Understanding Bitcoin

SIDDHESH V NAIK

ANIL DONGRE

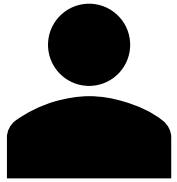
Disclaimer

The opinions presented/stated during this workshop are of the speakers alone.
They are not to be attributed to anyone else.

Bitcoin

Bitcoin: A Peer-to-Peer Electronic Cash System

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution



Satoshi Nakamoto

31st Oct 2008
Paper Published

3rd Jan 2009
System starts with 1 Peer

Today: System running with 13k+ peers distributed worldwide

Course Outline

Lesson 1. The Bitcoin Node

Lesson 2. Forming a Network

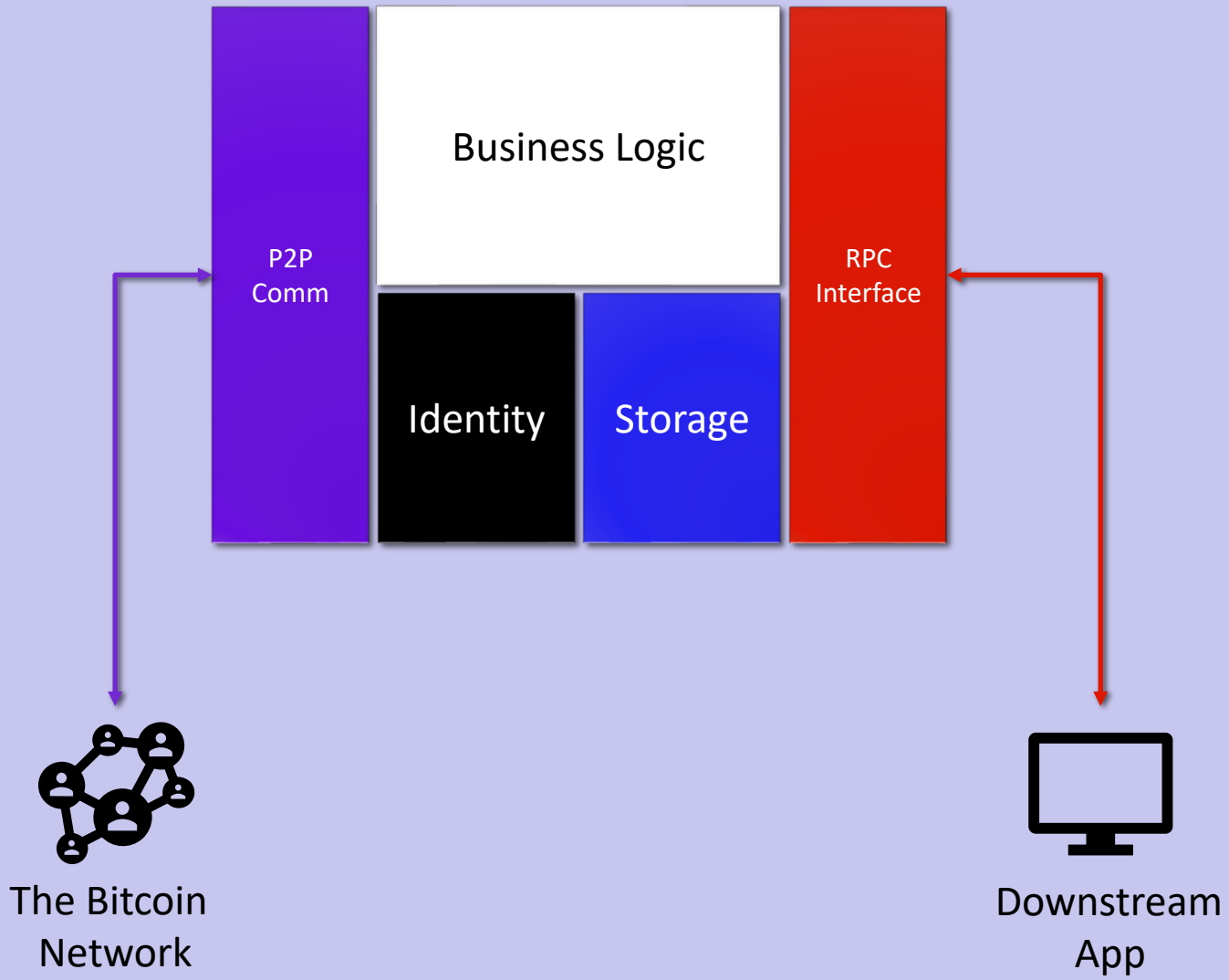
Lesson 3. Wallets

Lesson 4. Transactions

Lesson 5. Transaction Processing

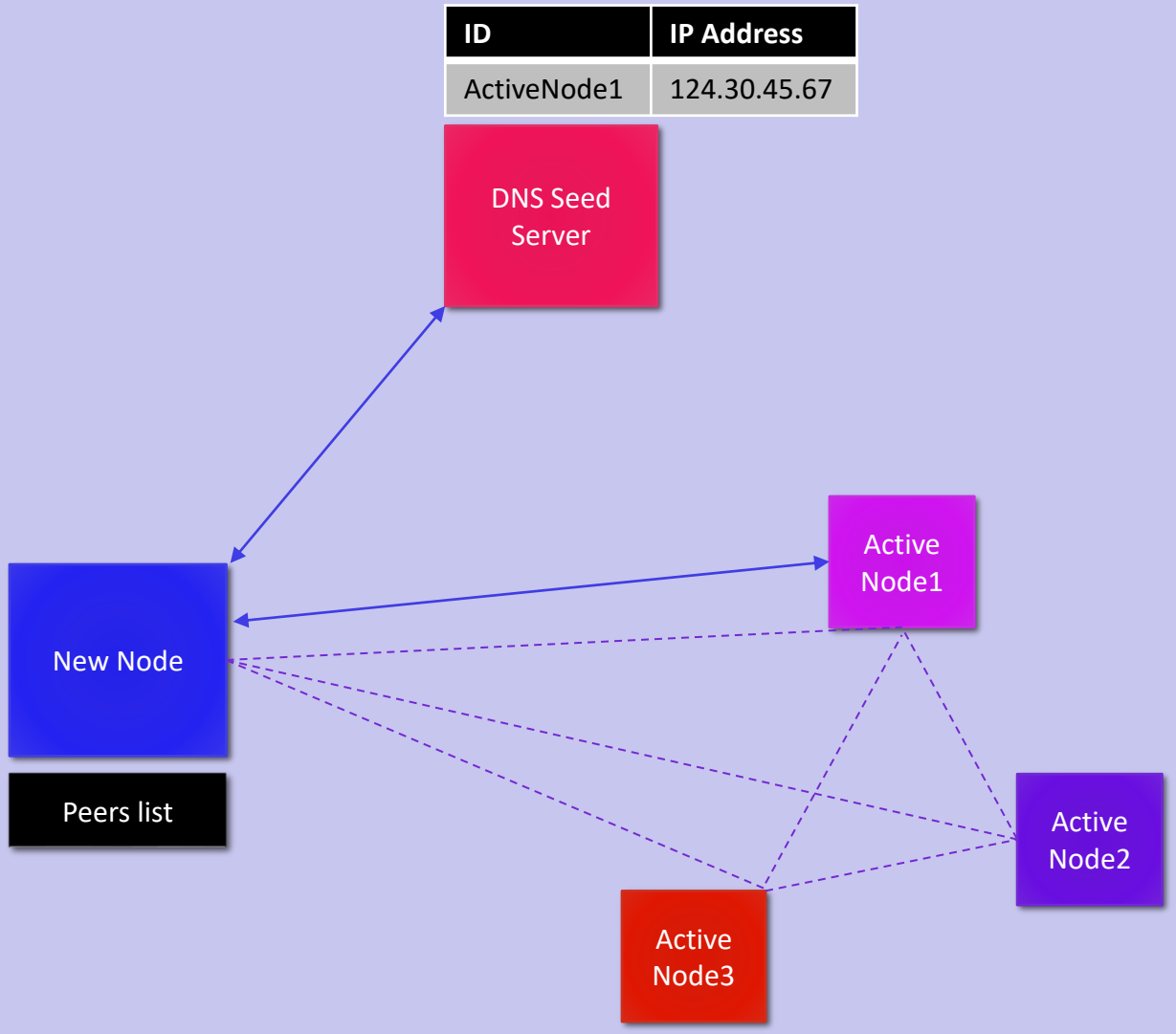
The bitcoin node

- Storage : For maintaining data of all past transactions
- Business Logic : For transaction processing
- P2P Communication : For interaction with other nodes in the network
- RPC Interface : For integration with downstream components
- Identity : Network wide unique identity of the node

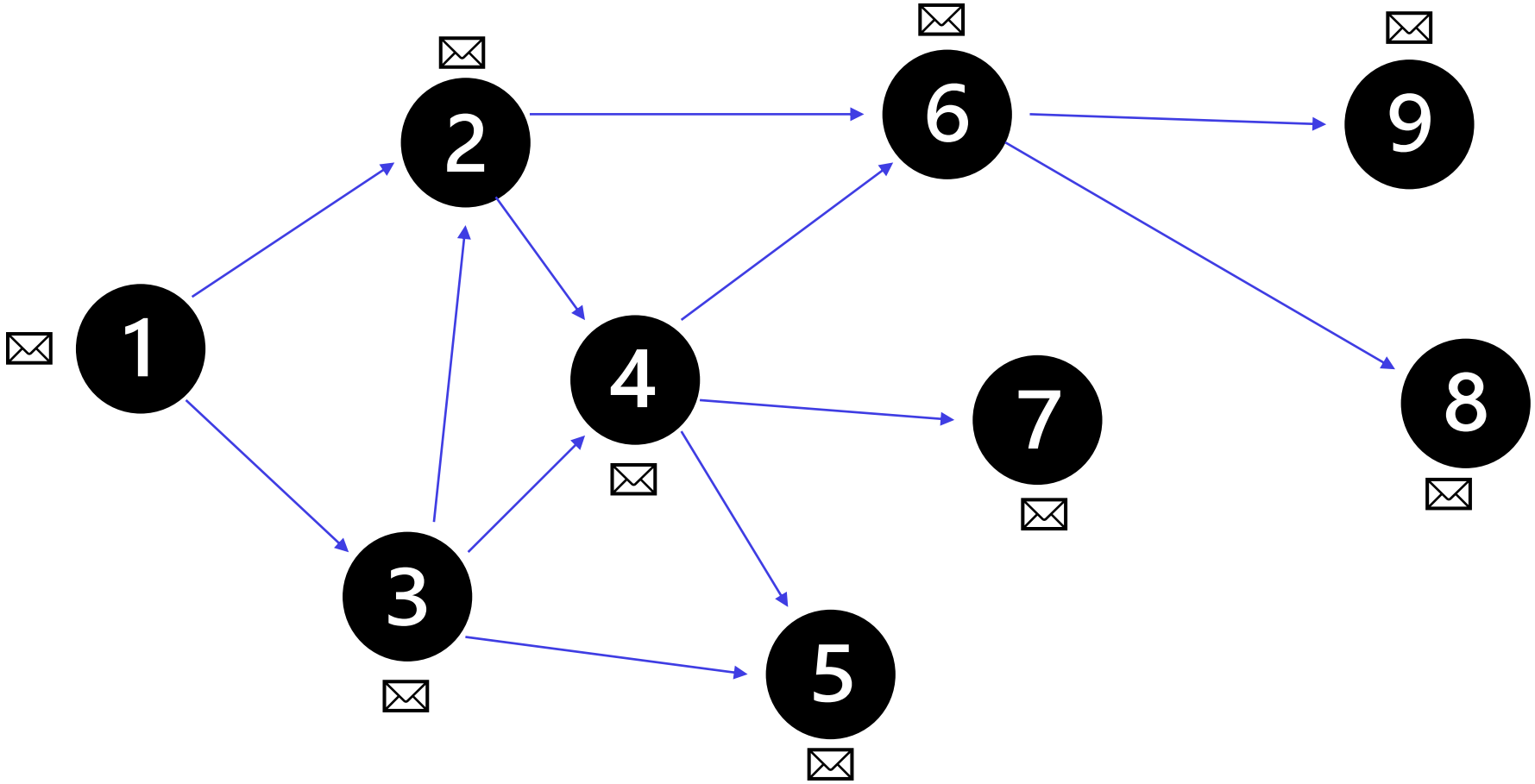


Forming a Network
1. Node discovery

- The node connects to well known DNS-Seeds
- The DNS Seeds maintain address book of Bitcoin nodes. These could be static or dynamic
- On connection these peers can be probed for addresses of other peers they know of
- The node then connects to any new nodes returned
- The node stores a list of known peers in its storage



Forming a Network
2. Gossip Protocol



What is a bitcoin wallet (Identity)

- A wallet at it core is a set of cryptographic key pairs
- Each pair consists of a private key, and a public key derived from it
- An address deduced from the public key is used to receive money, like a bank account number
- The private key is used to create digital signatures proving ownership, like banking PIN
- The wallet **may also** hold additional data needed for creation of transactions, however this is only for convenience

Private key
Not shared with anyone else
Access to this key proves ownership of assets

Public key
Can be shared with others
Used for cryptographic validation

Address
Deduced from the public key
Used to identify recipient of an eCash transfer transaction

