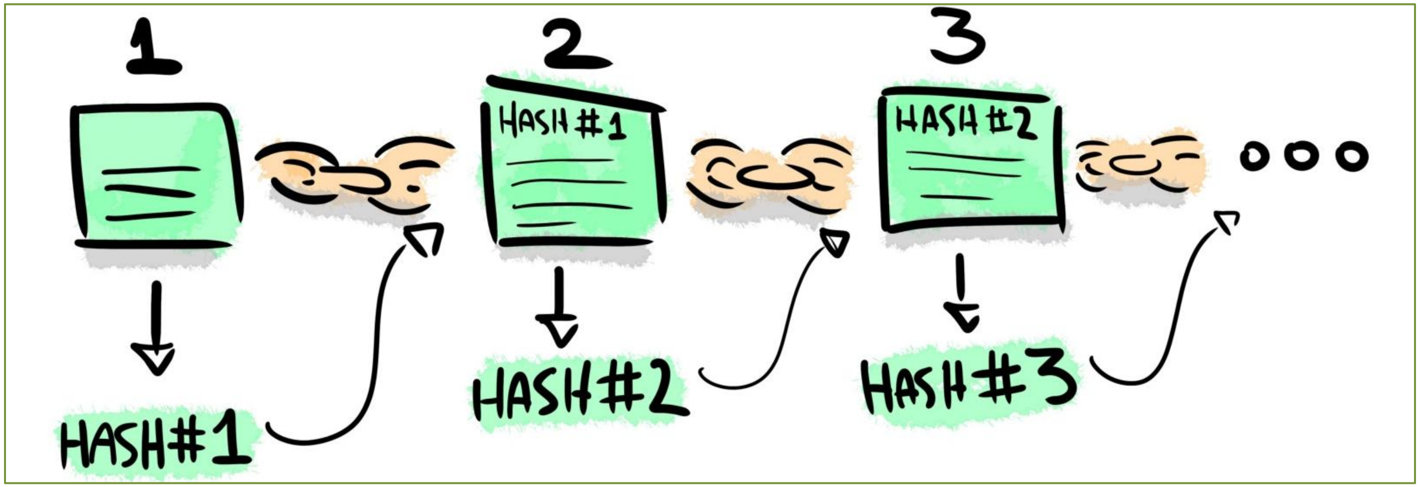
- Metadata in turn, contains Merkel Root of Transaction data

- Change the metadata, block hash will change - leads to broken chain

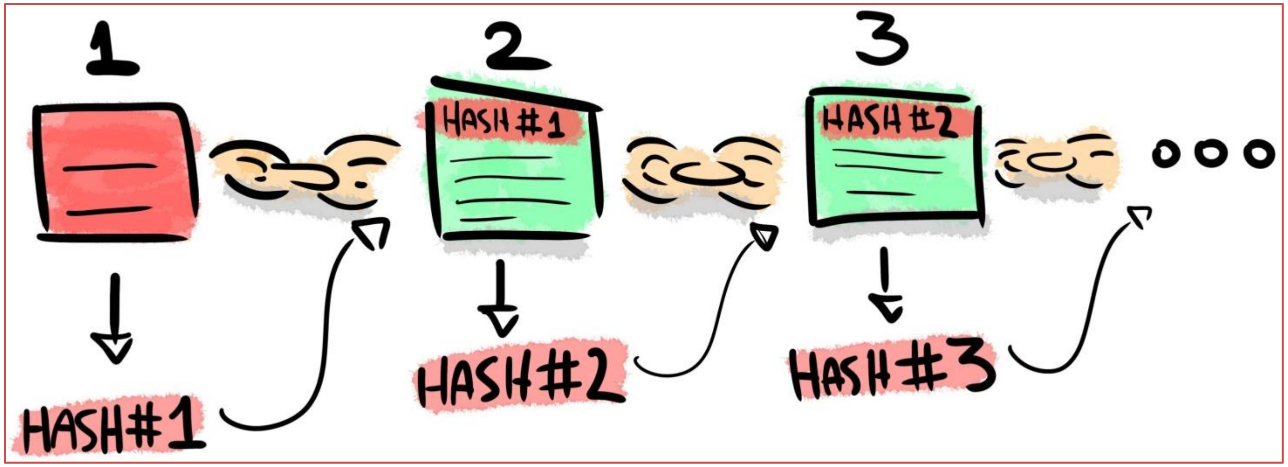
- Change the details of a transaction, the merkle root will change, which in turn changes the metadata hash, which will change the block id



Detect Tampering from Chain of Blocks



If Txn #1 is modified



What makes Blockchain Unique?

- **Decentralized: B**lockchains are managed by a network of nodes rather than a central authority
- **Transparent:** Transactions on a Blockchain are stored on the Blockchain across nodes, all participants can view transactions on the network in real-time
- **Immutable:** Blockchains are designed to enable permanent record keeping (with the help of Cryptographic chains) so that stored data cannot be altered after being added
- **Secure:** It is hard to change or destroy block chains because of its distributed nature

Features and Benefits

- Assurance related to data stored in Blockchain with respect to:
  - ➢ Immutability
  - ➢ Integrity
  - ➢ Authenticity
  - ➢ Verifiability
  - ➢ Accountability
- Malware Resistant

Blockchain Adoption Scenario

- FedEx - Supply chain management
- IBM
  - Supply chain management for walmart
  - Blockchain trade finance platform for Bank of Montreal (BMO), CaixaBank, Commerzbank, Erste Group, and the United Bank of Switzerland (UBS).
- Microsoft – Blockchain as a Service
- NASA - To Use Hyperledger Blockchain For Air Traffic Management
- Sweden - Land Registration
- MasterCard - Blockchain based payment gateways
- Bank of America - Banking Transactions
- JAPAN - Processing Government Tenders
- DHL-Accenture - Pharmacy
- Airbus and Lufthansa - Aviation; for tracking jet plane parts
- Lufthansa - Blockchain-based travel app for users with Winding Tree
- Air France - supply chain and to track workflows within aircraft maintenance systems

Potential Application Domains

- e-Governance
- Supply chain management
- e-voting
- Healthcare
- Financial Services
- Auditing & Compliance
- High Valued Asset Tracking
- Document Notarization System
- Access Auditing
- Log Management and etc…

Thank You

Contact us at:
cdacchain@cdac.in