



Module 3: Introduction to Bitcoin

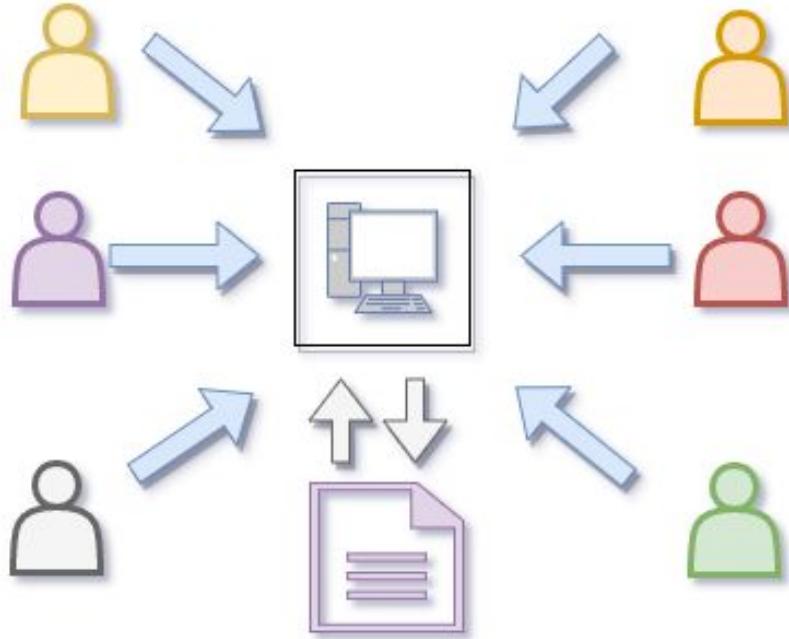
Priya R L, Lifna C S

Department of Computer Engineering, VESIT, Mumbai

Agenda

- **Blockchain Fundamentals - Recap**
- **What is Bitcoin?**
- **Creation of Coins**
- **Permission-less and Permissioned model**
- **Orphaned Blocks**
- **Bitcoin Basics - Sending Payments**
- **Bitcoin transaction Life cycle (Sender to Receiver)**
- **Bitcoin transactions**

Blockchain Fundamentals - Centralized Ledger



Centralized Ledger

www.ajithp.com

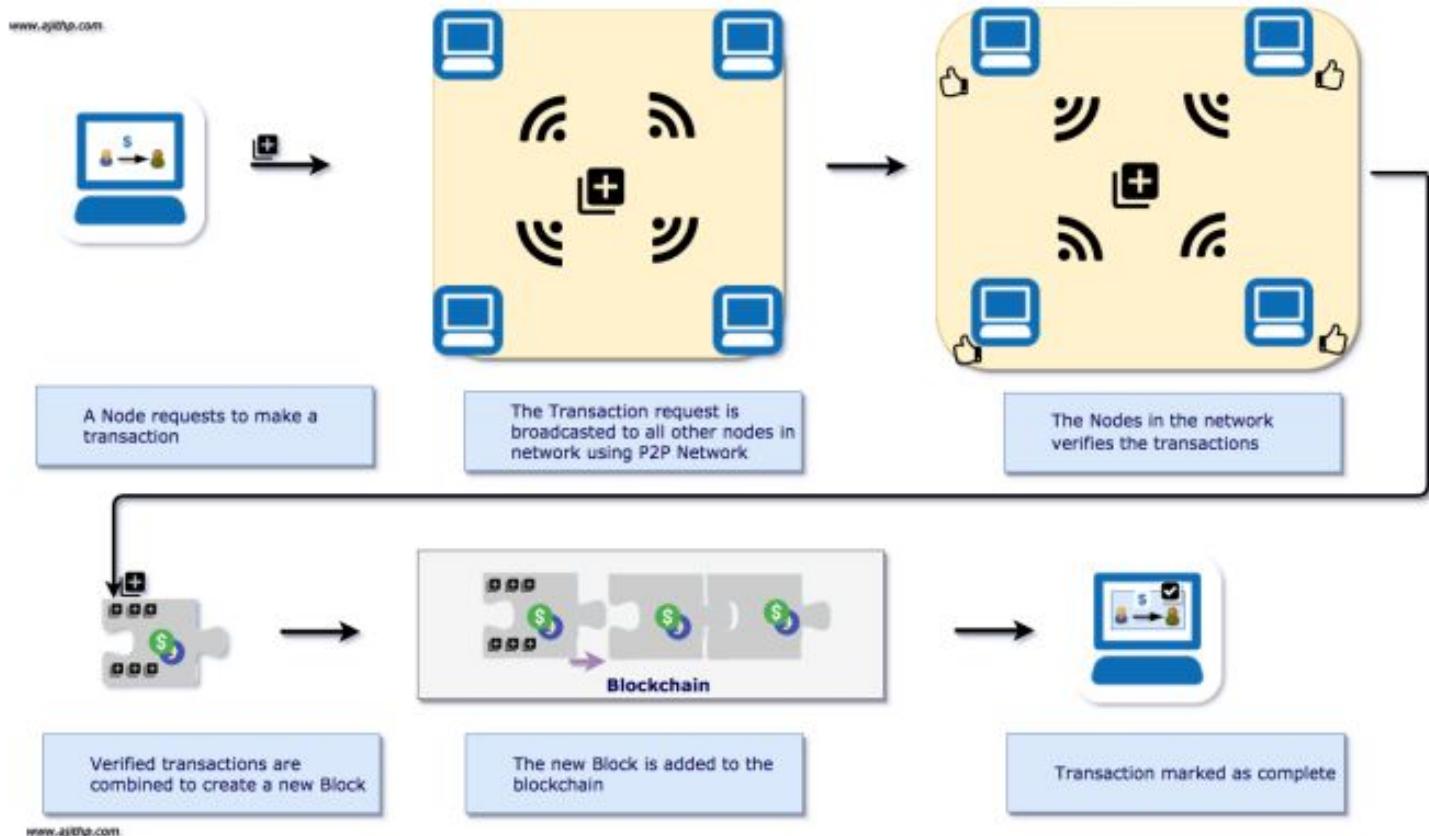
Courtesy : <https://ajithp.com/2018/02/01/block-chain-fundamentals/>

Blockchain Fundamentals - Centralized Ledger

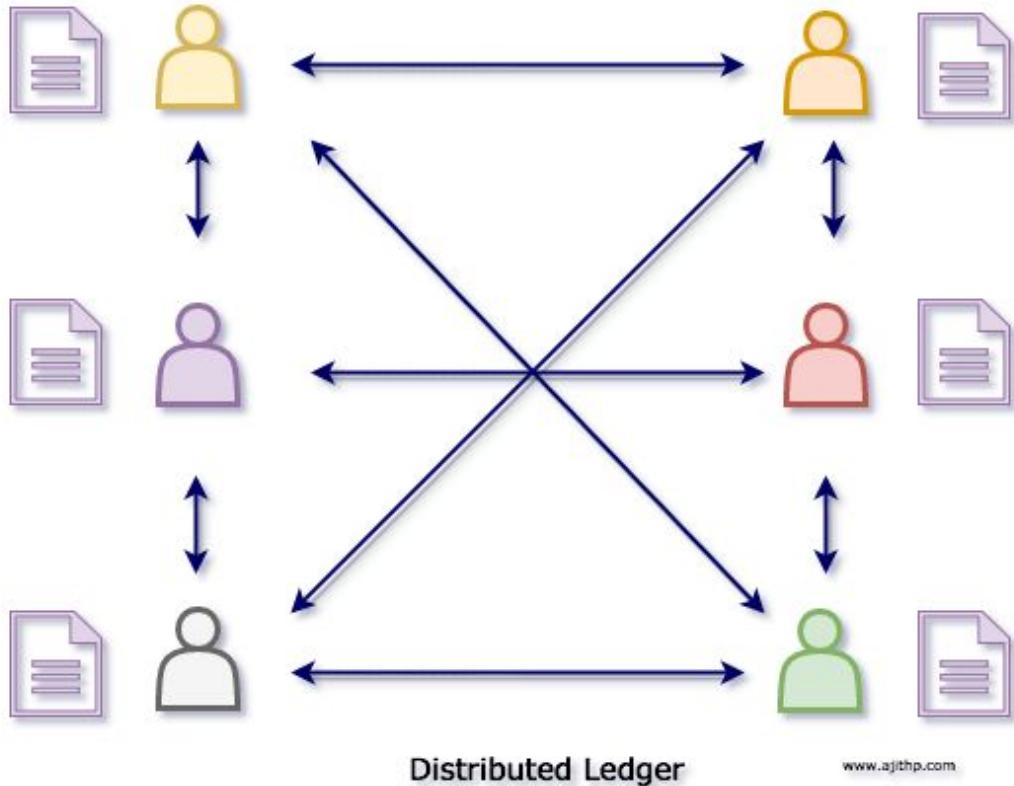


Courtesy : <https://ajithp.com/2018/02/01/block-chain-fundamentals/>

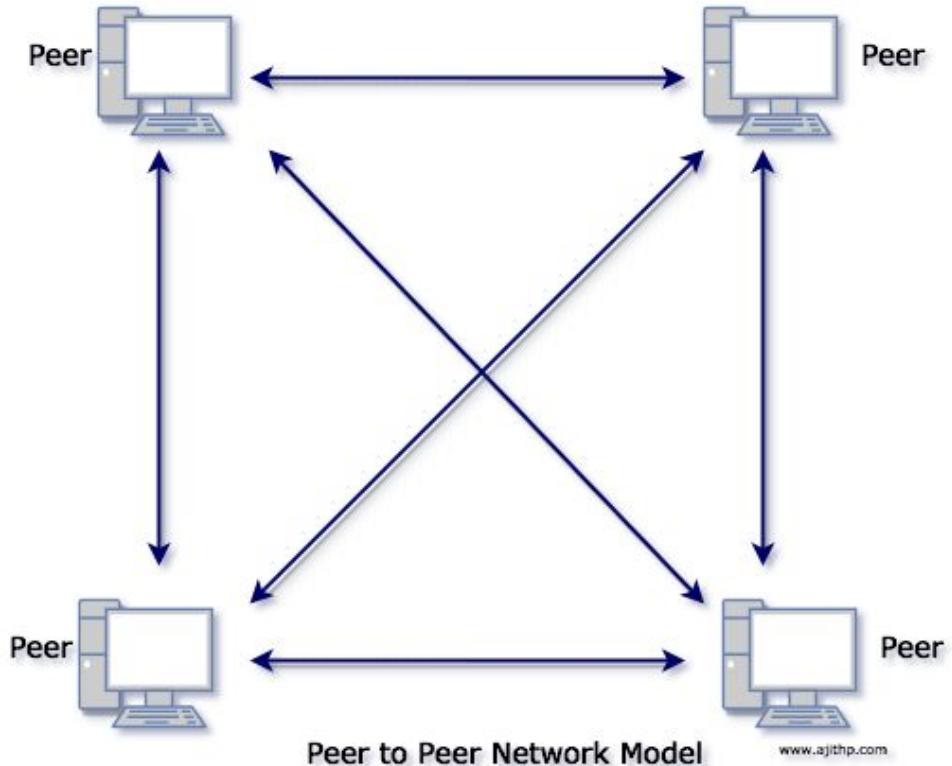
Blockchain Fundamentals - What is BC?



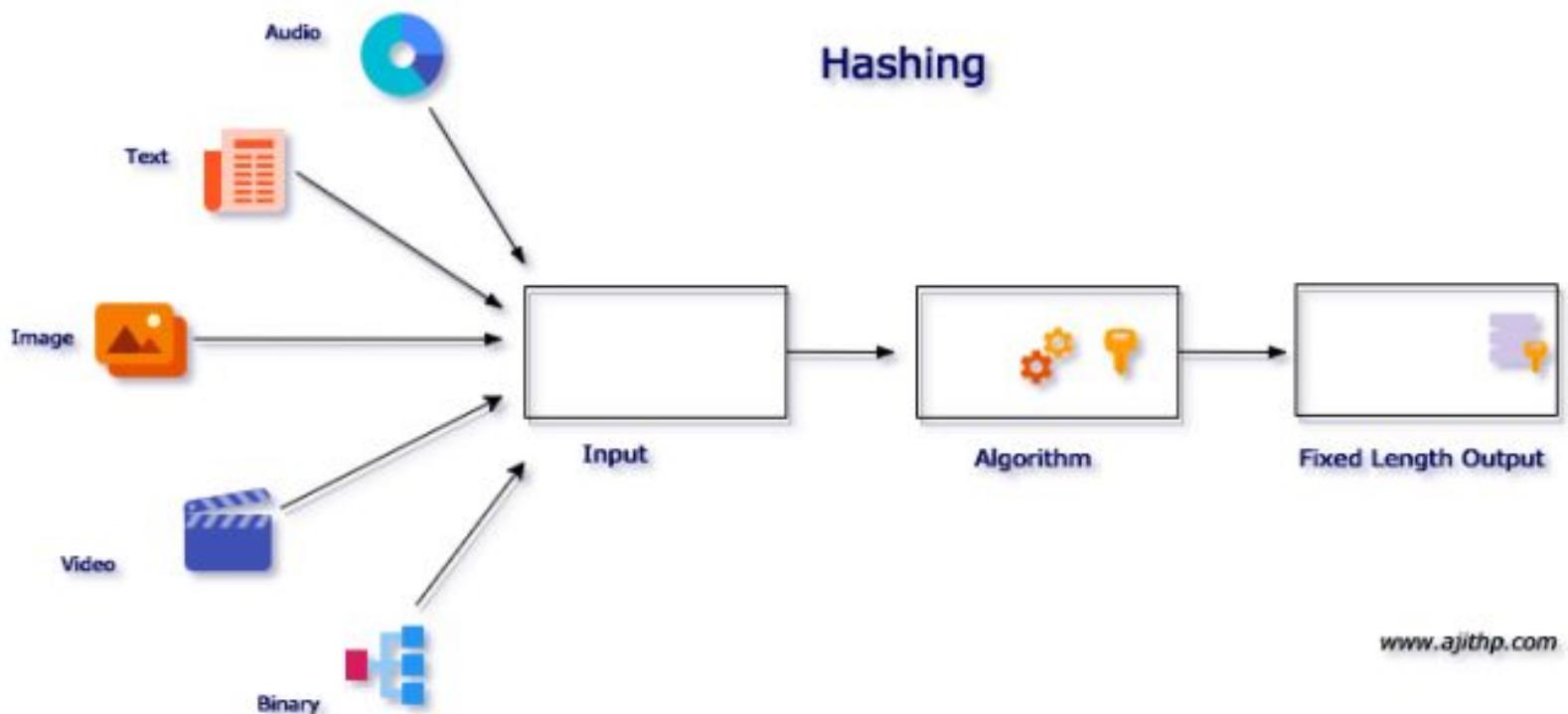
Blockchain Fundamentals - Distributed Ledgers



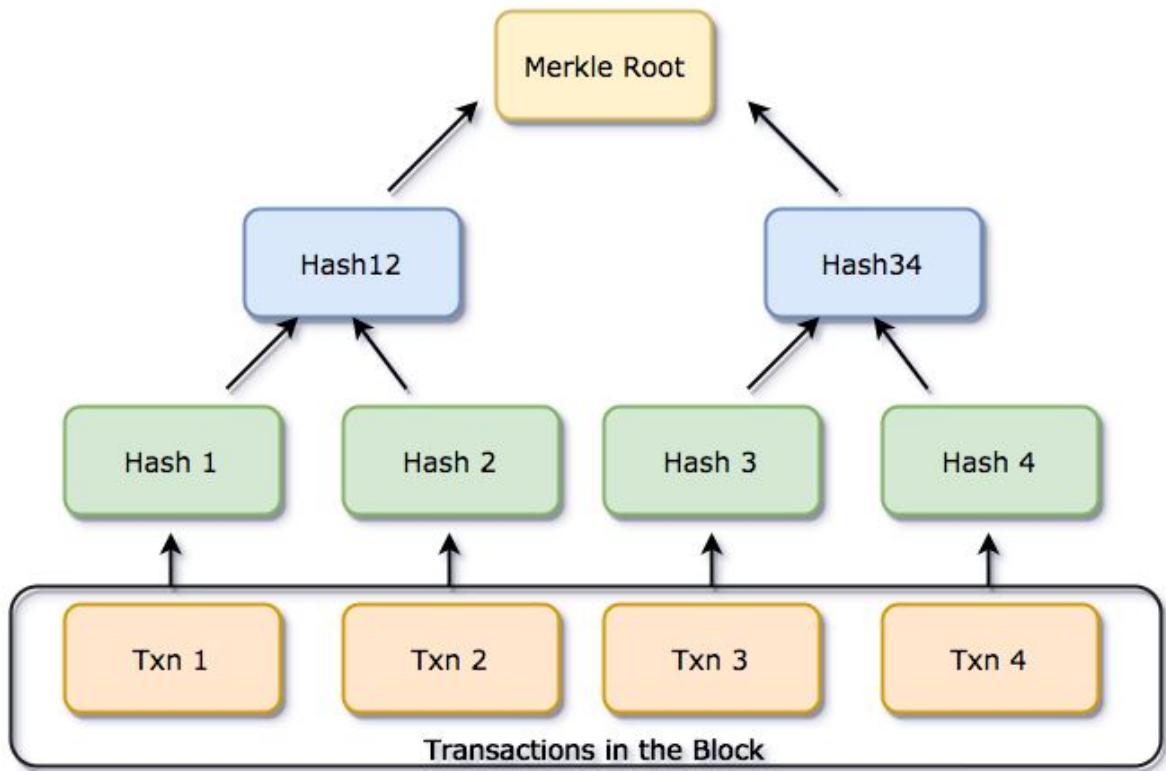
Blockchain Fundamentals - P2P Network



Blockchain Fundamentals - Hashing



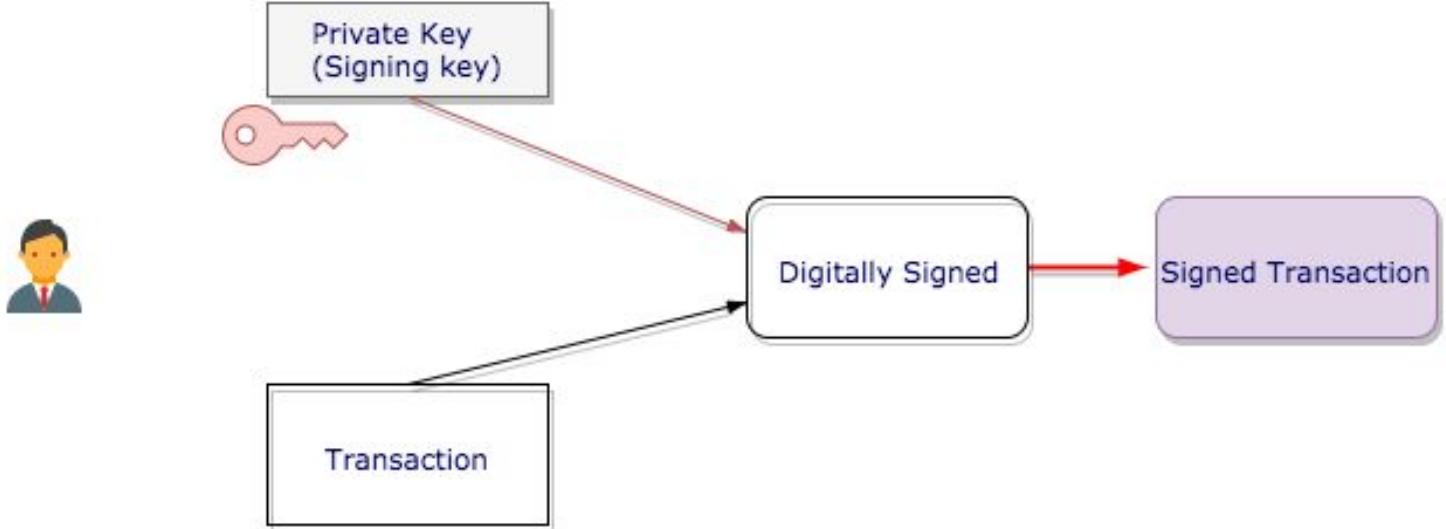
Blockchain Fundamentals - Merkle tree of a Block



Blockchain Fundamentals - Digital Signature

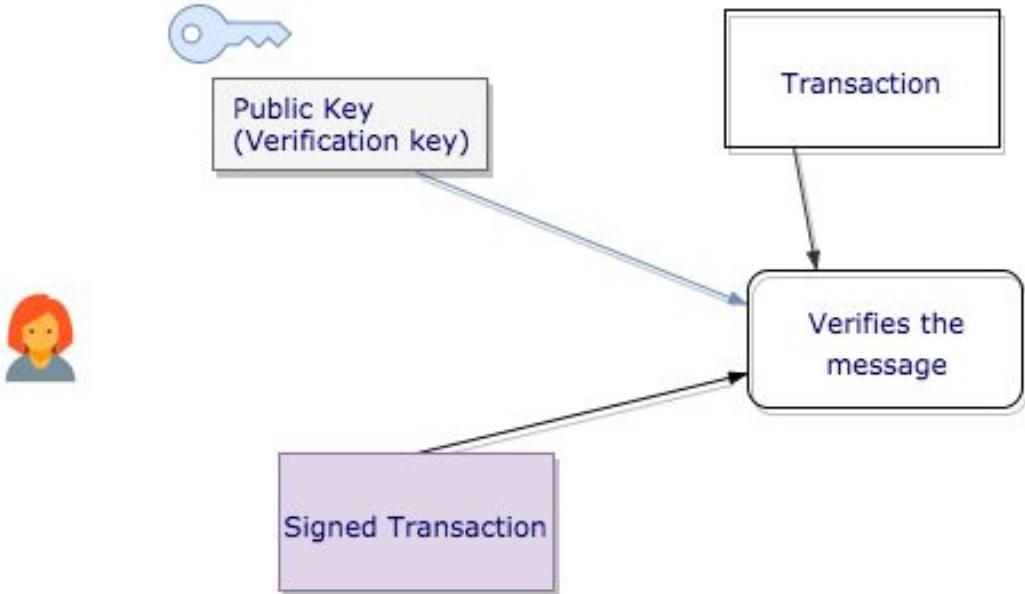


Blockchain Fundamentals - Digital Signature



Sam Signs his transaction with his private key and generate a signed transaction

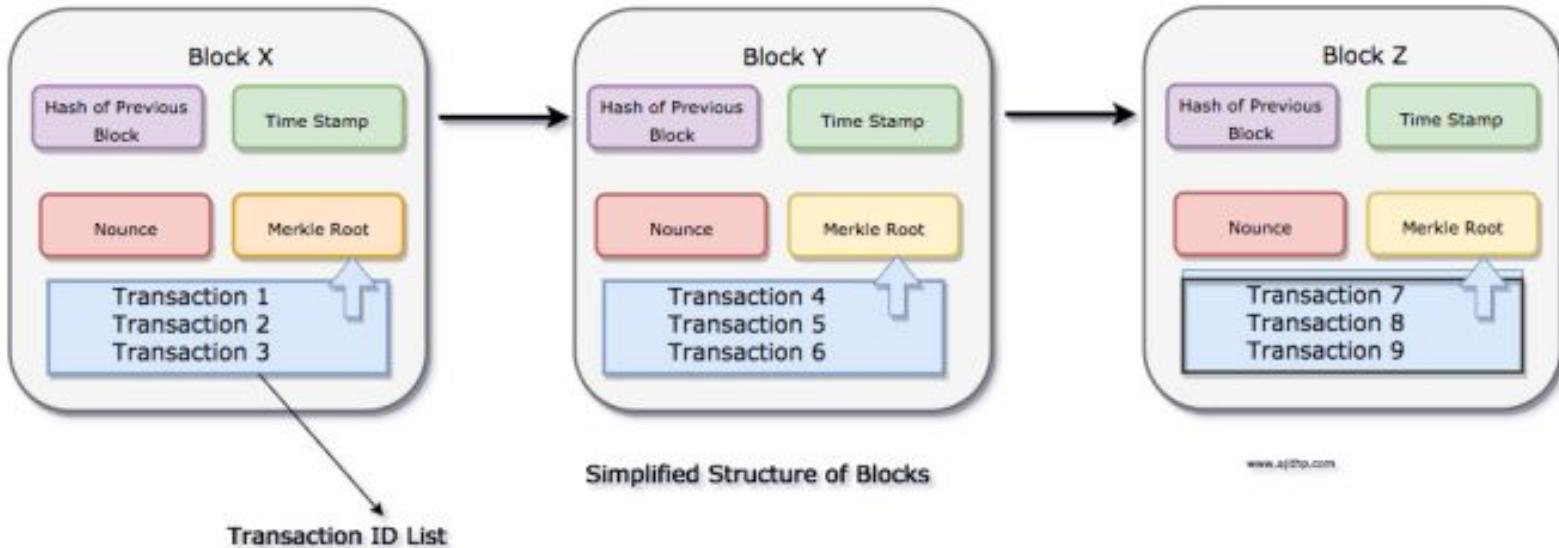
Blockchain Fundamentals - Digital Signature



Heather verifies the Transaction with three inputs

1. public key provided by Sam
2. Transaction Sent by Sam
3. Signed Transaction by Sam

Blockchain Fundamentals - What is a Block?



Blockchain Fundamentals - What is a Block?

Block #505234

Summary		Hashes
Number Of Transactions	1265	Hash 000000000000000003fa55faf6299751788bb49cd21f8b4b0f9ac0cf315214
Output Total	2,543.6082603 BTC	Previous Block 00000000000000000000100b5fab77217e62935986b30bac09cc055d0593474c6
Estimated Transaction Volume	599.91973715 BTC	Next Block(s) 000000000000000000005dff54314cc5ce3207fd857a32d9653a8d4f56ee29842
Transaction Fees	1.88207587 BTC	Merkle Root 3d481718f9973c52b547c266b85a66a6f08c2fe8cf1e8b22ba0db0721b36e6b
Height	505234 (Main Chain)	
Timestamp	2018-01-20 21:02:47	
Received Time	2018-01-20 21:02:47	
Relayed By	AntPool	
Difficulty	2,227,847,638,503.63	
Bits	394155916	
Size	1263.495 kB	
Weight	3992.709 kWU	
Version	0x20000000	
Nonce	4108077888	
Block Reward	12.5 BTC	

Transactions

fb081ab970b168c865e02902a3cc2dd1087ca6a343b72830ca5c23a6e5b7a22	2018-01-20 21:02:47
No Inputs (Newly Generated Coins)	 1Nh7uHdvYBfNwtQrM1G5EZAFPLC33B59rB Unable to decode output address

Blockchain Fundamentals - What is in transaction?

