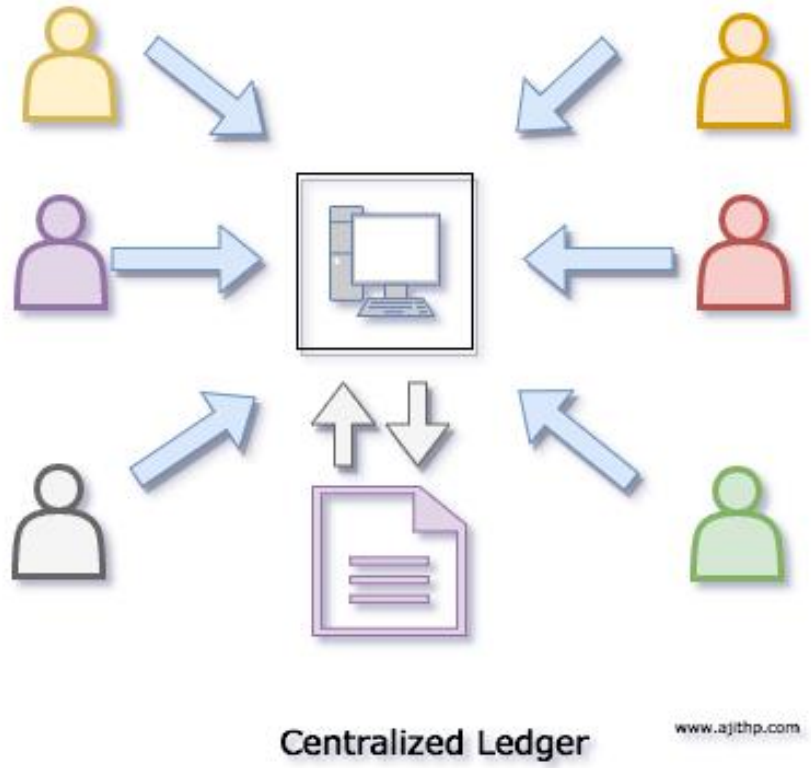
Module 3: Introduction to Bitcoin

Department of Computer Engineering, VESIT, Mumbai

Agenda

- **Blockchain Fundamentals - Recap**
- **What is Bitcoin?**
- **History of Bitcoin**
- **Getting the first Bitcoin**
- **Find the current price of Bitcoin**
- **Bitcoin transaction Life cycle (Sender to Receiver)**
- **Bitcoin transactions**

Blockchain Fundamentals - Centralized Ledger

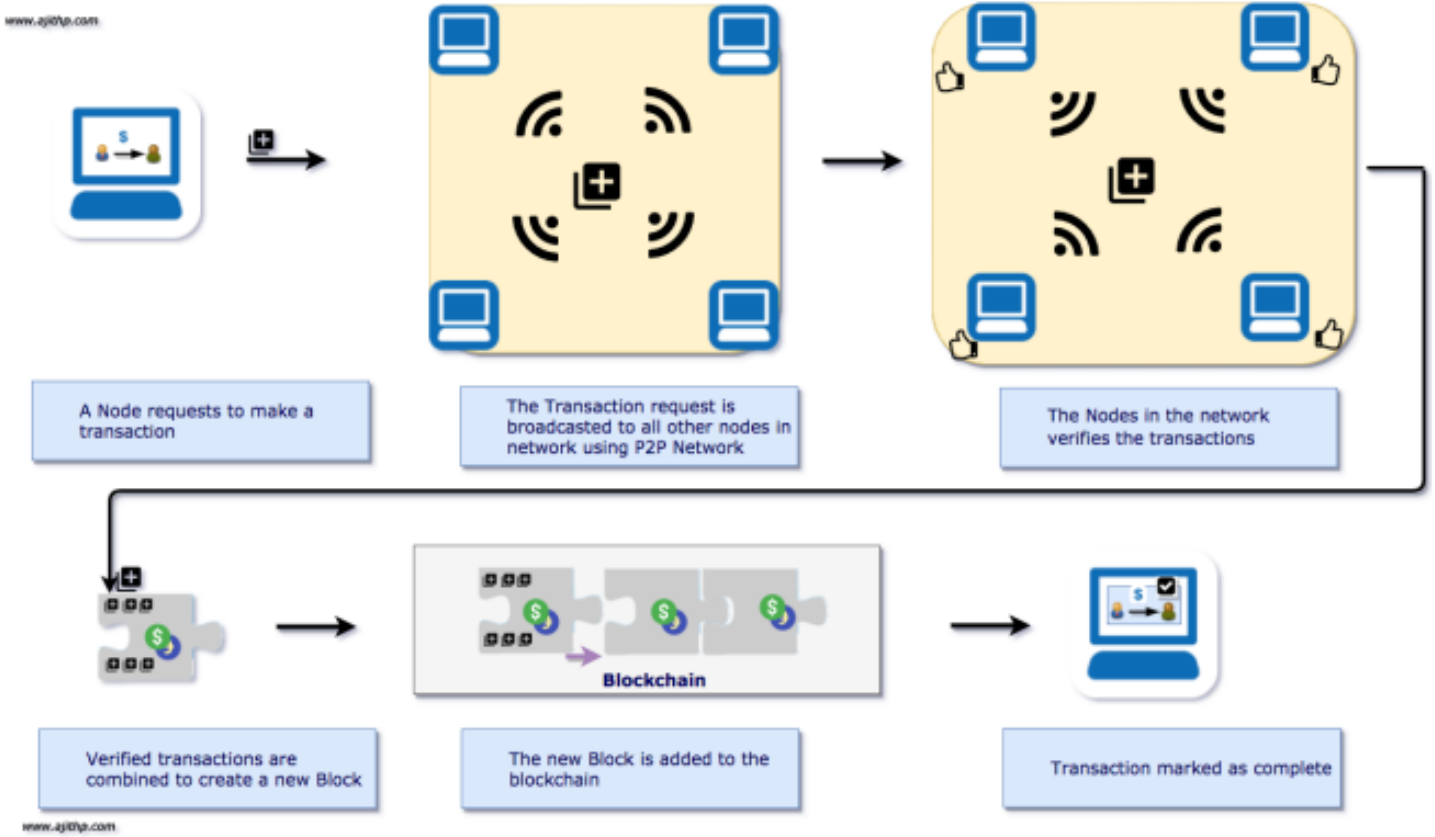


Courtesy : https://ajithp.com/2018/02/01/block-chain-fundamentals/

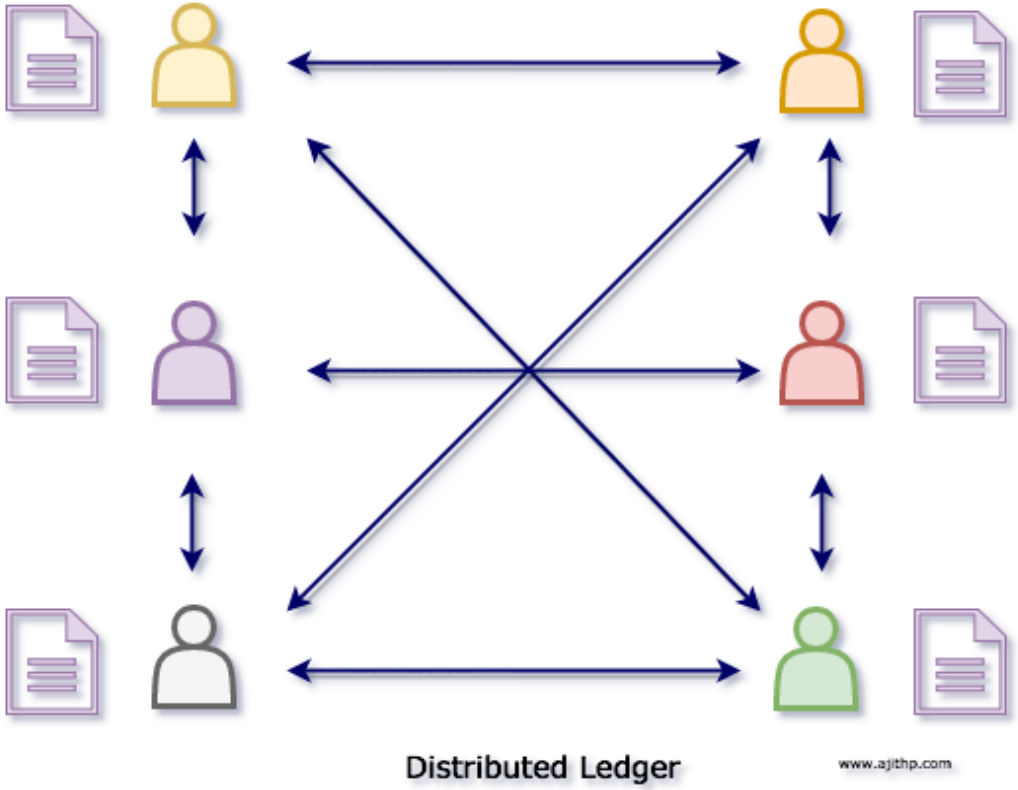
Blockchain Fundamentals - Centralized Ledger

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

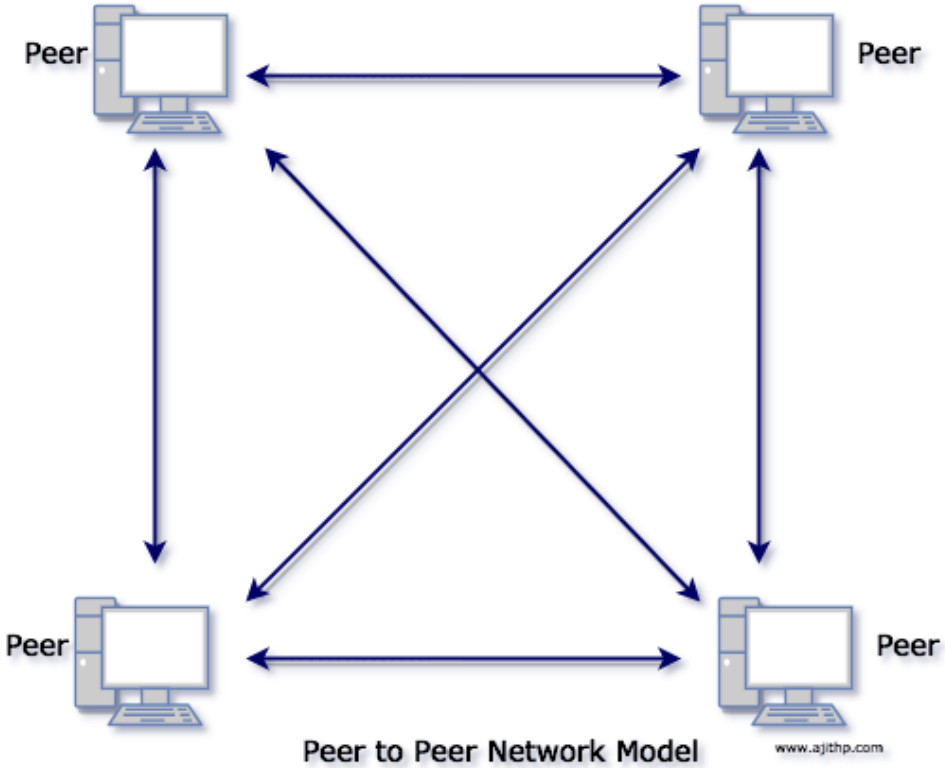
Blockchain Fundamentals - What is BC?



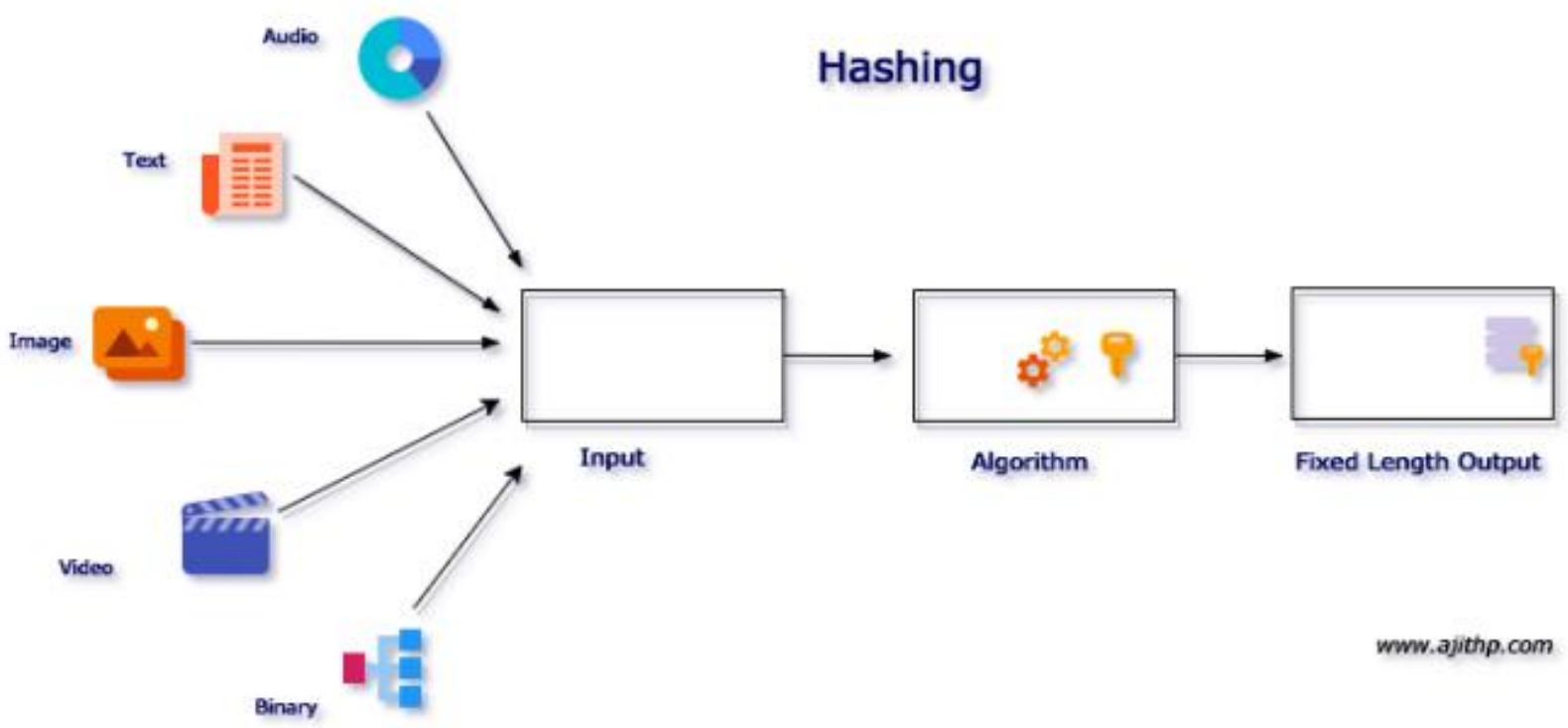
Blockchain Fundamentals - Distributed Ledgers



