Cryptocurrency

Rupesh Mishra

Introduction to Blockchain

1. Bitcoin, Altcoin, and Tokens
2. Cryptocurrency usage
3. Transactions in Blockchain
4. UTXO Model
5. double spending problem

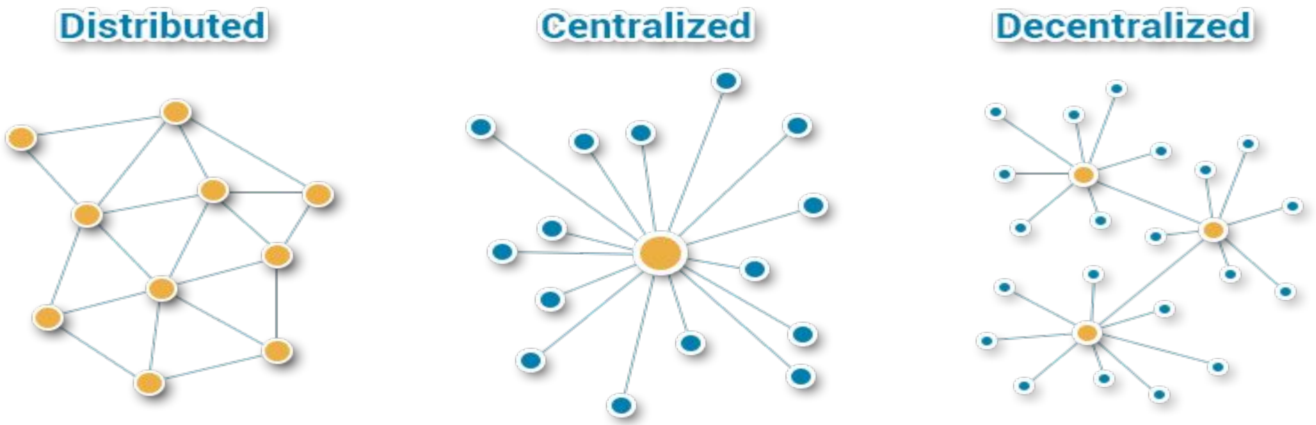
1. Consensus in Bitcoin,
2. Life of a miner
3. Mining Difficulty
4. Mining Pool
5. Mining Methods

Bank - The Gatekeeper of Financial World

- **Intermediary**
  - ✓ Transaction Fee
- **Expensive**
  - ✓ Security
  - ✓ Backoffice
- **Accessibility**
  - ✓ Elite class vs Lower class
- **Centralised**
  - ✓ Fraudulent Activity
  - ✓ Security Breach
- **Transparency**
  - ✓ Loan and Investments