Transaction

View information about a bitcoin transaction

f350e9c89c85d08f5c33cf38741bbcd2d4245cd807d0e4584712320ff7a73103ca

14T6J3tsdpmzNnBgUhoJqck3fitHrSeDd



1FjndP5pAPaXP9wNo4K3dZPcYd7N9B7H5f
3MvwMs0hxAozkYgWCKCdgi1FW2DW4bjnq2

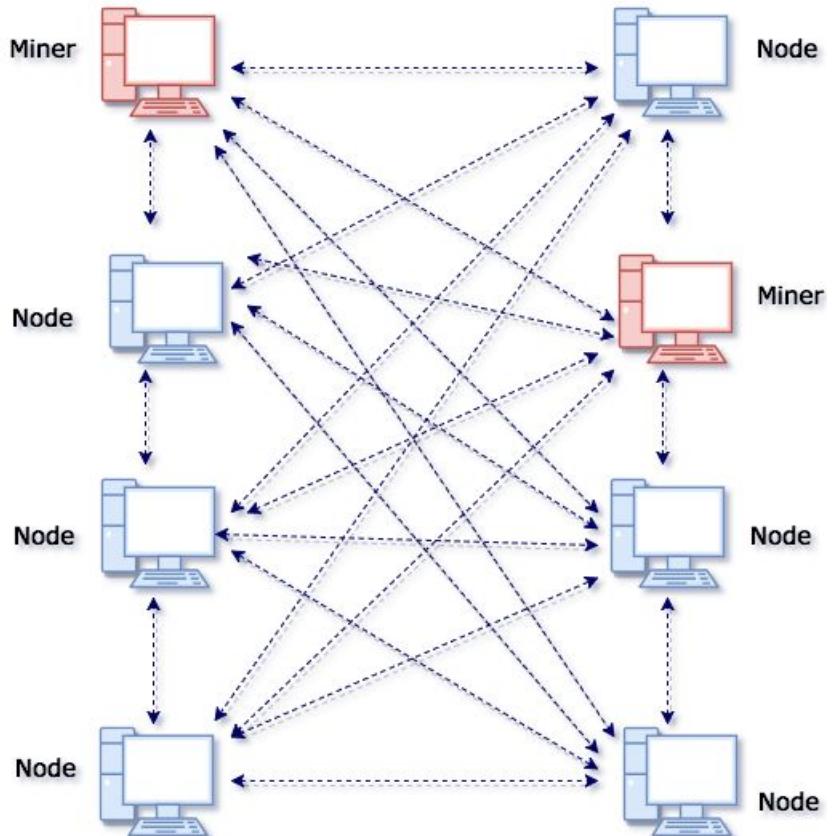
3.337846 BTC
0.312 BTC

3.649846 BTC

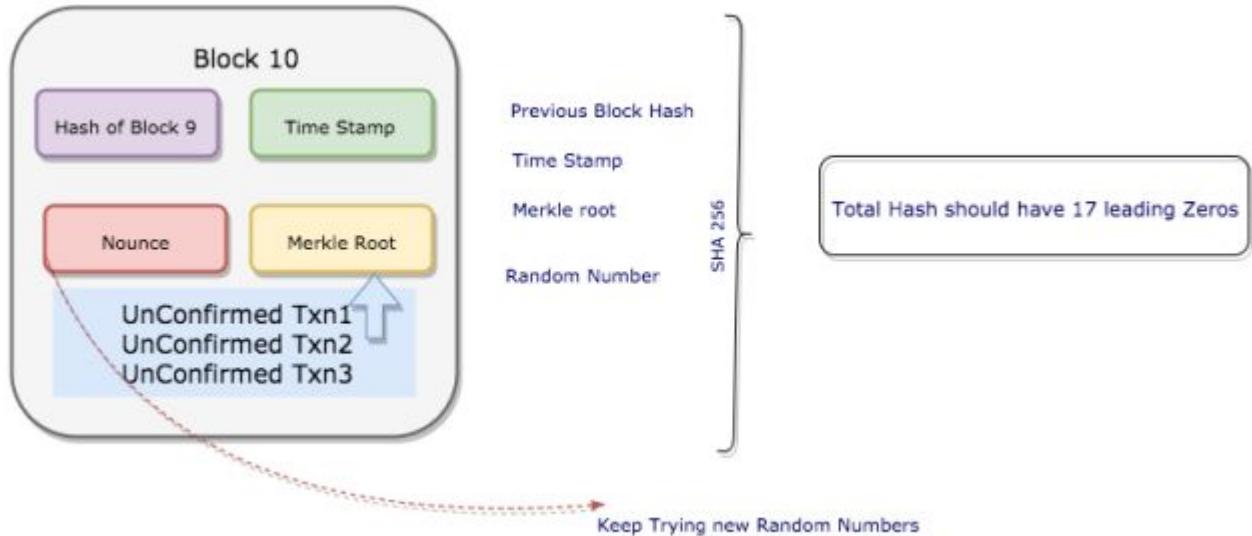
Summary	
Size	224 (bytes)
Weight	896
Received Time	2018-01-20 21:02:21
Included In Blocks	505234 (2018-01-20 21:02:47 + 0 minutes)
Confirmations	217 Confirmations
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	3.653346 BTC
Total Output	3.649846 BTC
Fees	0.0035 BTC
Fee per byte	1,562.5 sat/B
Fee per weight unit	390.625 sat/WU
Estimated BTC Transacted	0.312 BTC
Scripts	Show scripts & coinbase

Blockchain Fundamentals - Block Mining



Blockchain Fundamentals - Proof of Work (PoW)



Proof of work Logic implementation Bitcoin

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

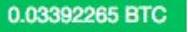
* Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008)
<https://bitcoin.org/bitcoin.pdf>

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 - Security

- The system is tamper-proof – it is “**extremely hard**” to make a change in the blockchain
 - Tampering the system becomes harder as the chain grows
- For Bitcoin, the transactions are pseudo-anonymous
 - Transactions are sent to public key addresses,- cryptographically generated addresses, computed by the wallet applications

e0200d0d26790a8f03c567171c24062ec1a05470ca160e064c086ad589c6f0f0	2018-03-21 06:36:31
13YE1yUQ1Qr2GzaKQQomp9rr5LmGWyRNHC 18nHE6jrg2uRq6aX1S2j54hedjkcRFeivu	0.02592724 BTC 0.00799541 BTC
	 0.03392265 BTC



Peer Addresses

- “**Address**” in bitcoin is synonymous to an “**Account**” in a bank.
- The wallet listens for transactions addressed to an account,
 - Encrypts the transactions by the public key of the target address
 - Only the target node can decrypt the transaction and accept it
- However, the actual transaction amount is open to all for validation

e0200d0d26790a8f03c567171c24062ec1a05470ca160e064c086ad589c6f0f0

2018-03-21 06:36:31

13YE1yUQ1Qr2GzaKQQomp9rr5LmGWyRNHC
18nHE6jrg2uRq6aX1S2j54hedjkcRFeivu



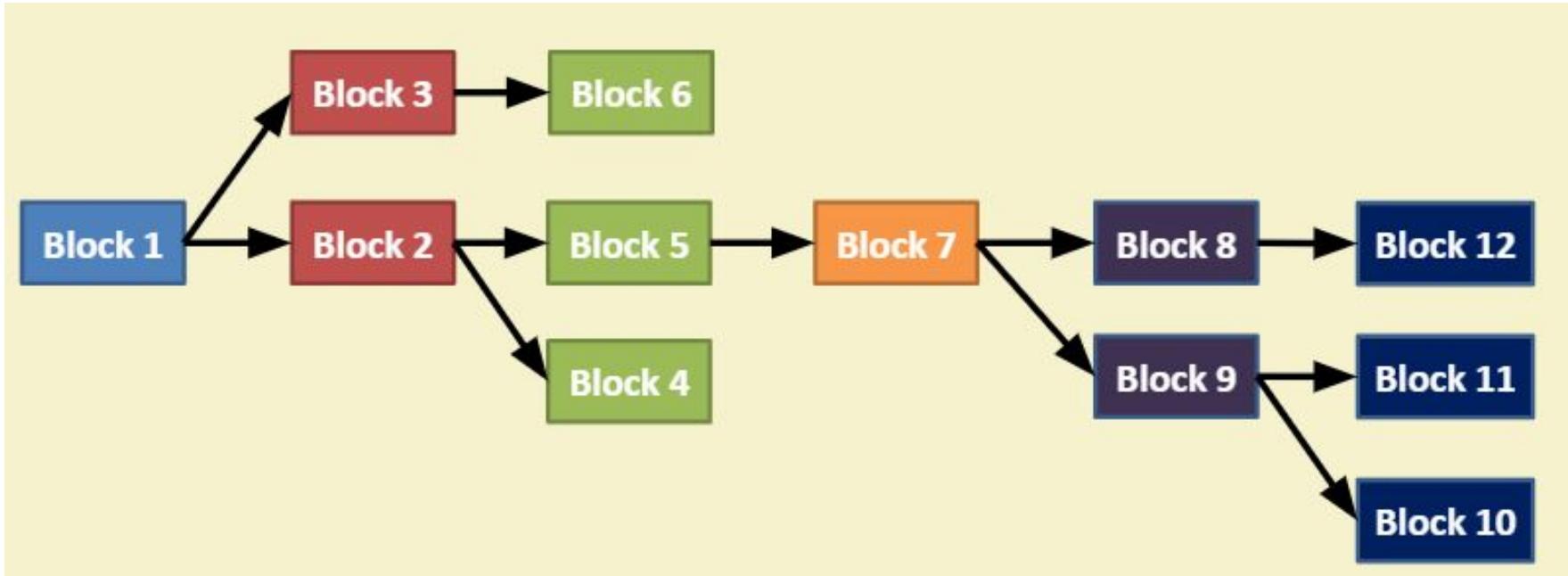
3GGQp33h2GJEWsjL9tSwhZtDBvhRPjE33m
1AhSeDT8nYDSW8WNTH494kteSbv8fVta1b

0.02592724 BTC
0.00799541 BTC

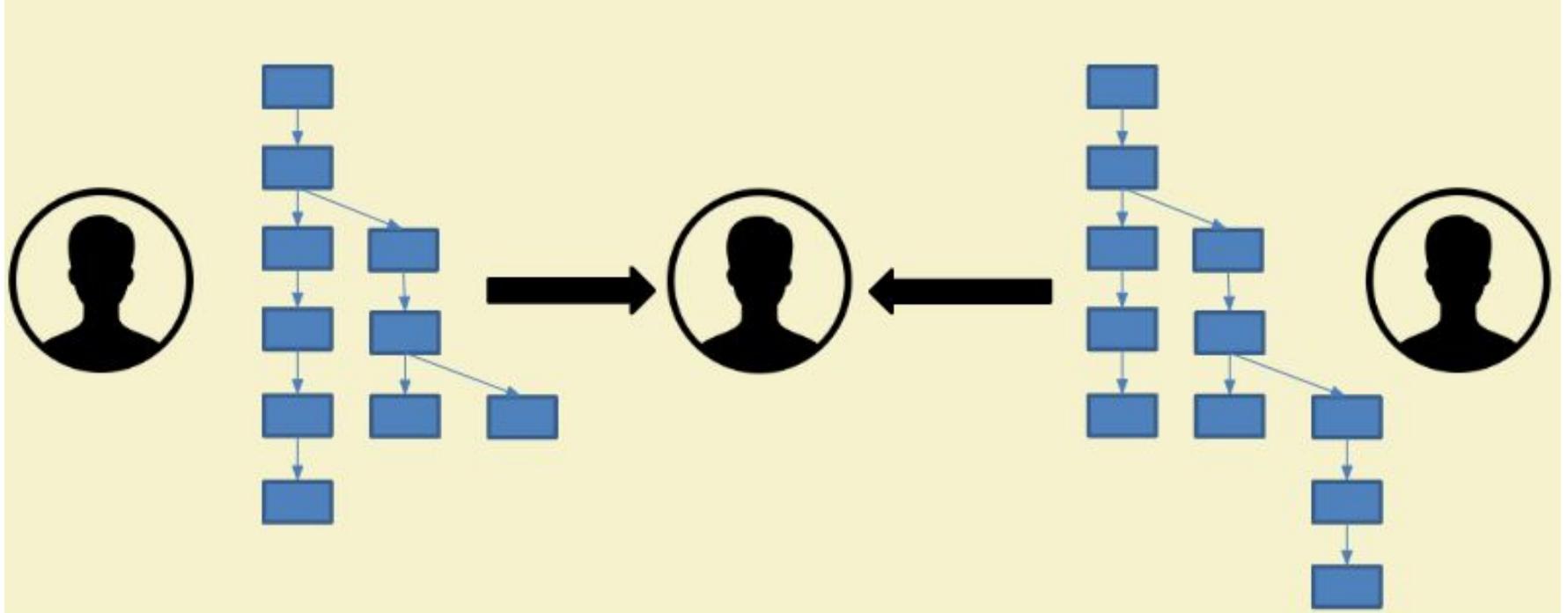
0.03392265 BTC

Blockchain (at Permission-less Model) as a Tree

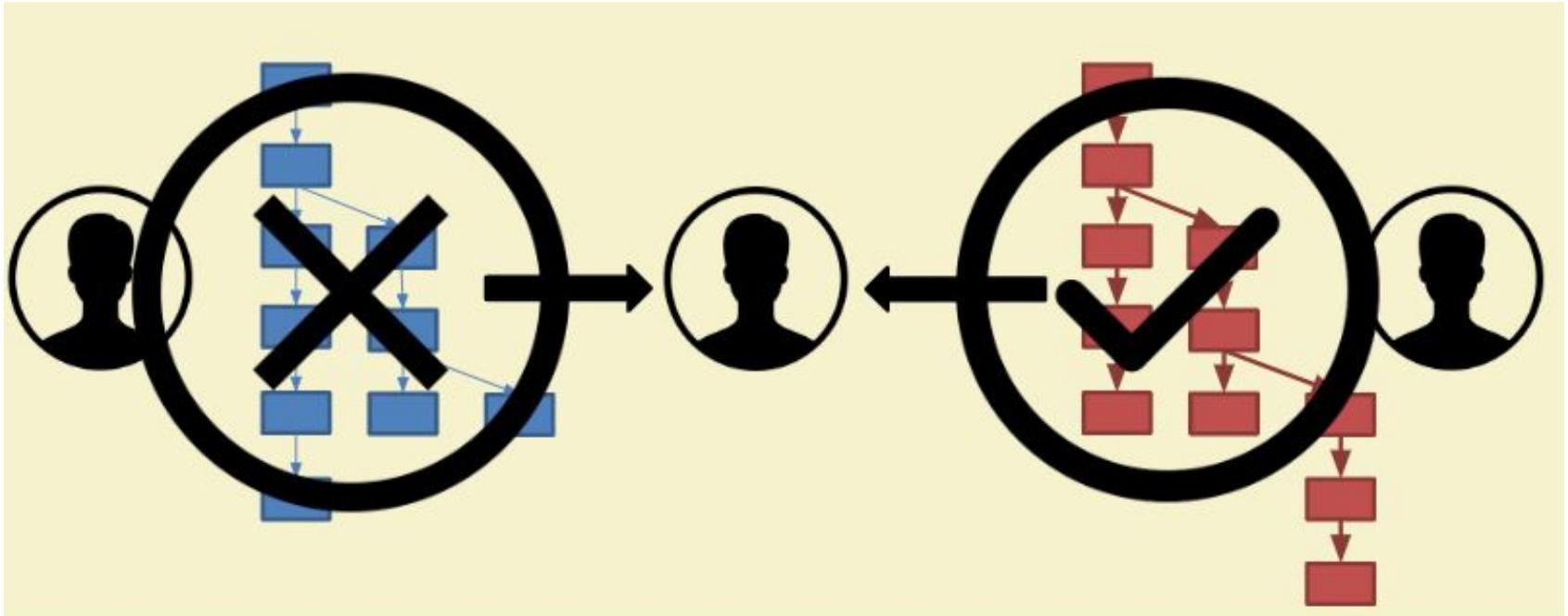
- The longest chain is the accepted chain



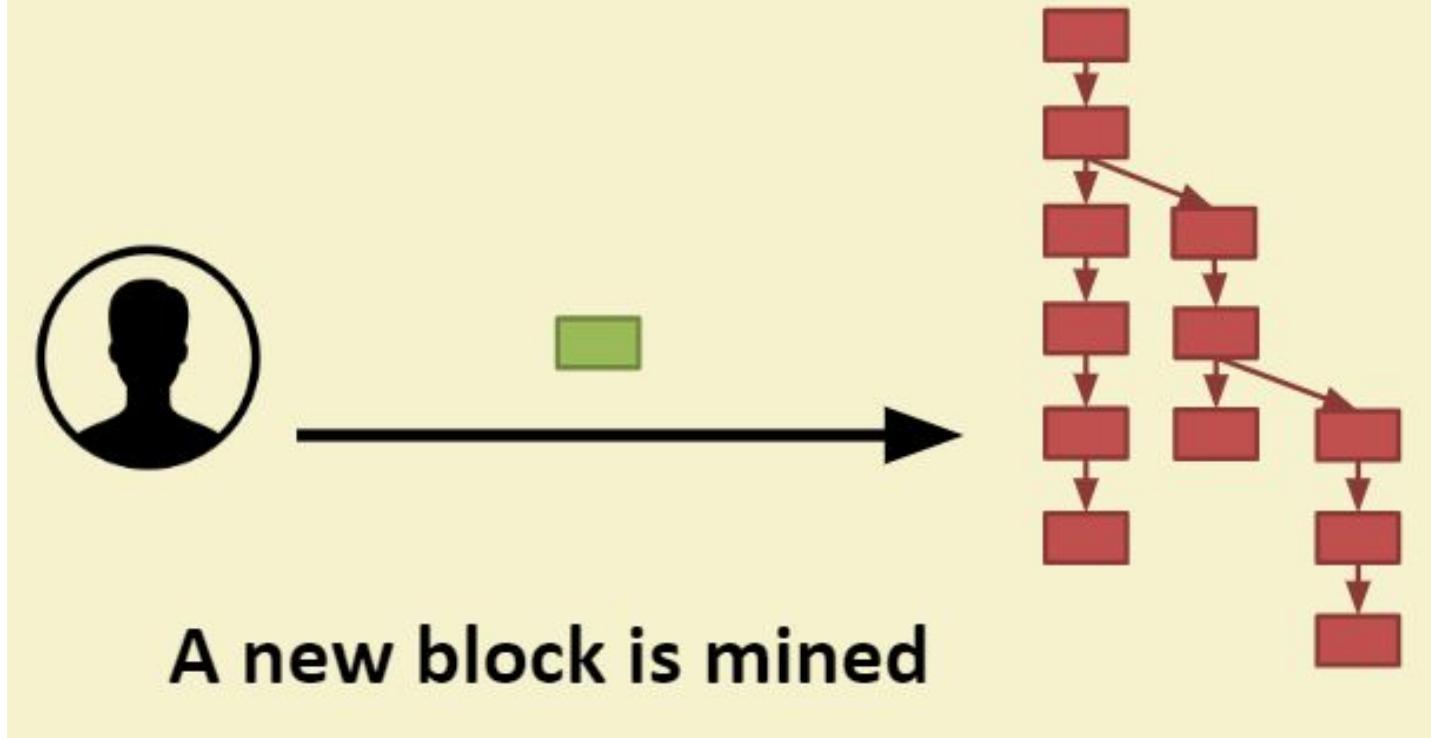
Accepting the Longest Chain



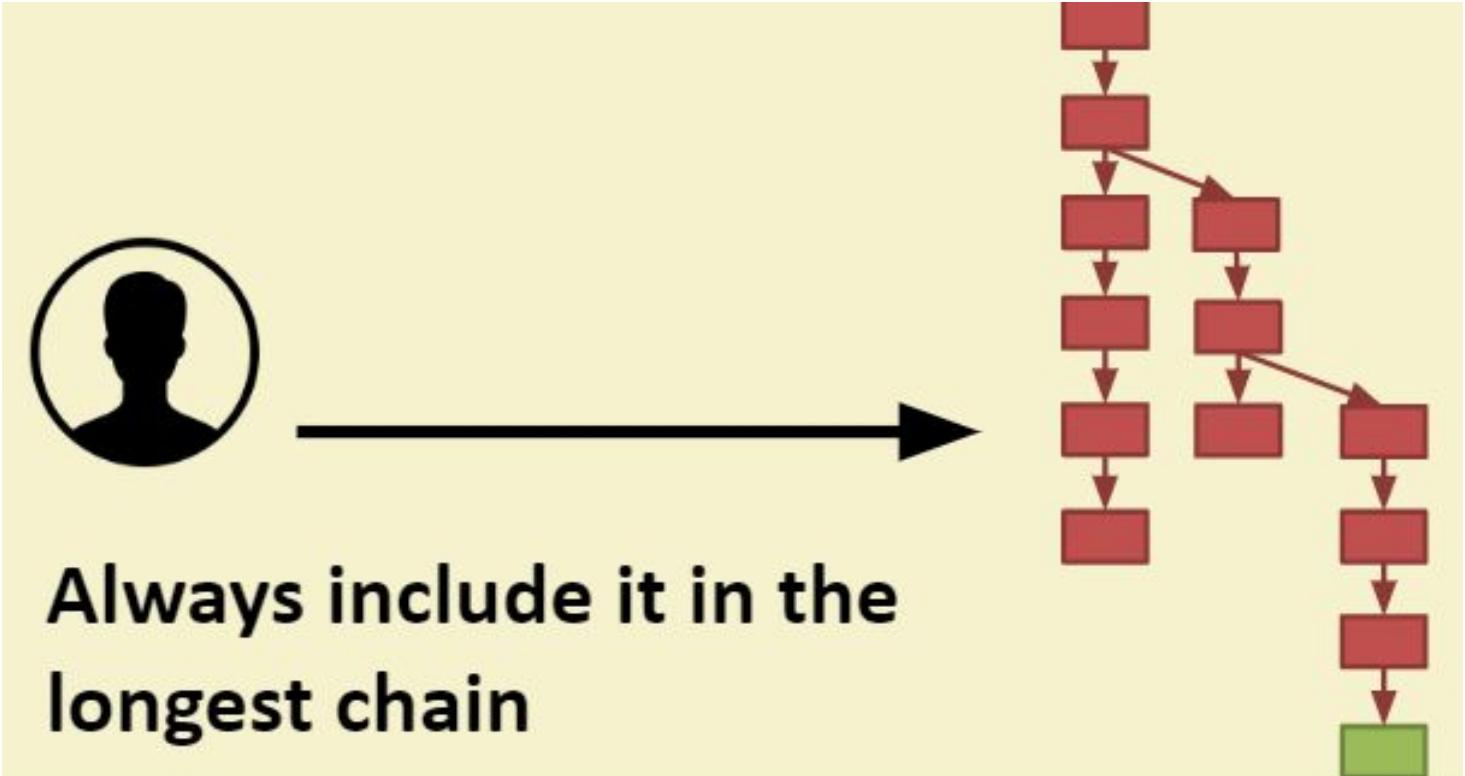
Accepting the Longest Chain



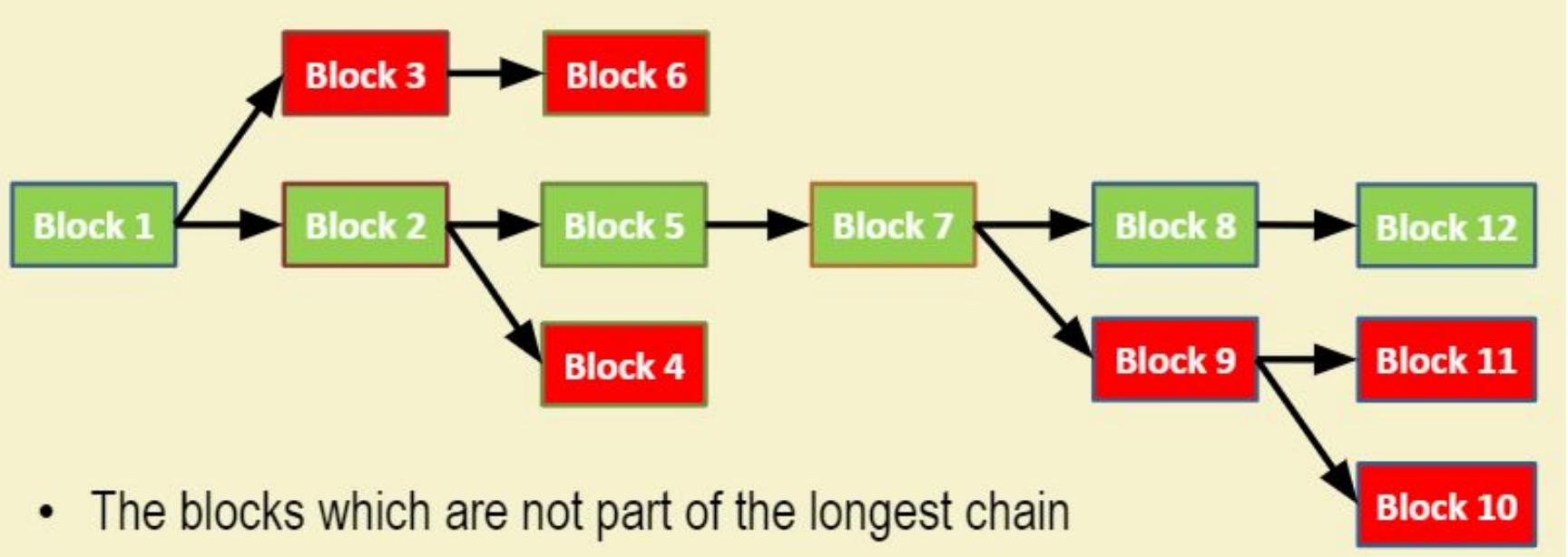
Accepting the Longest Chain



Accepting the Longest Chain



Orphaned Blocks





Since 1962

Bitcoin Block Explorer

LATEST BLOCKS

[SEE MORE →](#)

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)	Weight (kWU)
514498	10 minutes	558	7,462.34 BTC	BitFury	274.33	1,006.96
514497	20 minutes	420	1,304.07 BTC	SlushPool	169.58	600.54
514496	23 minutes	1141	6,975.70 BTC	SlushPool	573.67	2,072.44
514495	33 minutes	919	3,656.77 BTC	BTC.com	466.33	1,633.82

Source: <https://blockchain.info/>

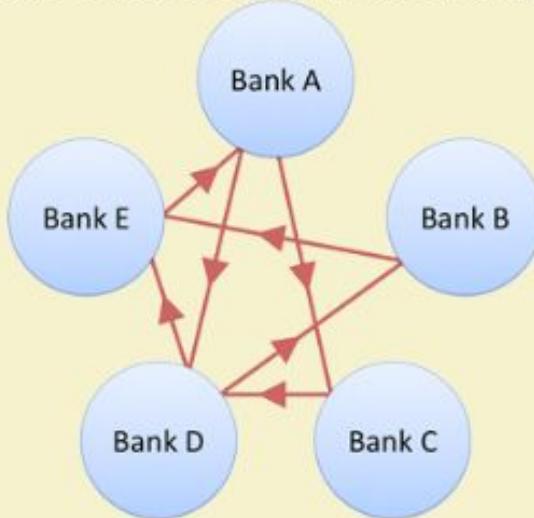


The Permissioned (Private) Blockchain Model

- Blockchain can be applied just beyond cryptocurrency
- The underlying notions of consensus, security and distributed replicated ledgers can be applied to even closed or **permissioned network** settings
- Most enterprise use cases only involve a few ten to a few hundred known participants

The Permissioned Model Applications

- Asset Movements and Tracking



Asset movements
in financial marketplaces

Source: <https://www.multichain.com>



Asset movements
in supply chains

What is Bitcoin?