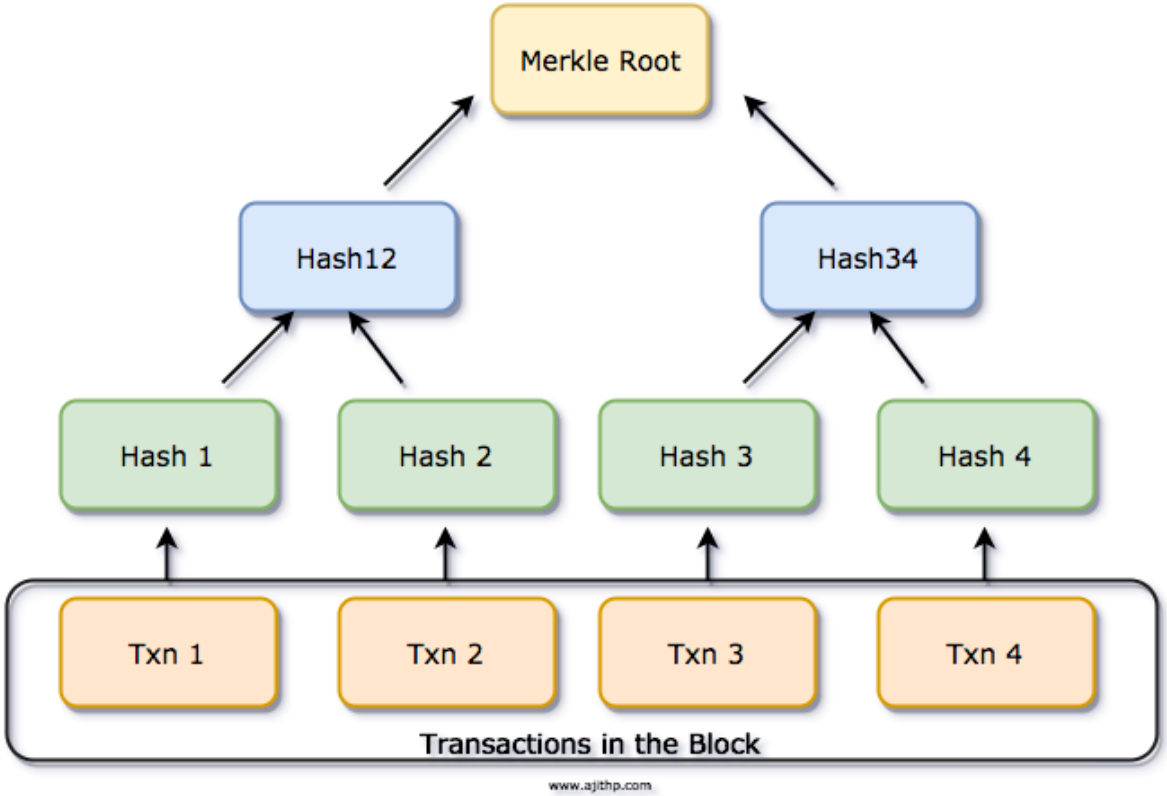
Blockchain Fundamentals - P2P Network



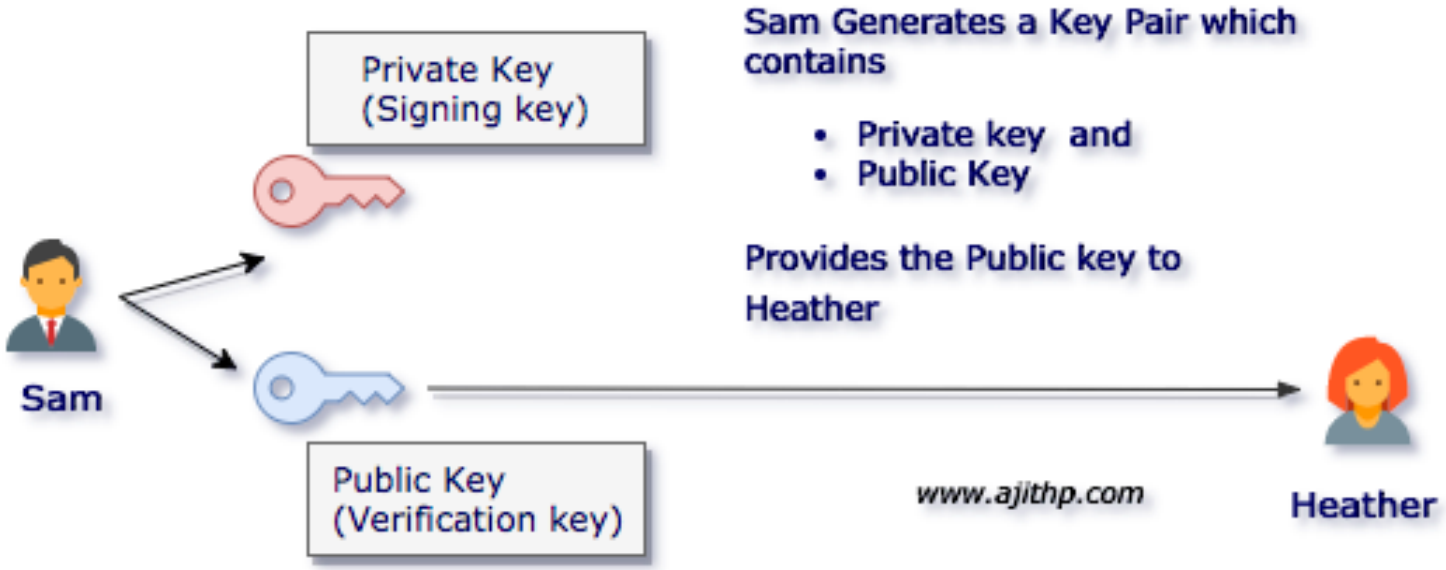
Blockchain Fundamentals - Hashing



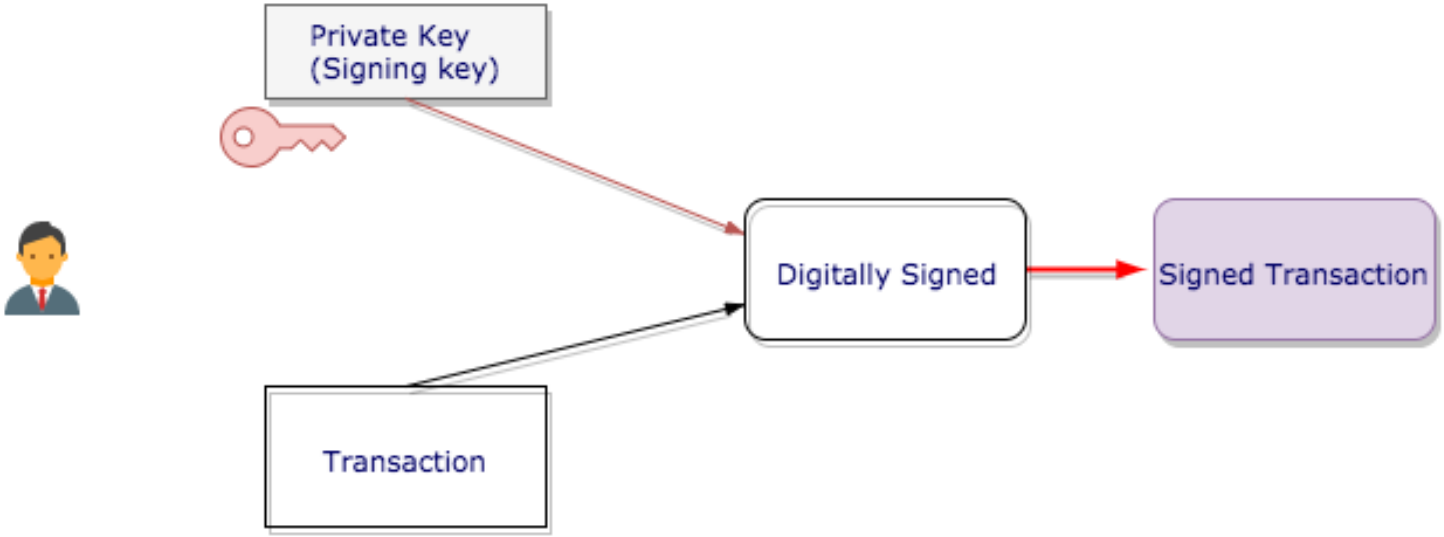
Blockchain Fundamentals - Merkle tree of a Block



Blockchain Fundamentals - Digital Signature

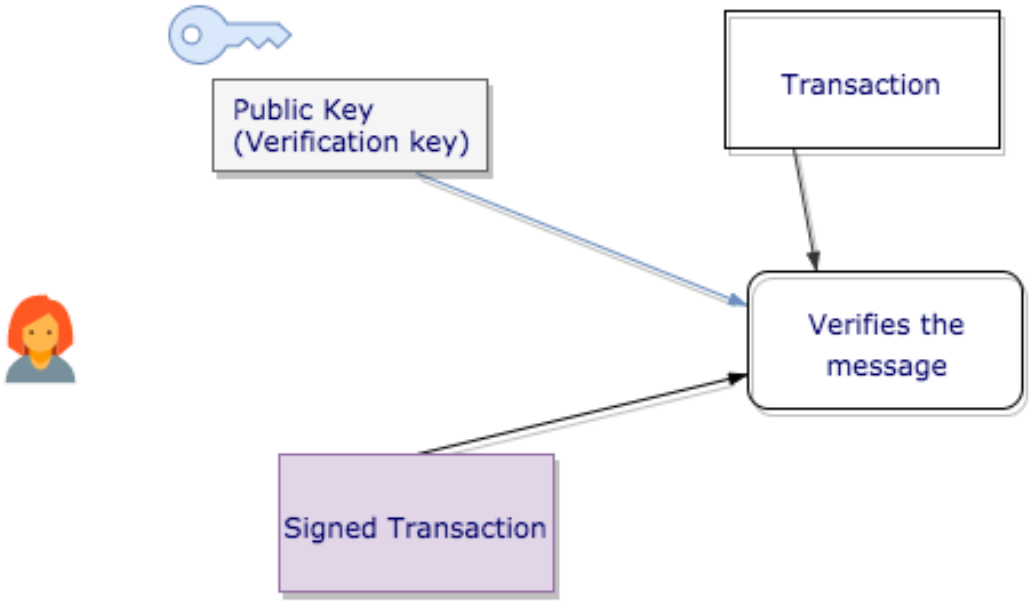


Blockchain Fundamentals - Digital Signature



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

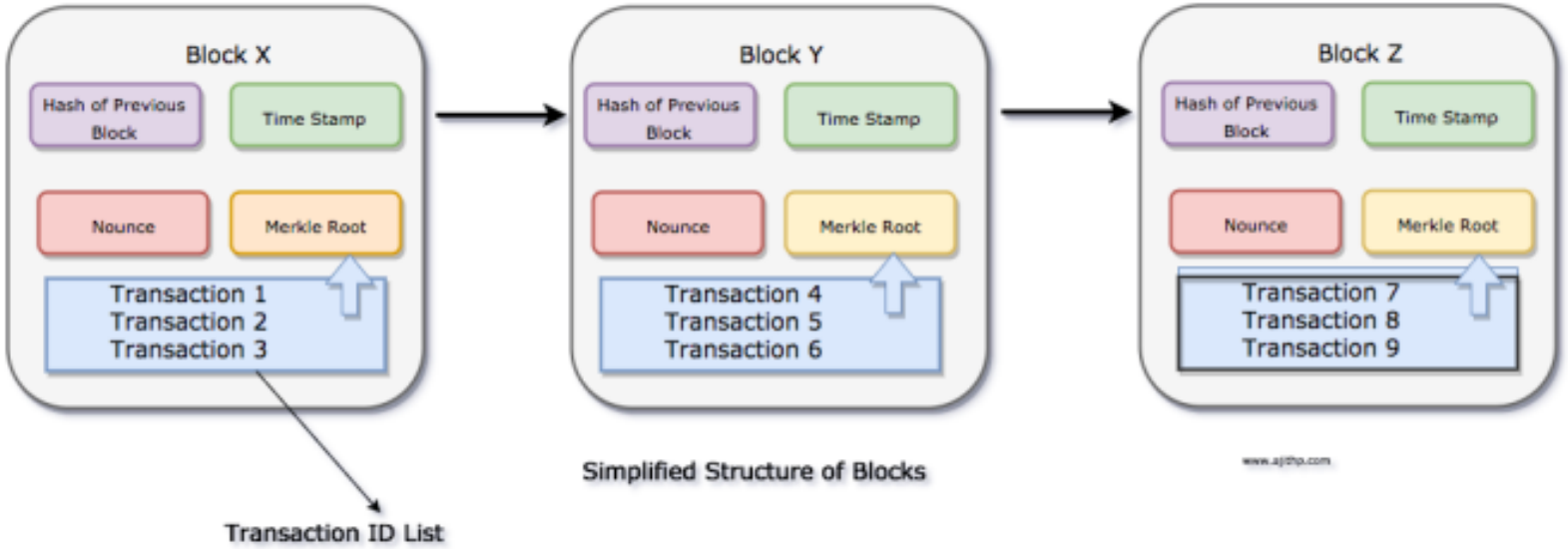
Blockchain Fundamentals - Digital Signature



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?



Simplified Structure of Blocks

Blockchain Fundamentals - What is a Block?

Block #505234

Summary	
Number Of Transactions	1265
Output Total	2,543.6082603 BTC
Estimated Transaction Volume	599.91973715 BTC
Transaction Fees	1.88207587 BTC
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

Hashes	
Hash	00000000000000000031fa55faffe629751789bb49cd21f8b4b0f6facccf315214
Previous Block	0000000000000000000100b5fabf721f7e6293598b30bac09bcce55d9593474d6
Next Block(s)	00000000000000000005dffb4314cc5ce3207fc957a32d96538a8d4f96ee29842
Merkle Root	3d491718f9973c52b547c266b95a66a6fc09c2fe9cf1e8b22ba0dbb721b36e8b

Transactions

ffc8f1abb970b168c865e32992a3cc2ddf087ca6a343b72839ca5c23a6e5b7a22		2018-01-20 21:02:47
No Inputs (Newly Generated Coins)	→	1Nh7uHdvY6fNwtQtM1G5EZAFPLC33B59rB Unable to decode output address
		14.38207587 BTC 0 BTC
		14.38207587 BTC

Blockchain Fundamentals - What is in transaction?

Transaction View information about a bitcoin transaction

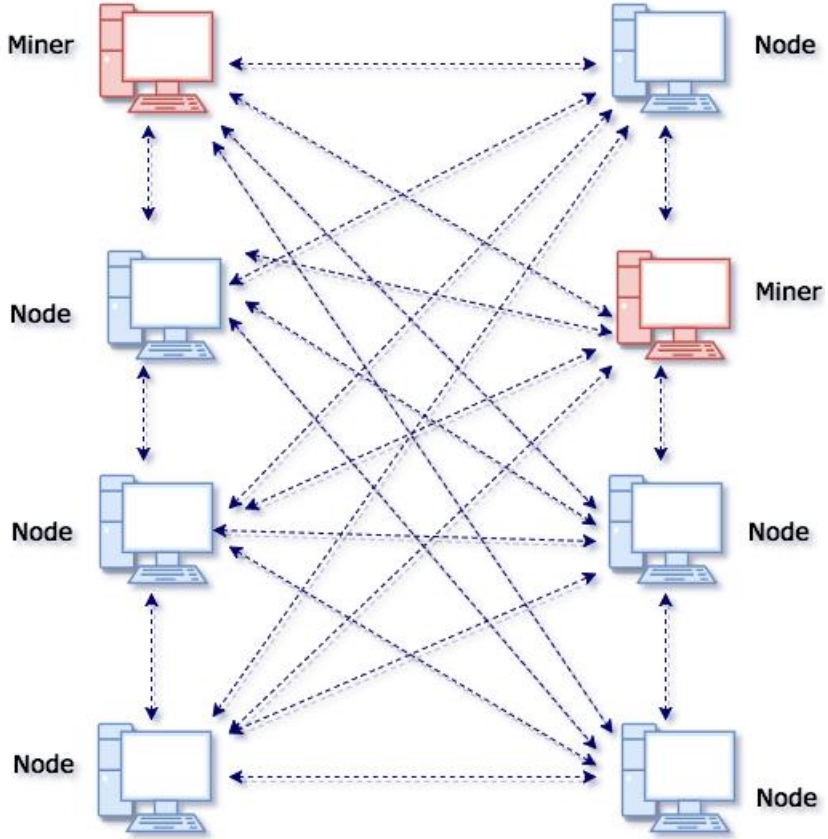
f350e9c89c85d08f5c33cf38741bbd2d4245cd807d0e4554712320f7a73103ca

14T6jJ3tsdpmzNn8gUhoJqck3fitHrSeDd	1FjndP5pAPaXP9wNc4K3dZPcYd7N9B7H5f	3.337846 BTC
	3MvwMsohxAozkYgWCKCdgi1FW2DW4bjnq2	0.312 BTC
		3.649646 BTC

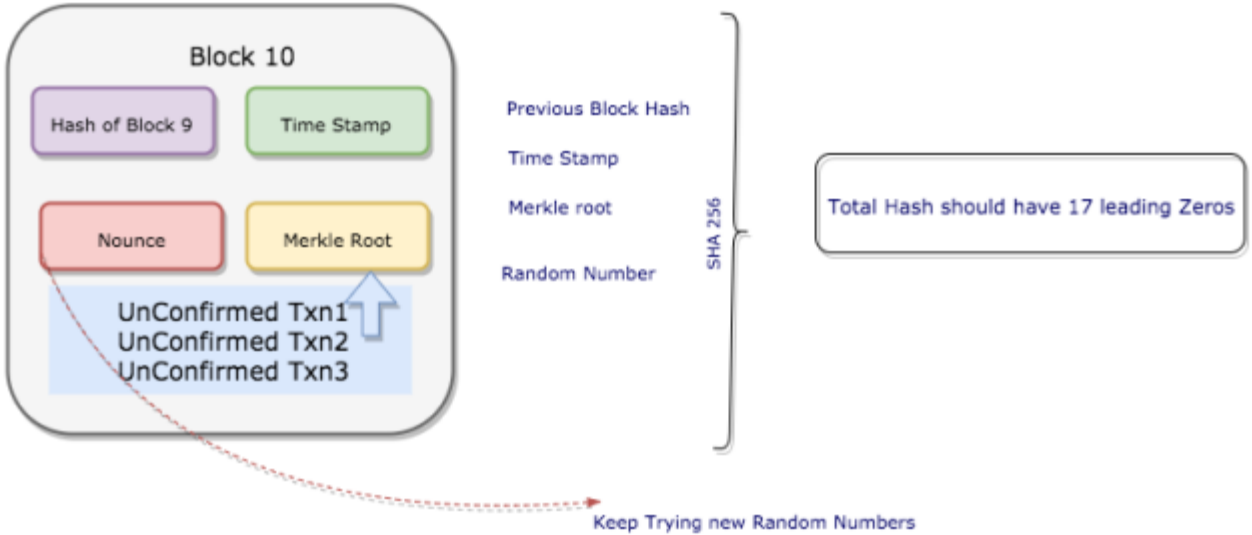
Summary	
Size	224 (bytes)
Weight	896
Received Time	2018-01-20 21:02:21
Included In Blocks	505234 (2018-01-20 21:02:47 + 0 minutes)
Confirmations	217 Confirmations
Visualize	View Tree Chart

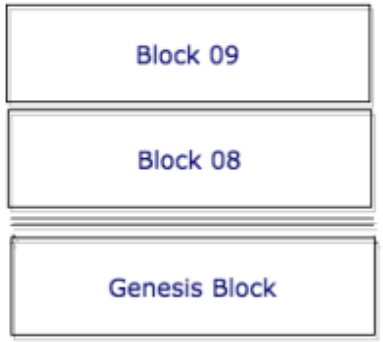
Inputs and Outputs	
Total Input	3.653346 BTC
Total Output	3.649846 BTC
Fees	0.0035 BTC
Fee per byte	1,562.5 sat/B
Fee per weight unit	390.625 sat/WU
Estimated BTC Transacted	0.312 BTC
Scripts	Show scripts & coinbase

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)

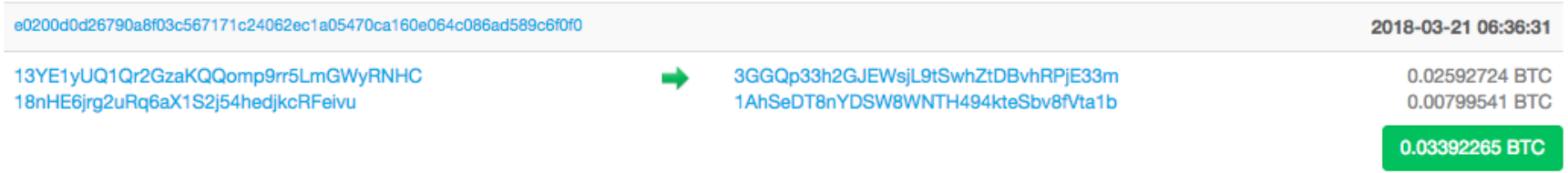
The Permission-less Model

- 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

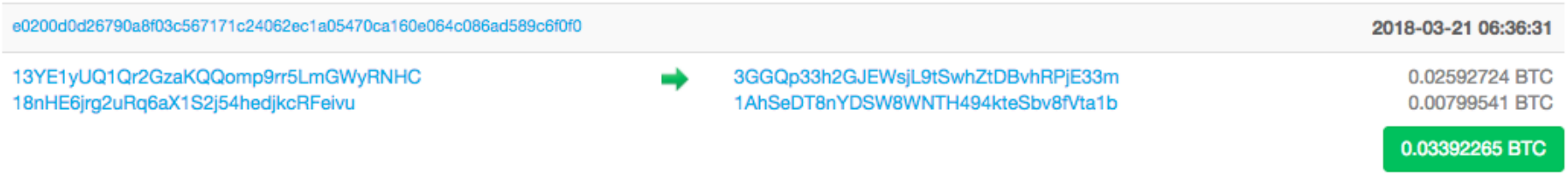


Peer Addresses

- "**Address**" in bitcoin is synonymous to an **"Account"** in a bank.