Optional additional metadata

Public Key Cryptography

YouTube Video
https://www.youtube.com/watch?v=xIDL_akeras

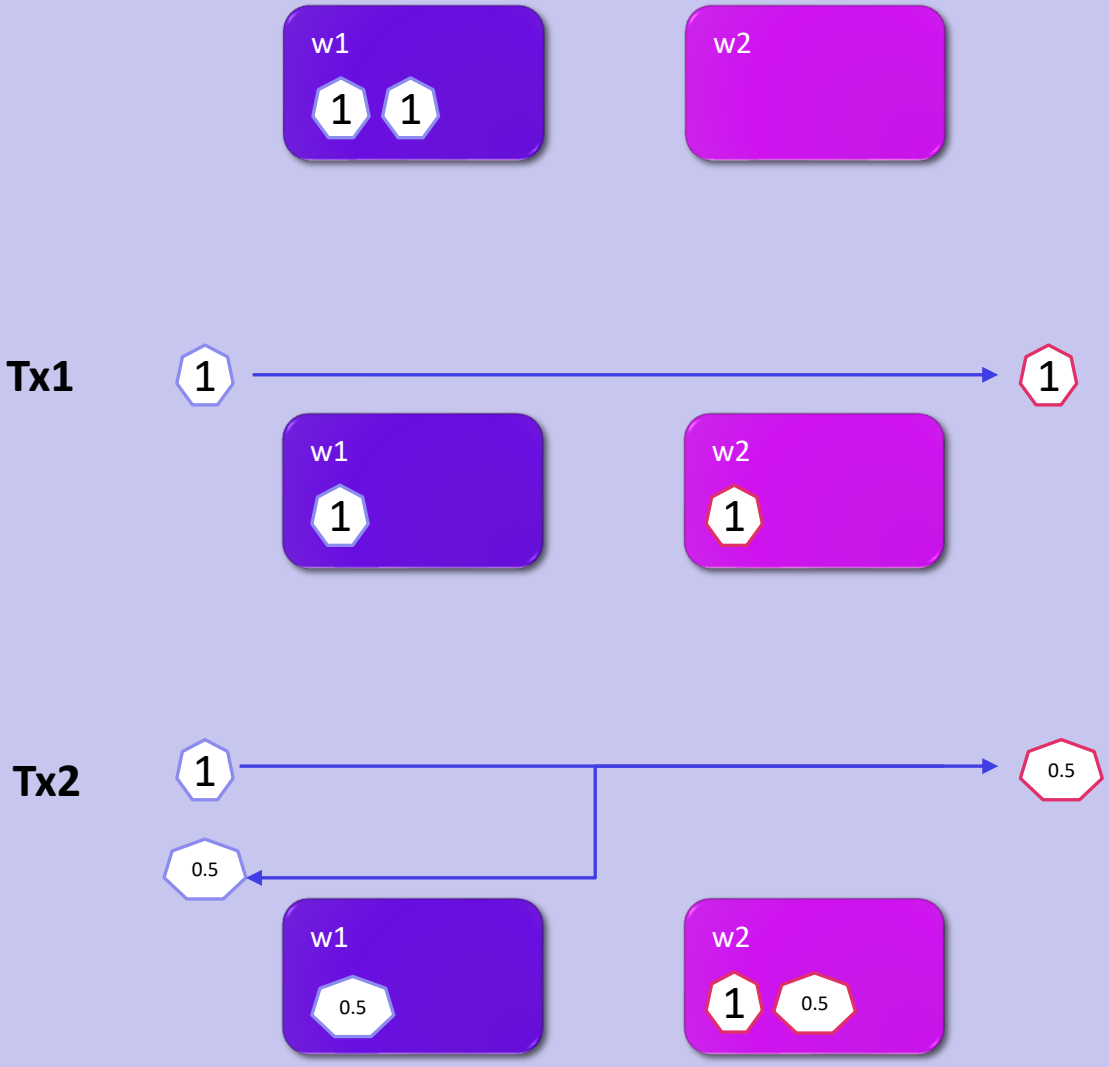
Hands-on website
https://andersbrownworth.com/blockchain/public-private-keys/keys

Bitcoin Transactions

- The Currency
- The UTXO Model
- Structure of a Bitcoin transaction
- Transaction chaining

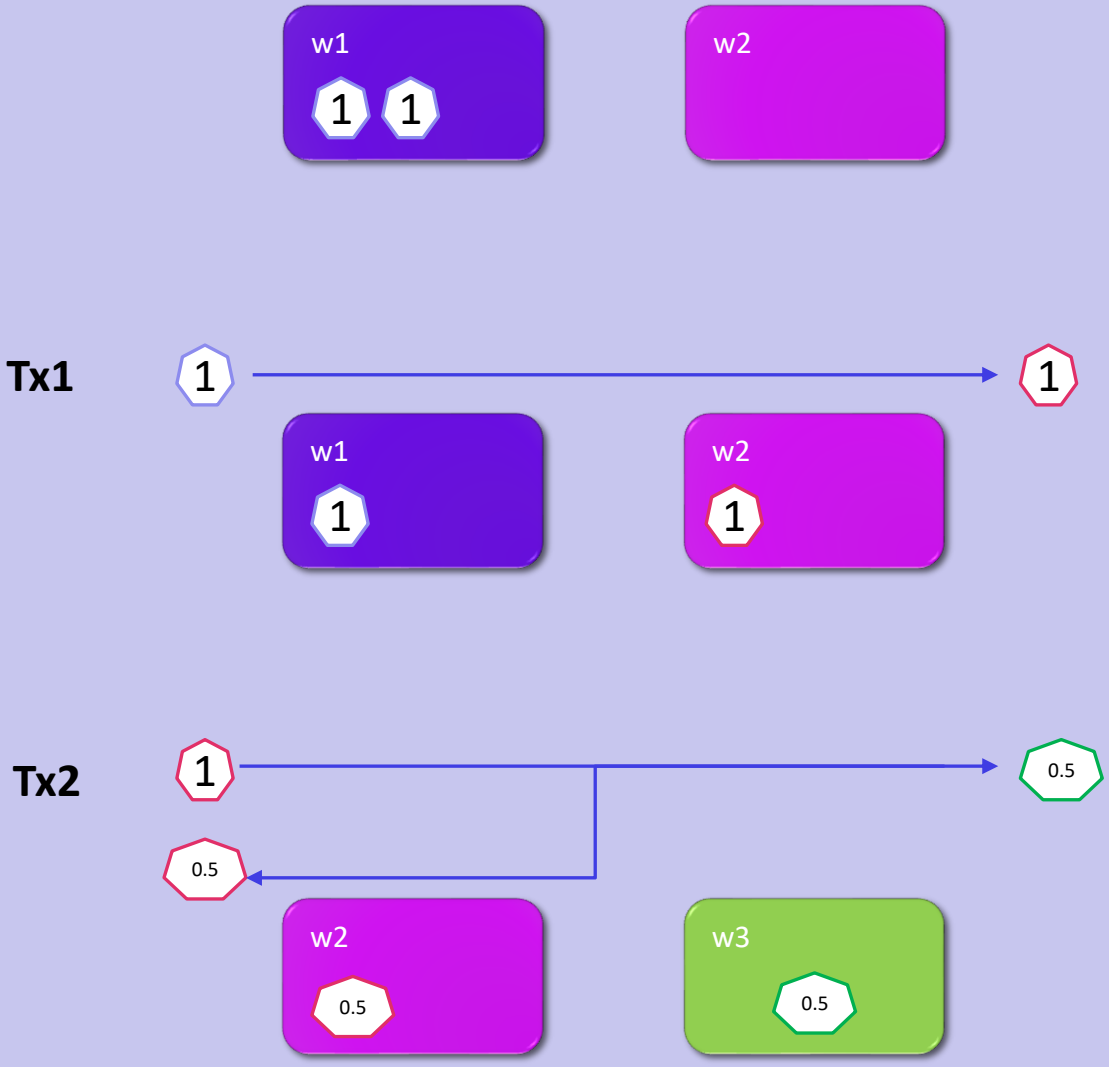
Currency Units

UNIT	SYMBOL	BITCOIN VALUE
bitcoin	BTC or ₿	1
millibit	mBTC	0.001
bit	µBTC	0.000 001
satoshi	sat	0.00 000 001
millisatoshi	msat	0.00 000 000 001