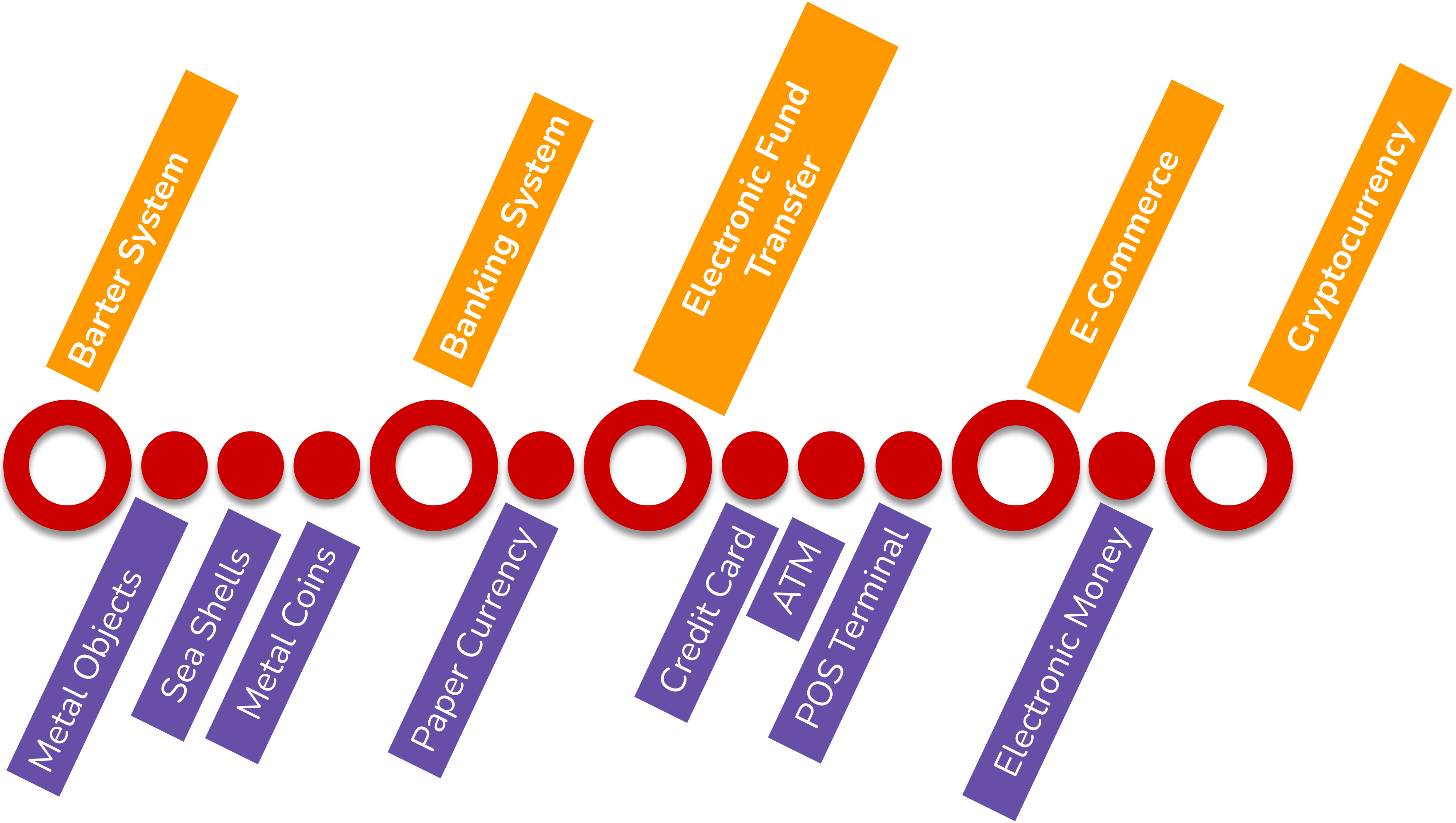
- **2008**
- **Financial Crisis**
- **Requirements**
  - ✓ Direct transfer of money
    - ■ No intermediary fees
    - ■ No intermediary validation
  - ✓ Without central authority
    - ■ Maintaining value of money
- **Transparency**
- **Privacy**
- **Cryptocurrency**