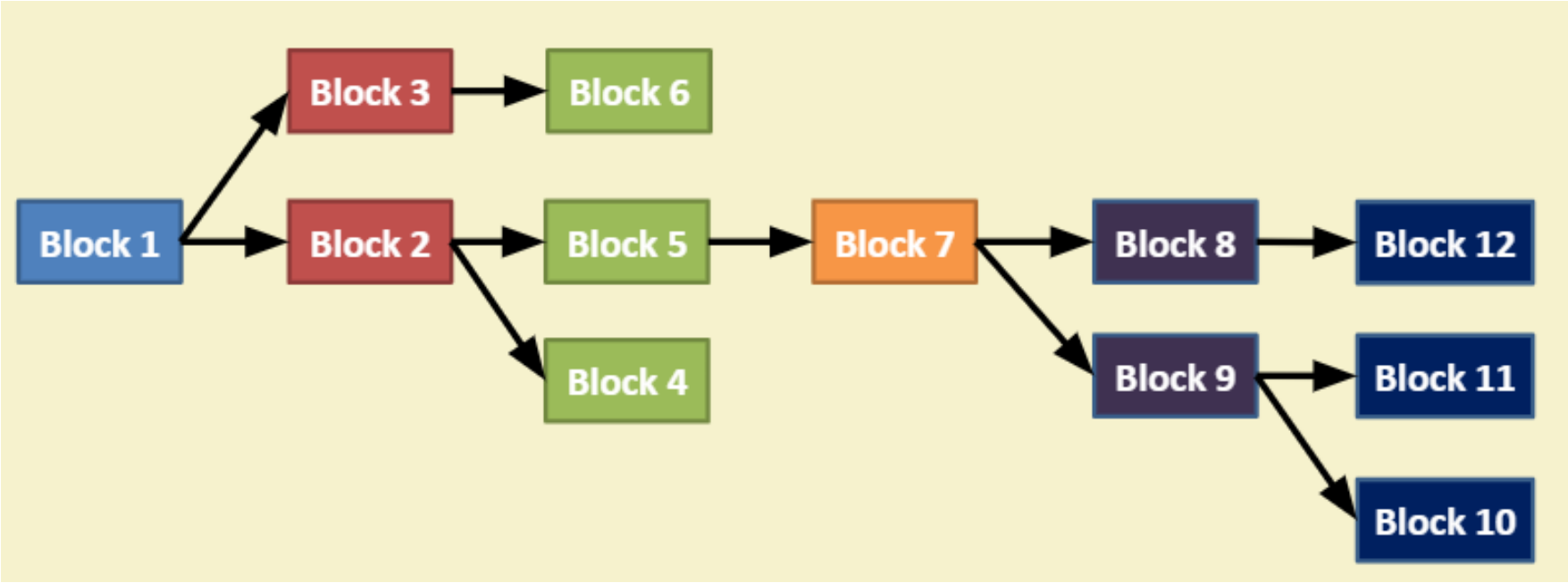
- The wallet listens for transactions addressed to an account,
  - Encrypts the transactions by the public key of the target address
  - Only the target node can decrypt the transaction and accept it

- However, the actual transaction amount is open to all for validation

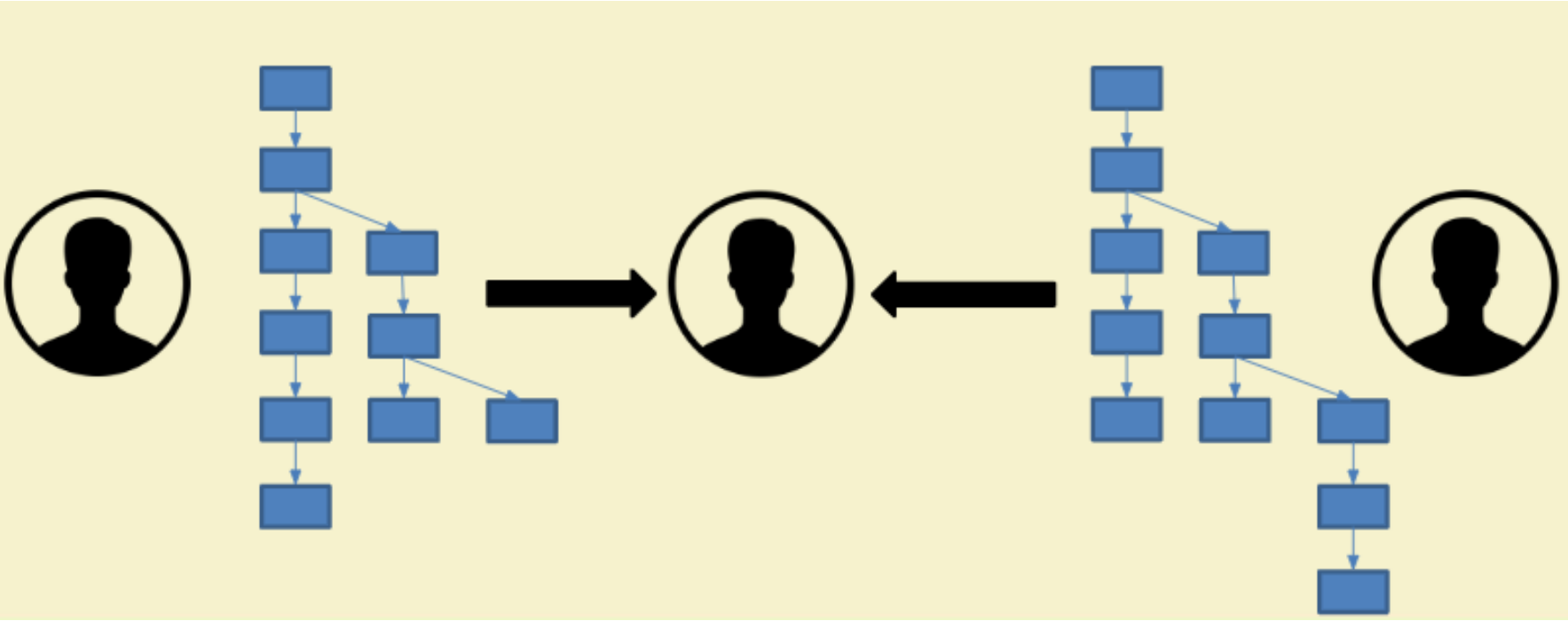


Blockchain (at Permission-less Model) as a Tree

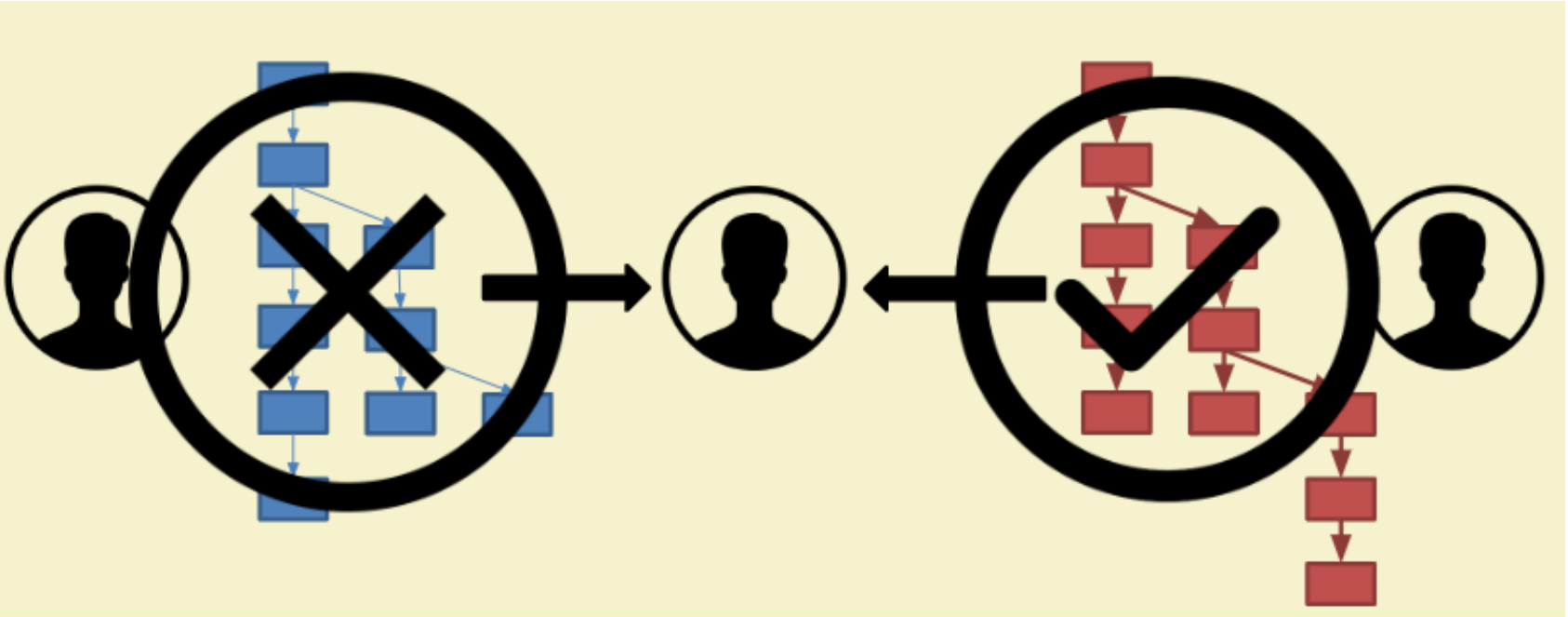
- The longest chain is the accepted chain