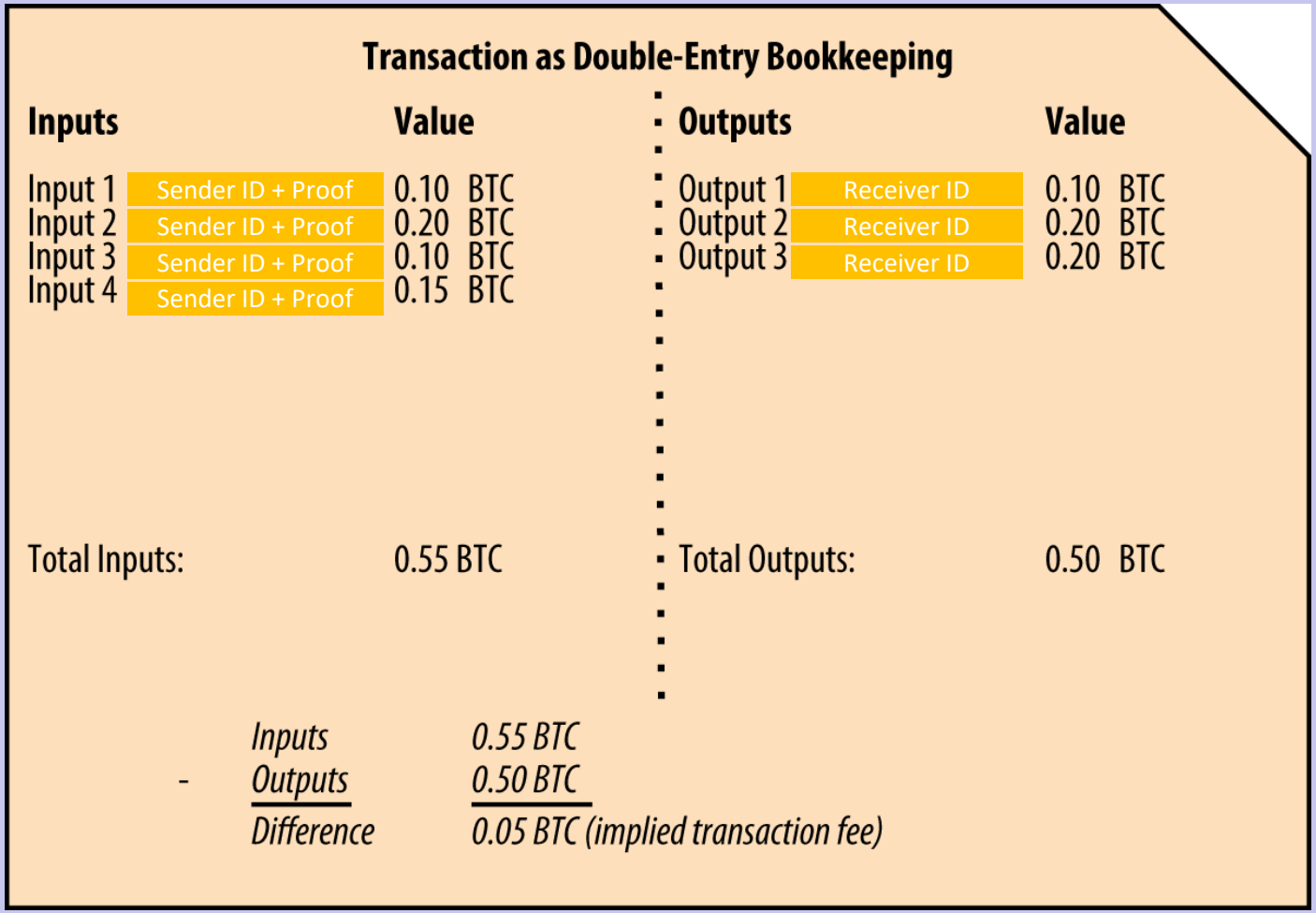
Understanding UTXO

- Emulates cash transactions to a great extent
- Each transaction involves a set of inputs and outputs
- Outputs of past transactions, called UTXOs or coins, act as inputs for current transaction
- As opposed to cash bills the coins are divisible



Transaction structure

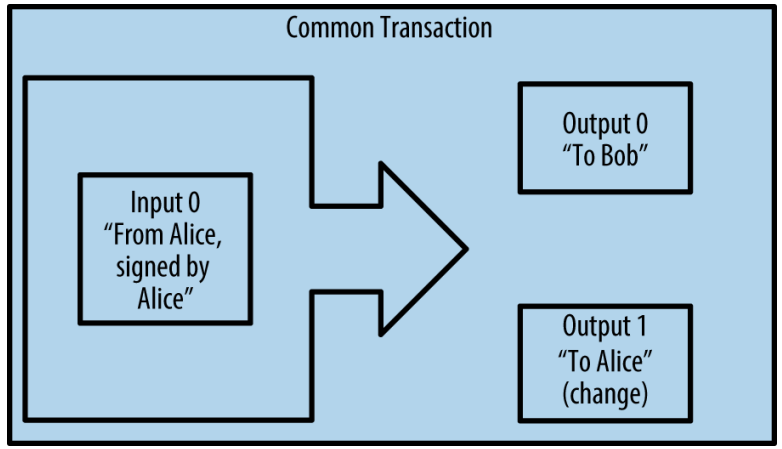
- A transaction can have one or many inputs
- A transaction must have at least one or more outputs
- The output value must be lesser than or equal to the input value
- The difference in input and output value is considered as transaction fee
- Identity of sender(s) and receiver(s)
- The transaction also holds the proof of ownership of inputs by the sender