Decentralised Network



- No central authority
- Self-Regulated
- P2P network architecture

- Every node is equal
  - ✓ In the hierarchy
  - ✓ To maintain the database



Barter System

Metal Objects

Sea Shells

Metal Coins

Banking System

Paper Currency

Electronic Fund Transfer

Credit Card

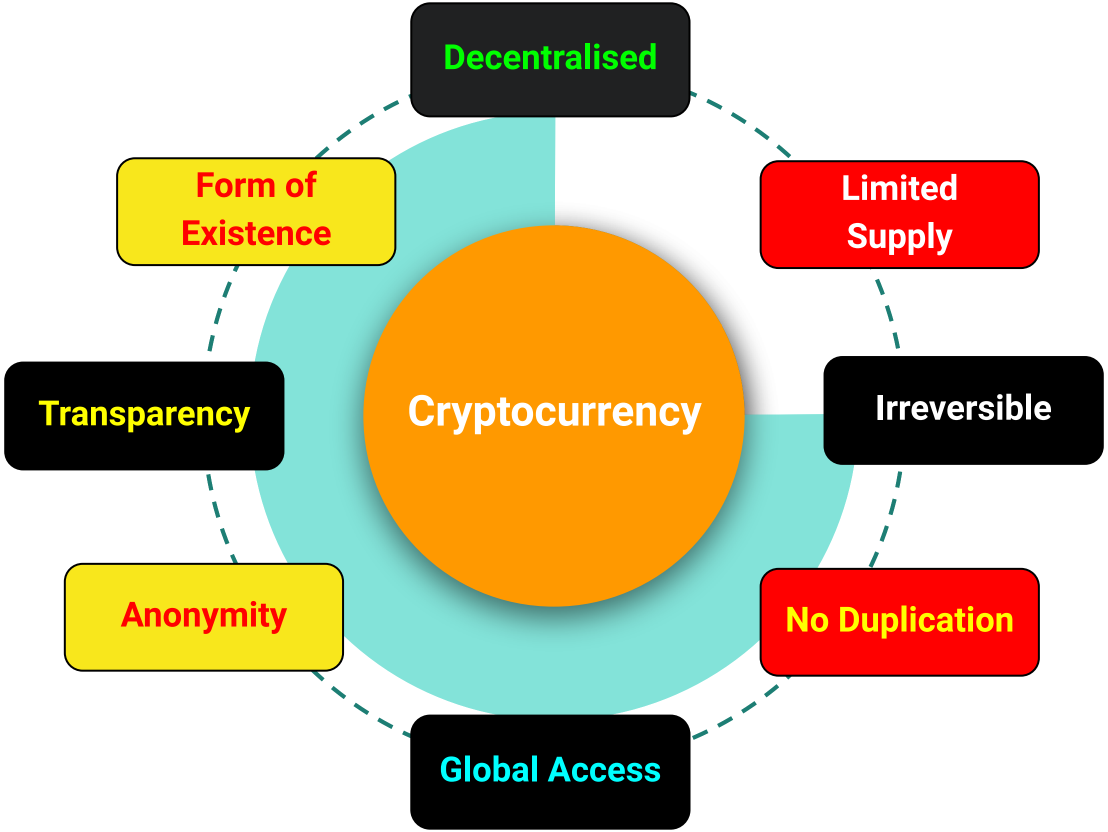
ATM

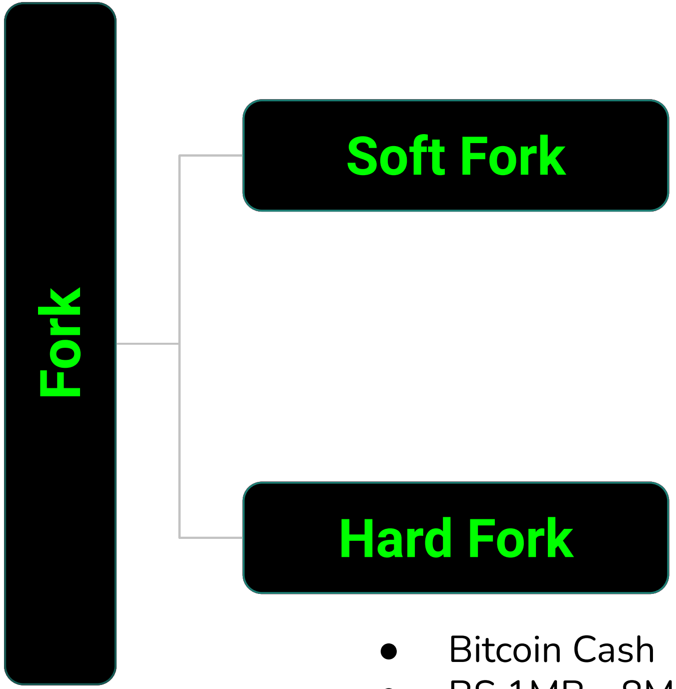
POS Terminal

E-Commerce

Electronic Money

Cryptocurrency


Decentralised
Limited Supply
Irreversible
No Duplication
Global Access
Anonymity
Transparency
Form of Existence
Cryptocurrency



Fork

Soft Fork

Hard Fork

- Bitcoin Cash
- BS 1MB - 8MB

- **Fork**
  - ✓ **Creates alternative version of Blockchain to add new features and functionality in the Blockchain Network**
    - ■ Upgrade
    - ■ New governance rulle
  - ✓ **Hard Fork**
    - ■ Radical Changes to Protocol
    - ■ No Backward compatible
    - ■ Node Upgrade to Participate
      - Old rules are Invalid
  - ✓ **Soft Fork**
    - ■ Backward Compatible
      - Old software recognise the blocks with new protocol
    - ■ Node upgrade not required
      - Old and new rules are maintained