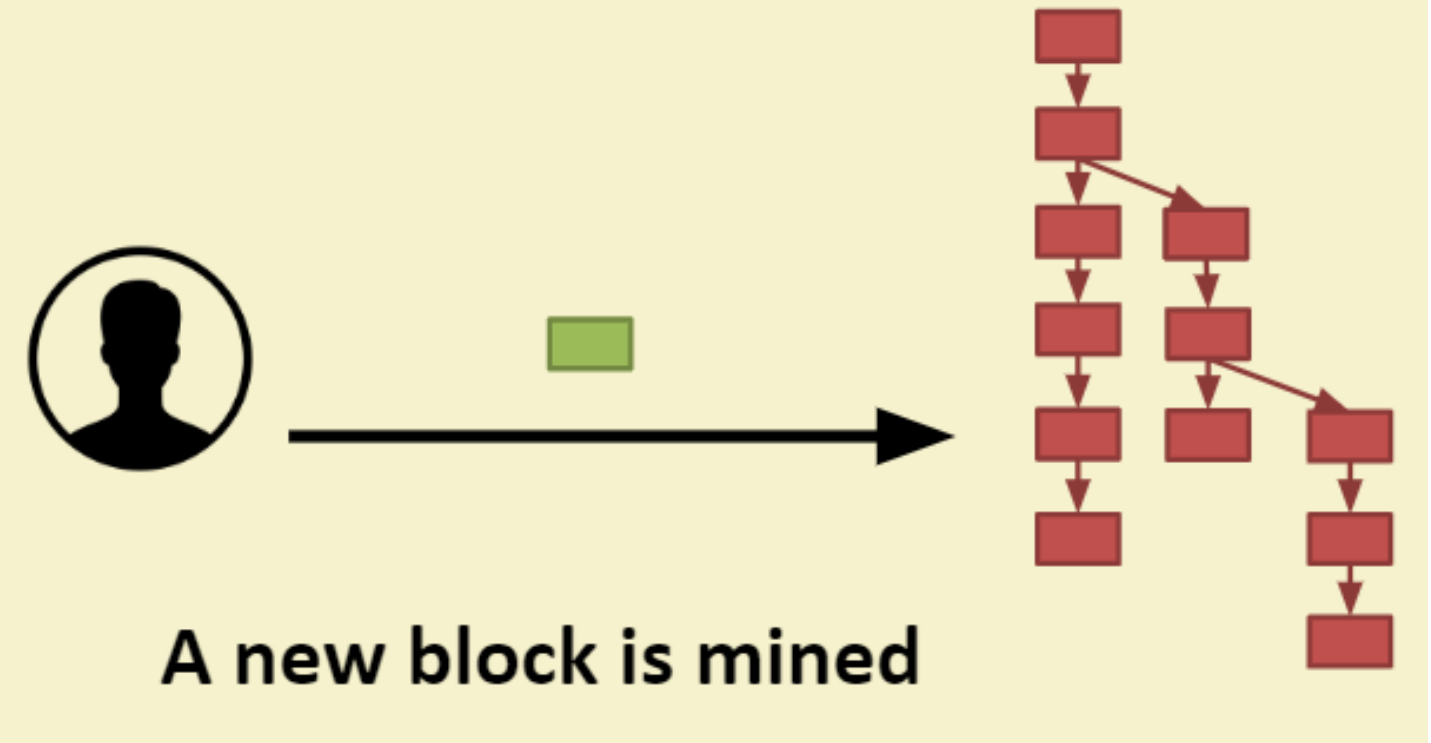
Accepting the Longest Chain



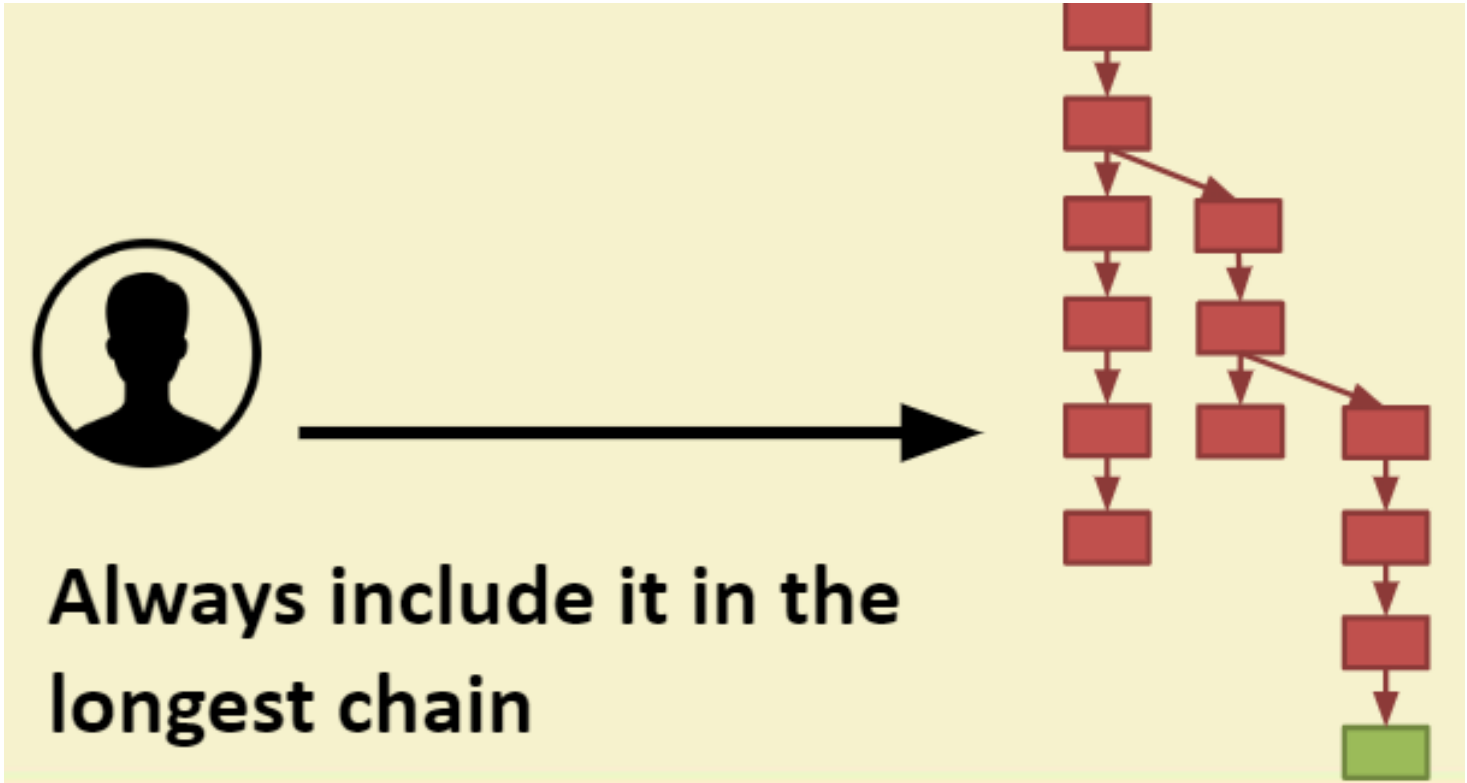
Accepting the Longest Chain



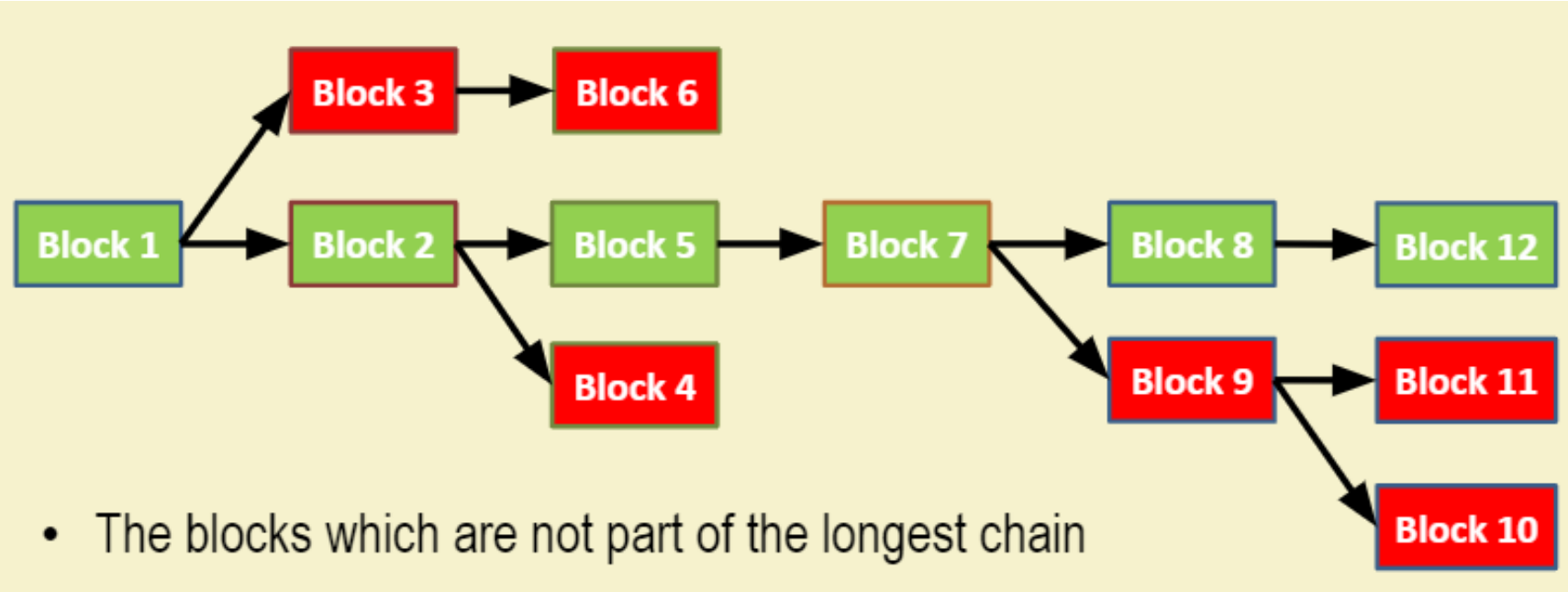
Accepting the Longest Chain



Accepting the Longest Chain



Orphaned Blocks



- The blocks which are not part of the longest chain

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

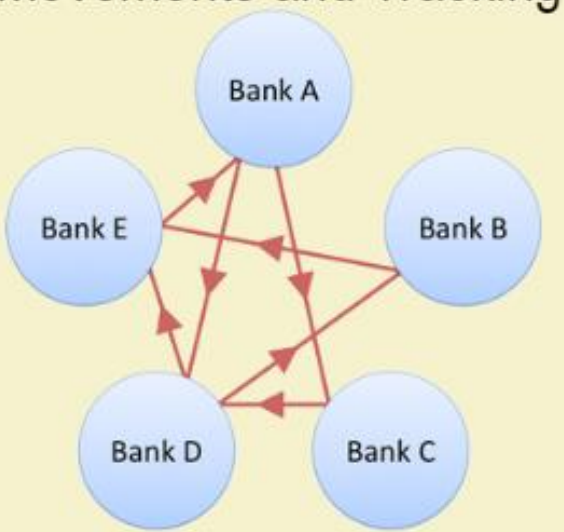
Source: https://blockchain.info/

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

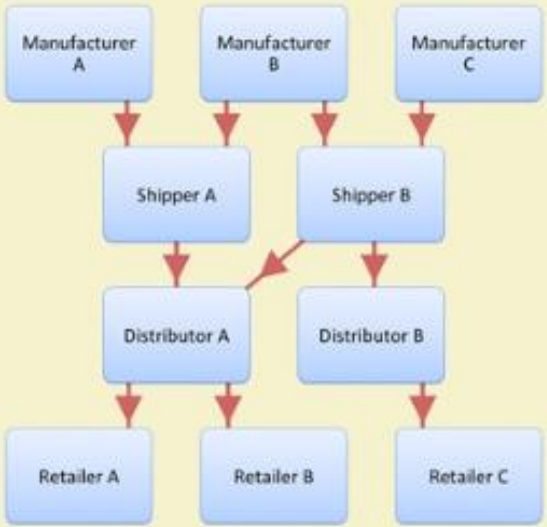
The Permissioned Model Applications

- Asset Movements and Tracking



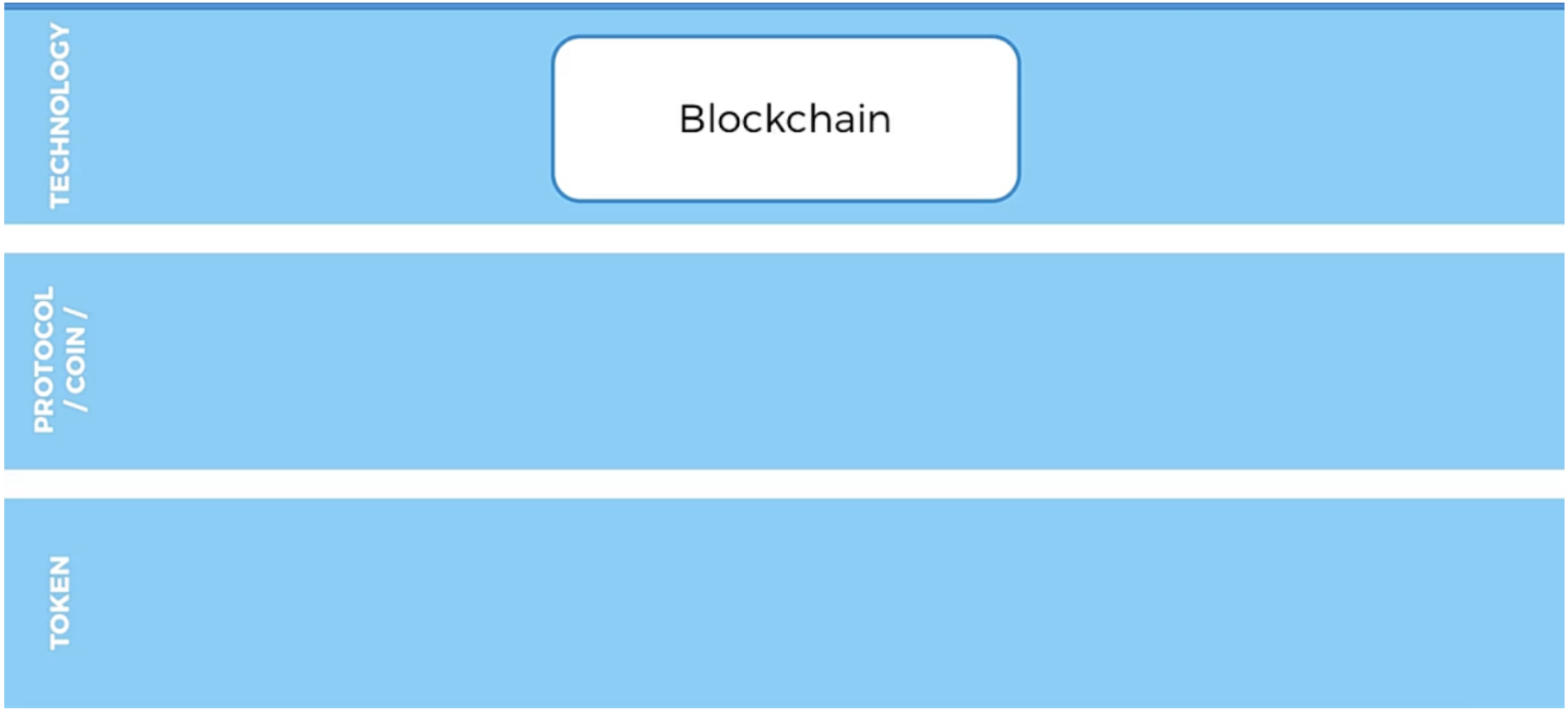
Asset movements
in financial marketplaces

Source: https://www.multichain.com

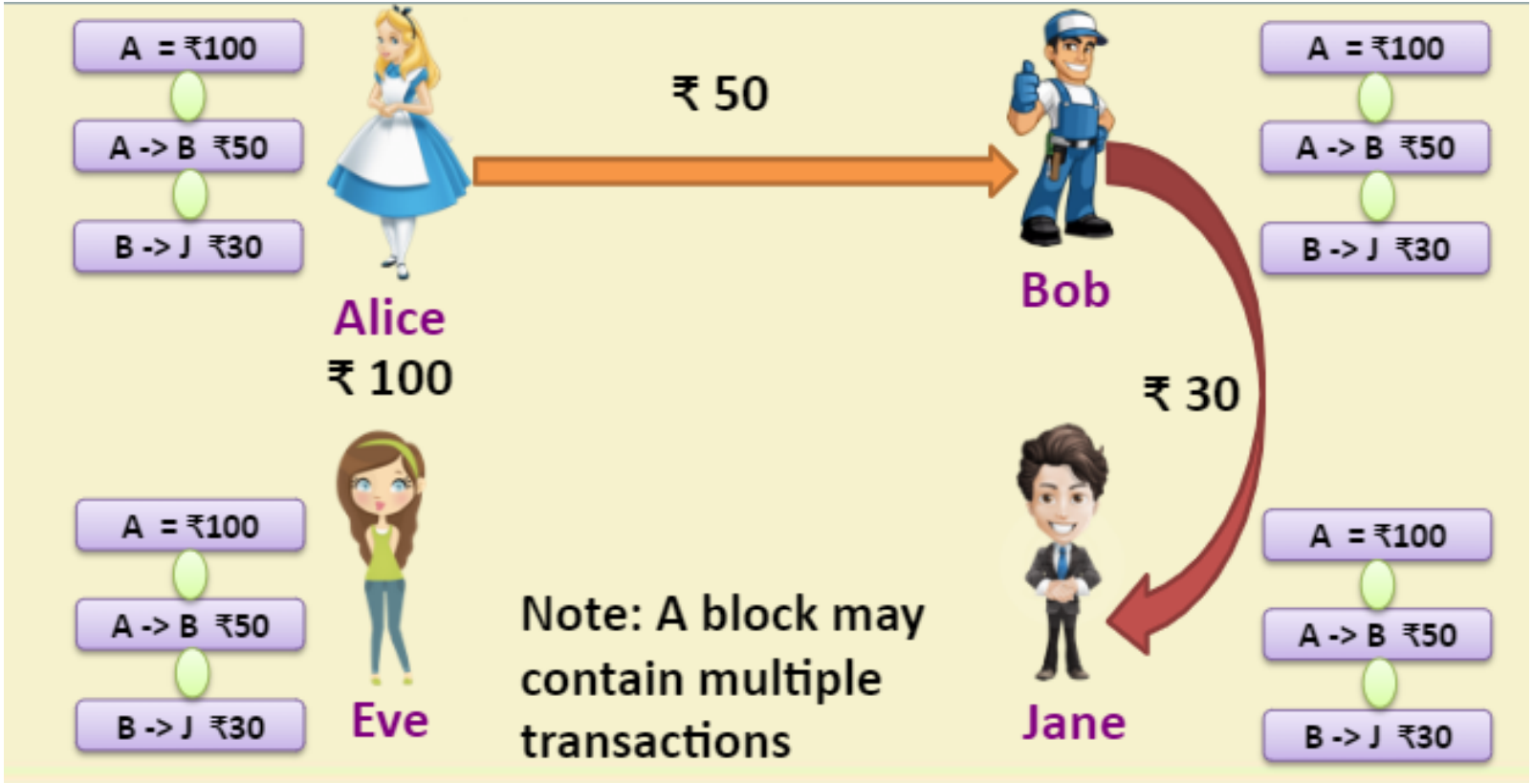


Asset movements
in supply chains

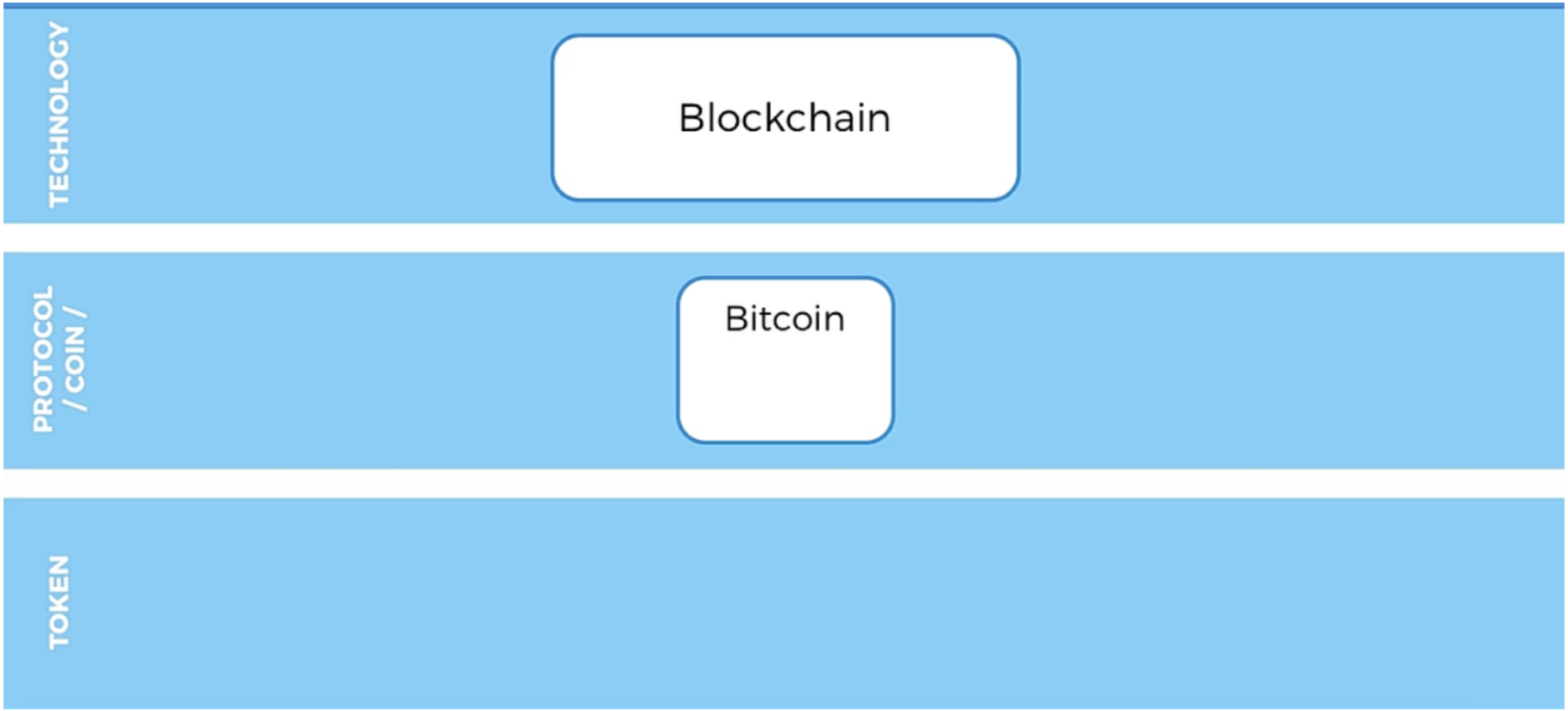
What is Bitcoin?



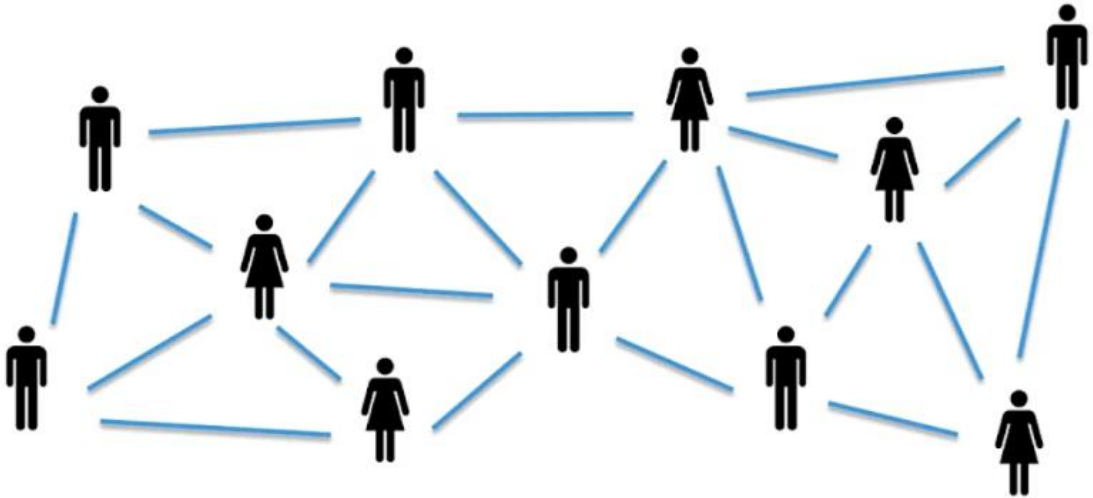
Technology behind Bitcoin - Blockchain



What is Bitcoin?



What is Bitcoin?



Satoshi Nakamoto

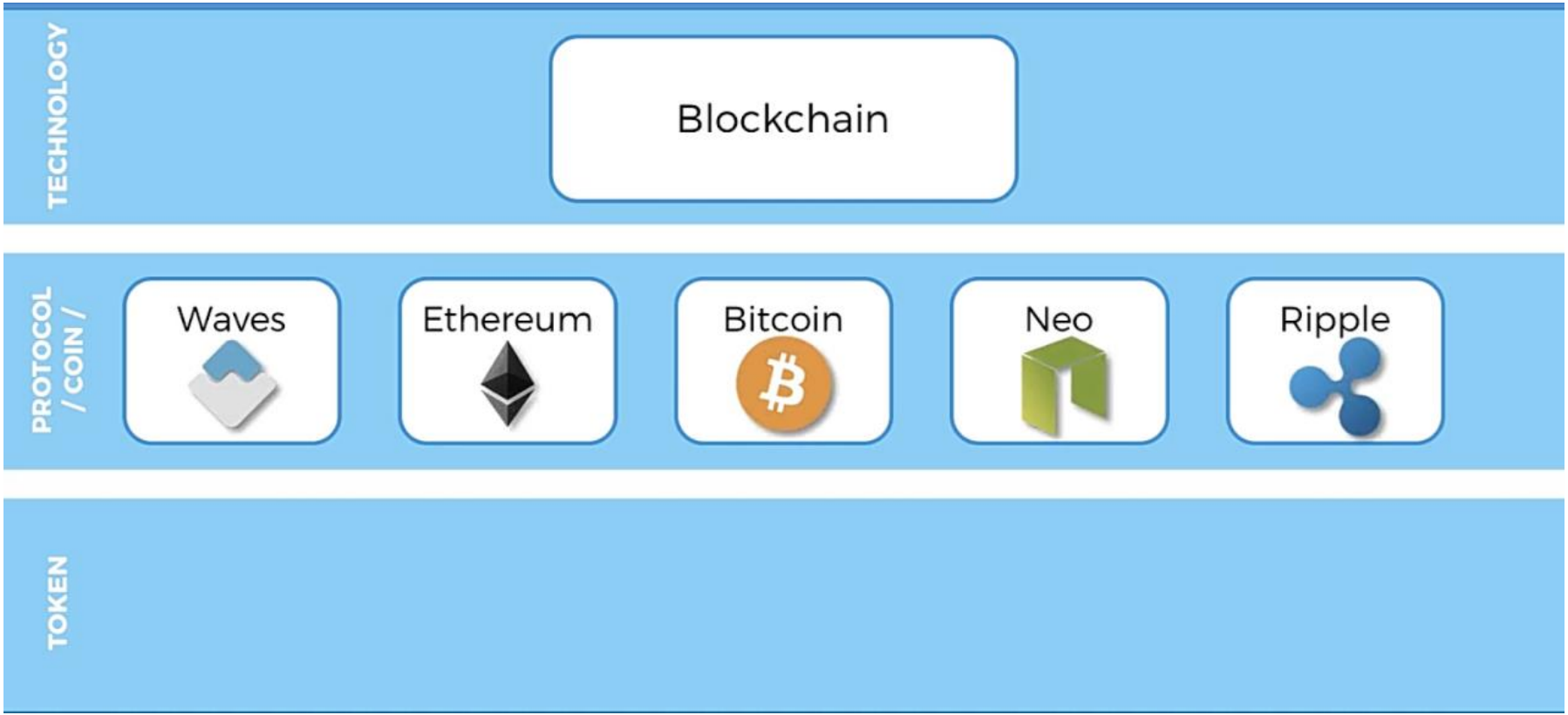
What is Bitcoin?