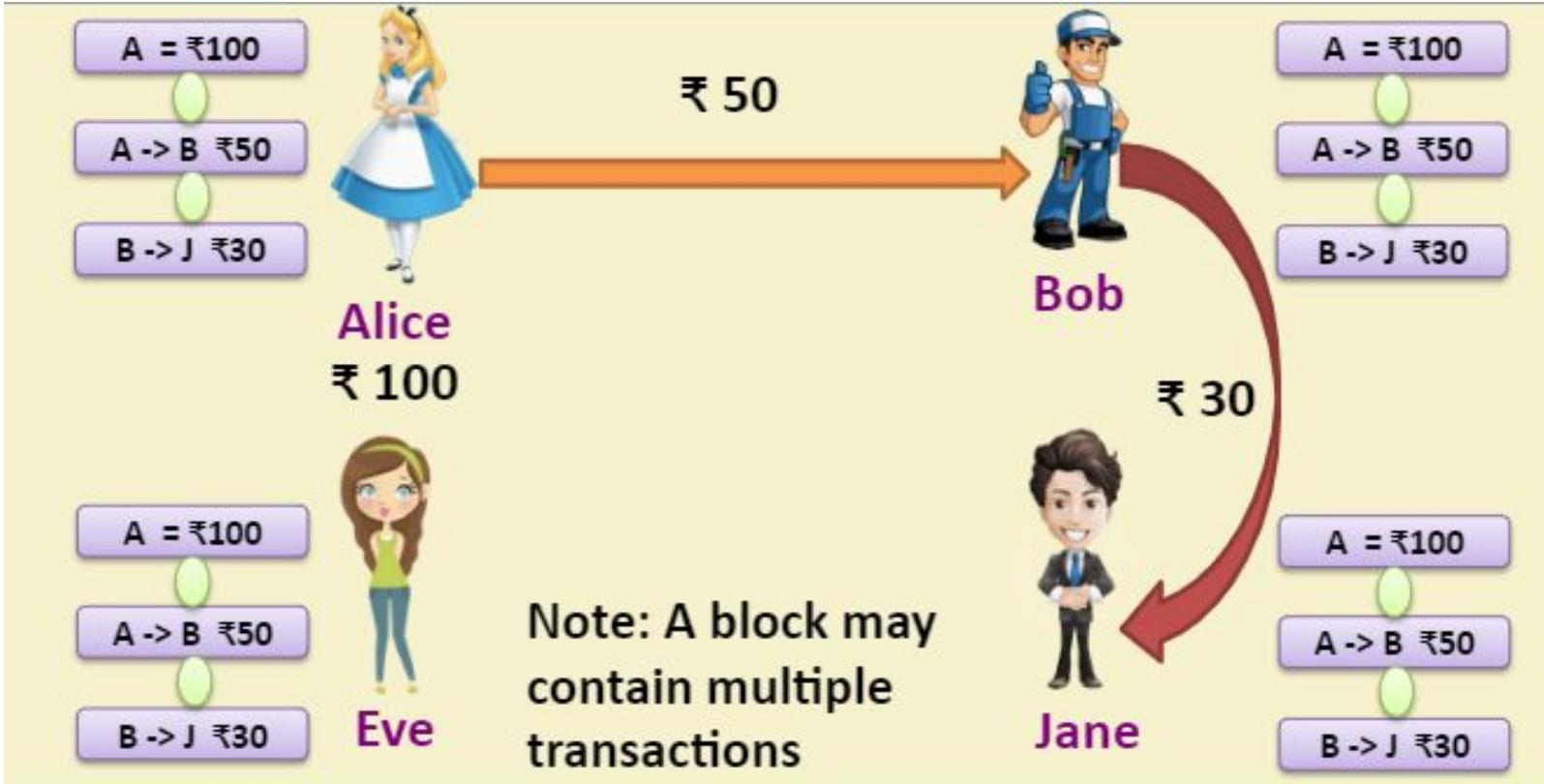
TECHNOLOGY

Blockchain

PROTOCOL / COIN /

TOKEN

Technology behind Bitcoin - Blockchain



What is Bitcoin?

TECHNOLOGY

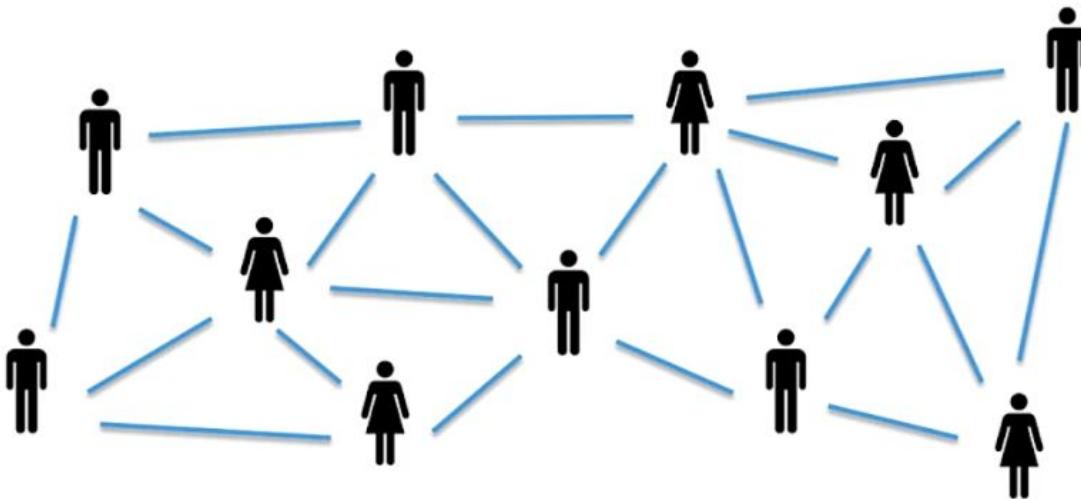
Blockchain

PROTOCOL / COIN /

Bitcoin

TOKEN

What is Bitcoin?



What is Bitcoin?

- “A **decentralized digital currency** enables instant payments to anyone, anywhere in the world” – en.bitcoin.it
- No central authority, uses peer-to-peer technology

Two broad operations

- **Transaction Management** – transfer of bitcoins from one user to another
- **Money Issuance** – regulate the monetary base

What is Bitcoin?

TECHNOLOGY

Blockchain

PROTOCOL / COIN /

Waves



Ethereum



Bitcoin



Neo



Ripple



TOKEN

What is Bitcoin?

TECHNOLOGY

Blockchain

PROTOCOL / COIN /

Waves



Ethereum



Bitcoin



Neo



Ripple



TOKEN

WCT

B1

WGR

INTL

TRX

AE

REP

SNT

RHOC

MKR

PPT

BNB



ACAT

TNC

DBC

RPX

QLC

TKY

ONT

IAM



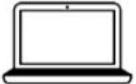
What is Bitcoin?

The Bitcoin Ecosystem:

- Nodes



- Miners



- Large Mines



- Mining Pools



Bitcoin Basics - Creation of Coins

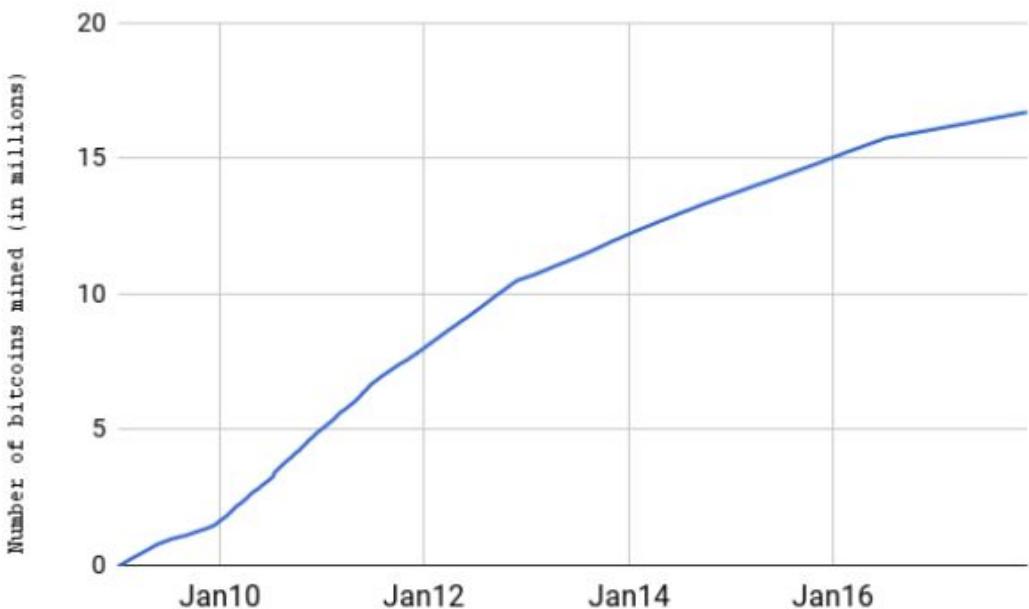
- **Controlled Supply:** Must be limited for the currency to have value – any maliciously generated currency needs to be rejected by the network
- Bitcoins are generated **during the mining** – each time a user discovers a new block
- The **rate of block creation is adjusted every 2016 blocks** to aim for a constant two week adjustment period

Bitcoin Basics - Creation of Coins

- The number of bitcoins generated per block is set to **decrease geometrically**, with a **50% reduction** for every **210,000 blocks**, or approximately 4 years
- This reduces, with time, the amount of bitcoins generated per block
 - Theoretical limit for total bitcoins: Slightly less than **21 million**
 - Miners will get less reward as time progresses
 - How to pay the mining fee – increase the transaction fee

Bitcoin Supply

- The block subsidy was initially 50 BTC per block
- Halves every 210,000 blocks \approx 4 years
- Became 25 BTC in Nov 2012 and 12.5 BTC in July 2016
- Total Bitcoin supply is 21 million



- The last bitcoin will be mined in 2140

Projected Bitcoin

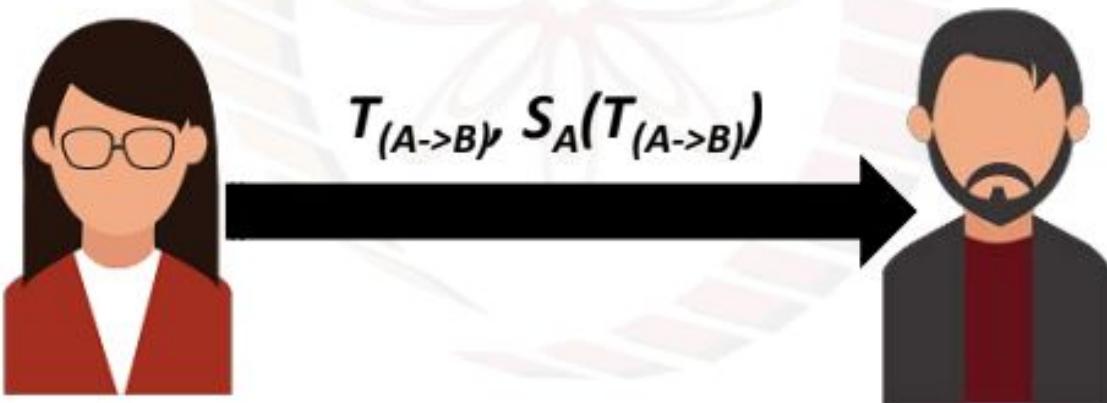
Date reached	Block	Reward Era	BTC/block	Year (estimate)	Start BTC	BTC Added	End BTC	BTC Increase	End BTC % of Limit
2009-01-03	0	1	50.00	2009	0	2625000	2625000	infinite	12.500%
2010-04-22	52500	1	50.00	2010	2625000	2625000	5250000	100.00%	25.000%
2011-01-28	105000	1	50.00	2011*	5250000	2625000	7875000	50.00%	37.500%
2011-12-14	157500	1	50.00	2012	7875000	2625000	10500000	33.33%	50.000%
2012-11-28	210000	2	25.00	2013	10500000	1312500	11812500	12.50%	56.250%
2013-10-09	262500	2	25.00	2014	11812500	1312500	13125000	11.11%	62.500%
2014-08-11	315000	2	25.00	2015	13125000	1312500	14437500	10.00%	68.750%
2015-07-29	367500	2	25.00	2016	14437500	1312500	15750000	9.09%	75.000%
2016-07-09	420000	3	12.50	2016	15750000	656250	16406250	4.17%	78.125%
2017-06-23	472500	3	12.50	2018	16406250	656250	17062500	4.00%	81.250%
	525000	3	12.50	2019	17062500	656250	17718750	3.85%	84.375%
	577500	3	12.50	2020	17718750	656250	18375000	3.70%	87.500%
	630000	4	6.25	2021	18375000	328125	18703125	1.79%	89.063%
	682500	4	6.25	2022	18703125	328125	19031250	1.75%	90.625%
	735000	4	6.25	2023	19031250	328125	19359375	1.72%	92.188%
	787500	4	6.25	2024	19359375	328125	19687500	1.69%	93.750%

Bitcoin Basics - Sending Payments

- Need to ensure that Eve cannot spend Alice's bitcoins by creating transactions in her name.
- Bitcoin uses public key cryptography to make and verify digital signatures.
- Each person has one or more addresses each with an associated pair of public and private keys (may hold in the bitcoin wallet)

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



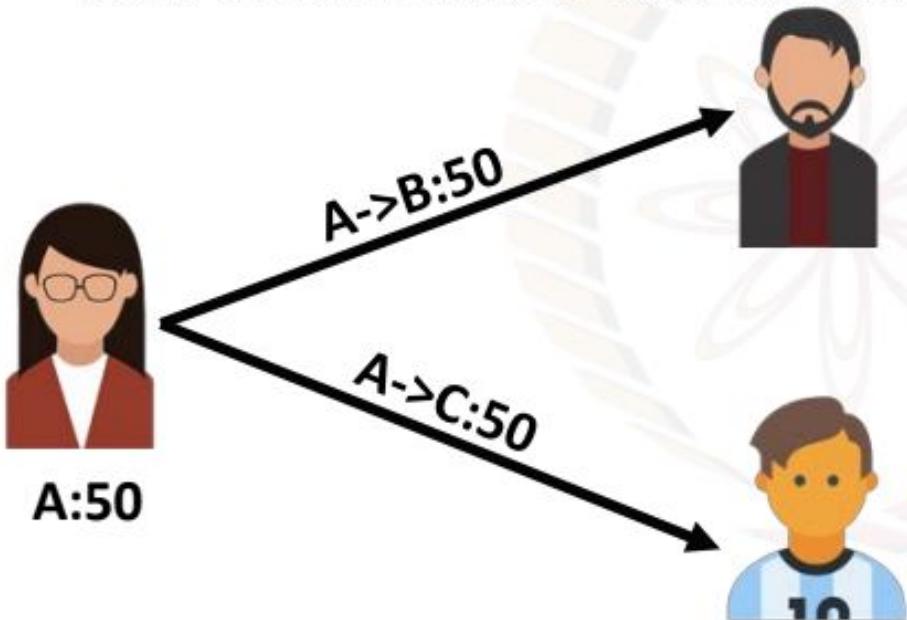
Bitcoin Basics - Sending Payments

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

Bitcoin Basics - 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?**

Bitcoin Basics - Handling Double Spending

- 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

Bitcoin Basics - Handling Double Spending

- 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

Bitcoin Basics - Handling Double Spending

- 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

Bitcoin Anonymity

- Bitcoin is permission-less, you do not need to setup any “account”, or required any email address, user name or password to login to the wallet
- The public and the private keys do not need to be registered, the wallet can generate them for the users
- The bitcoin address is used for transaction, not the user name or identity

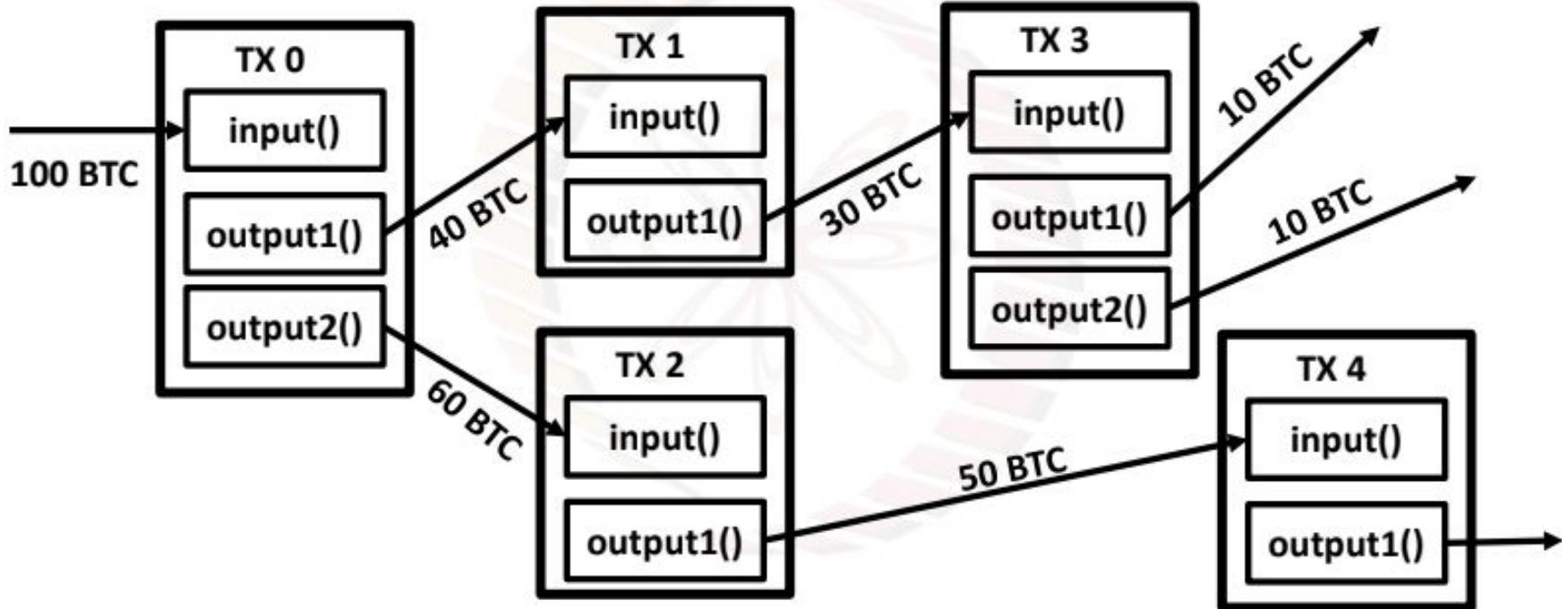
Bitcoin Anonymity

- A bitcoin address mathematically corresponds to a public key based on ECDSA – the digital signature algorithm used in bitcoin
- [A sample bitcoin address:](#)
`1PHYrmdJ22MKbJevpb3MBNpVckjZHt89hz`
- Each person can have many such addresses, each with its own balance
 - Difficult to know which person owns what amount

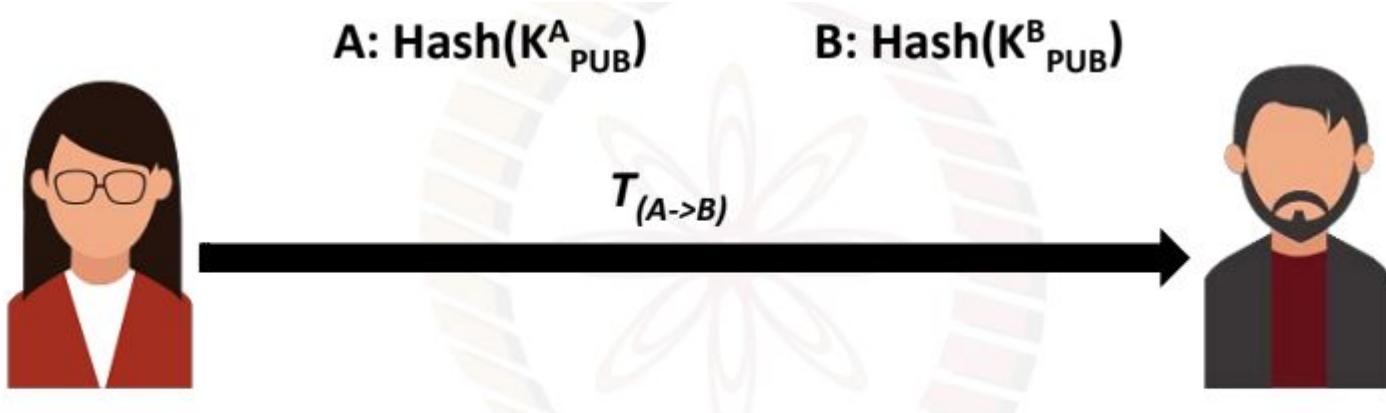
Bitcoin Transactions

- Alice makes a transaction of BTC 20 to Bob. How Bob will claim those transactions?
- A transaction is characterized by two parameters
 - Alice sends some bitcoins: **the output (out) of the transaction**
 - Bob receives some bitcoins: the **input (in) of the transaction**
- We need to determine that a transaction input correctly claims a transaction output

Bitcoin Transactions, Input and Output



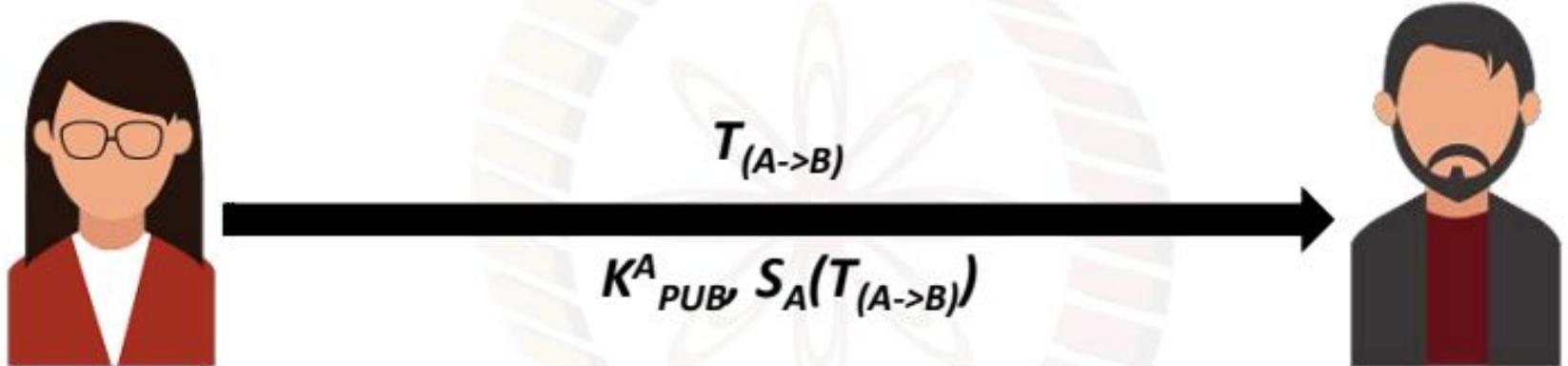
Bitcoin Transactions - A Simple Example



How Bob will verify that the transaction is actually originated from Alice?

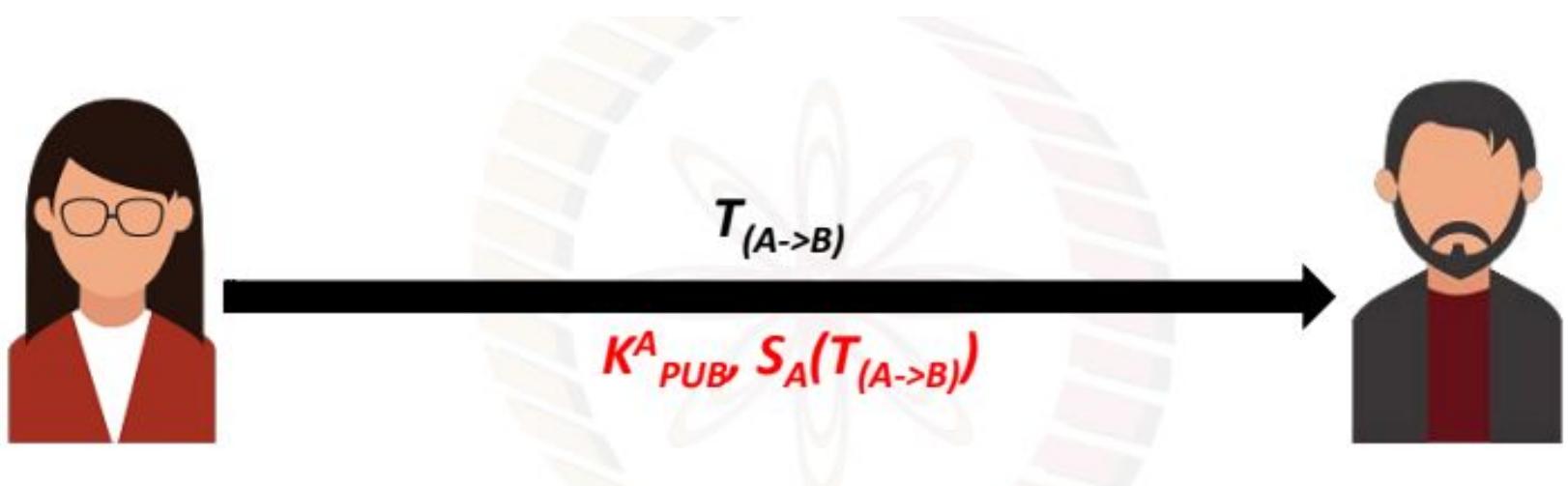


Bitcoin Transactions - A Simple Example



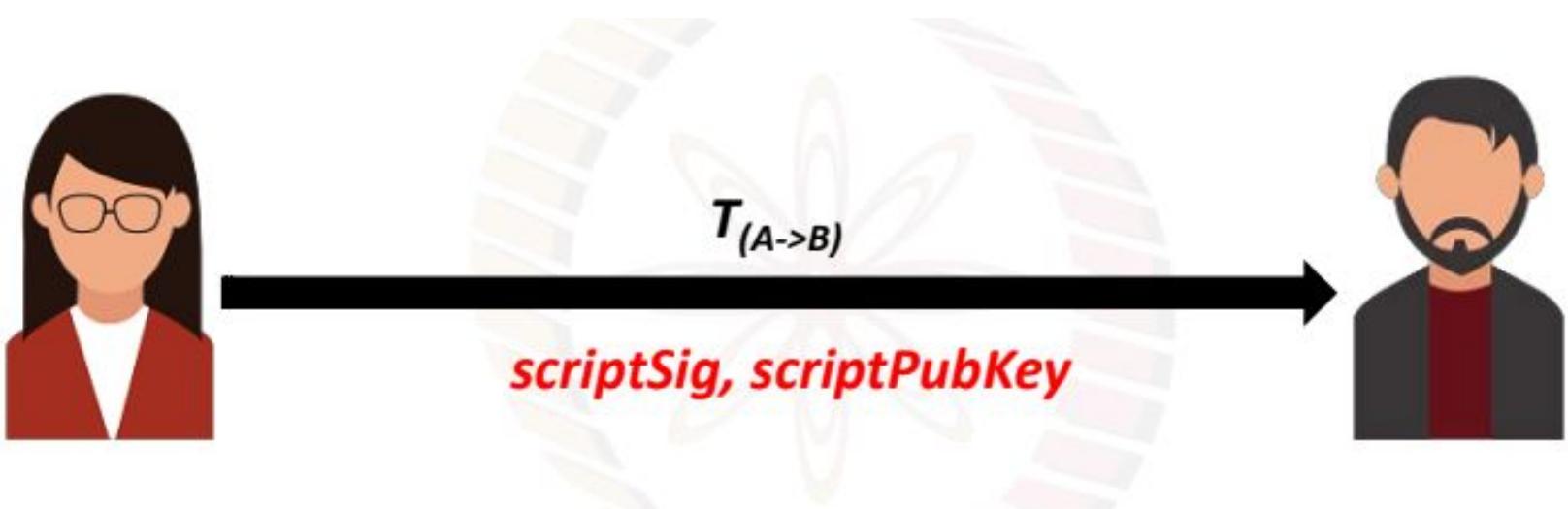
**Send the public key of Alice along with the
signature -> Bob can verify this**