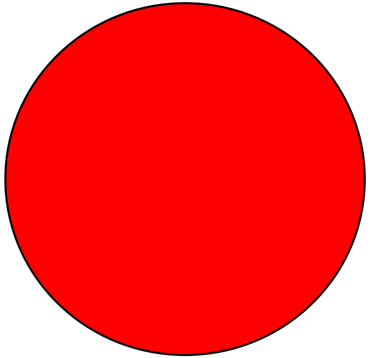
- **Bitcoin**
  - ✓ Represents Digital Currency
  - ✓ First
  - ✓ Having its own
    - ■ Value
    - ■ Blockchain
    - ■ Protocol
- **Source of Payment**
- **bitcoin**

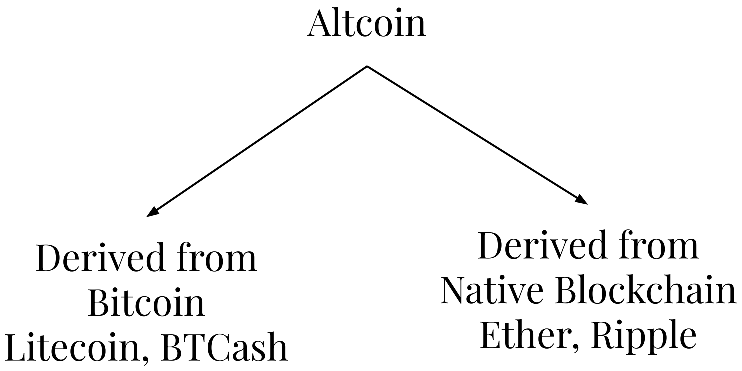
- **Altcoin**
  - ✓ Represents Digital Currency
  - ✓ After Bitcoin
  - ✓ Having its own
    - ■ Value
    - ■ Blockchain
    - ■ Protocol
- **Source of Payment**
- **Litecoin, DOGE**

- **Token**
  - ✓ Represents Digital Asset
  - ✓ Project Specific
  - ✓ Operate on others blockchain
  - ✓ ERC-20
- **Project Specific**
- **Multipurpose**

Cryptocurrency

LITECOIN
DIGITAL DECENTRALIZED PEER TO PEER
DIGITAL DECENTRALIZED PEER TO PEER
LTC



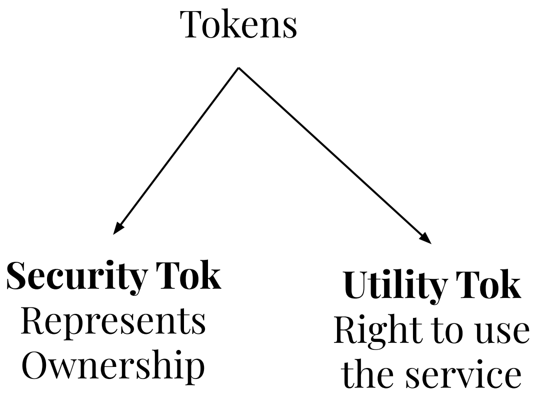


Altcoin

Derived from
Bitcoin
Litecoin, BTCash

Derived from
Native Blockchain
Ether, Ripple

Bitcoin



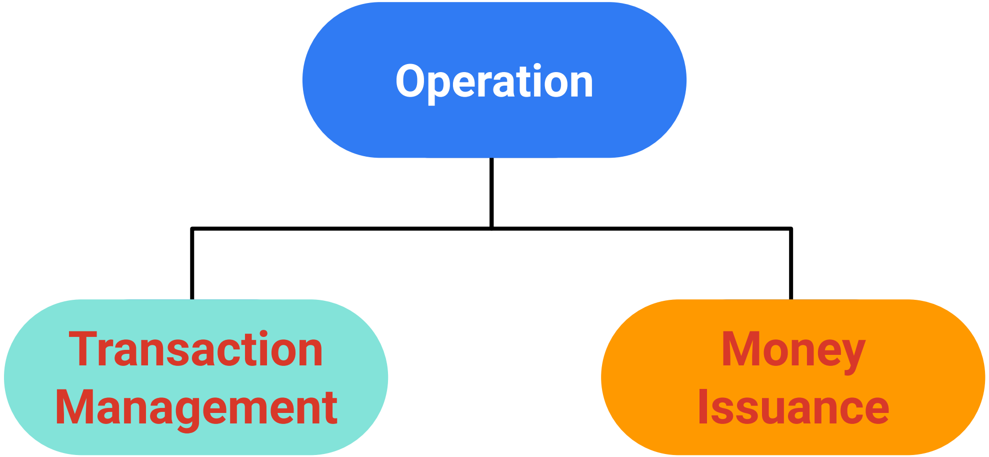
Tokens

Security Tok
Represents
Ownership

Utility Tok
Right to use
the service

Bitcoin

- Decentralised digital currency
- Instant Payment to anyone
- Cross country payment system
- No control of Governments
- Decentralised peer to peer network
- Temper proof