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

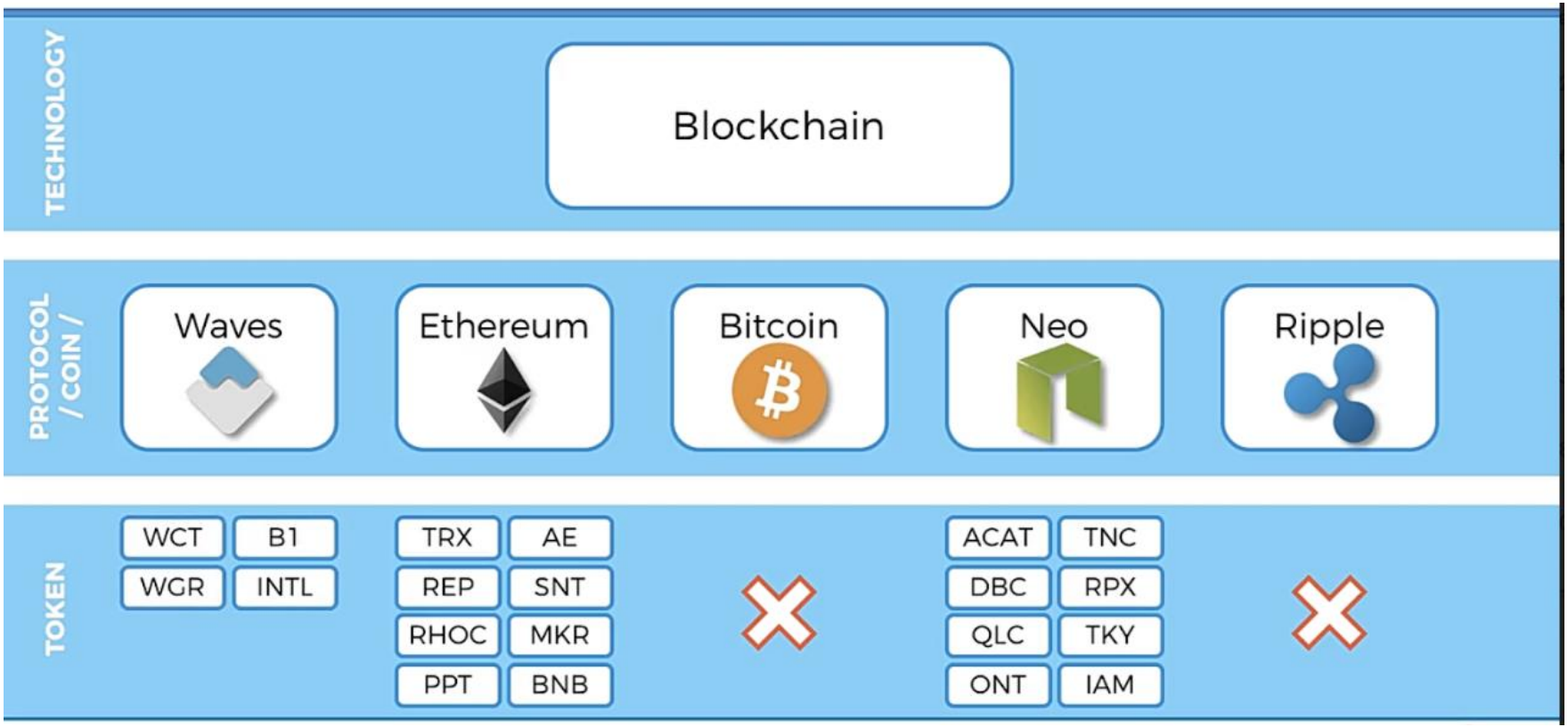
Two broad operations

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

What is Bitcoin?

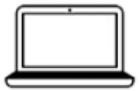


What is Bitcoin?



What is Bitcoin?

The Bitcoin Ecosystem:

- Nodes 
- Large Mines 
- Miners 
- 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

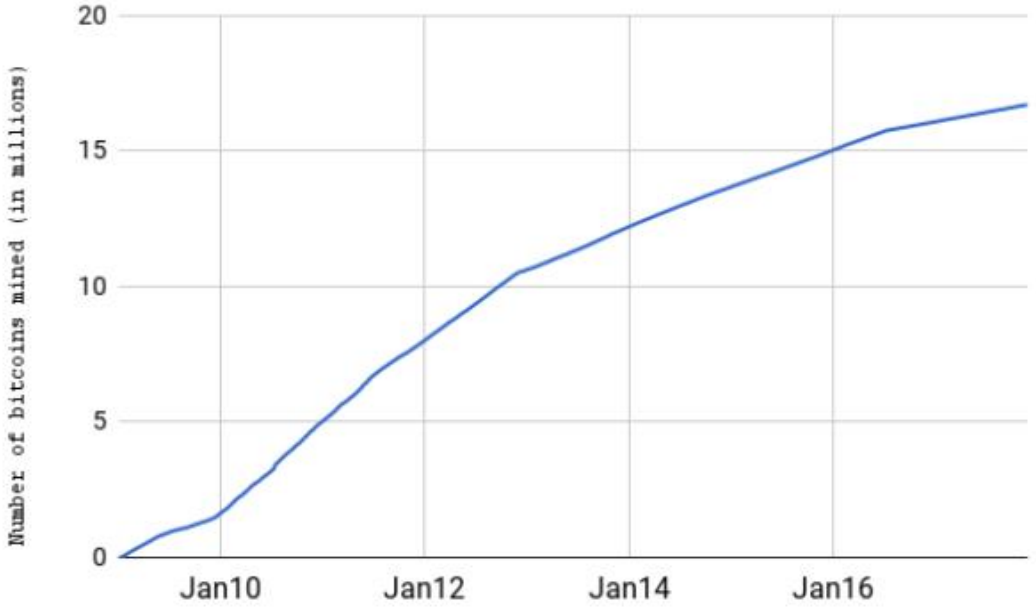
Bitcoin Basics - Creation of Coins

- 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 ≈ 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

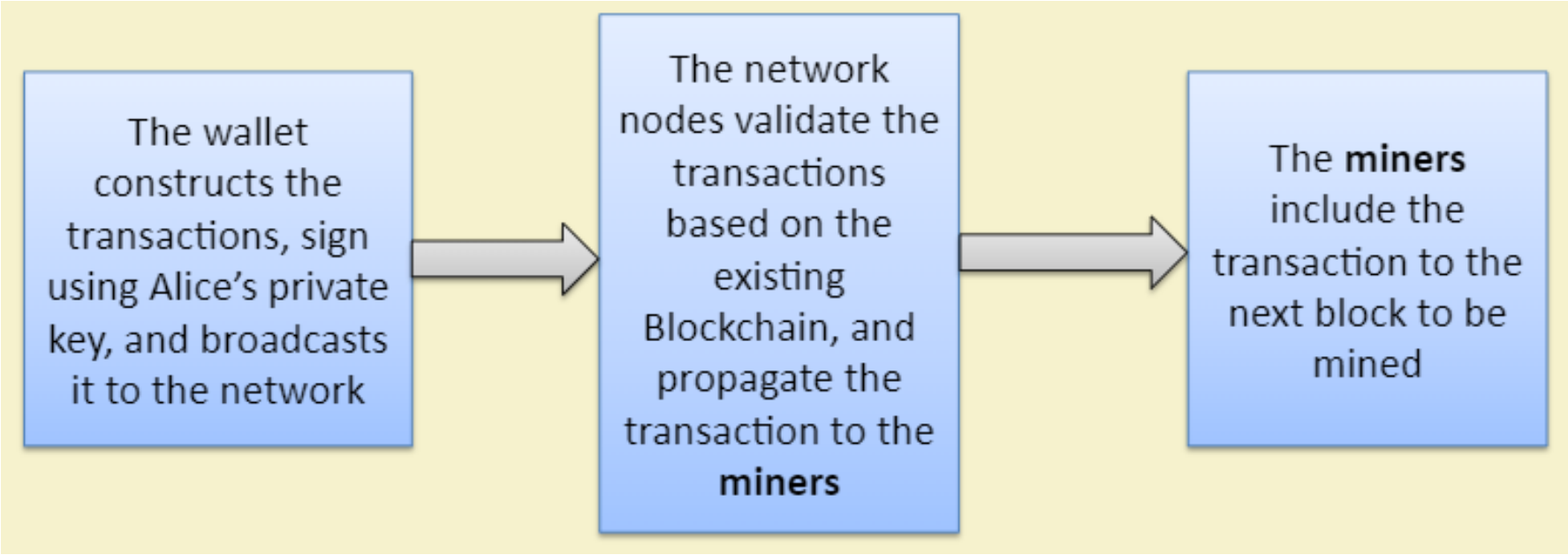
Date reached	Block	Reward Era	BTC/block	Year (estimate)	Start BTC	BTC Added	End BTC	BTC Increase	End BTC % of Limit
2009-01-03	0	1	50.00	2009	0	2625000	2625000	infinite	12.500%
2010-04-22	52500	1	50.00	2010	2625000	2625000	5250000	100.00%	25.000%
2011-01-28	105000	1	50.00	2011*	5250000	2625000	7875000	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 Transaction Lifecycle - The Sender

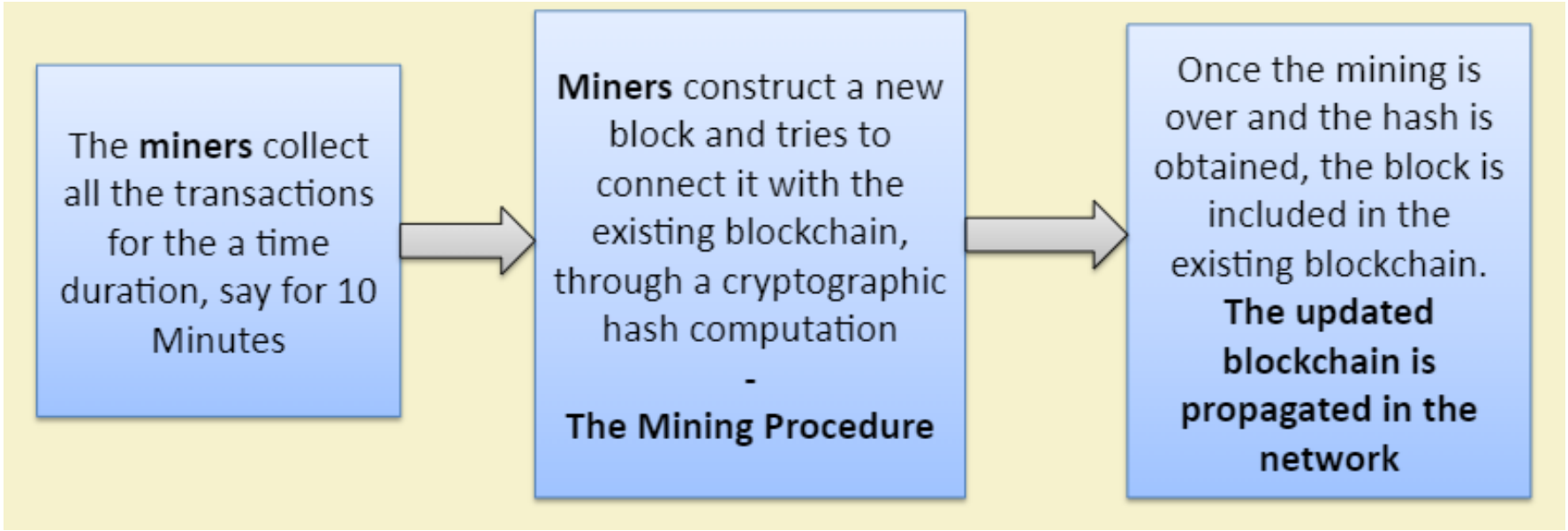
Alice opens her Bitcoin Wallet

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

Bitcoin Transaction Lifecycle - The Network



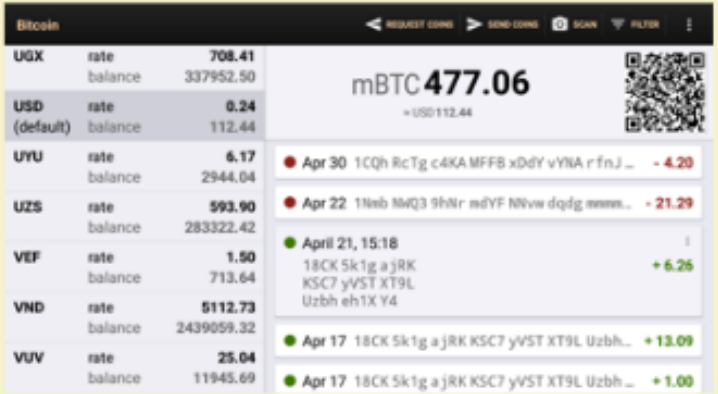
Bitcoin Transaction Lifecycle - The Miners



Bitcoin Transaction Lifecycle - The Receiver

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

The transaction reflects at Bob's wallet

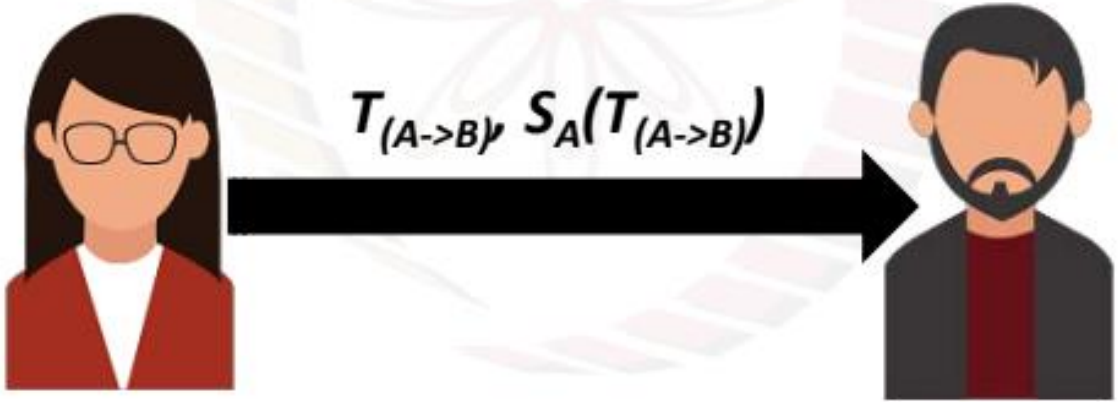


Bitcoin Basics - Sending Payments

- 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

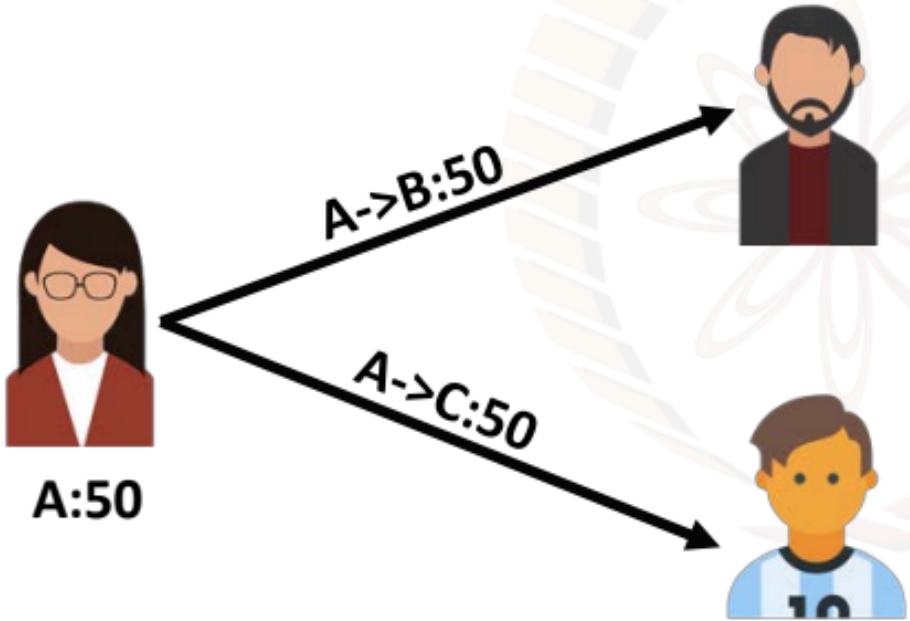
– Alice adds Bob's address and the amount of bitcoins to transfer in a "transaction" message

– 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:

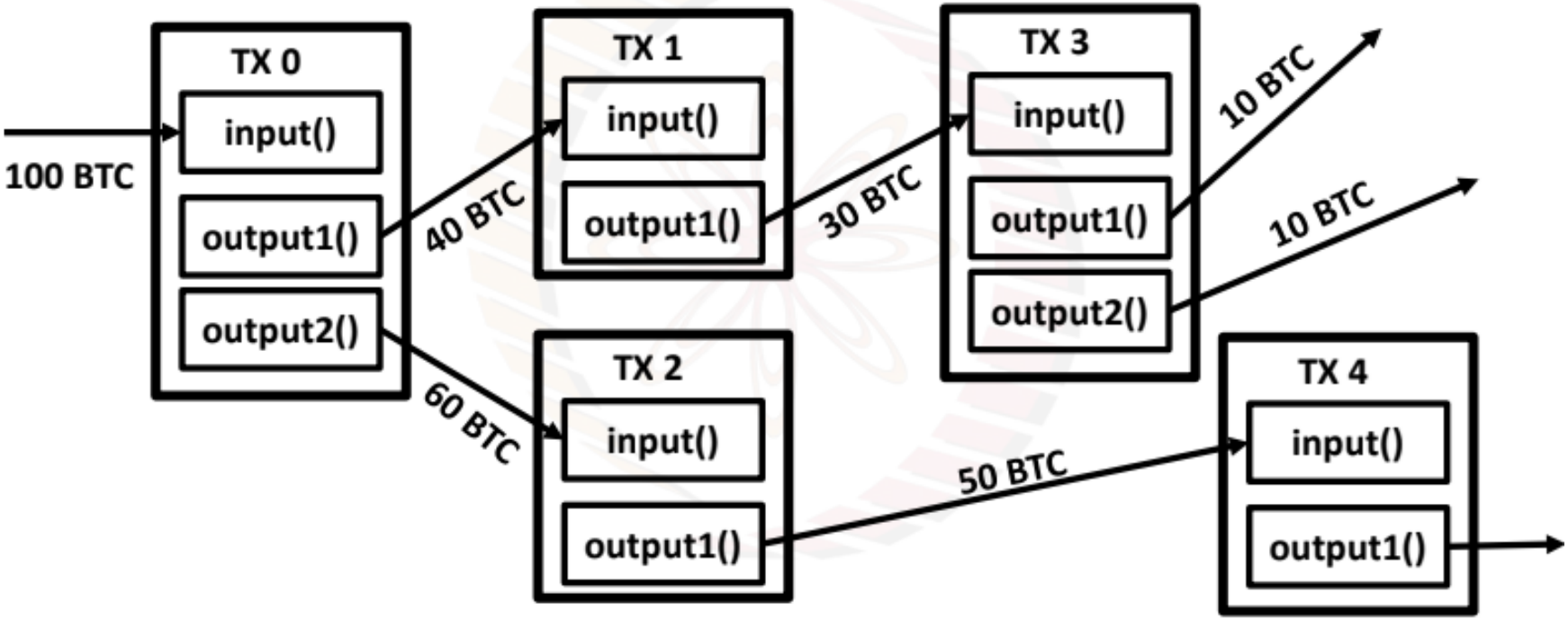
  1PHYrmdJ22MKbJevpb3MBNpVckjZHt89hz
- Each person can have many such addresses, each with its own balance

  – Difficult to know which person owns what amount

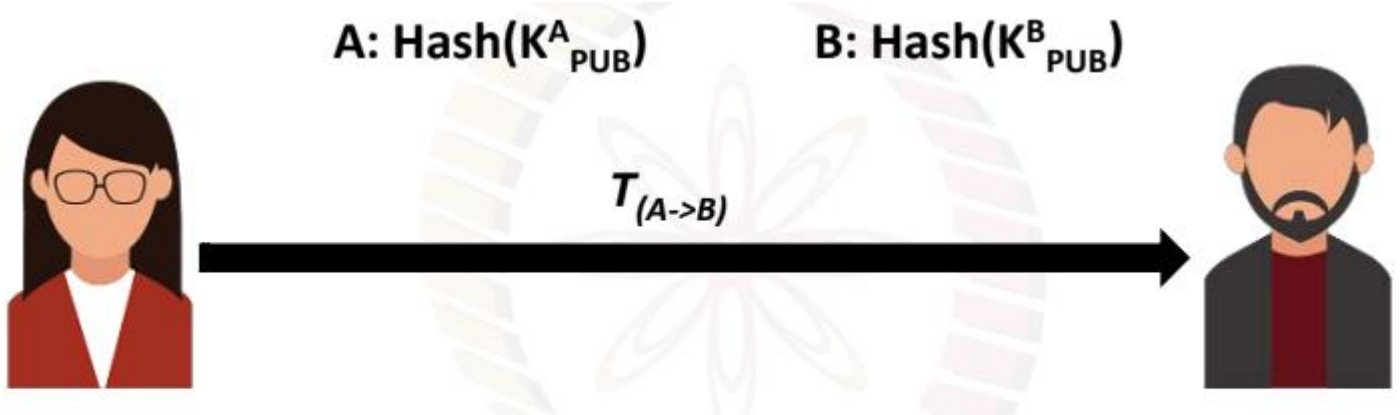
Bitcoin Transactions

- 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

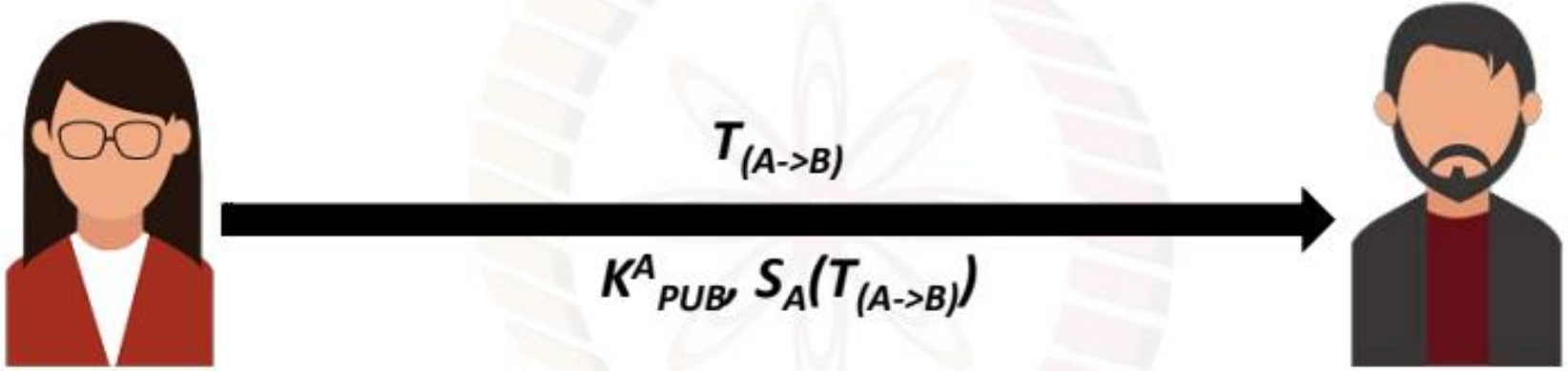


Bitcoin Transactions - A Simple Example



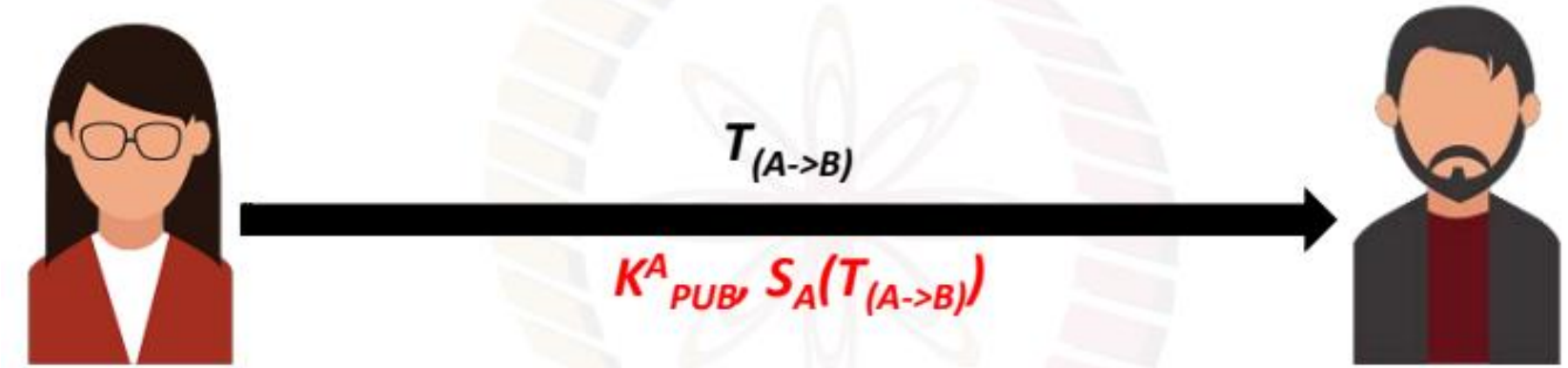
How Bob will verify that the transaction is actually originated from Alice?

Bitcoin Transactions - A Simple Example



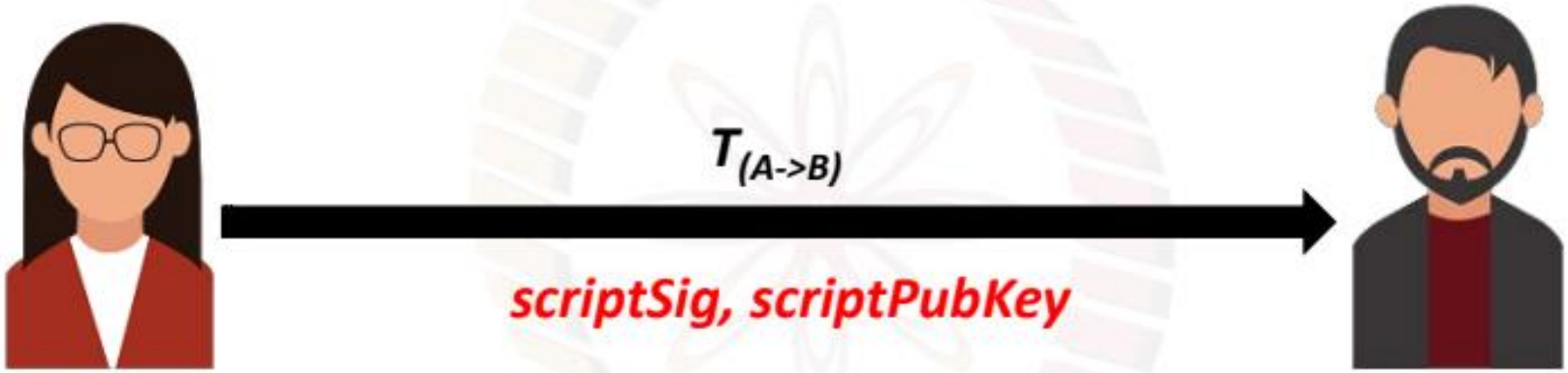
Send the public key of Alice along with the signature -> Bob can verify this

Bitcoin Transactions - A Simple Example



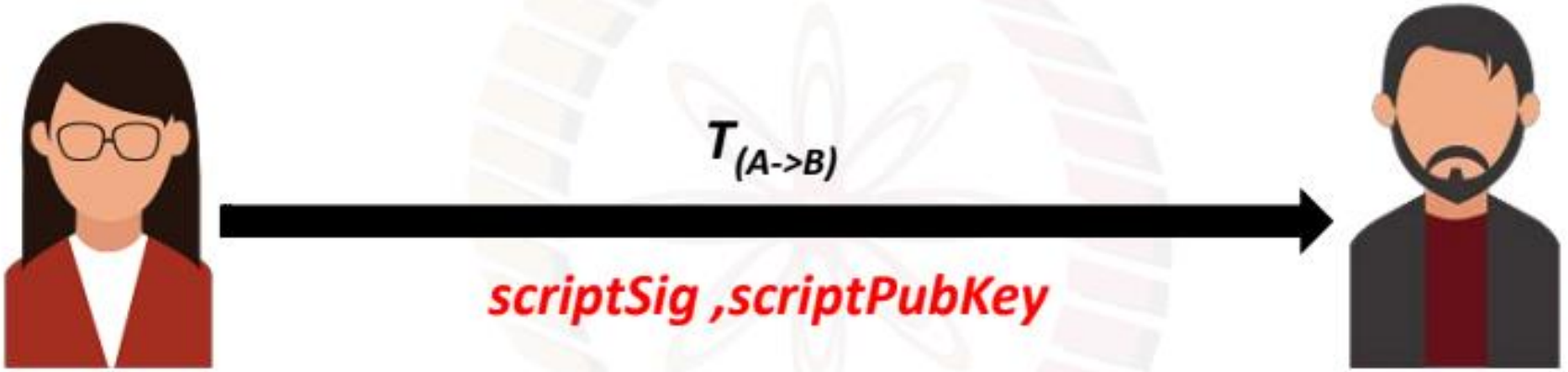
Bitcoin indeed transfers scripts instead of the signature and the public key

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

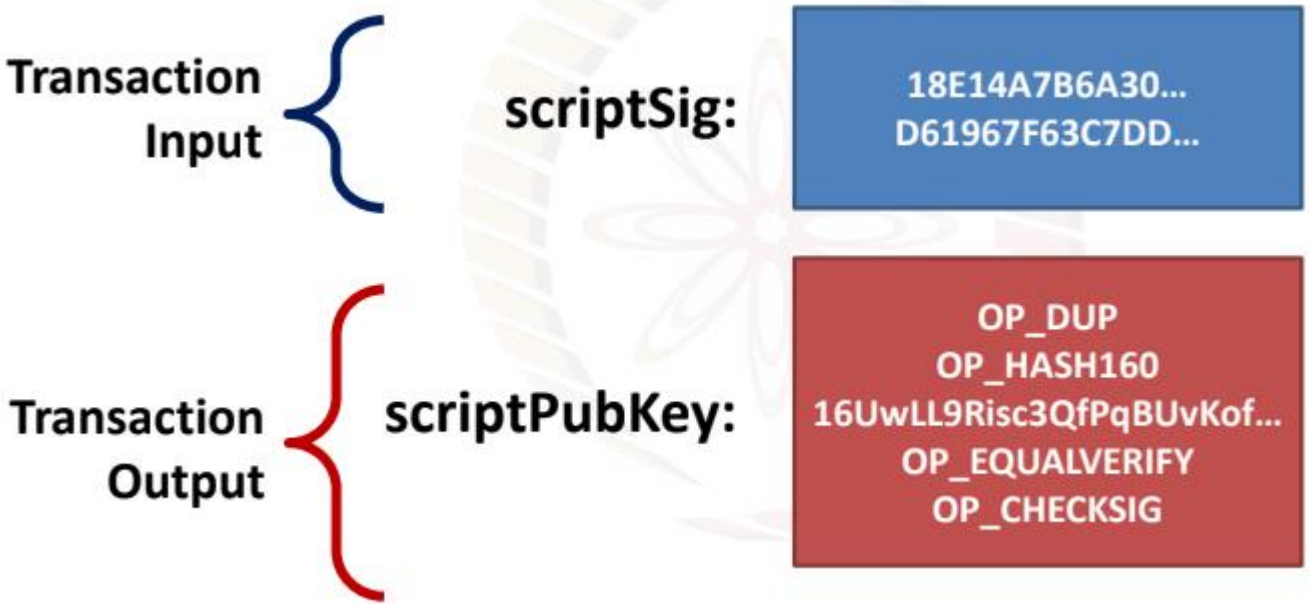
Bitcoin Transactions - A Simple Example

- 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

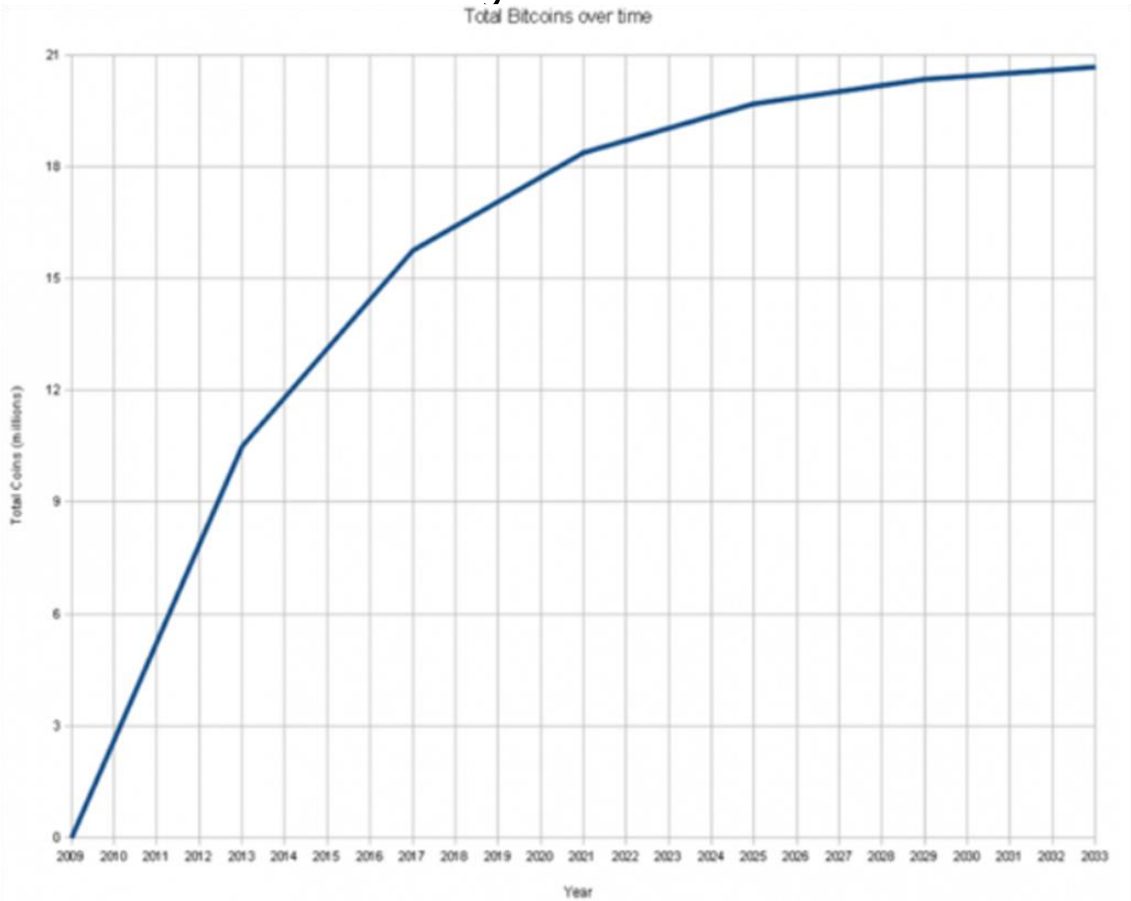
Agenda

- 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.