Bitcoin Transactions - A Simple Example



Bitcoin indeed transfers scripts instead of the signature and the public key

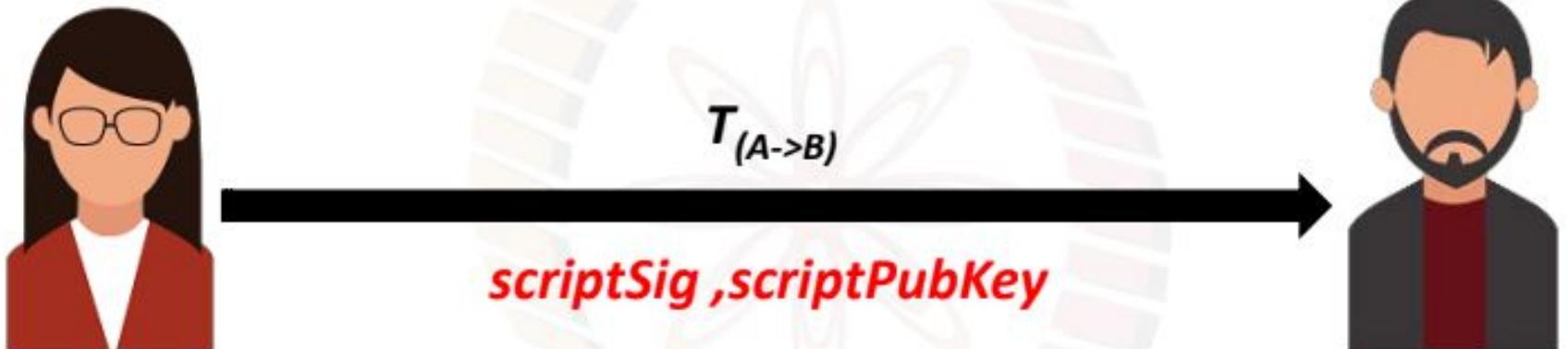
Bitcoin Transactions - A Simple Example



Bitcoin indeed transfers scripts instead of the signature and the public key



Bitcoin Transactions - A Simple Example



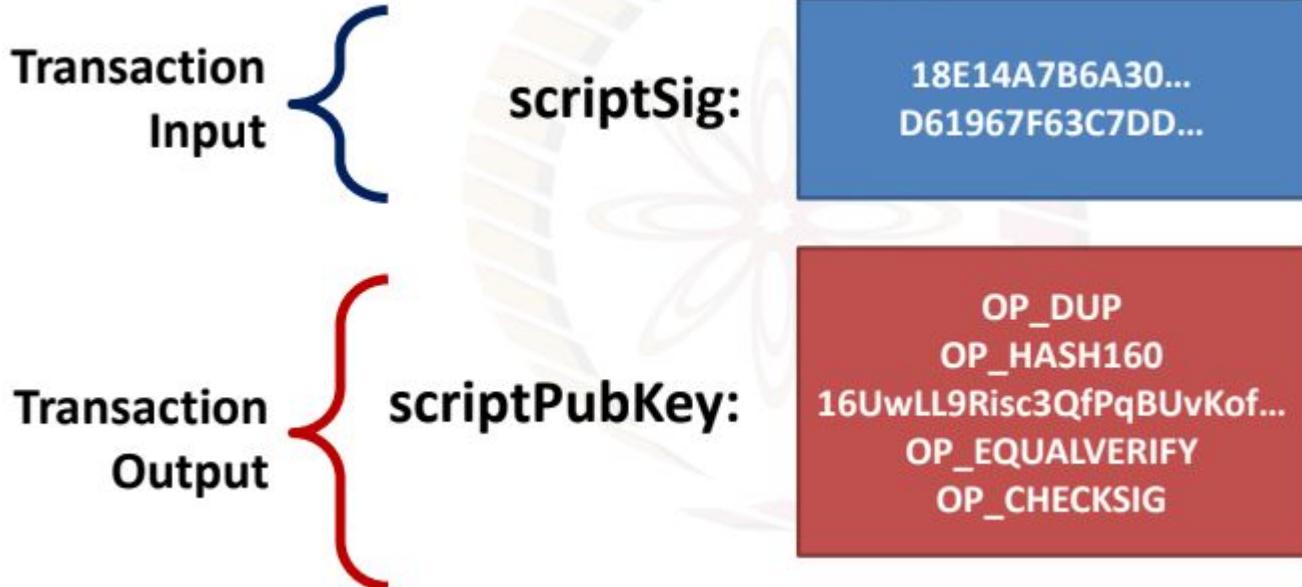
Bob can spend the bitcoins only if both the scripts return true after execution

Bitcoin Transactions - A Simple Example

- With every transaction Alice must provide
 - A **public key** that, when hashed, yields the address of Alice embedded in the script
 - A **signature** to provide ownership of the private key corresponding to the public key of Alice



Bitcoin Transactions - A Simple Example



Bitcoin Transactions - A Simple Example

- Simple, compact, stack-based and processed left to right
 - FORTH like language
- **Not Turing Complete** (no loops)
 - Halting problem is not there



Bitcoin Transaction Lifecycle - The Sender

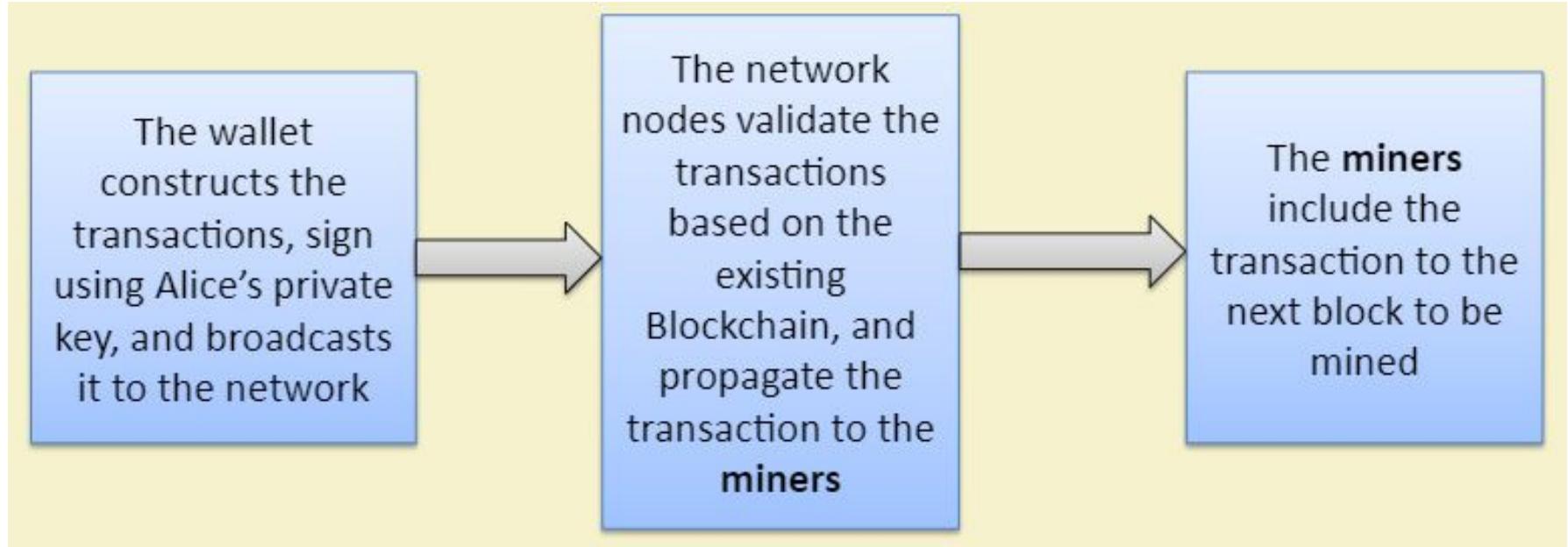


Alice opens her Bitcoin Wallet

Provides the address of Bob and the amount to transfer, and sends



Bitcoin Transaction Lifecycle - The Network



Bitcoin Transaction Lifecycle - The Miners

The **miners** collect all the transactions for the a time duration, say for 10 Minutes

Miners construct a new block and tries to connect it with the existing blockchain, through a cryptographic hash computation

The Mining Procedure

Once the mining is over and the hash is obtained, the block is included in the existing blockchain.

The updated blockchain is propagated in the network

Bitcoin Transaction Lifecycle - The Receiver

Bob opens his Bitcoin Wallet and refreshes, the blockchain gets updated

The transaction reflects at Bob's wallet

Bitcoin		
UGX	rate 708.41	
	balance 337952.50	
USD (default)	rate 0.24	
	balance 112.44	
UYU	rate 6.17	
	balance 2544.04	
UZS	rate 593.90	
	balance 283322.42	
VEF	rate 1.50	
	balance 712.64	
VND	rate 5112.73	
	balance 2439659.32	
VUV	rate 25.04	
	balance 11945.69	

mBTC 477.06

= USD 112.44



Apr 30 1CQhRcTg c4KA MFFB xDdY vYIA rFnJ... - 4.20

Apr 22 1lmb MvQ3 9fNnR mFYF NVw dqdg mm... - 21.29

April 21, 15:18 18CK Sk1g aJRK KSC7 yVST XT9L Uzbh... + 6.26

Apr 17 18CK Sk1g aJRK KSC7 yVST XT9L Uzbh... + 13.09

Apr 17 18CK Sk1g aJRK KSC7 yVST XT9L Uzbh... + 1.00



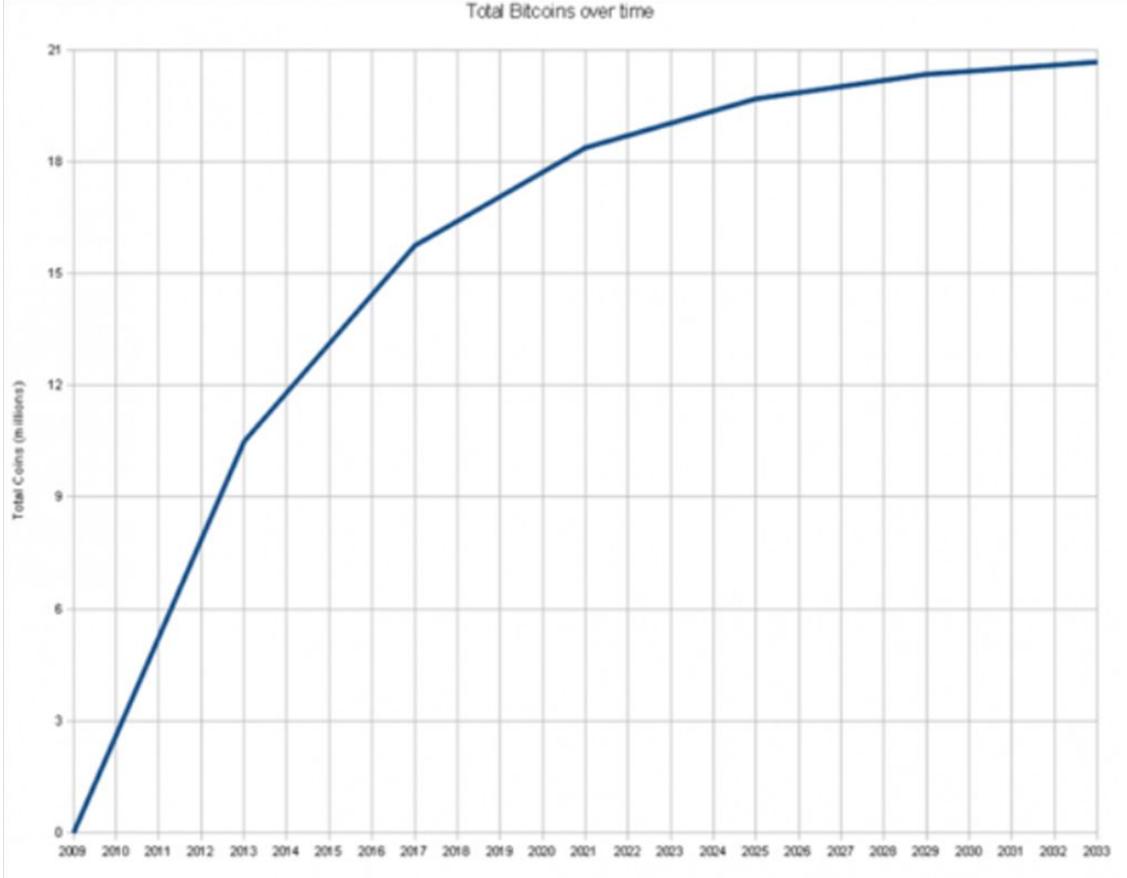
Agenda

- **History of Bitcoin**
- **Getting the first Bitcoin**
- **Find the current price of Bitcoin**
- **Bitcoin Scripting Language**
- **Bitcoin P2P Network**
- **Bitcoin Transaction Format**
- **Bitcoin transactions**

Where do Bitcoins come from?

- They're **mined**.
- **High-powered computers** solve complicated math problems.
- Each time a problem is solved, the **finder** is paid a **bounty**.

Bitcoins Monetary Creation



Source:

https://en.bitcoin.it/wiki/Controlled_supply

Owning Bitcoins

- Users create accounts called **wallets**.
- Wallets are secured using passwords and contain the private keys used for transferring bitcoins.



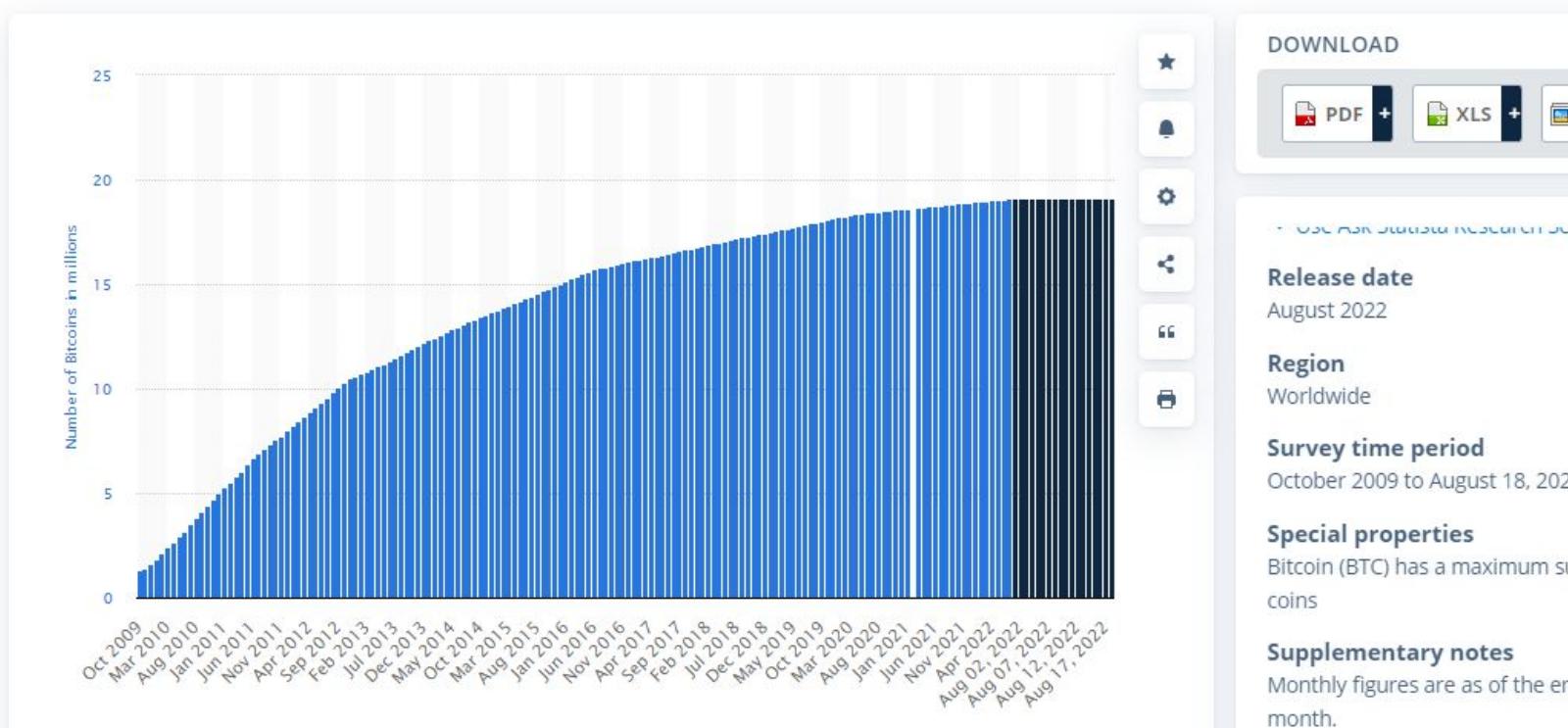


Size of the Bitcoin Economy

- Total number of BitCoins generated cannot exceed 21 million
- Average price of a Bitcoin: around **\$300 - Price has been unstable.**
- 30 Transactions per min. (Visa transaction 200,000 per minute.)

Size of the Bitcoin Economy

Number of Bitcoin tokens in circulation from October 2009 to August 18, 2022
(in millions)





Security in Bitcoin

- **Authentication** - Am I paying the right person? Not some other impersonator?
- **Integrity** – Is the coin double-spent?
 - Can an attacker reverse or change transactions?
- **Availability** – Can I make a transaction anytime I want?
- **Confidentiality** – Are my transactions private? Anonymous?

Security in Bitcoin



- **Authentication** - Am I paying the right person? Not some other impersonator? : [Public Key Crypto: Digital Signatures](#)
- **Integrity** : Digital Signatures and Cryptographic Hash
 - Is the coin double-spent?
 - Can an attacker reverse or change transactions?
- **Availability** – Can I make a transaction anytime I want? : [Broadcast messages to the P2P network](#)
- **Confidentiality** – Are my transactions private? Anonymous? : [Pseudonymity](#)

Security in Bitcoin

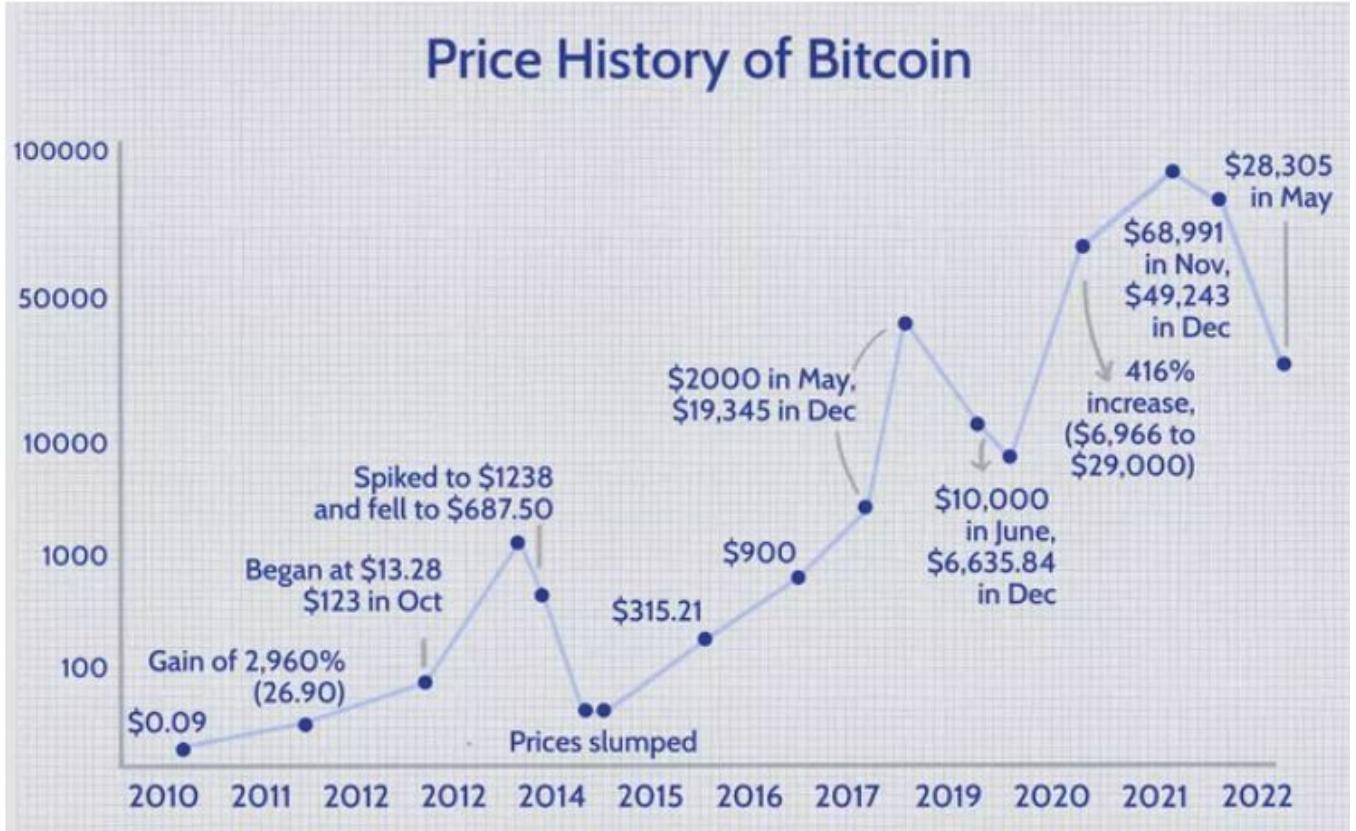
Validation

- Is the coin legit? (proof-of-work) : Use of Cryptographic Hashes
- How do you prevent a coin from double-spending? - Broadcast to all nodes

Creation of a virtual coin/note

- How is it created in the first place? - Provide incentives for miners
- How do you prevent inflation? (What prevents anyone from creating lots of coins?) - Limit the creation rate of the BitCoins

Price History of Bitcoin





Finding the Current Price of Bitcoin

		Watchlist	Portfolio	Cryptocurrencies	Categories	DeFi	NFT	Metaverse	Polkadot	BNB Chain	Solana	Avalanche	Show rows	100	Filters	Customize	More
#	Name			Price	1h %	24h %	7d %		Market Cap							Last 7 Days	
1	Bitcoin BTC Buy	\$21,697.69	▲ 0.43%	▲ 1.10%	▼ 7.62%	\$415,112,796,009	\$32,257,299,350 1,486,670 BTC	19,131,662 BTC									
2	Ethereum ETH Buy	\$1,707.40	▲ 0.39%	▲ 3.48%	▼ 8.20%	\$208,484,891,687	\$15,894,469,831 9,309,139 ETH	122,106,291 ETH									
3	Tether USDT Buy	\$1.00	▼ 0.00%	▼ 0.00%	▼ 0.00%	\$67,551,413,682	\$48,070,821,901 48,069,499,168 USDT	67,549,554,915 USDT									

Courtesy: <https://coinmarketcap.com/>



Bitcoin Scripting Language



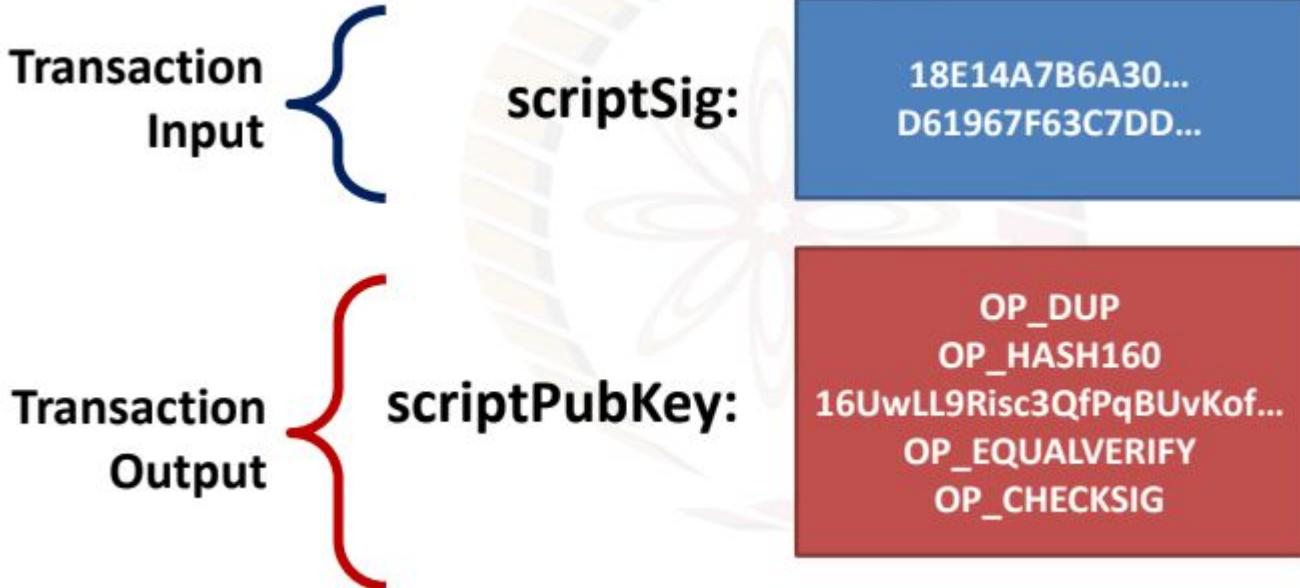
Bitcoin Scripts



With every transaction Alice must provide

- A public key that, when hashed, yields the address of Alice embedded in the script
- A signature to provide ownership of the private key corresponding to the public key of Alice

Bitcoin Scripts



Bitcoin Scripts

scriptPubKey: OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY
OP_CHECKSIG

scriptSig: <sig> <pubKey>

- The stack is initially empty. Both the scripts are combined – input followed by output

<sig> <pubKey> OP_DUP OP_HASH160 <pubKeyHash>
OP_EQUALVERIFY OP_CHECKSIG

Bitcoin Scripts

<sig> <pubKey> OP_DUP OP_HASH160 <pubKeyHash>
OP_EQUALVERIFY OP_CHECKSIG

- The stack is initially empty. Both the scripts are combined

<pubKey>
<sig>

OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG



Bitcoin Scripts

OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG

<pubKey>

<pubKey>

<sig>

- Top stack item is duplicated

OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG

Bitcoin Scripts

OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG

- Top stack item is hashed (RIPEMD-160 hashing)

<pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG

<pubHash>
<pubKey>
<sig>





Bitcoin Scripts

<pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG

- The constant is pushed in the stack

OP_EQUALVERIFY OP_CHECKSIG

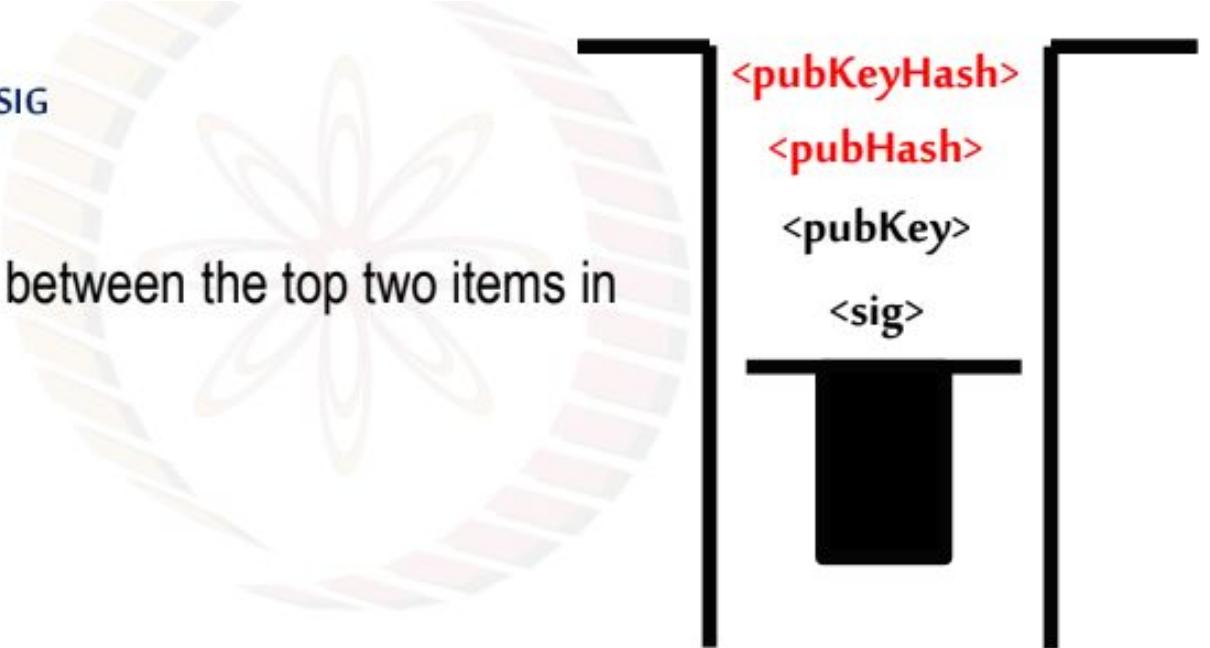
<pubKeyHash>
<pubHash>
<pubKey>
<sig>

Bitcoin Scripts

OP_EQUALVERIFY OP_CHECKSIG

- Equality is checked between the top two items in the stack

OP_CHECKSIG



<pubKeyHash>
<pubHash>
<pubKey>
<sig>

Bitcoin Scripts

OP_CHECKSIG

- Signature is checked based on the top two stack item

TRUE

<pubKey>
<sig>

Courtesy : <https://en.bitcoin.it/wiki/Script>

Bitcoin Scripts Instructions

Total 256 opcodes (15 disabled, 75 reserved)

- Arithmetic operations
- if-then conditions
- Logical operators
- Data handling (like OP_DUP)
- Cryptographic operations
- Hash functions
- Signature verification
- Multi-signature verification



Bitcoin Scripts Instructions

Freezing funds until a time in the future

scriptPubKey: <expiry_time> OP_CHECKLOCKTIMEVERIFY
OP_DROP OP_DUP OP_HASH160 <pubKeyHash>
OP_EQUALVERIFY OP_CHECKSIG

scriptSig: <sig> <pubKey>



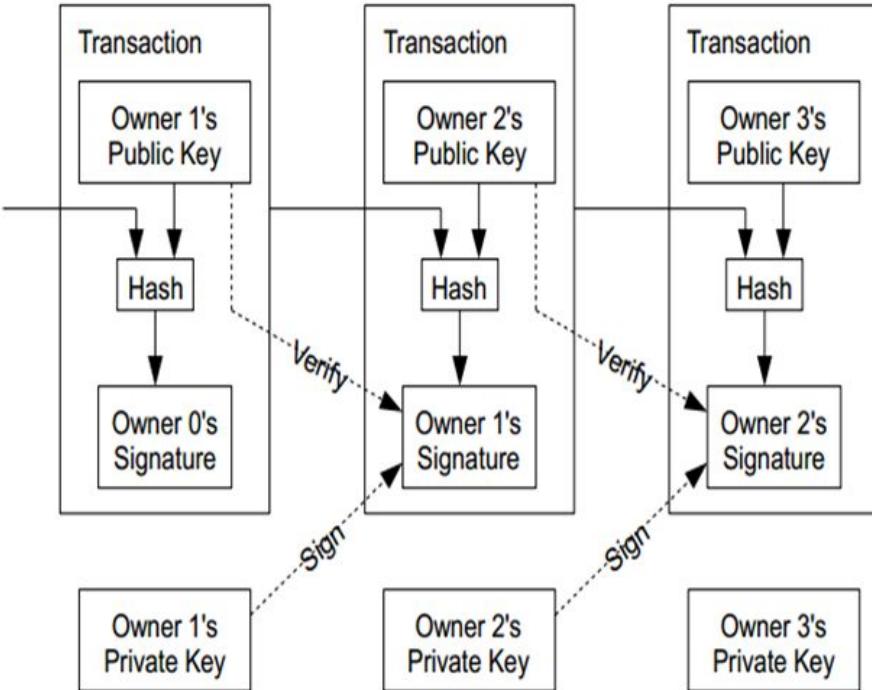
Bitcoin P2P Network

Bitcoin P2P Network

- An ad-hoc network with random topology, Bitcoin protocol runs on **TCP port 8333**
- All nodes (users) in the bitcoin network are treated equally
- New nodes can join any time, **non-responding nodes are removed after 3 hours**

Bitcoin Network

- Electronic coin == chain of digital signatures
- BitCoin transfer: $\text{Sign}(\text{Previous transaction} + \text{New owner's public key})$
- Anyone can verify $(n-1)$ th owner transferred this to the nth owner.
- Anyone can follow the history
- Given a BitCoin

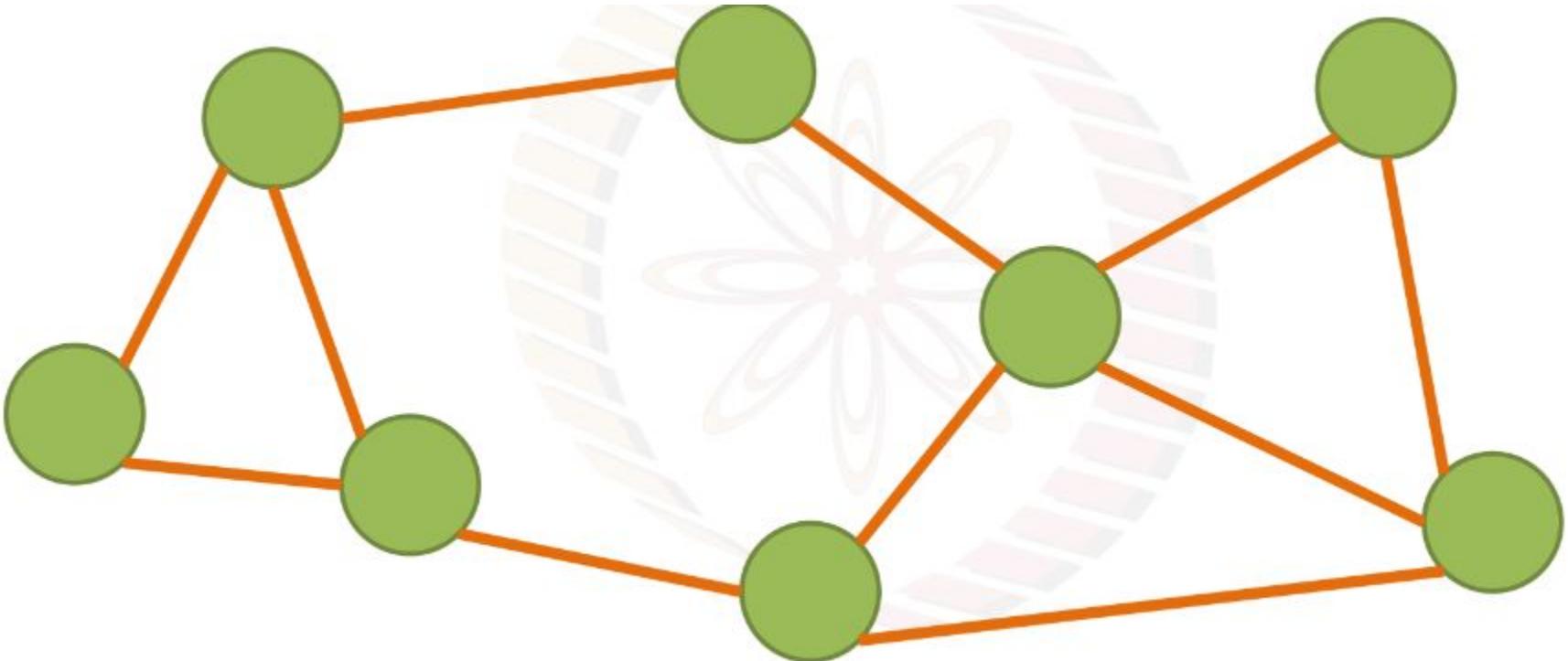


Bitcoin P2P Network

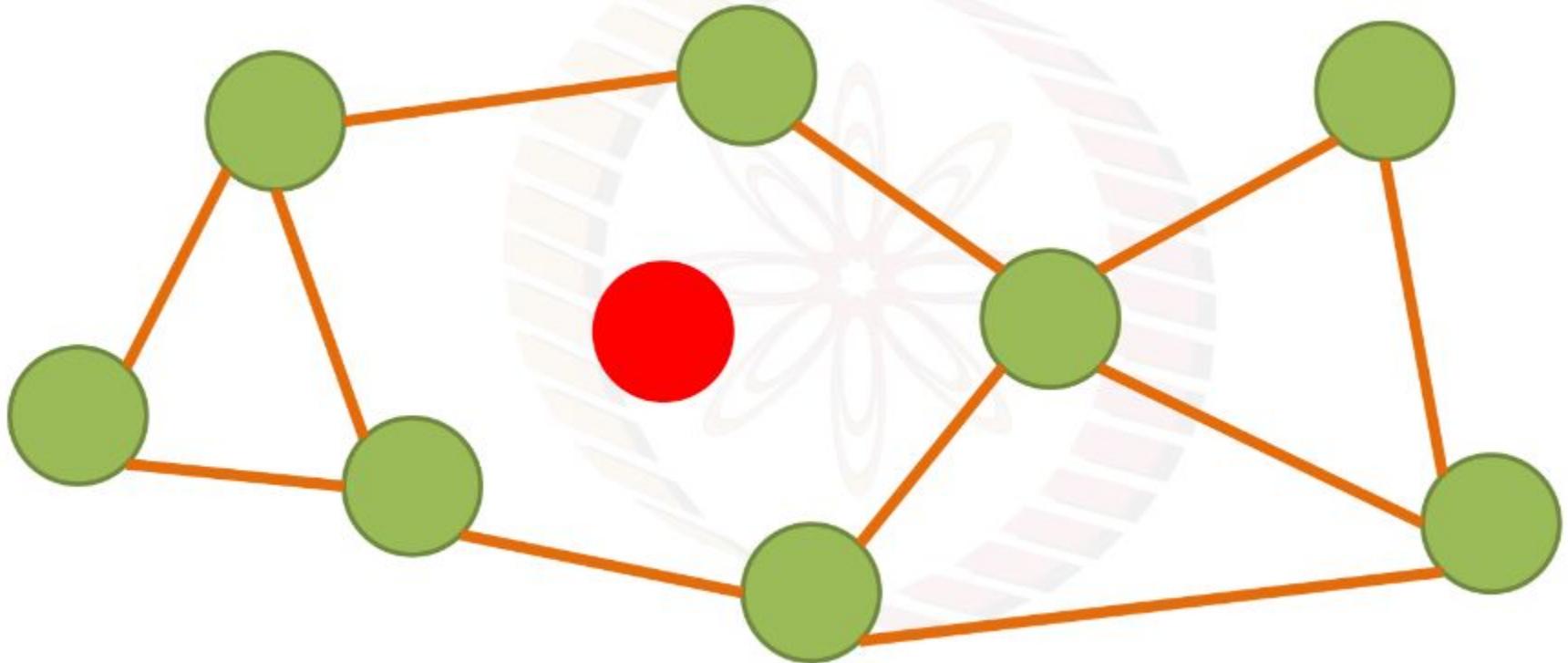
- **Each P2P node runs the following algorithm:**
 - New transactions are broadcast to all nodes.
 - Each node (miners) collects new transactions into a block.
 - Each node works on finding a proof-of-work for its block. **(Hard to do. Probabilistic. The one to finish early will probably win.)**
 - When a node finds a proof-of-work, it broadcasts the block to all nodes.
 - Nodes accept the block only if all transactions in it are valid (**digital signature checking**) and not already spent (check all the transactions).
 - Nodes express their acceptance by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.