Bitcoin Creation

- **Limited and Controlled Supply**
- **New currency generated**
  - ✓ Mining
  - ✓ Miner receives for new block
- **Rate adjustment**
  - ✓ 2016 Block
  - ✓ Geometric Reduction with 50% for every 210000 blocks

- **With increase in time less bitcoins generated**
- **Less reward received by miner**
- **21 Million Bitcoin**
- **Transaction Fees**
  - ✓ Increase
  - ✓ Users

Sending Payment

- **Other person can not spend bitcoin owned by another person**
  - ✓ Public Key Cryptography
  - ✓ Digital Signature
  - ✓ ECDSA
  - ✓ Bitcoin address associated with key pair

- **To send bitcoin from user A to B**
  1. Address of User B is sent
  2. Creates Transection
  3. Add address of A and B along with amount of bitcoin
  4. Sign Transection with Pr Key
  5. Announce public key for validation
  6. Broadcast transection in the network

Transection

● Amount	● 50 BTC
● Receiver of Payment	● Bob
● Sender of Payment	● Alice
● Sender Authorization	● Signature of Alice
● Tx: A -> B 5BTC	● What to sign?

Account Based model

- **Alice : 10Eth**
- **Bob : 5 Eth**
- **Tx: A -> B 2 Eth**
- **Alice : 8 Eth**
- **Bob : 7 Eth**
- **Stores List of Account and Balance**
- **Transaction is Valid if Account has sufficient Balance**
- **Debit amount from Sender Account**
- **Credit amount to Receiver Account**

UTXO

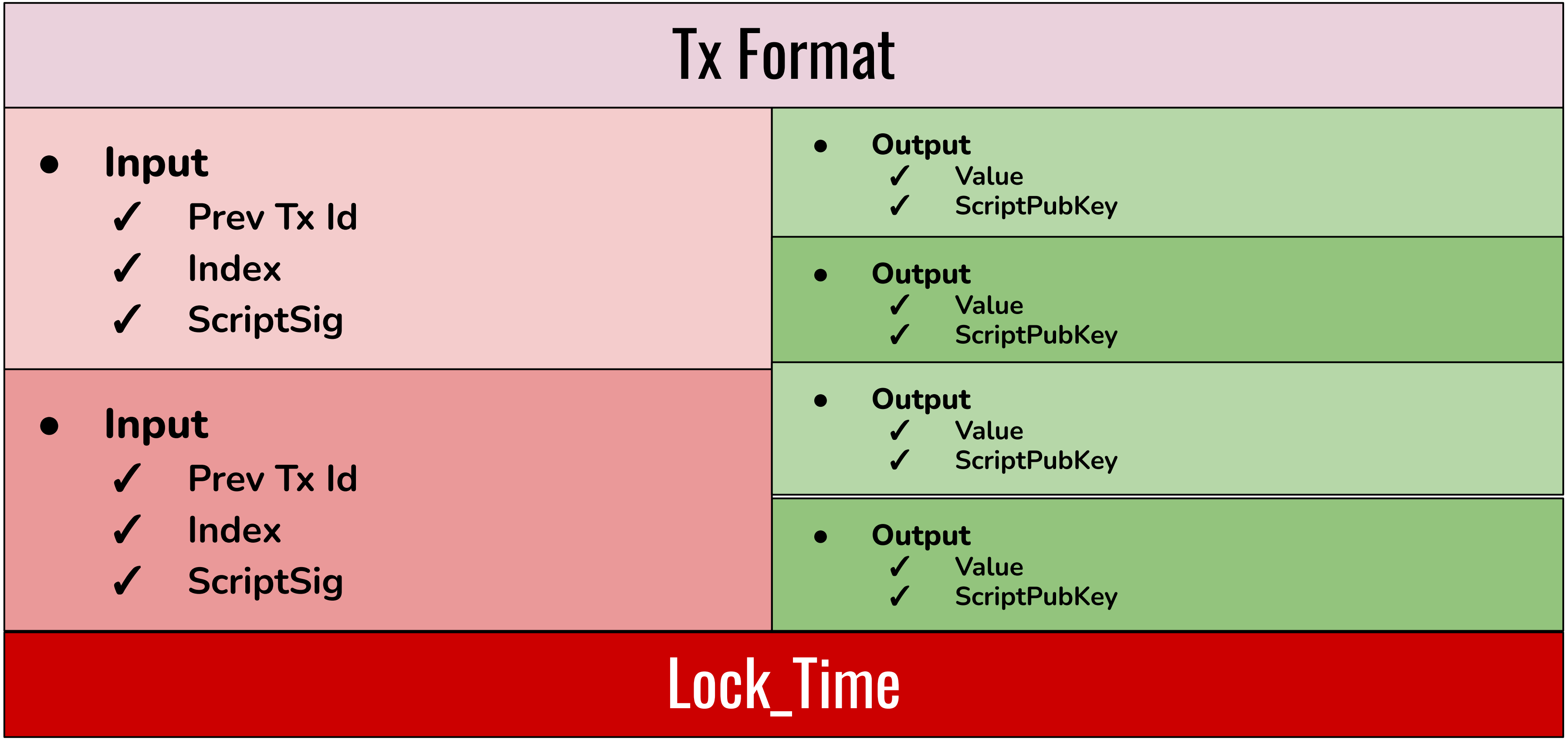
- **All coins are different**
- **During Transaction**
  - ✓ Specific coin is spent
  - ✓ Old Coin consumed and Destroyed
  - ✓ New coin created
- **Coin can be spend only once**
- **E.g. Alice owns 7 BTC**
- **Tx: [1: A -> B 5 BTC] [2: A -> A 2 BTC]**
- **Old 7 BTC is destroyed and new “5 BTC and 2 BTC” coins are created**