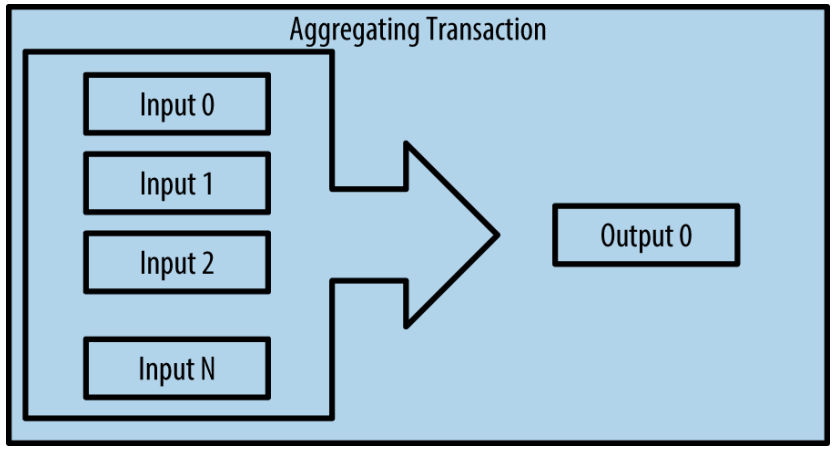
SOURCE : MASTERING BITCOIN BY ANDREAS ANTONOPOULOS

Transaction types

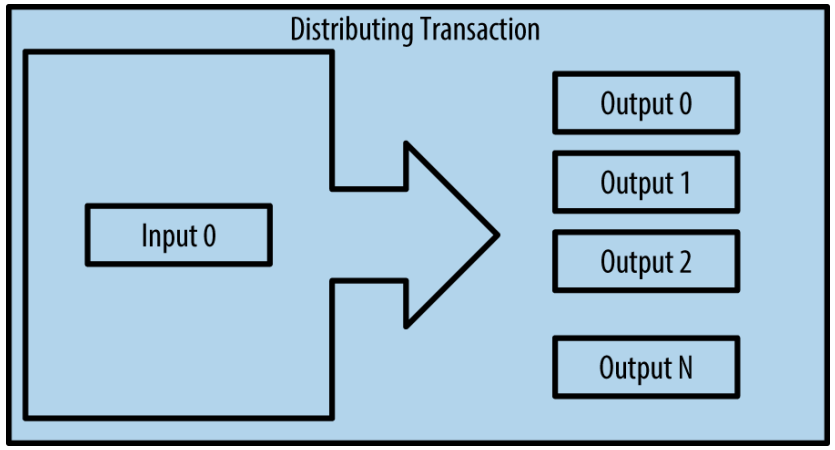
Common



Aggregating



Distributing

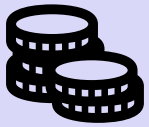


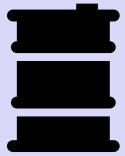
SOURCE : MASTERING BITCOIN BY ANDREAS ANTONOPOULOS

Token Fungibility

Fungible Tokens

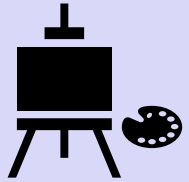
- Interchangeable
- Divisible
- Uniform





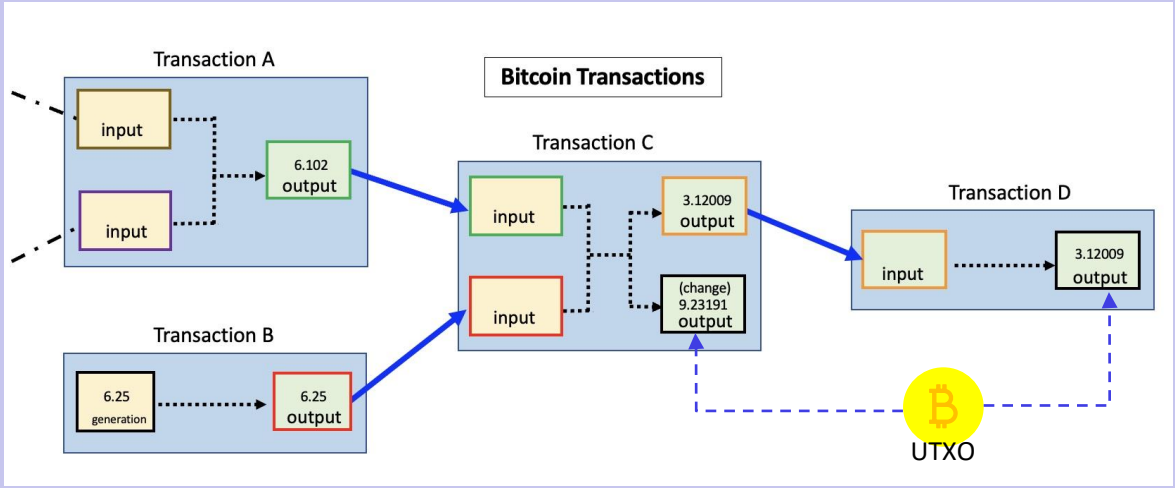
Non-Fungible Tokens (NFT)

- Cannot be interchanged
- Non divisible
- Unique

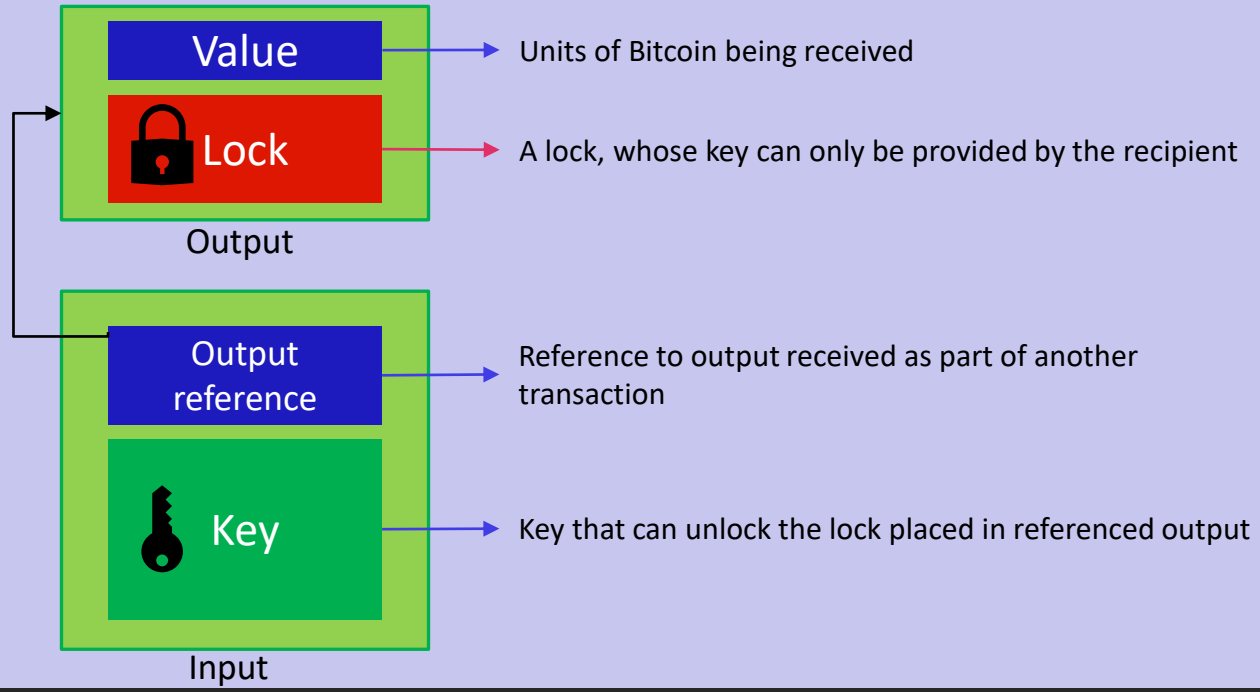


Transaction Chaining

- A transaction typically references previous transactions outputs as its inputs – Spending
- The new transaction consumes the inputs to create new outputs – UTXOs or Coins
- The outputs have embedded in them a ‘lock’ whose key only the new owner can provide
- When the new owner wants to spend the output, she creates a new input that contains, a reference to the unspent output and the key to unlock it