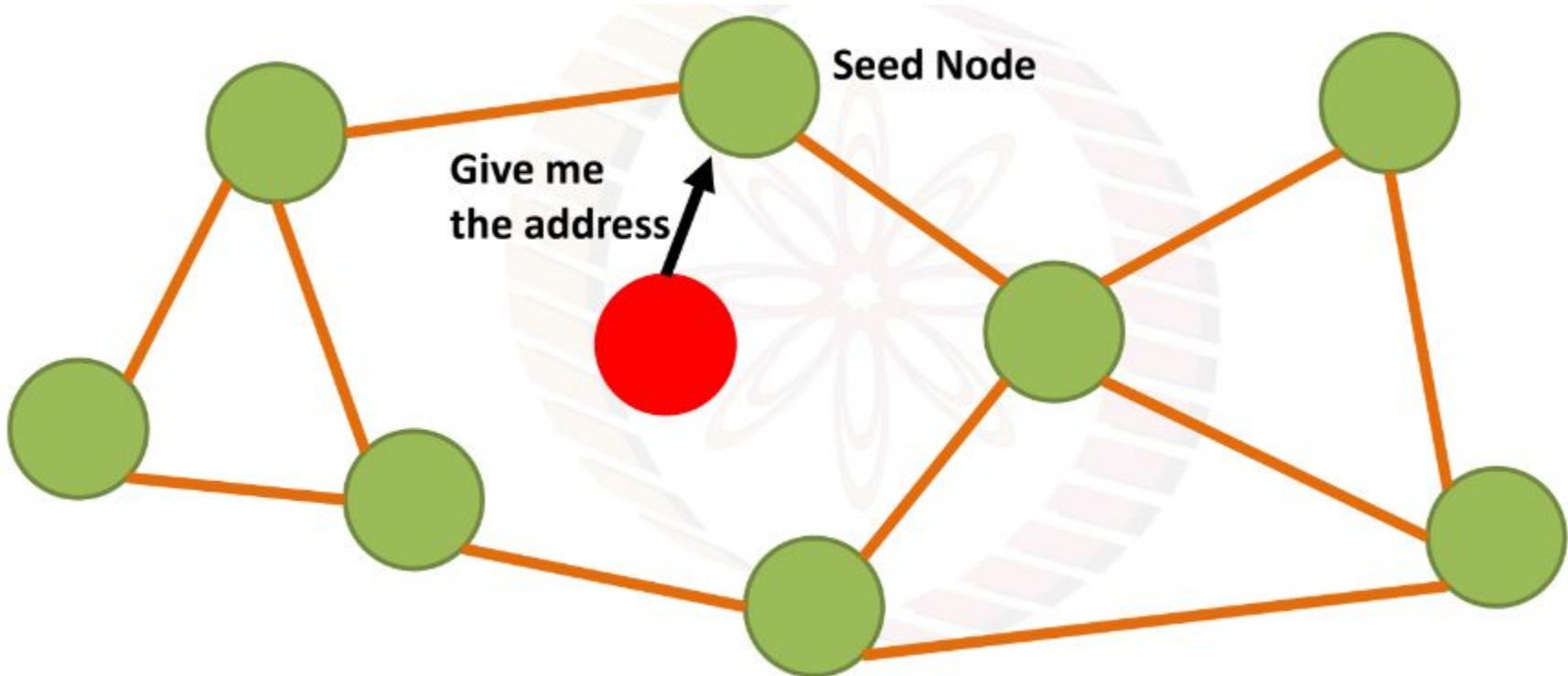
Joining in a Bitcoin P2P Network



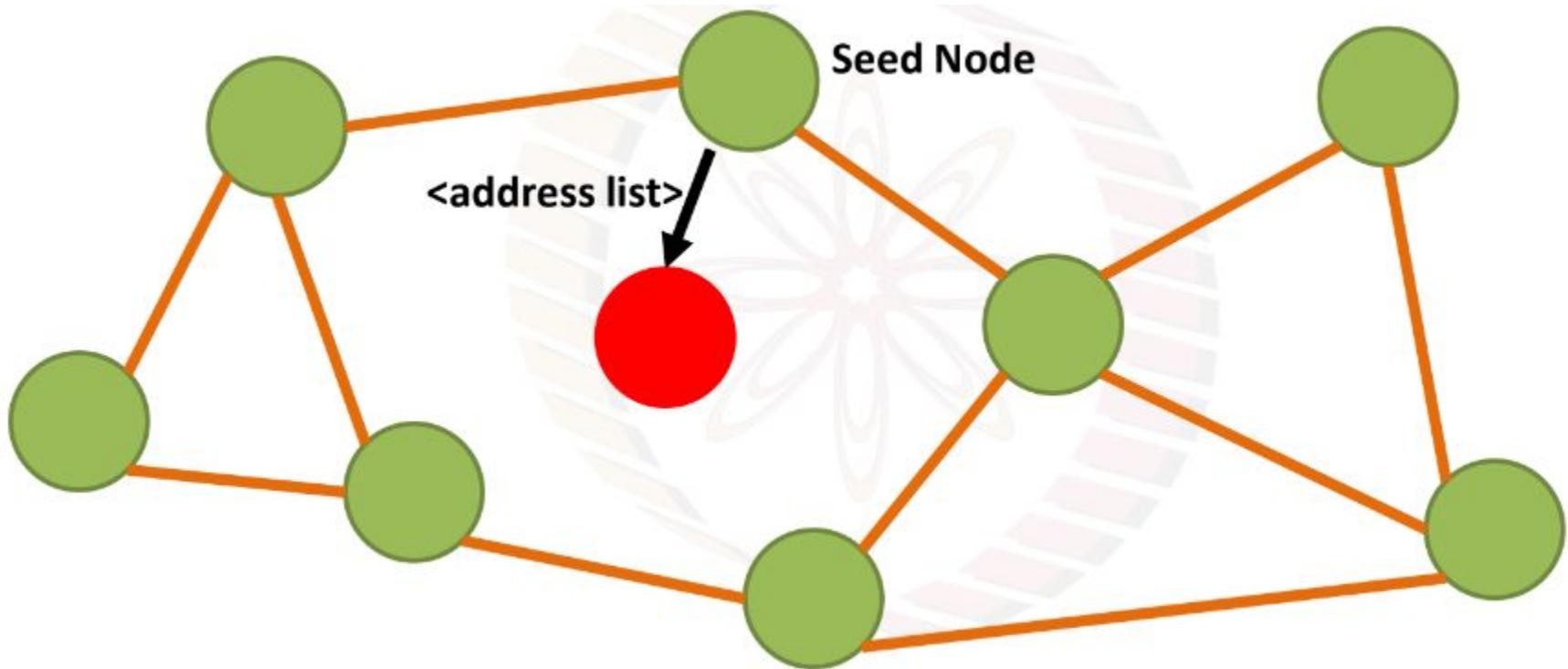
Joining in a Bitcoin P2P Network



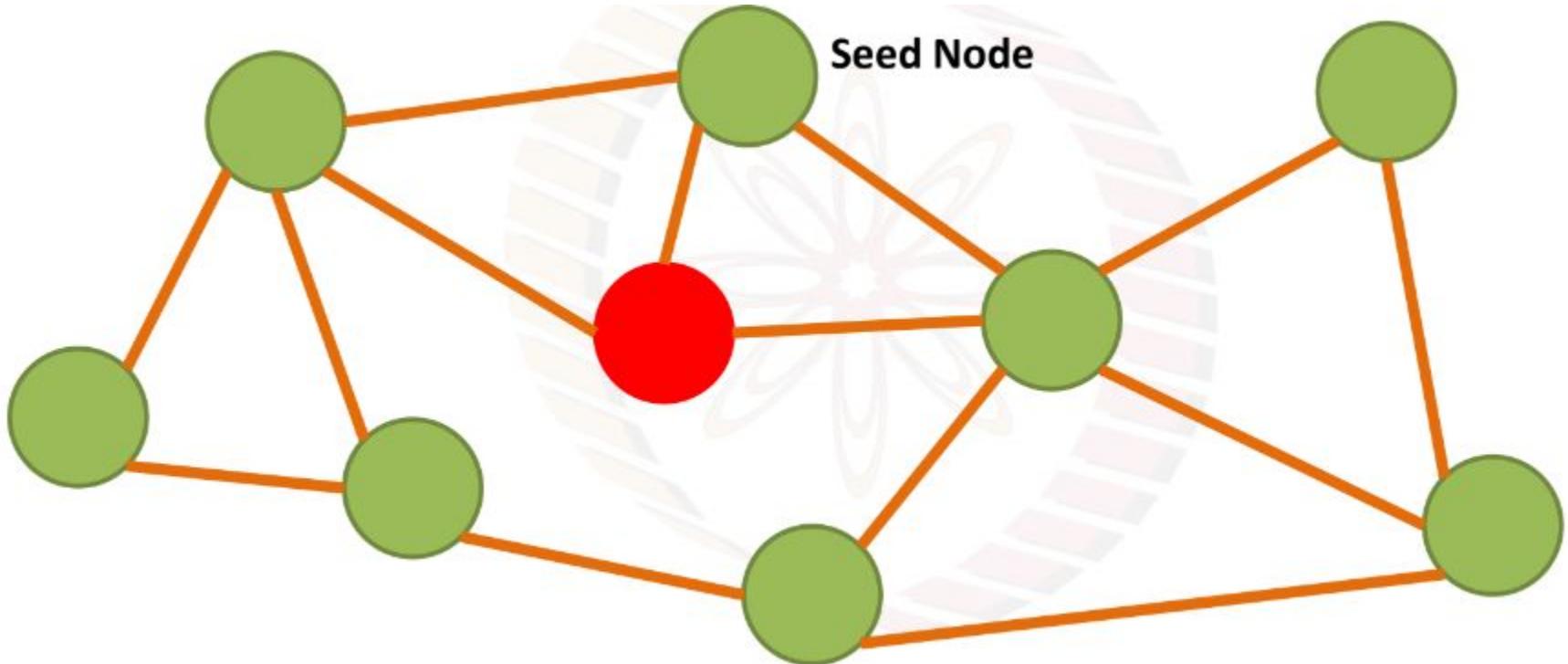
Joining in a Bitcoin P2P Network



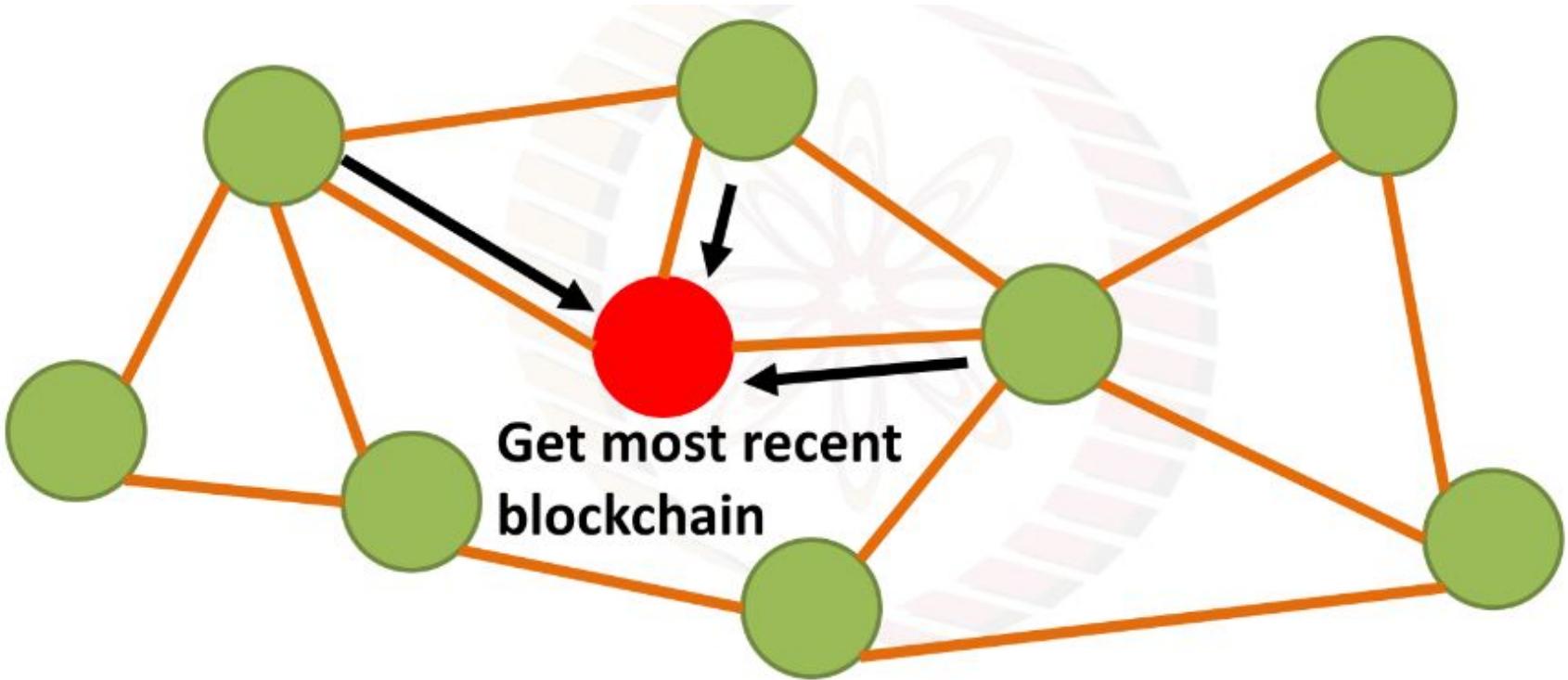
Joining in a Bitcoin P2P Network



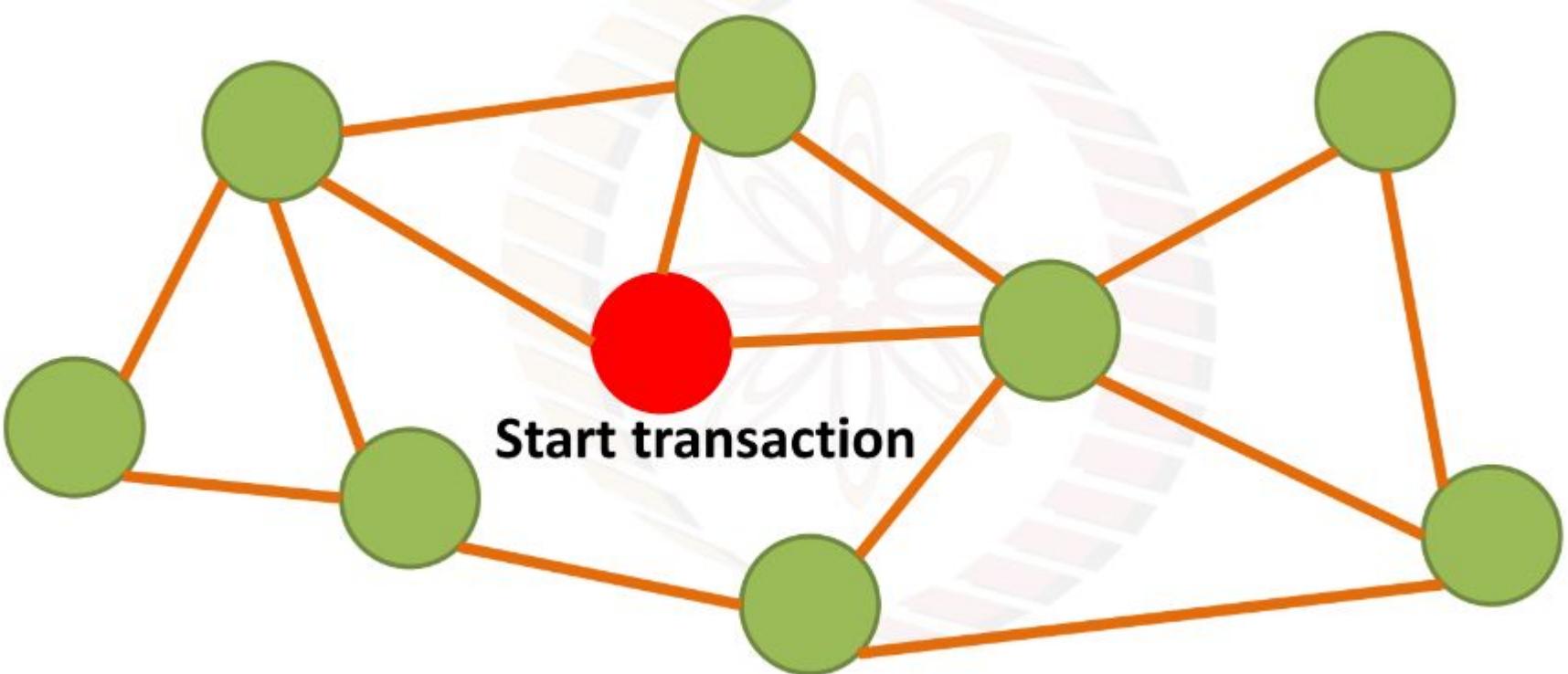
Joining in a Bitcoin P2P Network



Joining in a Bitcoin P2P Network



Joining in a Bitcoin P2P Network

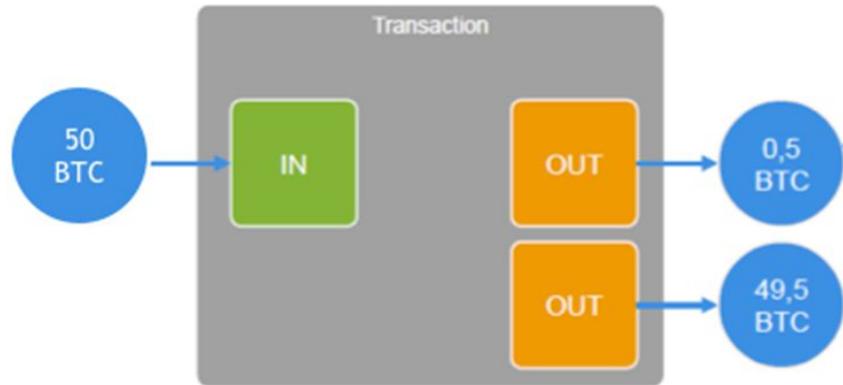




Bitcoin Transaction Format

Bitcoin Transaction Flow

Mining Coinbase



Regular Address to Address Transaction

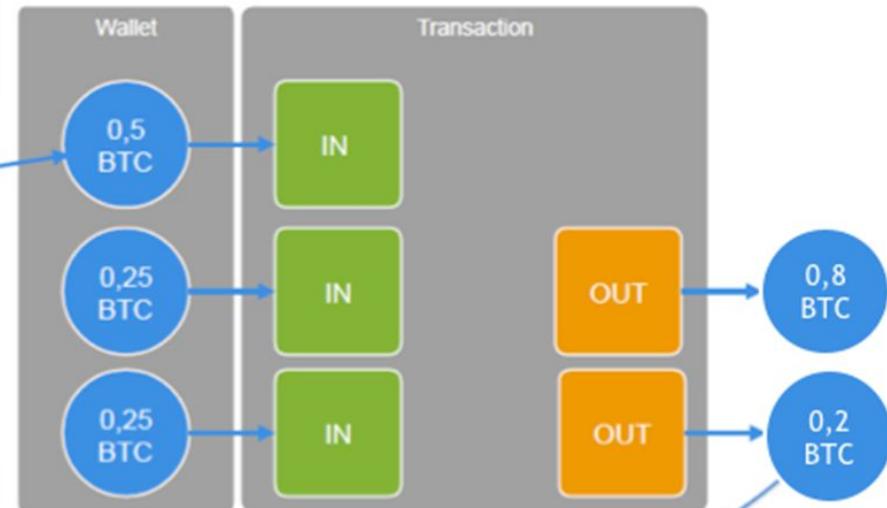


Image source: Scorechain

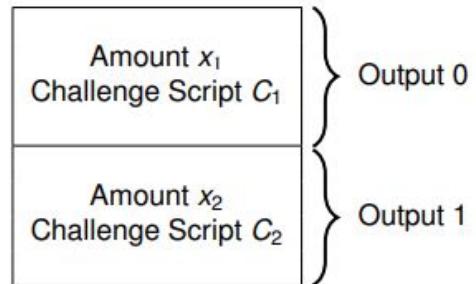
Coinbase Transaction Format

Pre-SegWit

Block Format

Block Header
Number of Transactions n
Coinbase Transaction
Regular Transaction 1
Regular Transaction 2
:
Regular Transaction $n - 1$

Coinbase Transaction



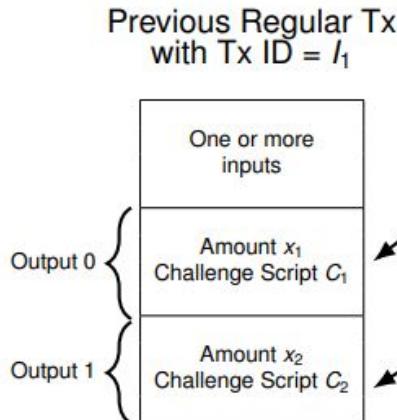
Output Format

nValue
scriptPubkeyLen
scriptPubkey

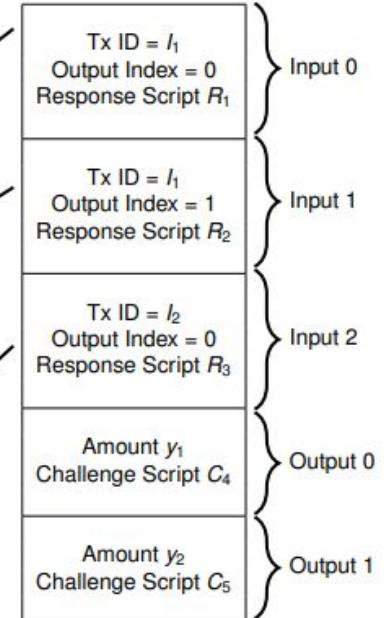
- **nValue** contains number of satoshis locked in output
 - 1 Bitcoin = 10^8 satoshis
- **scriptPubkey** contains the challenge script
- **scriptPubkeyLen** contains byte length of challenge script

Regular Transaction Format

Pre-SegWit



Regular Transaction

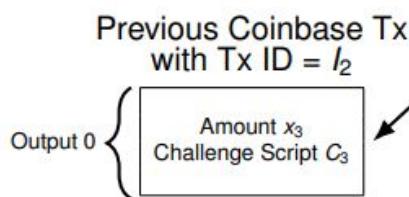


Input Format

hash
n
scriptSigLen
scriptSig
nSequence

Output Format

nValue
scriptPubkeyLen
scriptPubkey



- **hash** and **n** identify output being unlocked
- **scriptSig** contains the response script

Bitcoin Transactions

How Bitcoin Transaction Works?

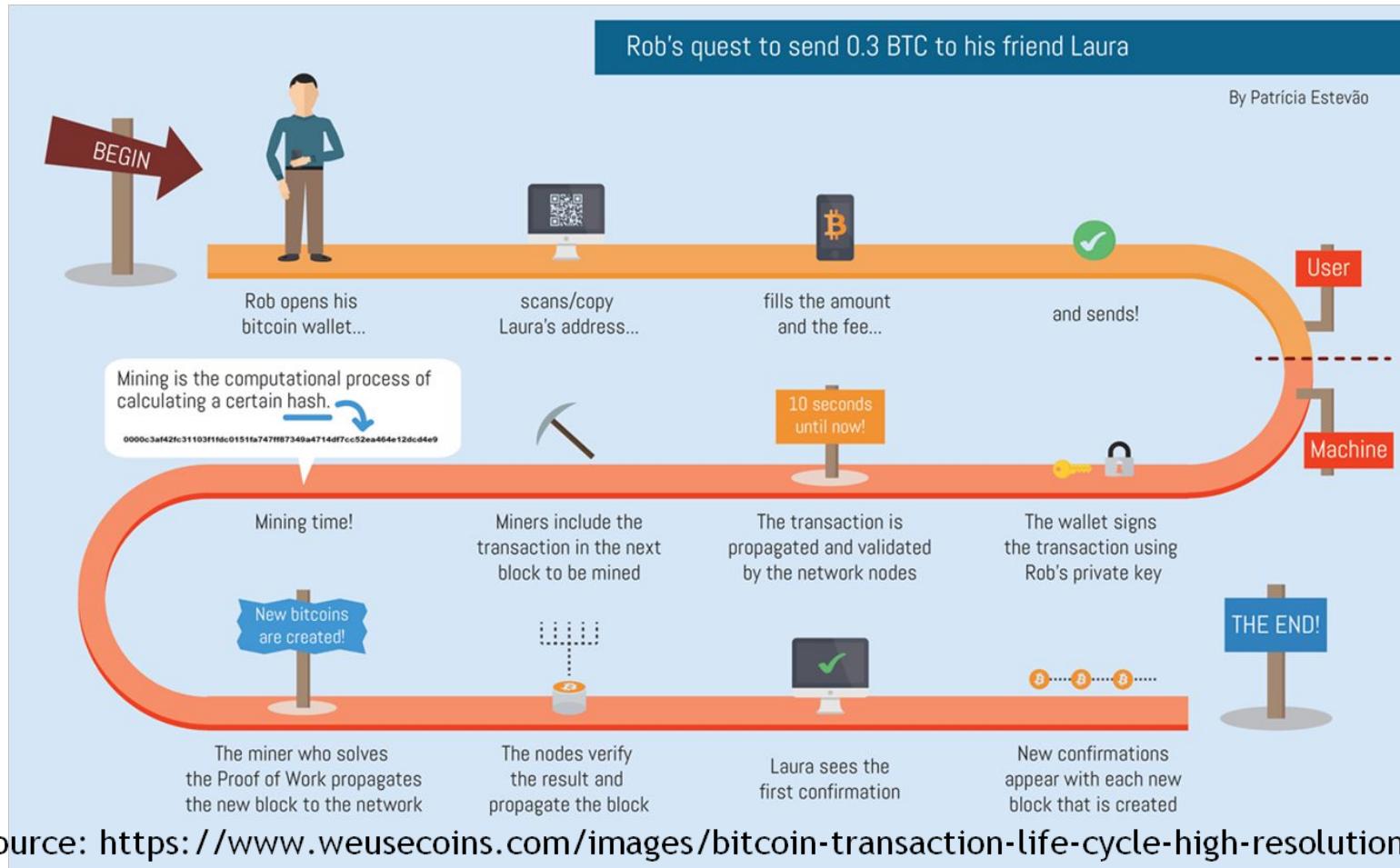


Image source: <https://www.weusecoins.com/images/bitcoin-transaction-life-cycle-high-resolution.png>

Bitcoin Transactions

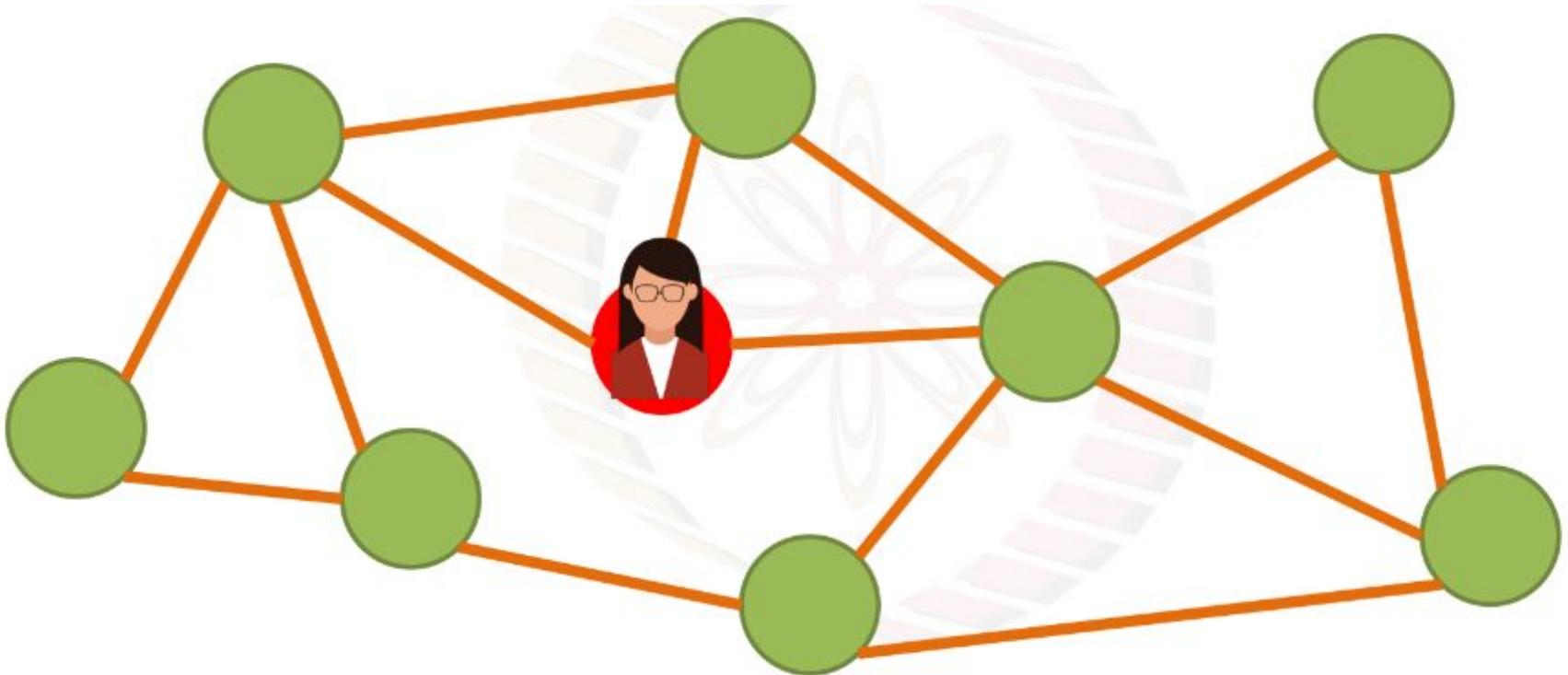


Transaction in a Bitcoin Network

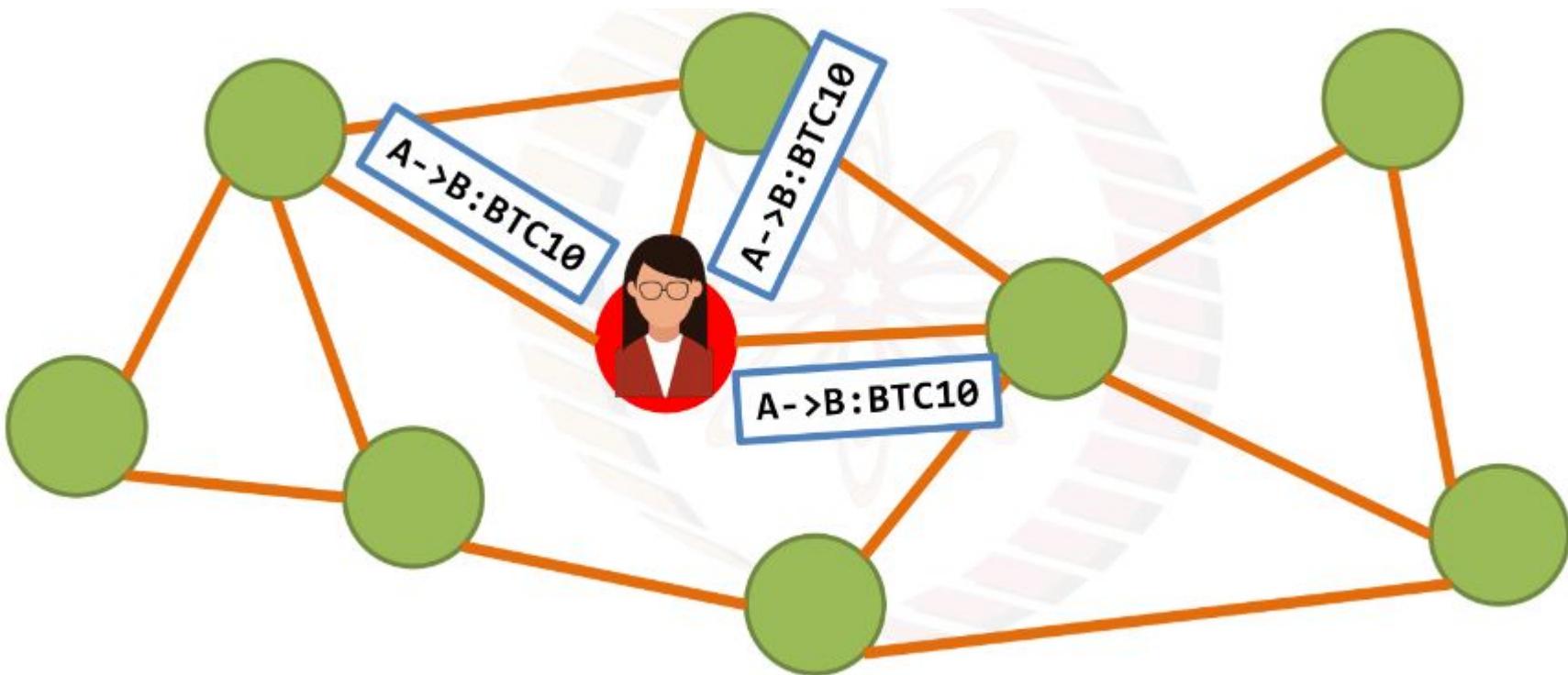
- Alice joins the Bitcoin network by opening her applet
- Alice makes a transaction to Bob: **A->B: BTC 10**
- Alice includes the scripts with the transactions
- Alice broadcasts this transaction in the Bitcoin network



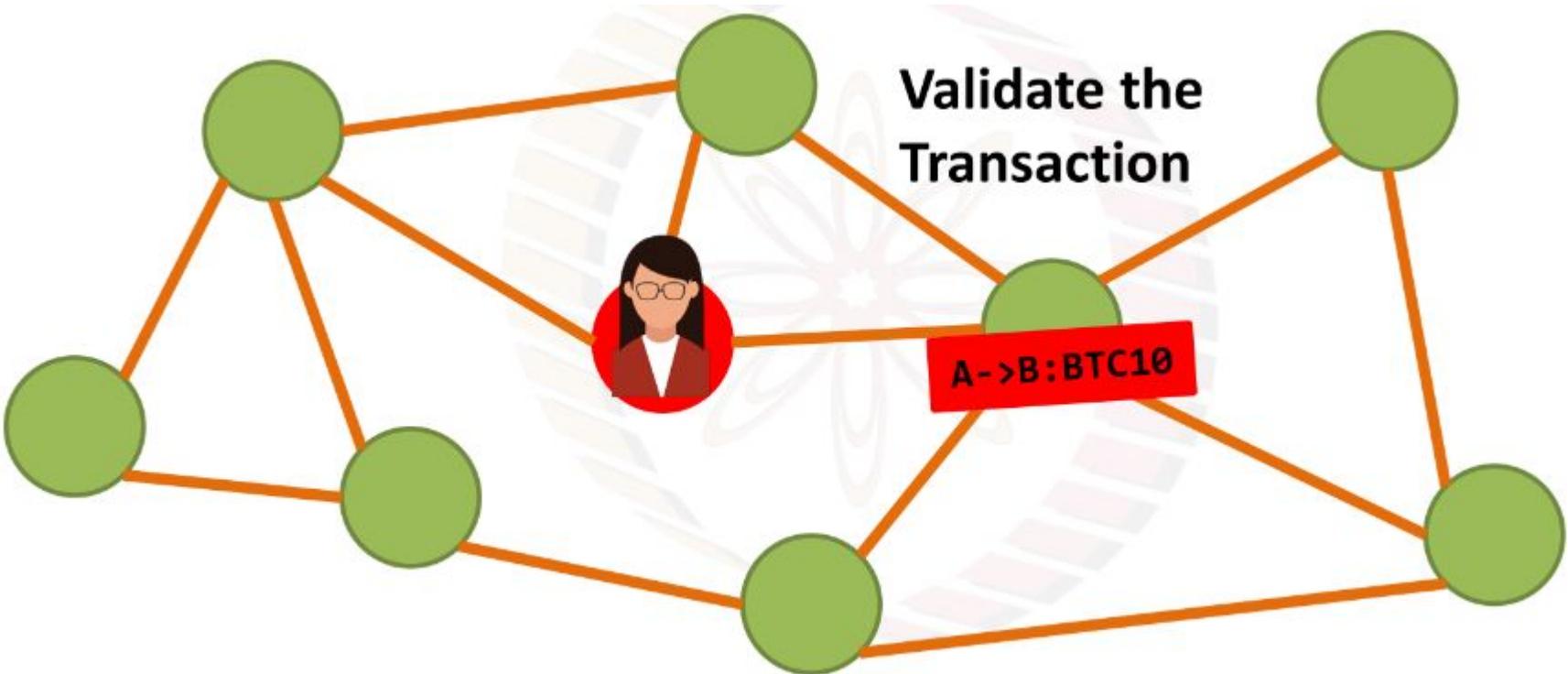
Transaction flooding in a Bitcoin Network



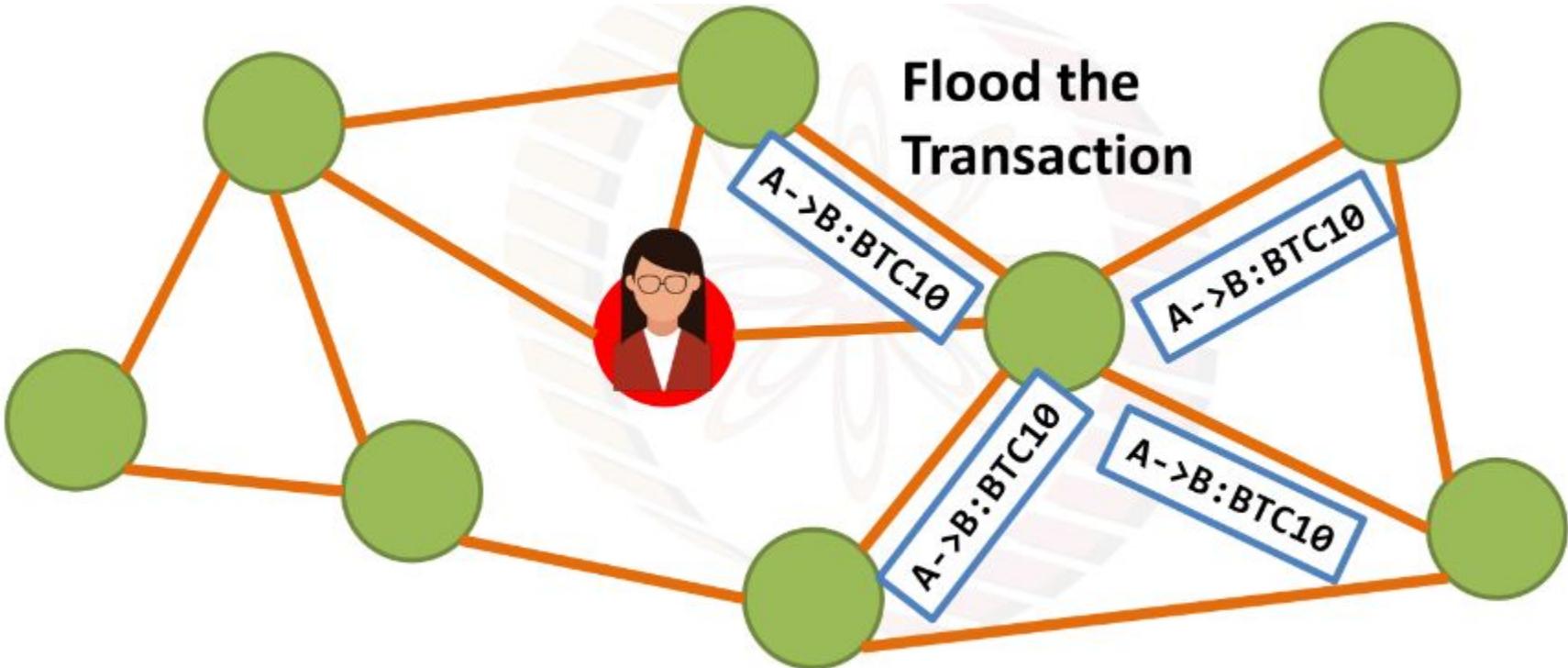
Transaction flooding in a Bitcoin Network