Tx Format

- **Input**
  - ✓ Prev Tx Id
  - ✓ Index
  - ✓ ScriptSig

- **Output**
  - ✓ Value
  - ✓ ScriptPubKey

Lock_Time



Tx Format

- **Input**
  - ✓ Prev Tx Id
  - ✓ Index
  - ✓ ScriptSig
- **Input**
  - ✓ Prev Tx Id
  - ✓ Index
  - ✓ ScriptSig

- **Output**
  - ✓ Value
  - ✓ ScriptPubKey
- **Output**
  - ✓ Value
  - ✓ ScriptPubKey
- **Output**
  - ✓ Value
  - ✓ ScriptPubKey
- **Output**
  - ✓ Value
  - ✓ ScriptPubKey

Lock_Time

Transaction format

- **Previous Transaction ID**
  - ✓ Output of previous transaction stored in UTXO
- **Index**
  - ✓ Specific part of output of previous Transaction
- **Prev and Index are unique identifier of a Output**
- **Coin**
  - ✓ Output of Transaction

- **Script Sig**
  - ✓ Authorization of owner of coin
- **Value**
  - ✓ Coin Amount
  - ✓ Satoshi
- **ScriptPubKey**
  - ✓ Condition on which coin can be redeemed
  - ✓ E.g. PubKey of Bob
- **ScriptSig**
  - ✓ Satisfying the condition

Transection

- **ScriptPubKey is predicate**
- **ScriptSig satisfy the predicate**
- **To spend a coin**
  - ✓ Produce Satisfying ScripSig
- **Anyone who can produce satisfying ScriptSig can spend money/coin**
- **Input and Output are Independent**

- **Double Spending**
  - ✓ Validation by node
  - ✓ Consensus Rule
    - ■ Sum(Input) >= Sum(Output)
    - ■ Fees
    - ■ Evaluation of ScriptSig and ScriptPubKey is correct
    - ■ Output is not already spent
    - ■ Lock Time
- **Coinbase Tx(Exception)**
    - ■ First Transaction
    - ■ No Input
    - ■ Block Reward and Fees

UTXO Model

- **Unspent Transaction Output**
- **Cryptocurrency remains after transection**
- **Transaction Component**
  - ✓ Input
  - ✓ Output
- **Transaction Complete**
  - ✓ UTXO recorded as Input