Source: Bitcoin Wiki

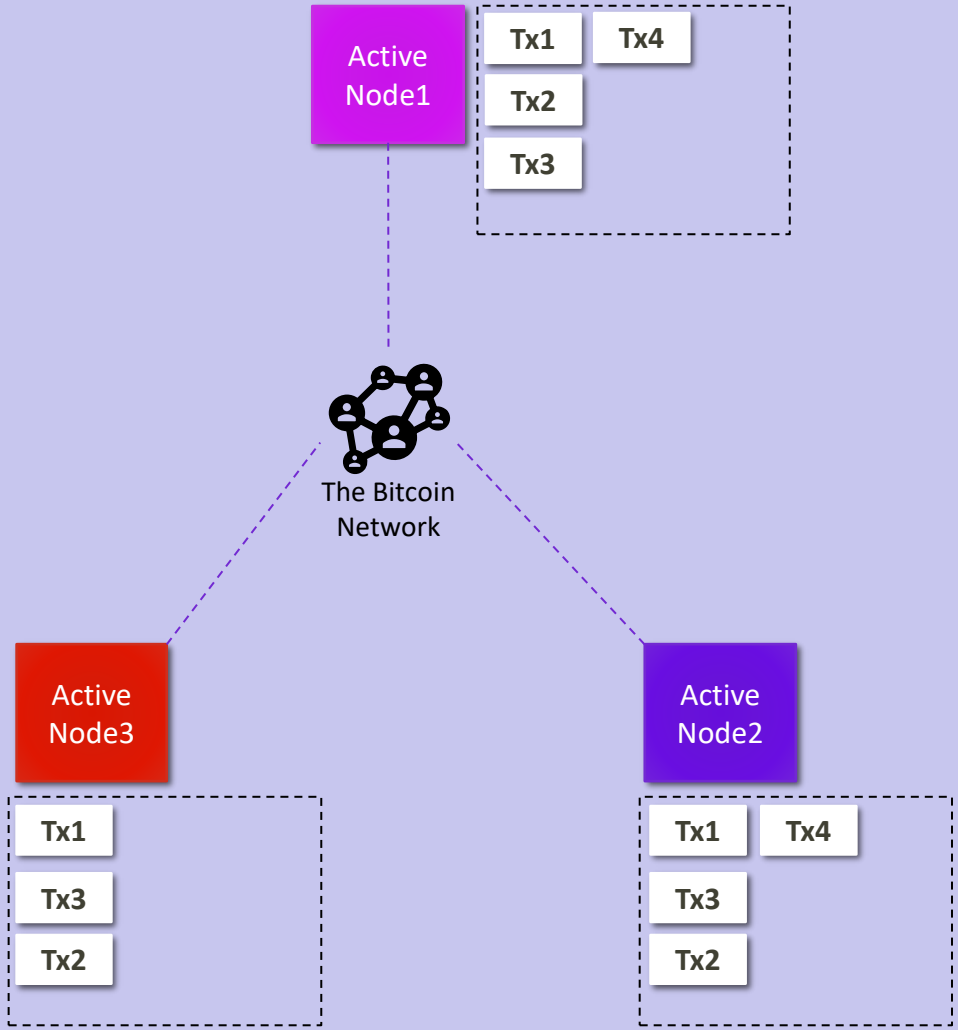


Processing the transactions

- Transaction submission
- Batching transactions
- Consensus
- The Ledger

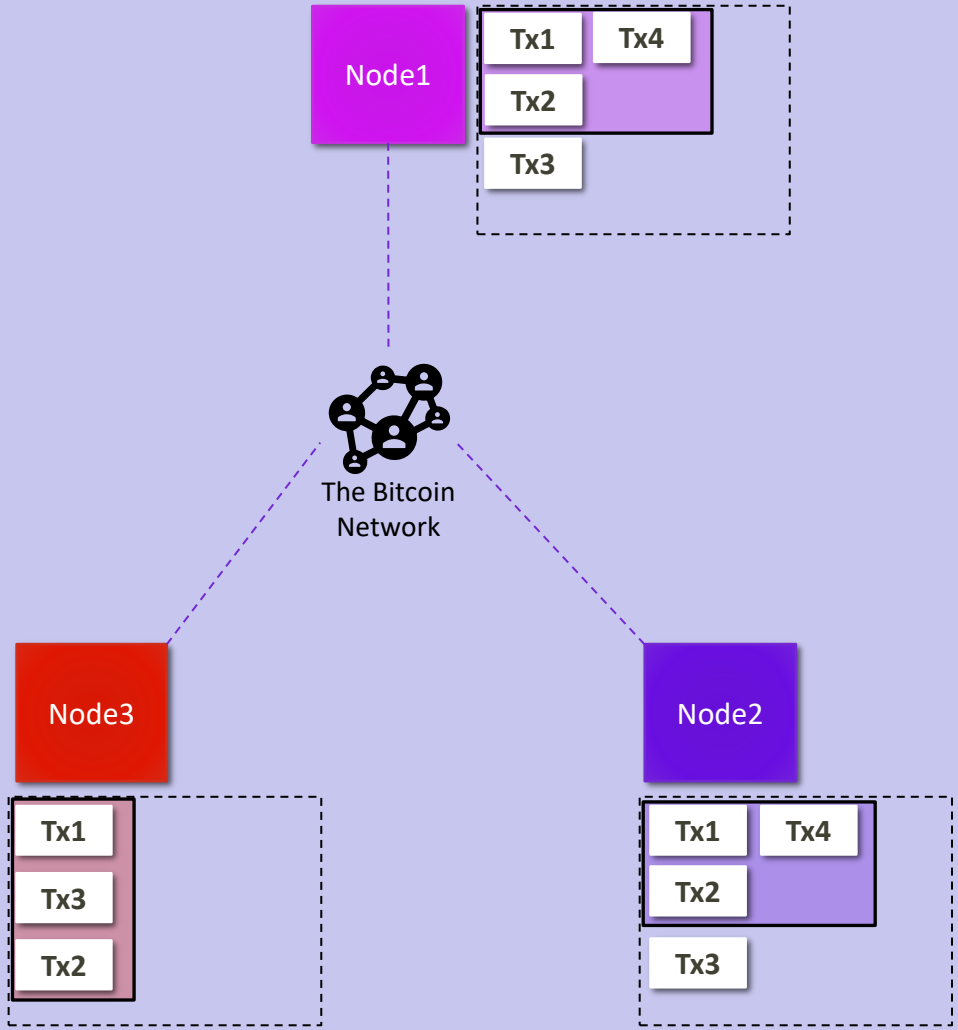
Transaction Submission

- Transaction request is submitted to one of the peers
- The request is propagated to the whole network with gossip protocol
- Each peer maintains a set of all received transaction request. This set is called ‘Mempool’
- Different peers may have different set of transactions and transaction order due to network latencies and message drops
- We need consensus on the order and validity of transactions