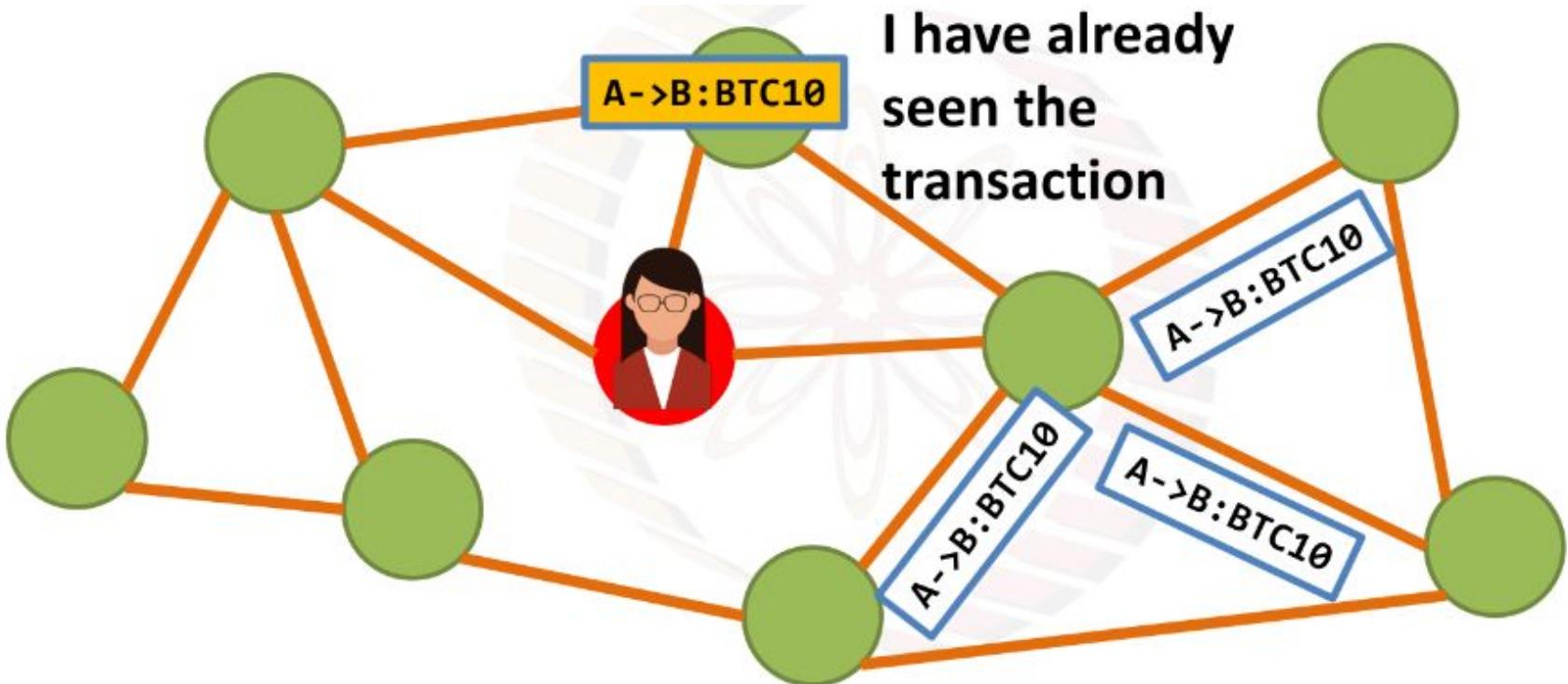
Transaction flooding in a Bitcoin Network



Transaction flooding in a Bitcoin Network



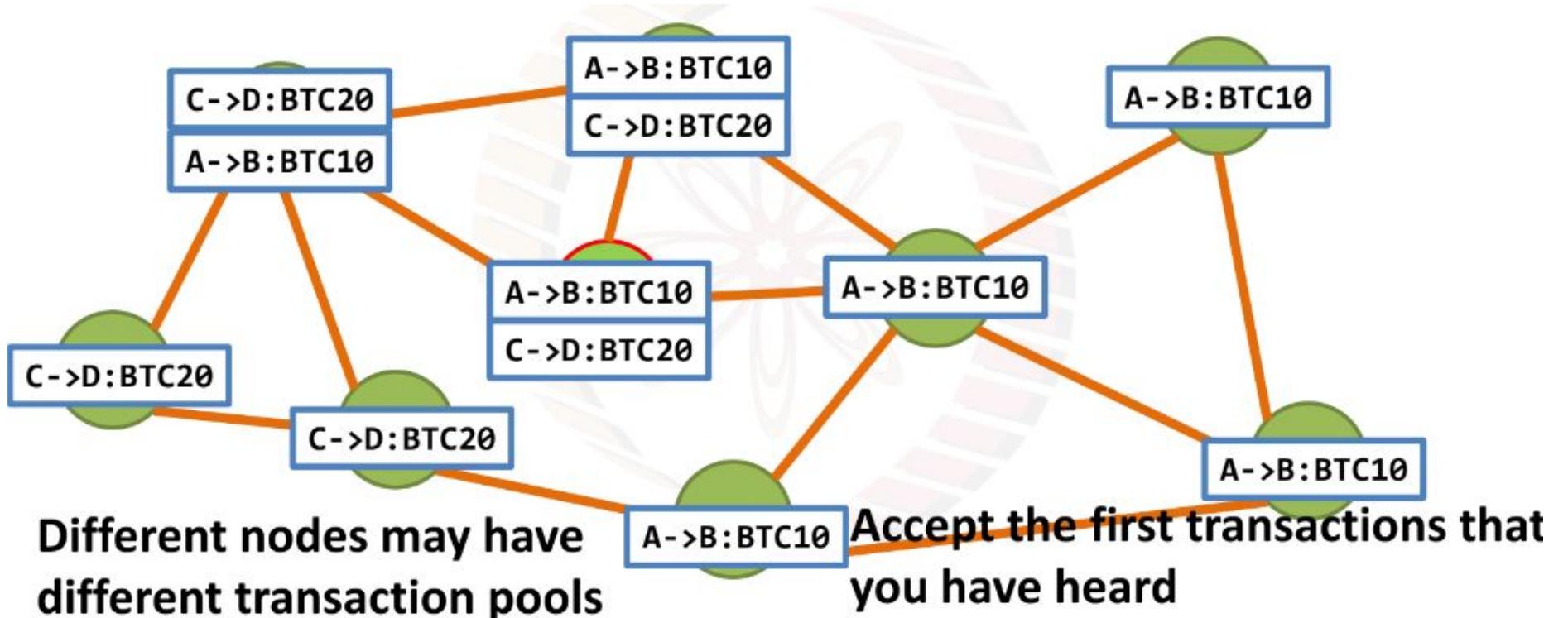
Transaction flooding in a Bitcoin Network



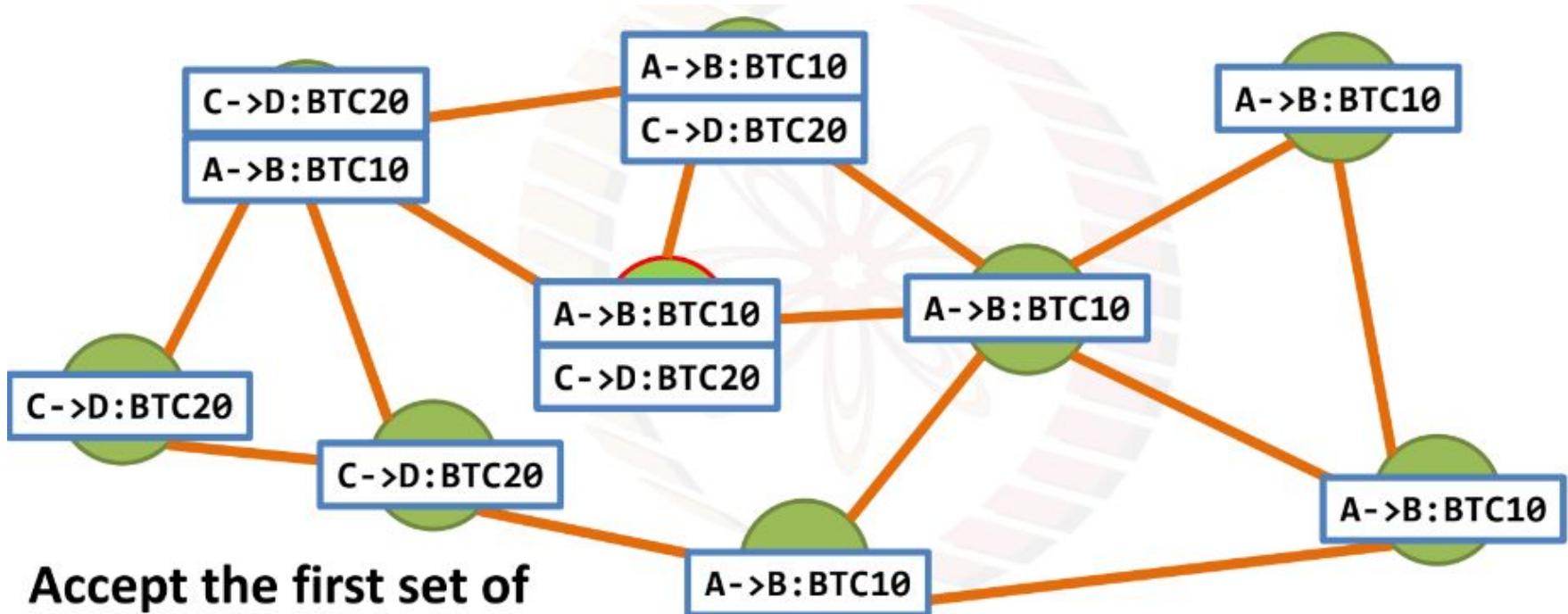
Which transaction should you Relay?

- The transaction is valid with current blockchain
 - No conflict
 - No double spending
- The script matches with a pre-given set of whitelist scripts – **avoid unusual scripts, avoid infinite loops**
- Does not conflict with other transactions that I have relayed after getting the blockchain updated – **avoid double spending**

Transaction flooding in a Bitcoin Network

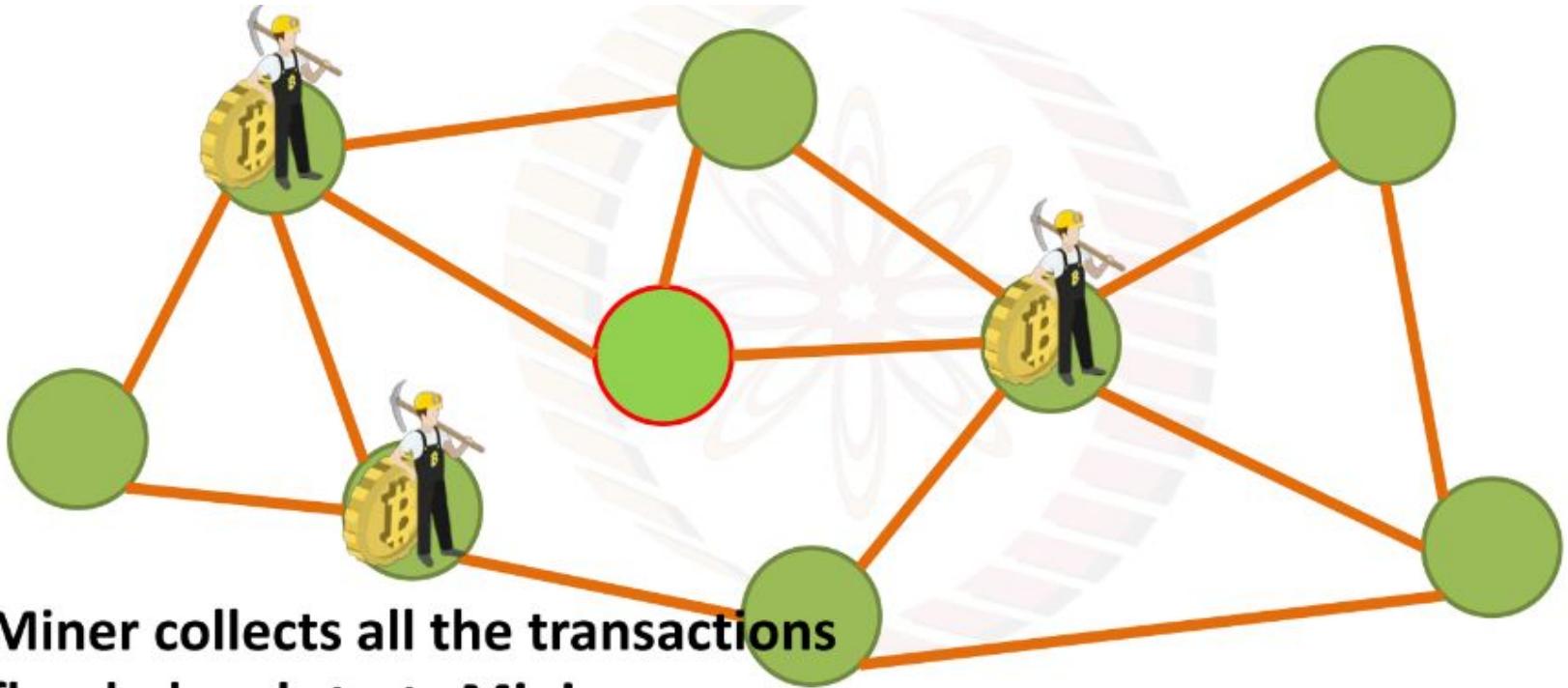


Transaction flooding in a Bitcoin Network



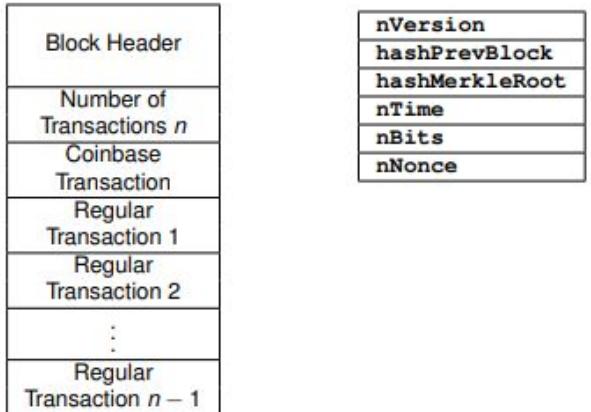
Accept the first set of transactions that you have heard

Mining in a Bitcoin Network



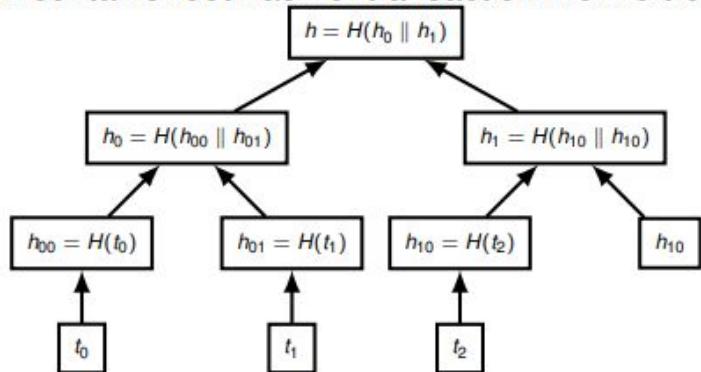
**Miner collects all the transactions
flooded and starts Mining**

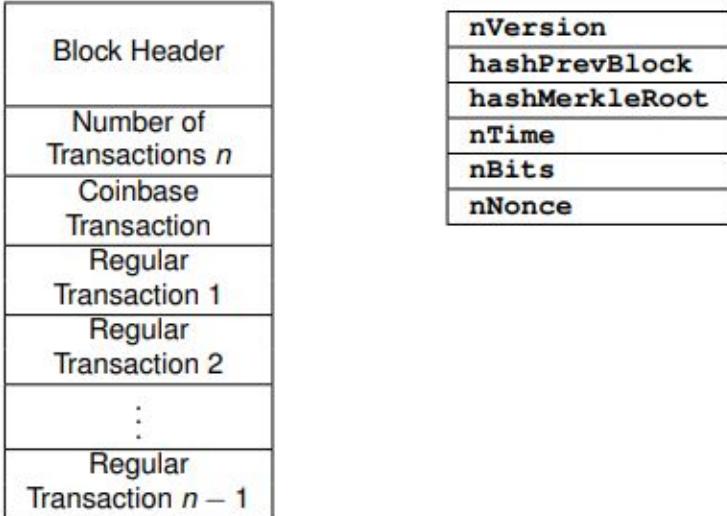
- Process of adding new blocks to the blockchain
- Nodes which want to perform transactions broadcast them
- Miners collect some of these transactions into a candidate block



Bitcoin Mining

- **hashPrevBlock** contains double SHA-256 hash of previous block's header
- **hashMerkleRoot** contains root hash of transaction Merkle tree





Bitcoin Mining

- **nBits** encodes a 256-bit target value T , say

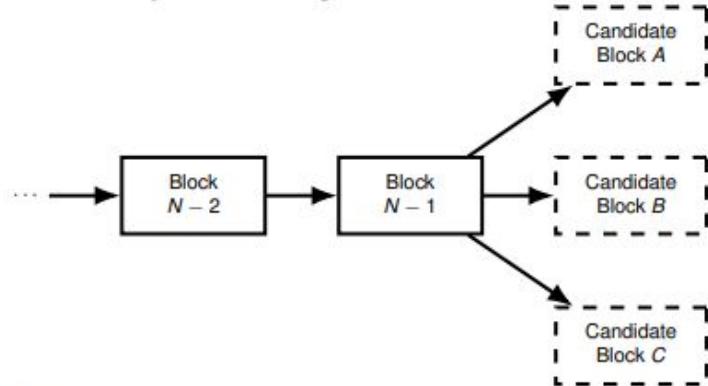
$$T = \text{0x } \underbrace{00 \dots 00}_{\text{16 times}} \underbrace{\text{FFFFF} \dots \text{FFFFF}}_{\text{48 times}}$$

- Miner who can find **nNonce** such that

$$\text{SHA256}(\text{SHA256}(\text{nVersion} \parallel \text{HashPrevBlock} \parallel \dots \parallel \text{nNonce})) \leq T$$

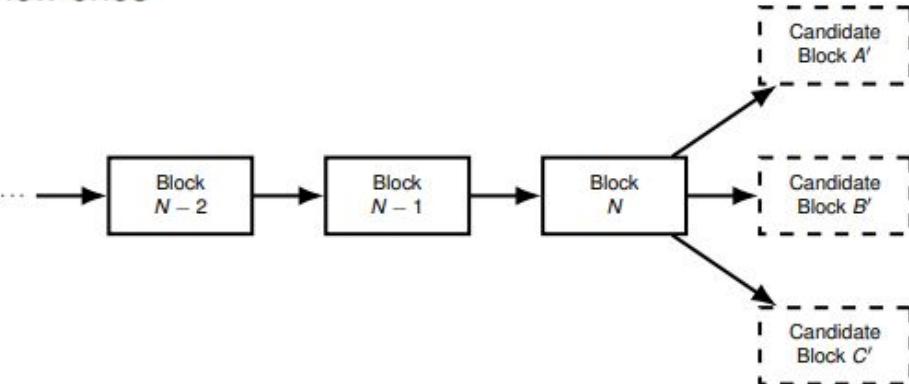
can add a new block

- Nodes broadcast transactions
- Miners accept valid transactions and reject invalid ones (solves double spending)
- Miners try extending the latest block

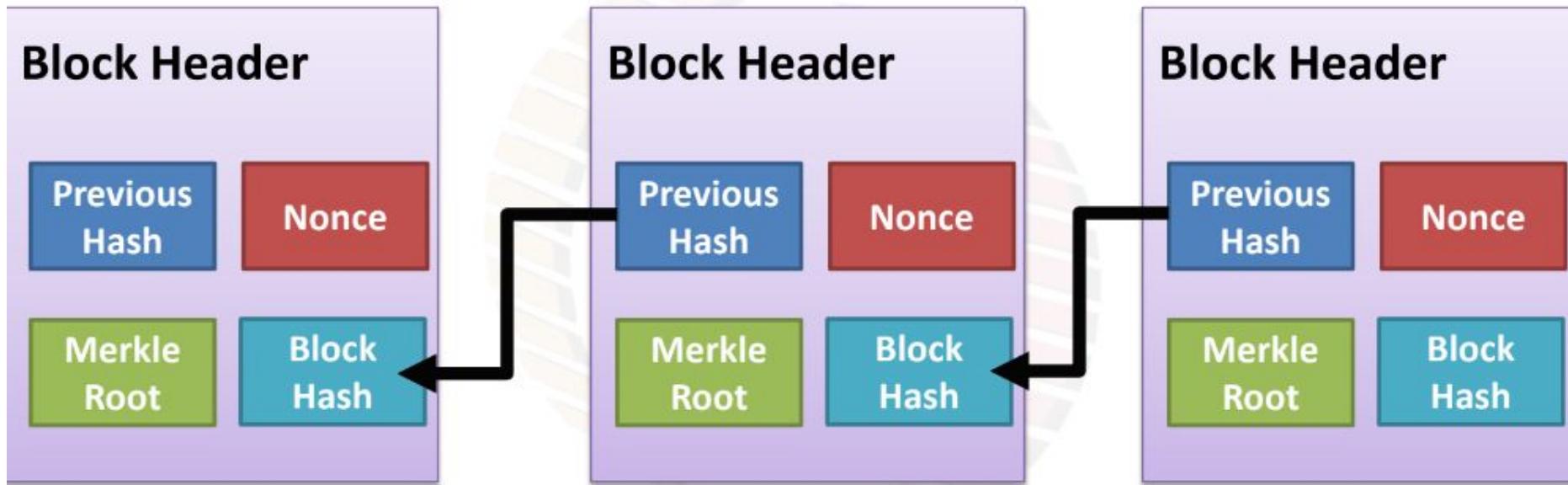


Block Addition Workflow

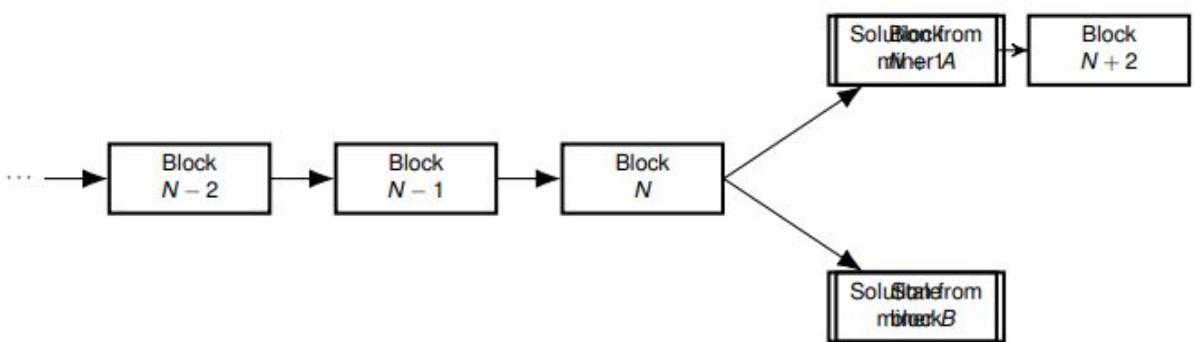
- Miners compete to solve the search puzzle and broadcast solutions
- Unsuccessful miners abandon their current candidate blocks and start work on new ones



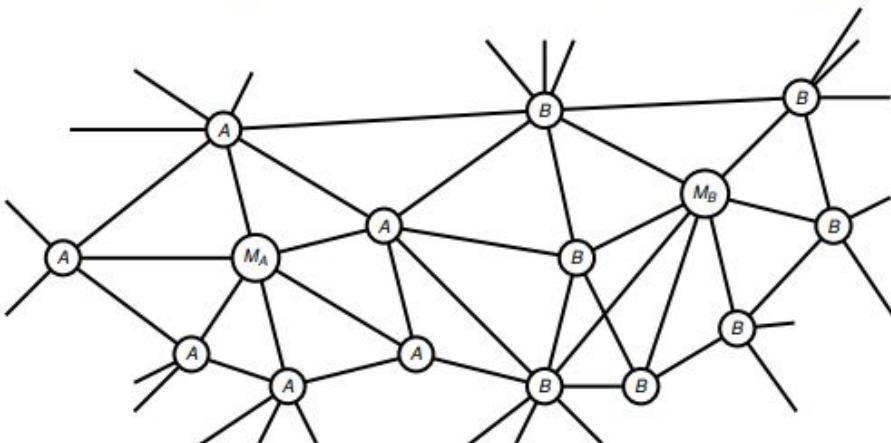
Block Generation Puzzle



Find out the nonce which generates the desired hash (certain zero bits at the prefix - **0000000000000000000000004a2b84f93a285b7a7.....**



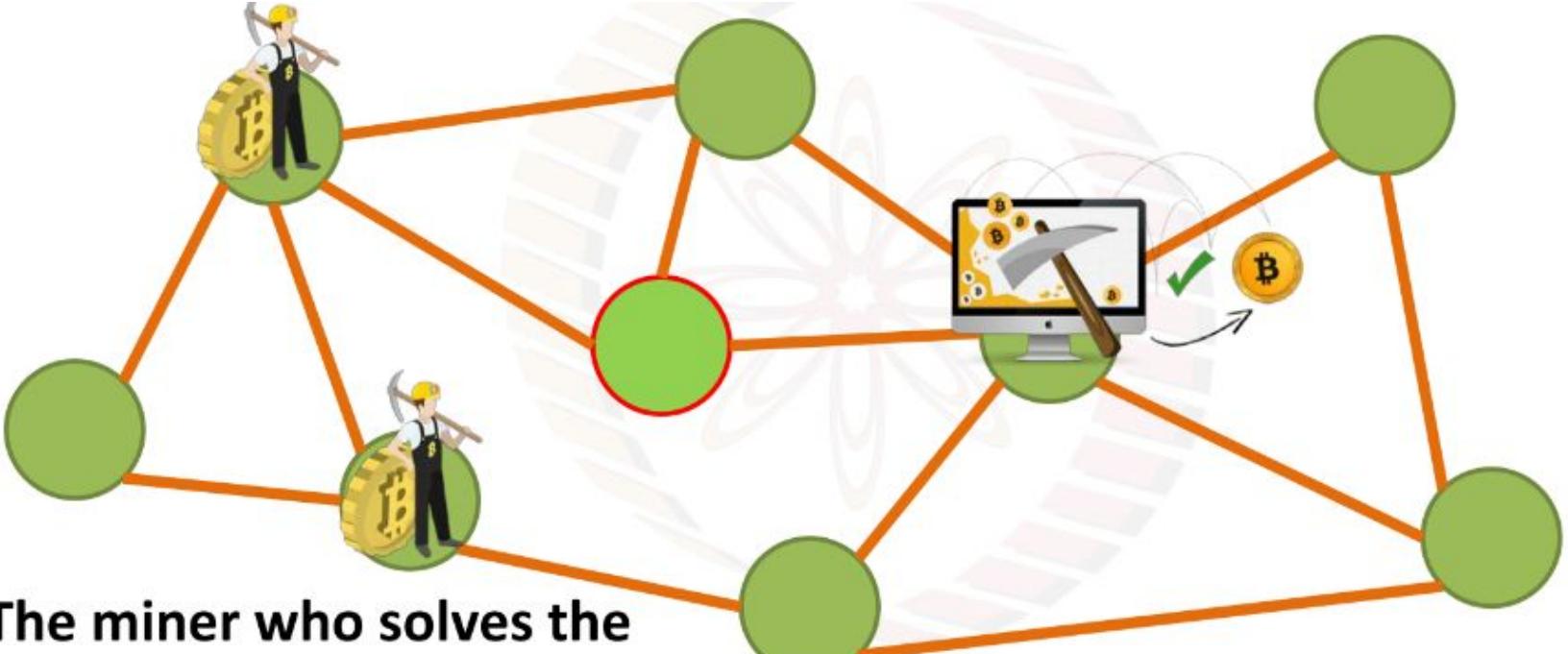
- Both miners will broadcast their solution on the network
- Nodes will accept the first solution they hear and reject others