- **Anonymity**
- **Transparency**
- **Track ownership of all portions of cryptocurrency**
- **UTXOs are associated with the public addresses visible to the entire network**
- **Bitcoin uses UTXO**

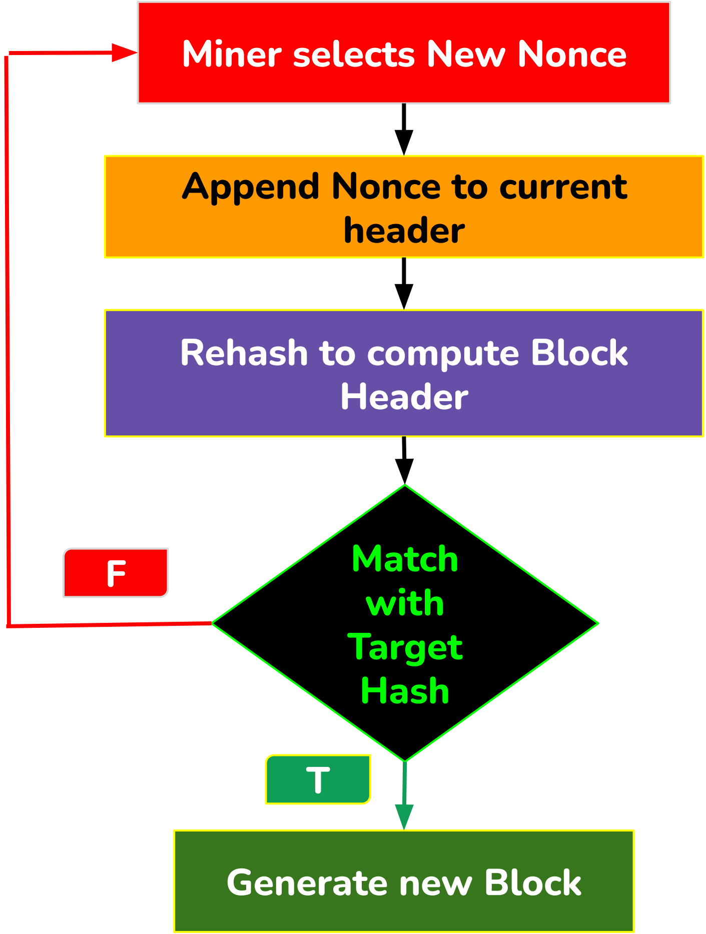
Crypto Mining

- **Miners**
  - ✓ Generate wealth
  - ✓ Technical Knowledge
  - ✓ Setting up computing software and equipment
- **Blockchains with various mining techniques.**
  - ✓ Consensus algorithm
  - ✓ Incentive system.

- **Types of Miners**
  - ✓ Solo Miners
  - ✓ Pool Miners
- **Types of mining (processors or equipment)**
  - ✓ CPU Mining
  - ✓ GPU Mining
  - ✓ ASIC Mining
  - ✓ Cloud Mining

New Block Generation using Pow

- **Hash**
  - ✓ Data mapping to fixed size value
  - ✓ Maintain Integrity
  - ✓ Collision resistant and Difficulty
- **Mining**
  - ✓ Special type of node
  - ✓ Calculate new block hash
  - ✓ Helps in maintaining consensus
- **Nonce**
  - ✓ Number used once
  - ✓ Create new block
  - ✓ Validate block hash



Cryptocurrency Safety

- **Best practice in using Exchanges**
  - ✓ Choose regulated exchanges that have safety and security measures in place.
- **Storing Cryptocurrency**
  - ✓ Store your crypto in desktop or mobile wallets (short-term)
  - ✓ Paper and hardware wallets (long-term)
  - ✓ Use standard wallets
- **Transaction Safety**
  - ✓ Study the transaction requirements of a cryptocurrency
  - ✓ Security precautions
- **Enable Security Measures**
  - ✓ Protect wallets and backups with strong passwords.

Link

https://docs.google.com/presentation/d/1m9zMuPMg6twW0SYtApKM5IBccgG7v0VP2kePwD61OvE/edit?usp=sharing

https://docs.google.com/presentation/d/1m9zMuPMg6twW0SYtApKM5IBccgG7v0VP2kePwD61OvE/edit?usp=sharing