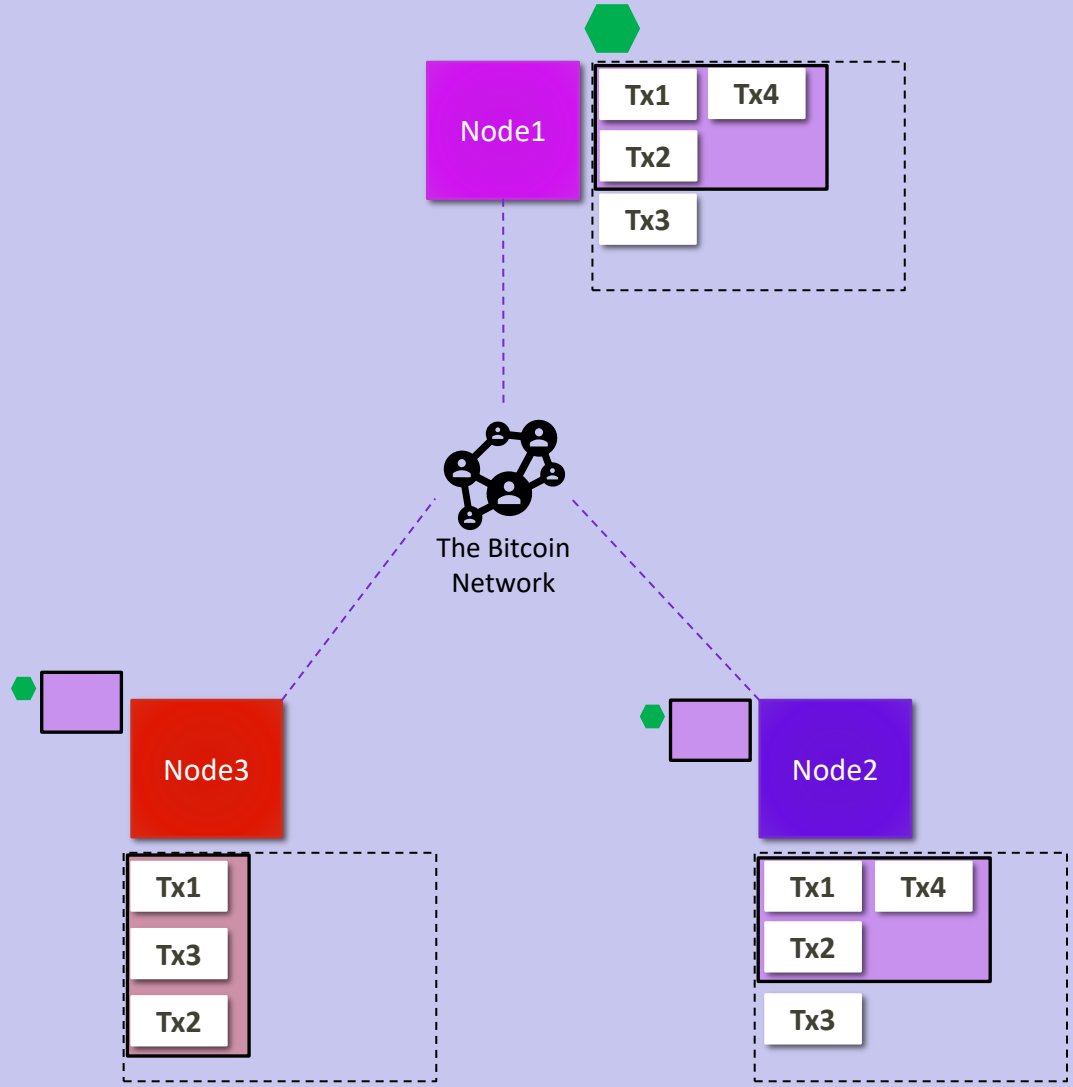
Transaction batching

- Consensus building needs back and forth between peers
- To reduce the number of such interactions the transaction requests are clubbed into a structure called ‘Block’
- A block mostly contains only a subset of transaction requests in Mempool
- Priority of selection is determined by the transaction fees
- Transactions are validated before inclusion in a block



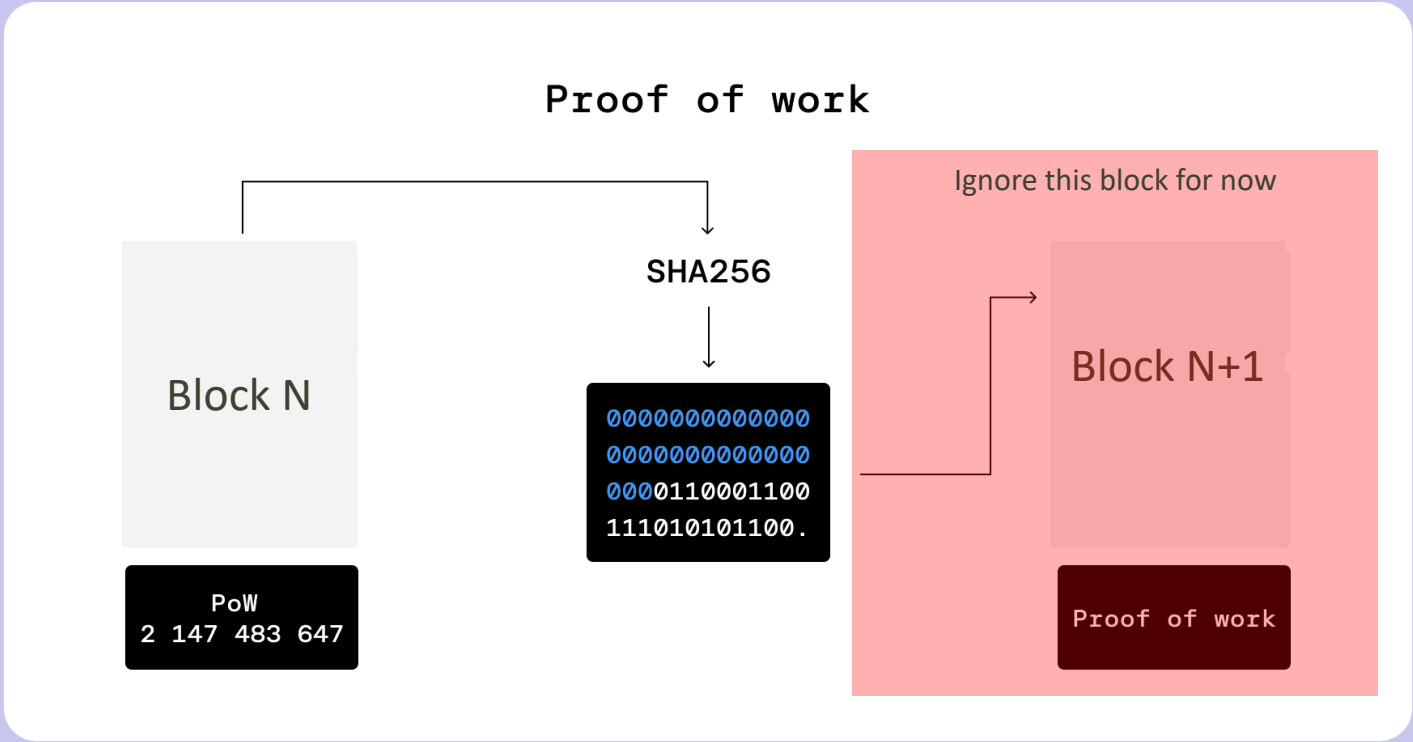
Building consensus

- The peers, also called ‘Miners’ try to solve a puzzle as mandated by the bitcoin protocol
- Any of the peers may find the solution based on effort put in
- Once a peer find the solution, it propagates the block along with the solution to the network
- Once other peers receives this block, **they validate it,** abandon the puzzle solving process, discard local block and accept the received block
- The peer solving the puzzle 1st receives the fees from all transactions included in the block



What exactly is the puzzle?