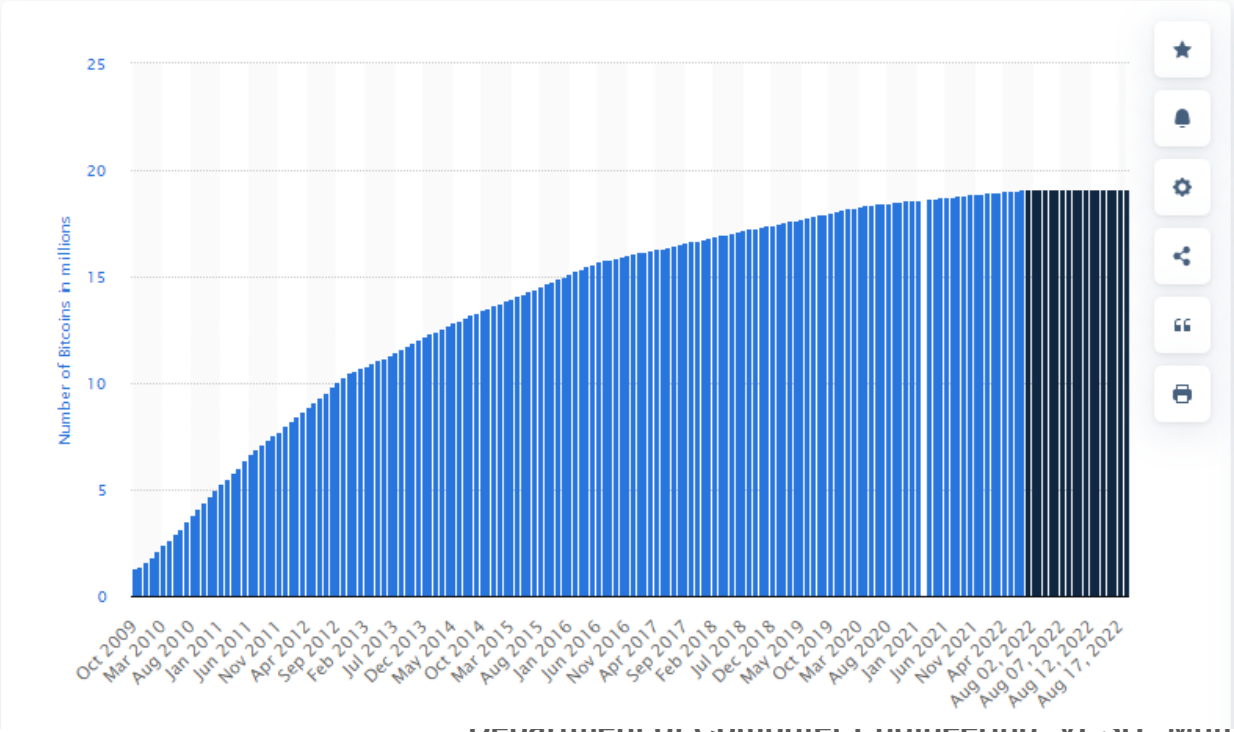
Size of the Bitcoin Economy

- 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)



DOWNLOAD

PDF + XLS +

Release date
August 2022

Region
Worldwide

Survey time period
October 2009 to August 18, 202

Special properties
Bitcoin (BTC) has a maximum su
coins

Supplementary notes
Monthly figures are as of the en
month.

https://www.statista.com/statistics/247280/number-of-bitcoins-in-circulation/

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 | Telegram Bot | Base Ecosystem | Gaming | SocialFi | Show rows 100 | Filters | Customize

#	Name	Price	1h %	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply	Last 7 Days
1	Bitcoin BTC	$25,986.91	0.31%	0.57%	11.52%	$505,803,278,052	$10,334,433,579 397,739 BTC	19,463,775 BTC	
2	Ethereum ETH	$1,667.68	0.38%	0.25%	9.69%	$200,479,822,167	$4,432,369,634 2,657,102 ETH	120,215,151 ETH	
3	Tether USDt USDT	$0.9996	0.01%	0.03%	0.08%	$82,810,679,236	$17,508,097,240 17,515,544,582 USDT	82,846,484,081 USDT	

Courtesy: https://coinmarketcap.com/

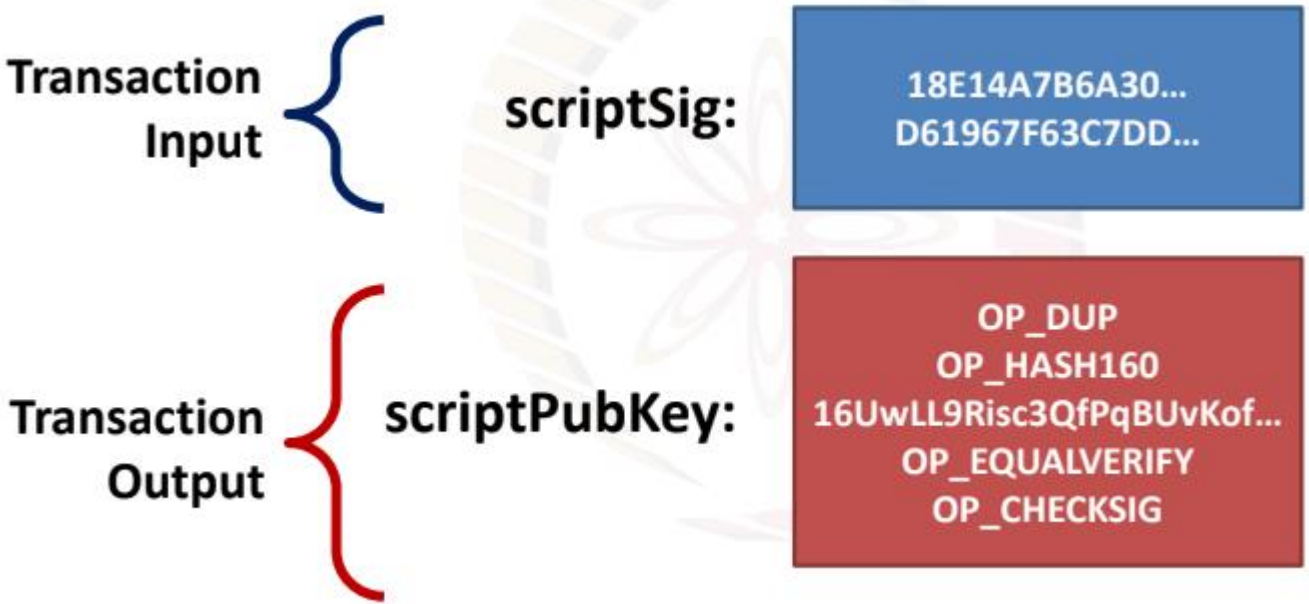
Bitcoin Scripting Language

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



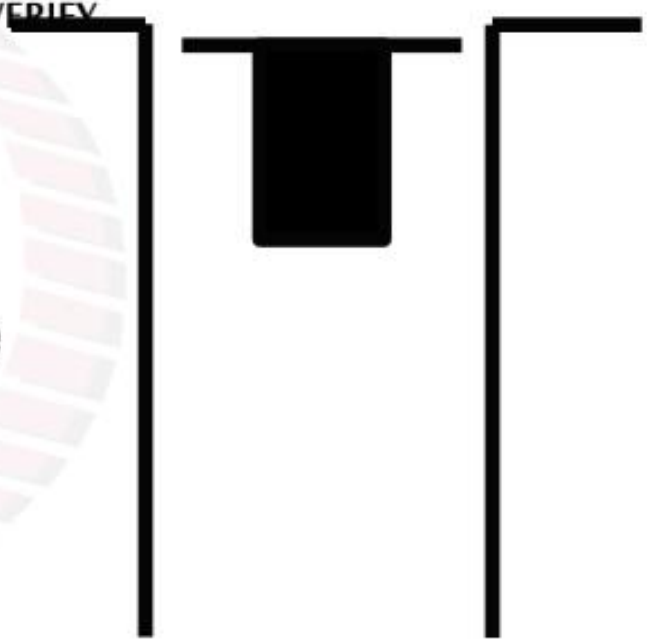
Bitcoin Scripts

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

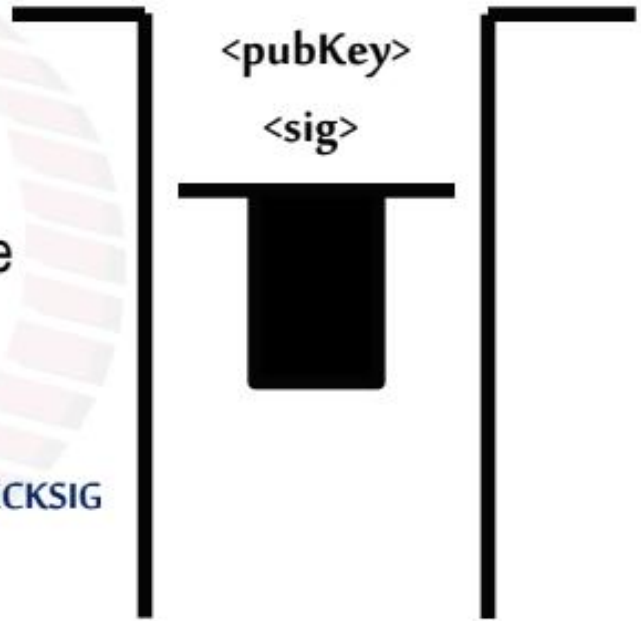
<sig> <pubKey> OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG



Bitcoin Scripts

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

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



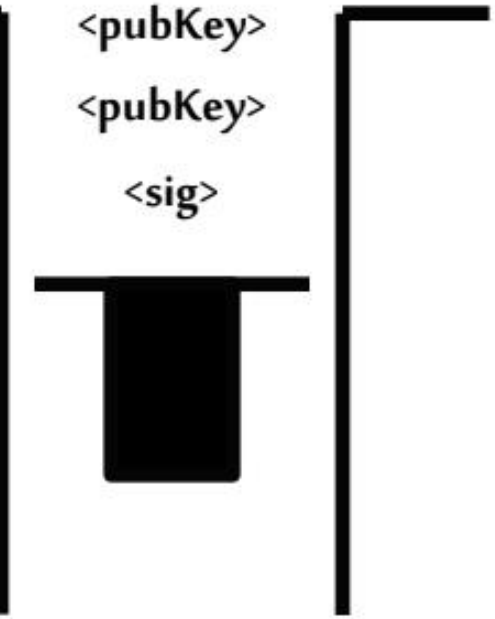
OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG

Bitcoin Scripts

OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG

- Top stack item is duplicated

OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG

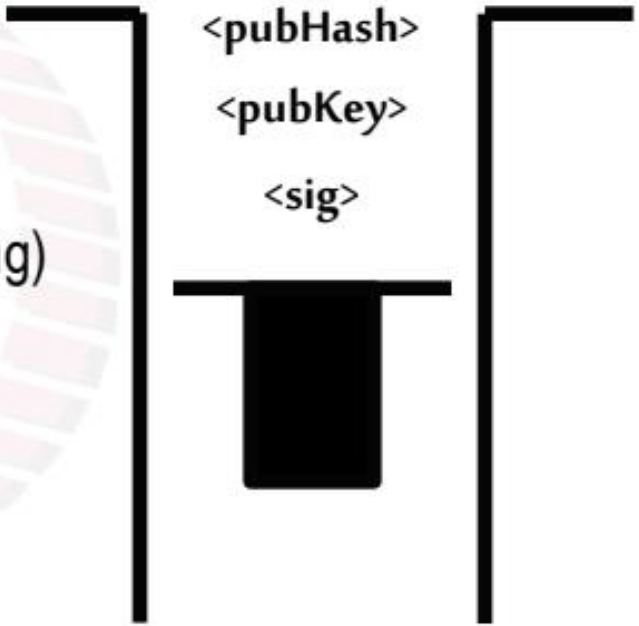


Bitcoin Scripts

OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG

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

<pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG

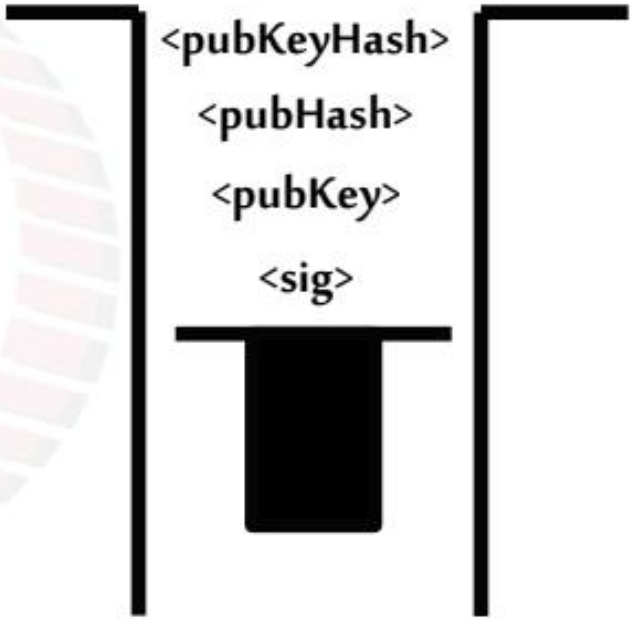


Bitcoin Scripts

<pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG

- The constant is pushed in the stack

OP_EQUALVERIFY OP_CHECKSIG

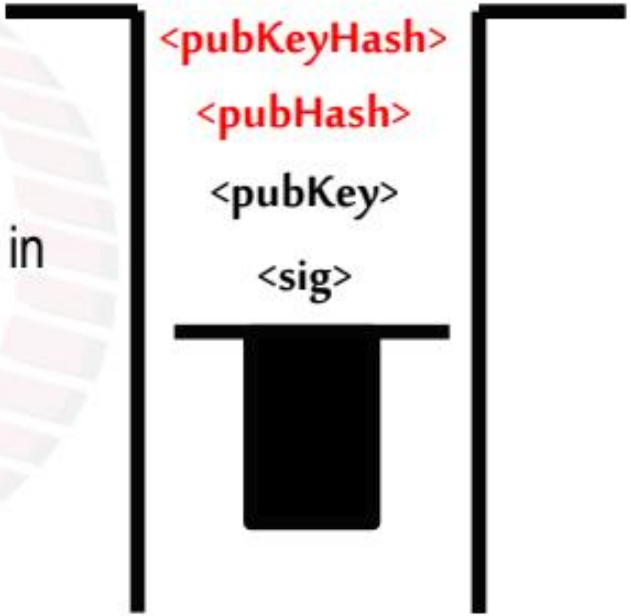


Bitcoin Scripts

OP_EQUALVERIFY OP_CHECKSIG

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

OP_CHECKSIG

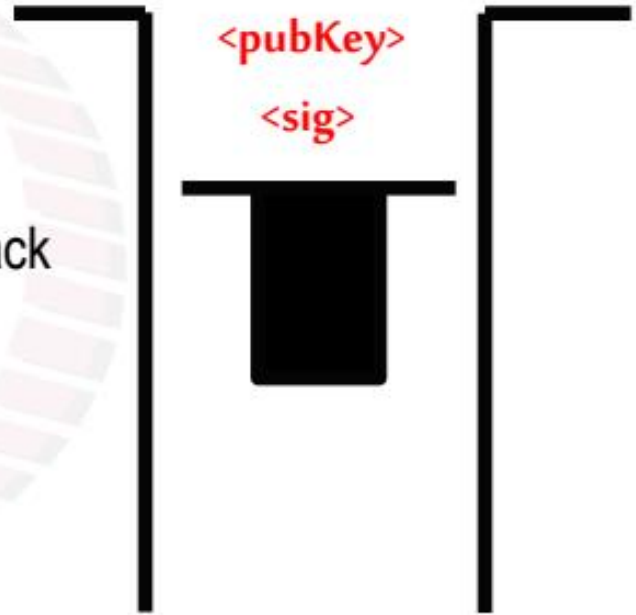


Bitcoin Scripts

OP_CHECKSIG

- Signature is checked based on the top two stack item

TRUE



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>

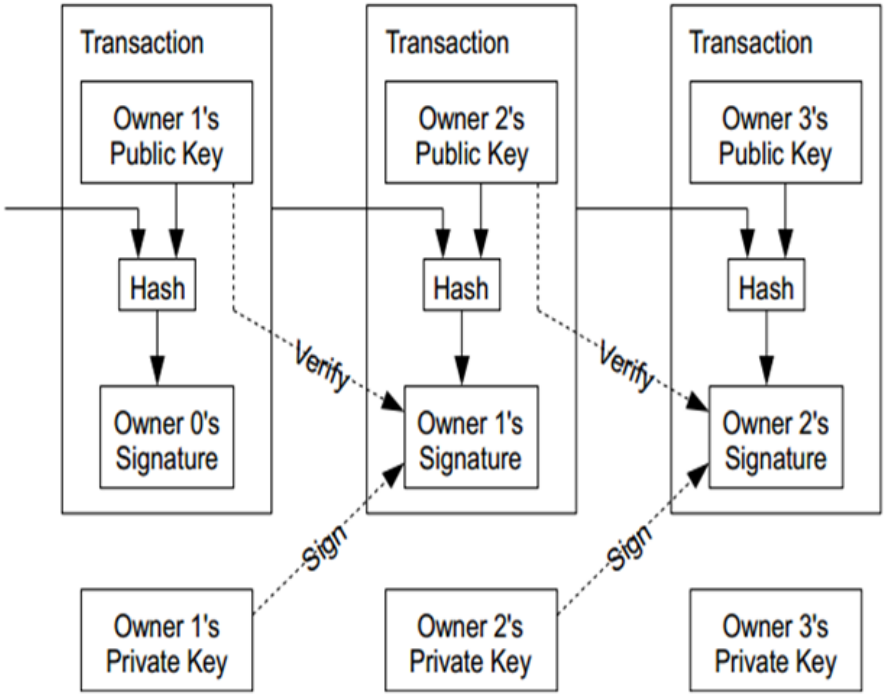
Bitcoin P2P Network

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

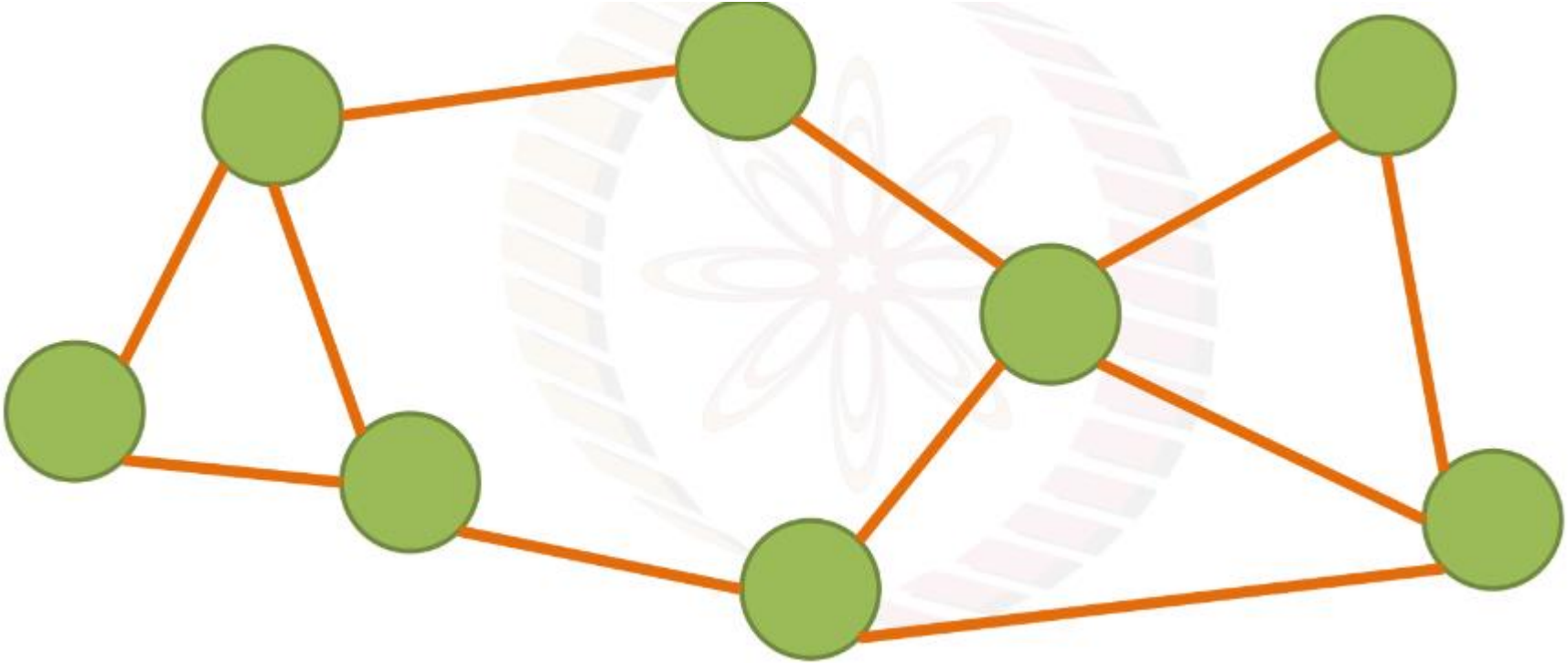
- **Electronic coin == chain of digital signatures**
- BitCoin transfer: Sign(Previous transaction + New owner's public key)
- Anyone can verify (n-1) th owner transferred this to the nth owner.
- Anyone can follow the history
- Given a BitCoin