- Nodes always switch to the longest chain they hear
- Eventually the network will converge and achieve consensus

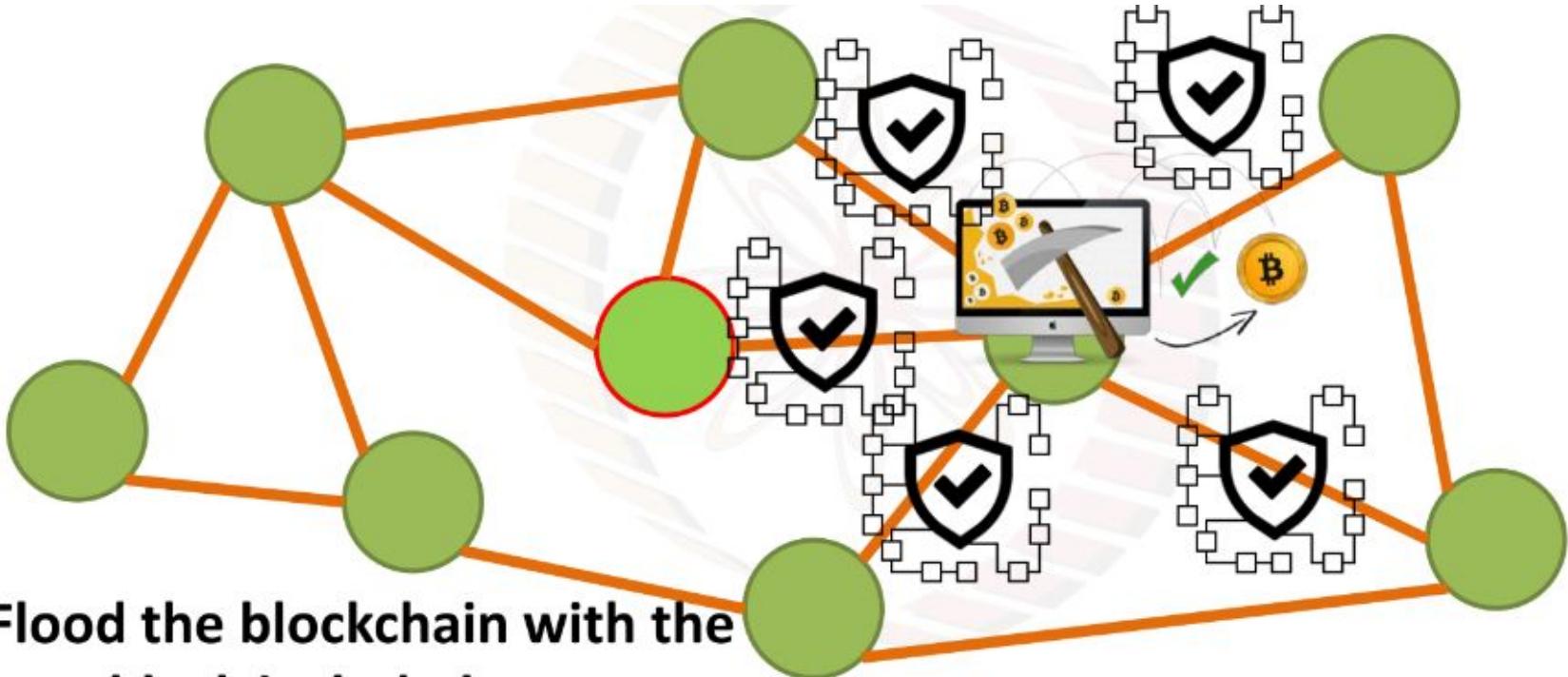
**What if
two
miners
solve the
puzzle at
the same
time?**

Block Generation



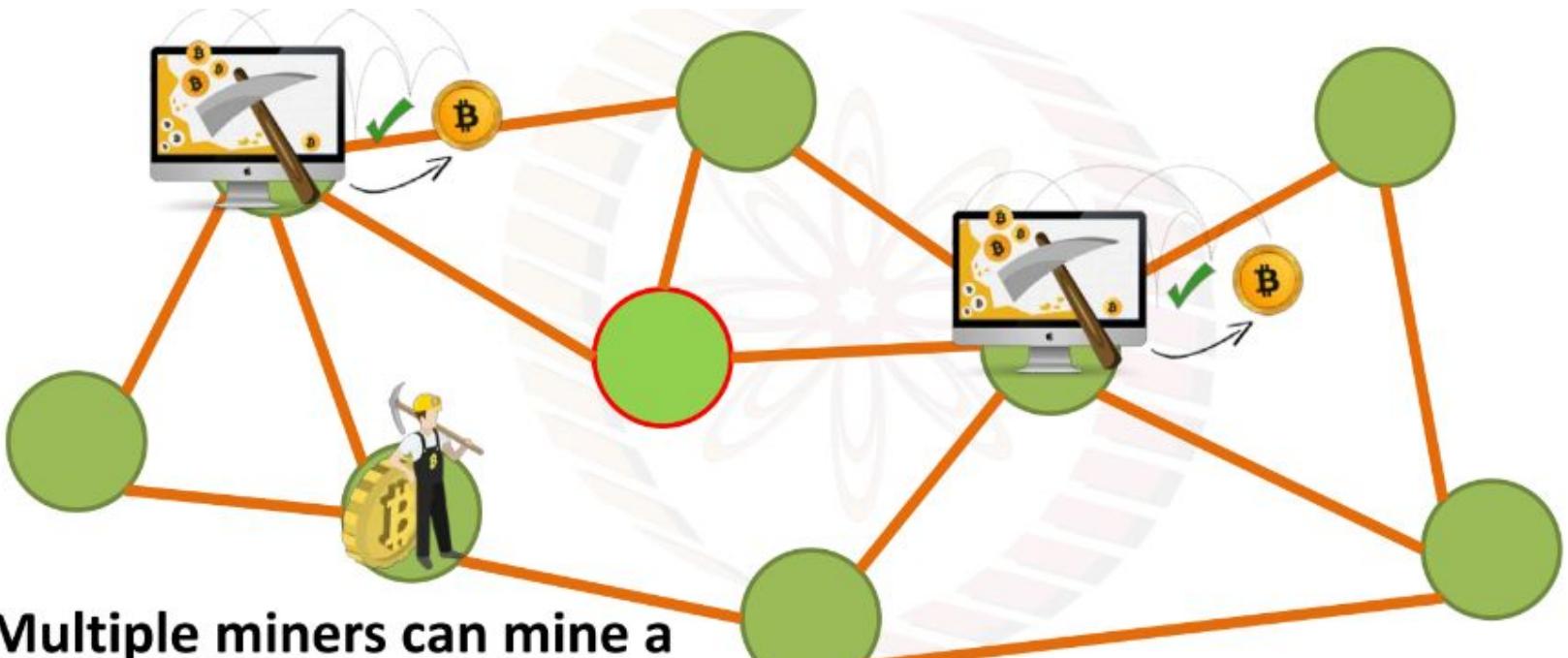
**The miner who solves the
puzzle first, generates a new block**

Block Flooding



**Flood the blockchain with the
new block included**

Block Propagation



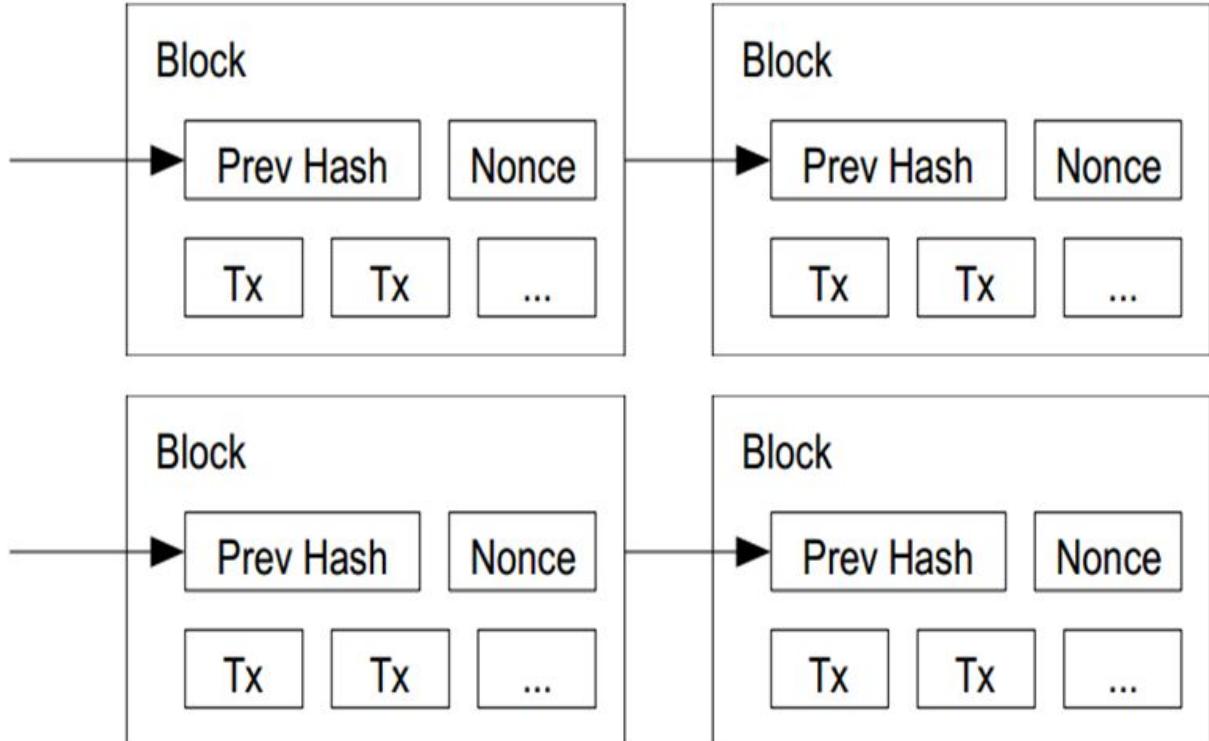
Multiple miners can mine a new block simultaneously or in a near identical time

Tie Breaking

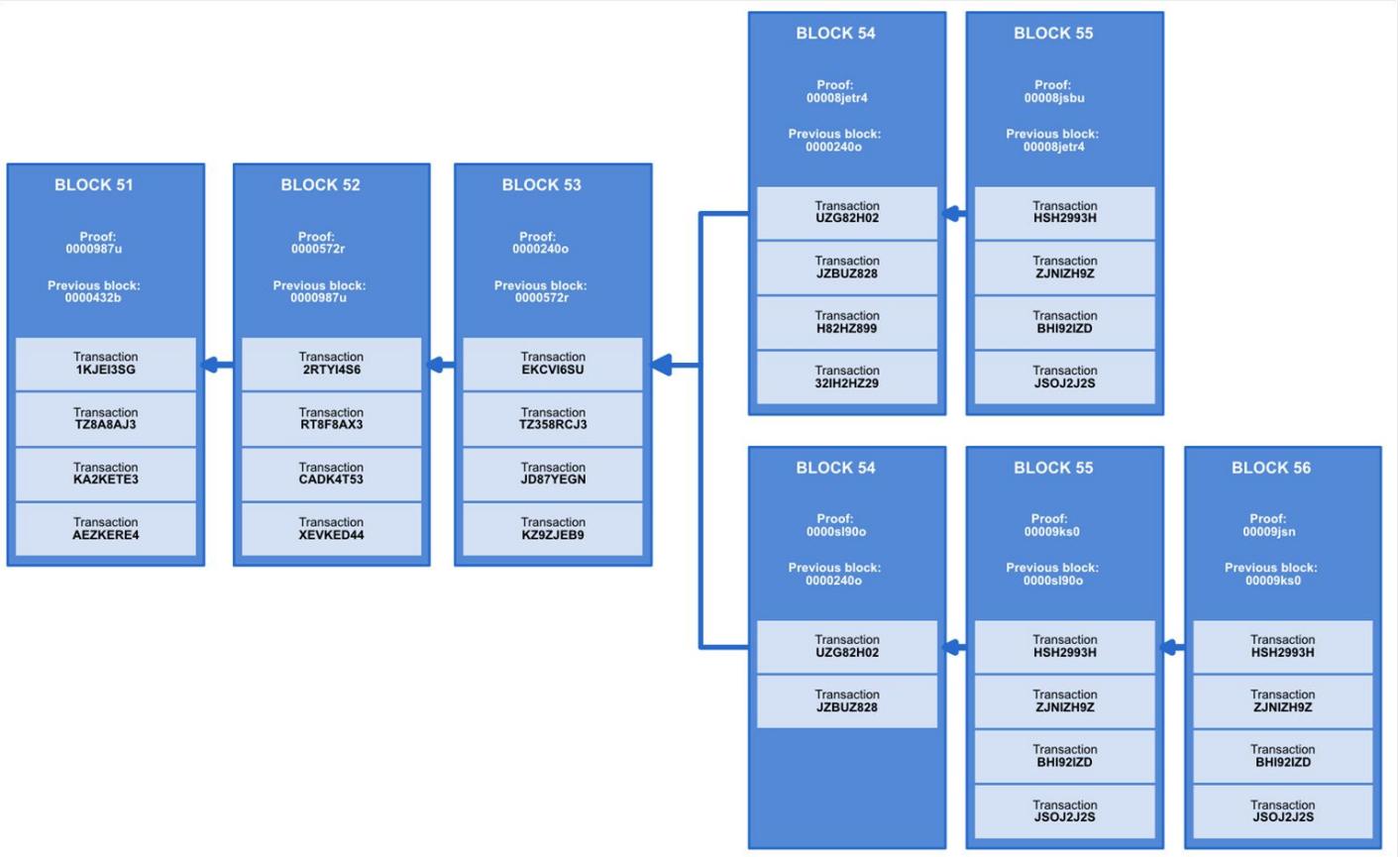
Two different Blockchains (or Blocks) may satisfy the required PoW

Two nodes may find a correct block simultaneously.

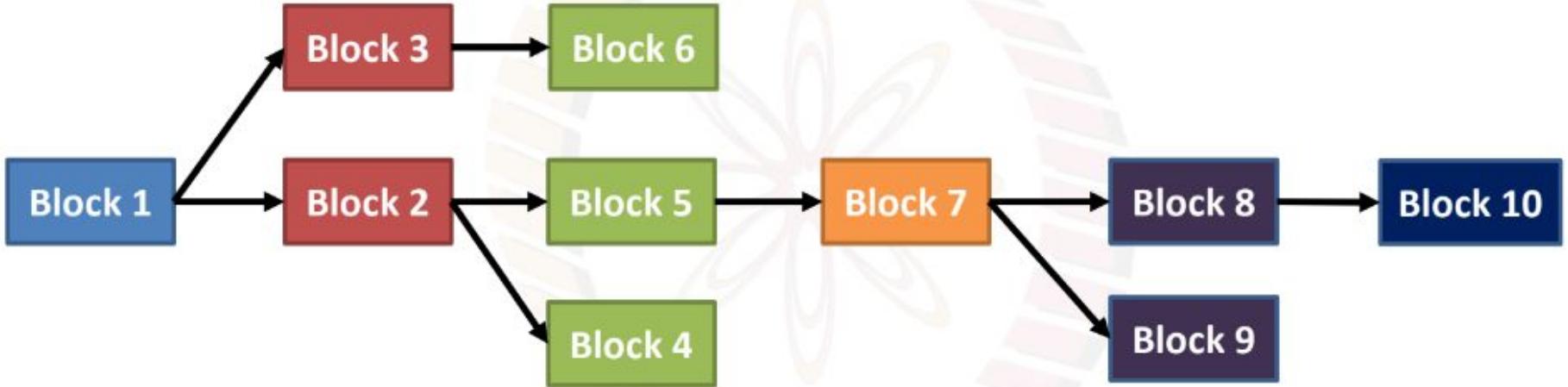
- Keep both and work on the first one
- If one grows longer than the other, take the longer one



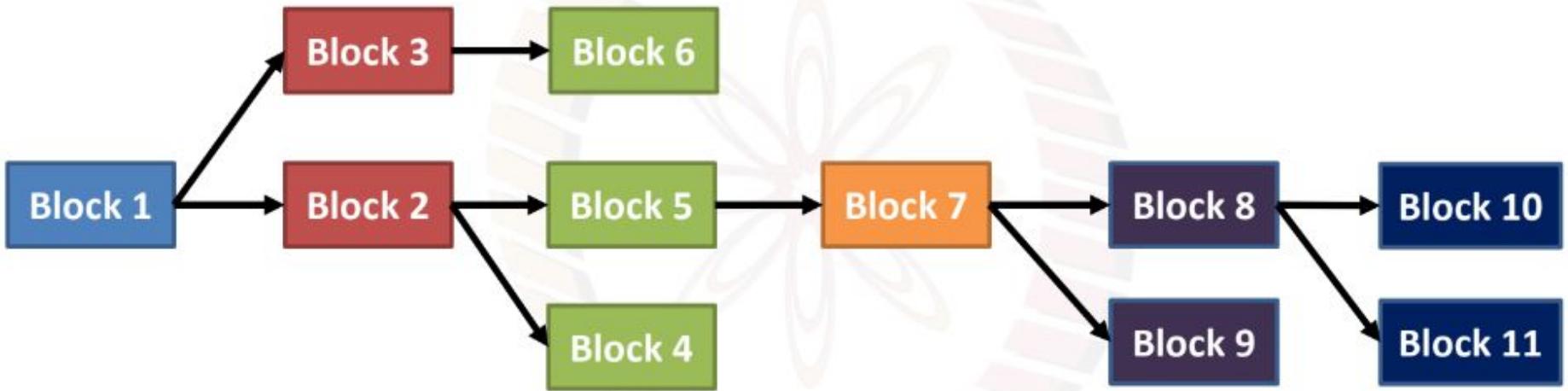
Forks



Block Propagation - Accept the Longest Chain



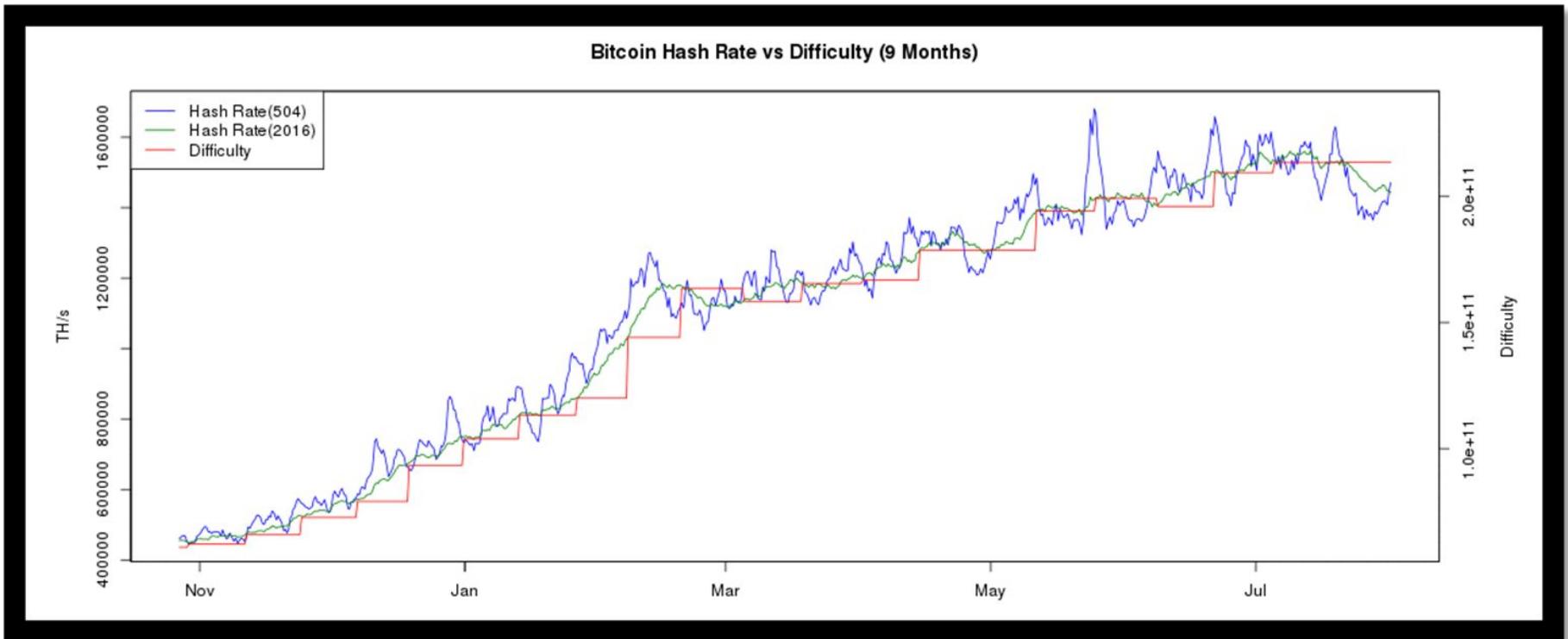
Block Propagation - Accept one of the Longest Chain



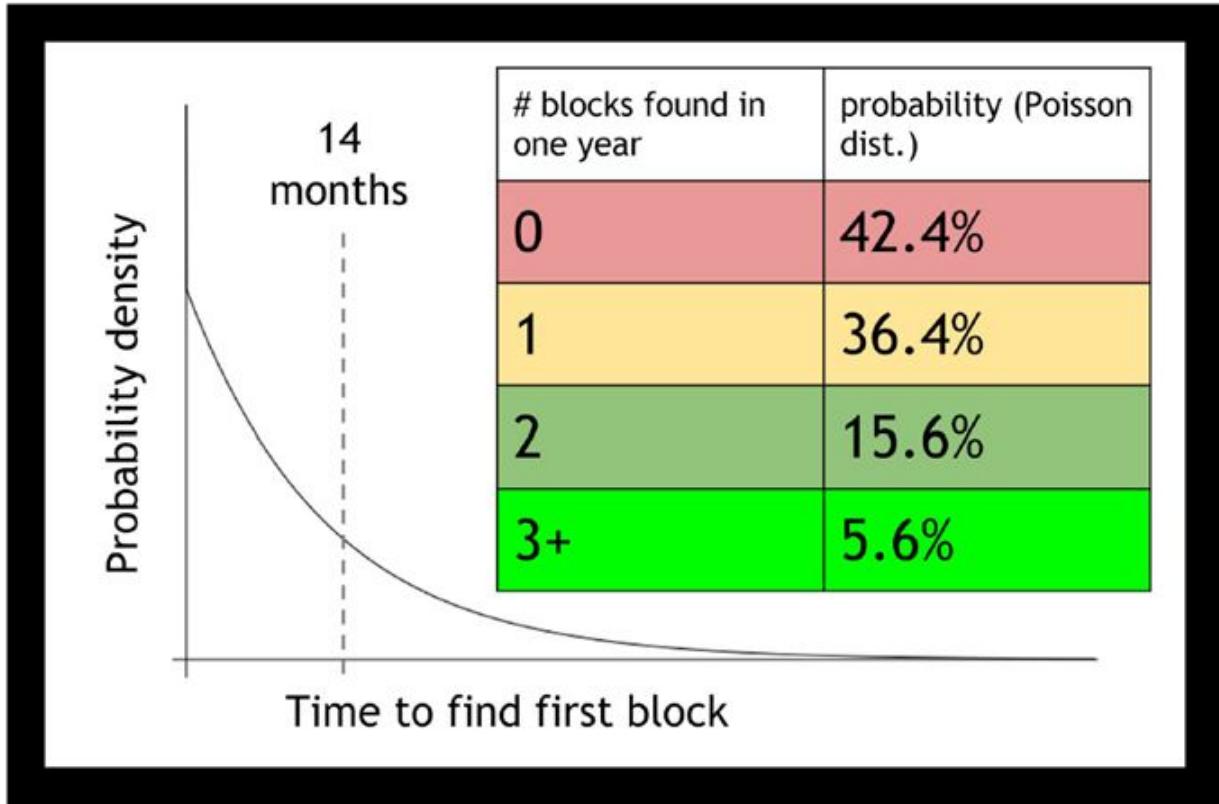
Which Block to Relay?

- Block contains the **correct hash** based on the existing blockchain
- All the **transactions inside the block are valid**
 - Check the scripts
 - Validate with the existing blockchain
- The block is included in the current longest chain
 - **Do not relay the forks**

Bitcoin Hash rate Vs Difficulty



Mining Pools



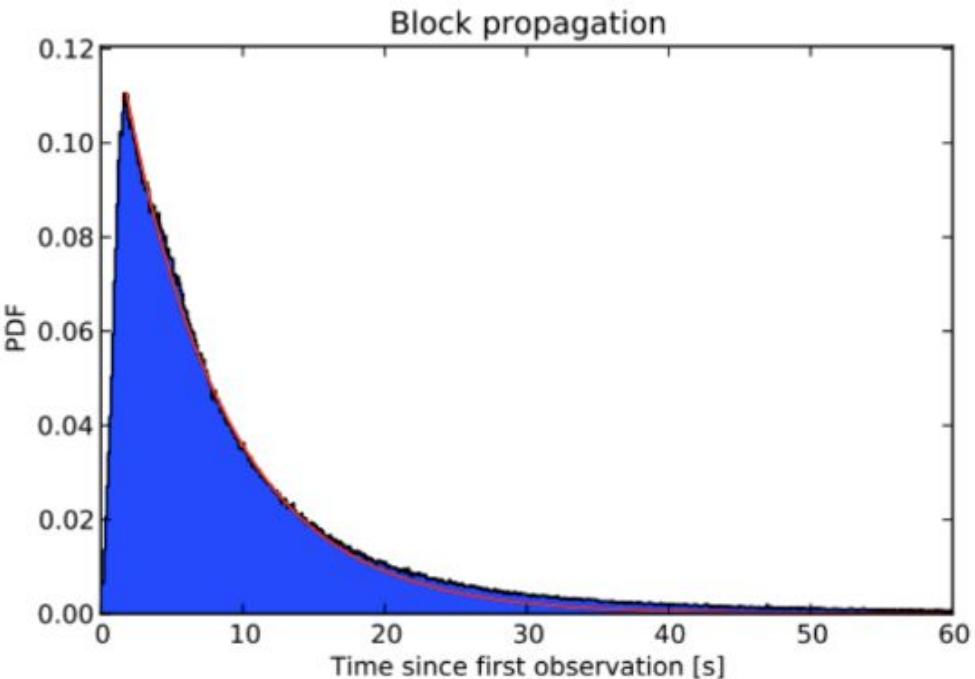


Block Propagation Latency

- Mean time = 12.6 Seconds
- 95% of the nodes can see the block within 40 seconds

Decker, Christian, and Roger Wattenhofer. "Information propagation in the bitcoin network." 2013 IEEE Thirteenth

International Conference on Peer-to-Peer Computing (P2P). IEEE, 2013.



Bitcoin References

- Code <https://github.com/bitcoin/bitcoin/>
- Reddit <https://www.reddit.com/r/Bitcoin/>
- Stackoverflow <https://bitcoin.stackexchange.com/>
- Forum <https://bitcointalk.org/>
- IRC https://en.bitcoin.it/wiki/IRC_channels
- Princeton book <http://bitcoinbook.cs.princeton.edu/>
- Mastering Bitcoin, Andreas Antonopoulos Notes
- <https://www.ee.iitb.ac.in/~sarva/bitcoin.html>