- Bitcoin uses Hash functions as computational puzzle. The solution is difficult to compute but easy to verify
- The Miners compute a hash of the block created + a ‘nonce’ such that the hash has a certain number of 0s
- The miners iterate through a large set of nonce values until a matching hash is produced
- The complexity is set such that the network gets 1 block after every 10 mins



Source: Coinloan

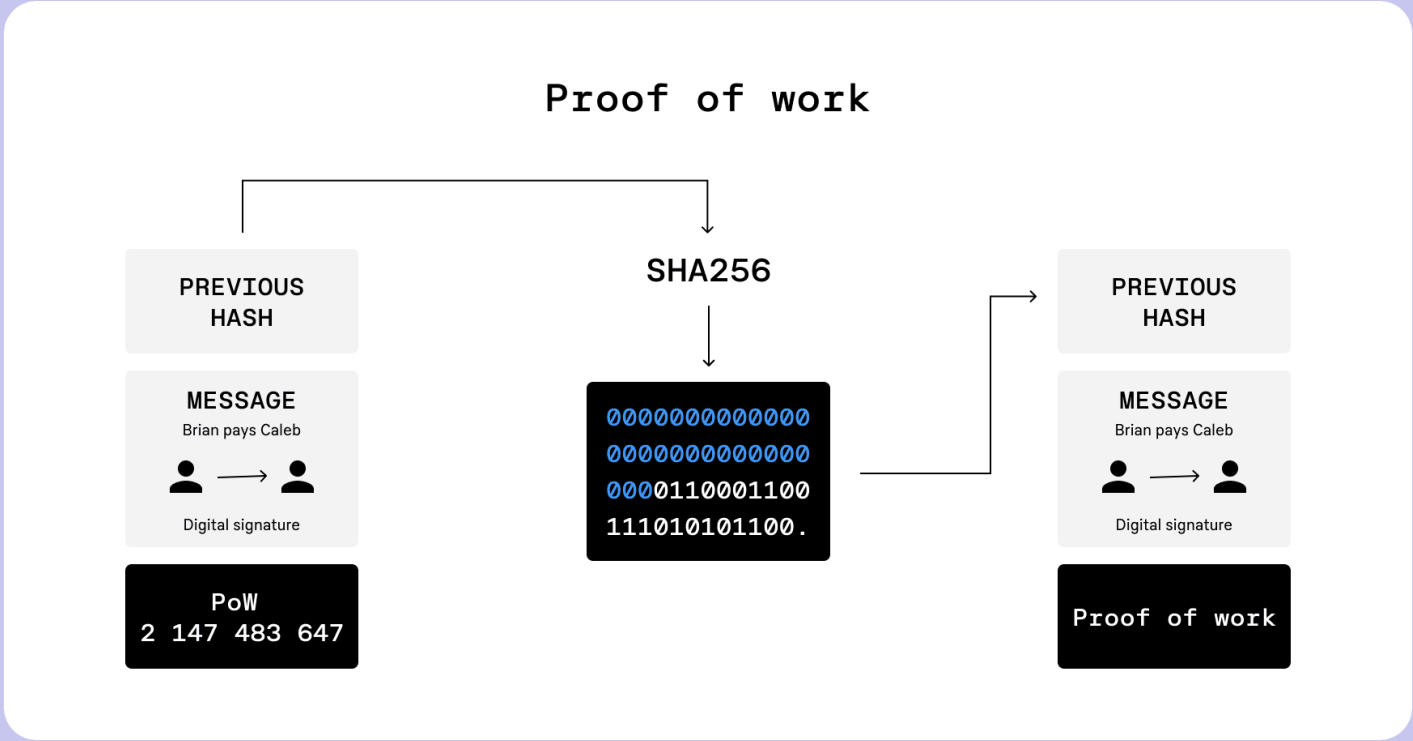
Bitcoin : Hands-On

https://www.youtube.com/watch?v=_160oMzblY8

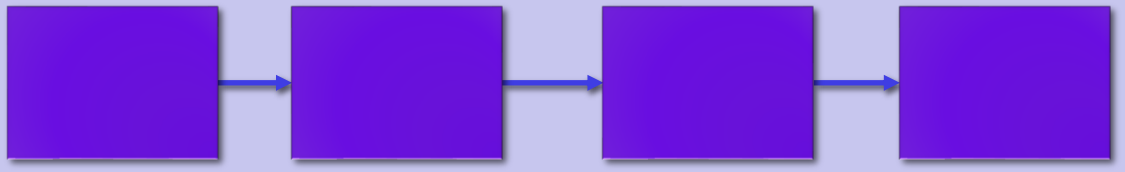
Source: Investopedia

Ensuring Immutability

- When calculating the hash, the miners also include the hash calculated on previous accepted block
- The data used as source is ‘Previous block hash + current block + nonce’
- This results in the blocks to be ‘chained’
- Any tampering in a block will change its hash and all subsequent blocks
- This mandates the tempering party to be able to ‘re-mine’ the modified and all subsequent blocks
- With mining being a computation heavy activity, this becomes nearly impossible after a certain number of blocks



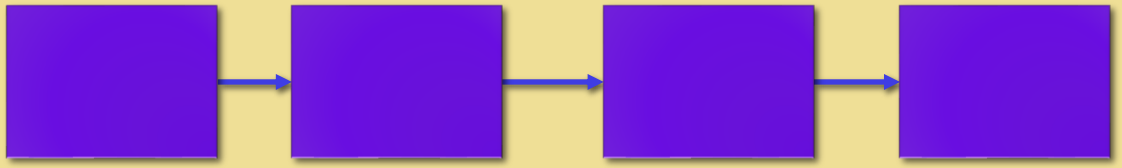
Source: Coinloan



The Distributed Ledger

- The protocol as we saw ensures all the peers have the exact same snapshot of the data
- This includes what transactions happened and the order of these transactions
- This is maintained in the ‘Block’-’Chain’
- In addition, the peers also maintain an index of all the UTXOs
- This helps in efficient validation of the transactions

Peer Storage



TXN ID	OUTPUT INDEX	OWNER ADDRESS
TXN1	0	ADD1
TXN2	0	ADD2
TXN2	1	ADD3
TXN3	0	ADD4

Bitcoin : Hands-On

https://www.youtube.com/watch?v=_160oMzblY8

Source: Investopedia

- Does every payer and payee need to deploy a node now?

No. A bitcoin user only needs to have a wallet to be able to send or receive bitcoins

- Then which node does a user connect to?

The bitcoin protocol ensures all the connected nodes see the exact same copy of the ledger. Hence a user may connect to any of the currently live nodes.
This removes lock-in or dependency on any specific service provider. And as the network is public, there is always an option of running a node yourself

- If a user can connect to any node, it means my money, my balance is available on all nodes. Where is the promised privacy?

The ledger tracks transactions and balances only based on the bitcoin address. This provides a layer of anonymity.
However, the users need to still take some additional measures to reduce the chances of co-relation to off-chain identity

Hands On

- Install Green Wallet app
- Create a wallet
- Obtain test coins
- View transaction on the block explorer
- Transfer coins

https://www.youtube.com/watch?v=jU8Nefrj8p4

Hands On

- Test net faucet

https://www.youtube.com/watch?v=KyWi8Dlp1nA&list=PL1xGN4d9nOKuCkUZQExTHsYzLPptQ28NM&index=3

Thank You!