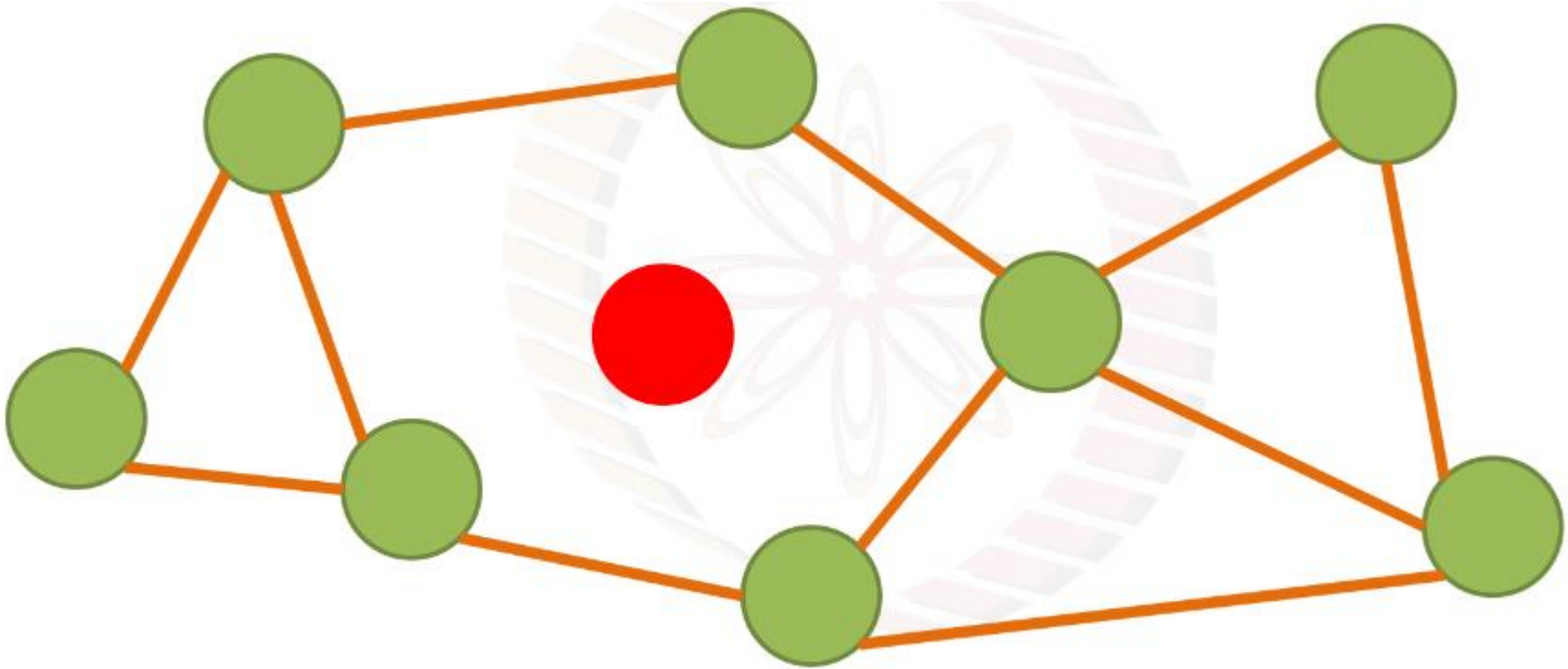
Bitcoin P2P Network

- **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.

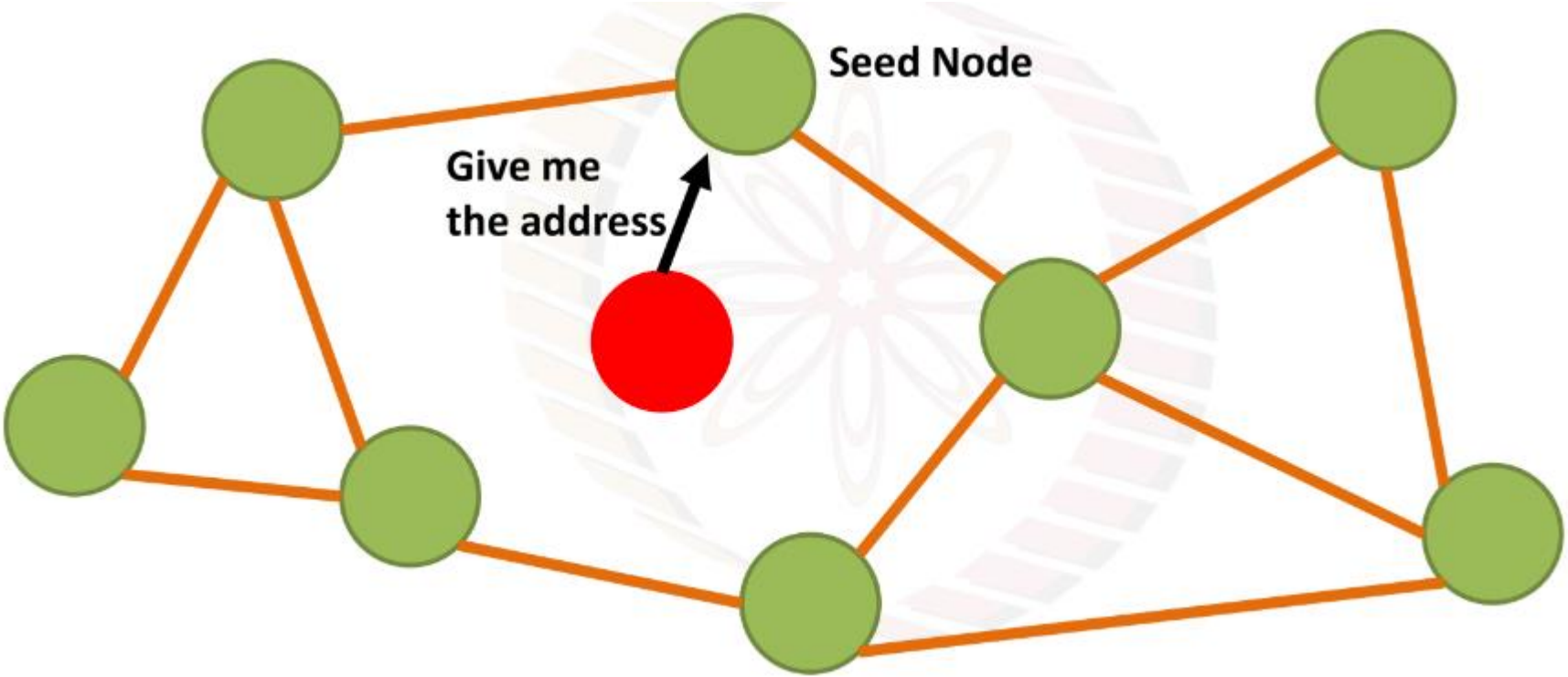
Joining in a Bitcoin P2P Network



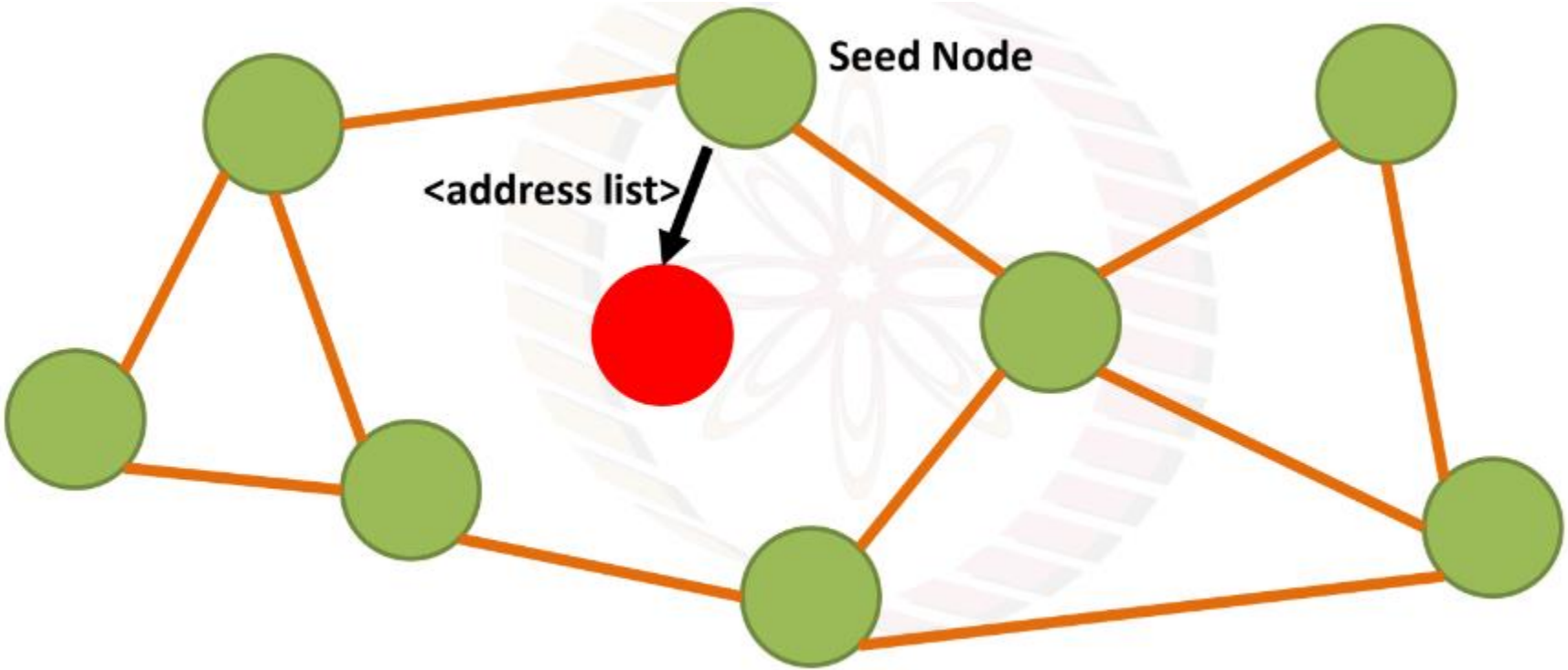
Joining in a Bitcoin P2P Network



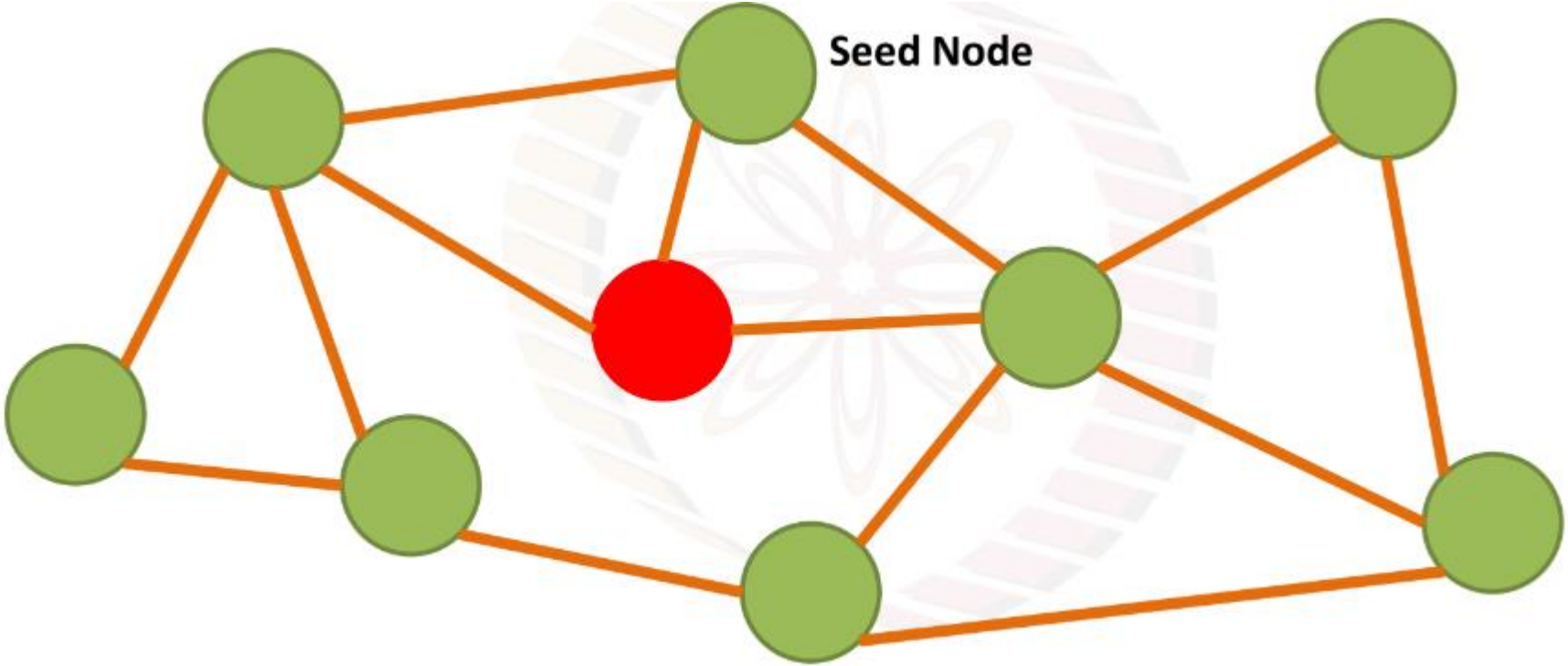
Joining in a Bitcoin P2P Network



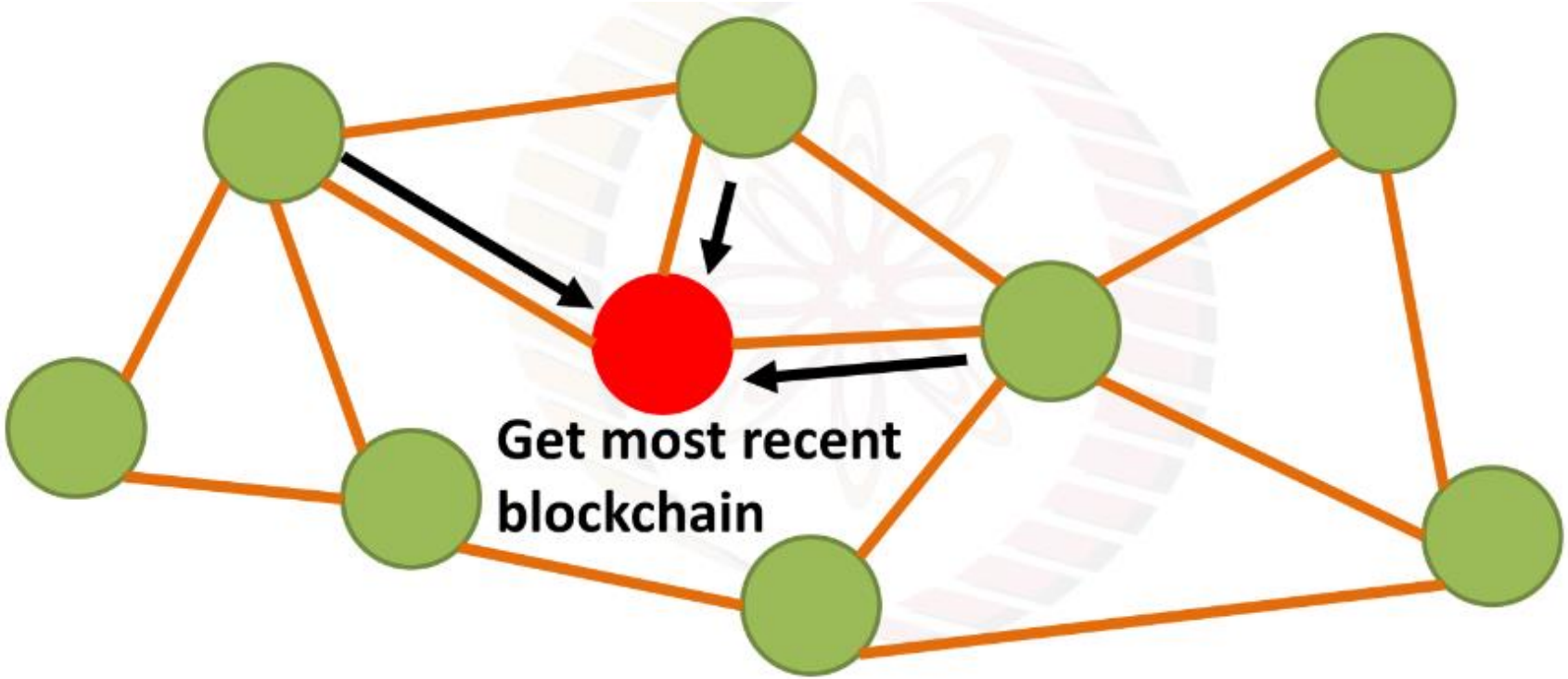
Joining in a Bitcoin P2P Network



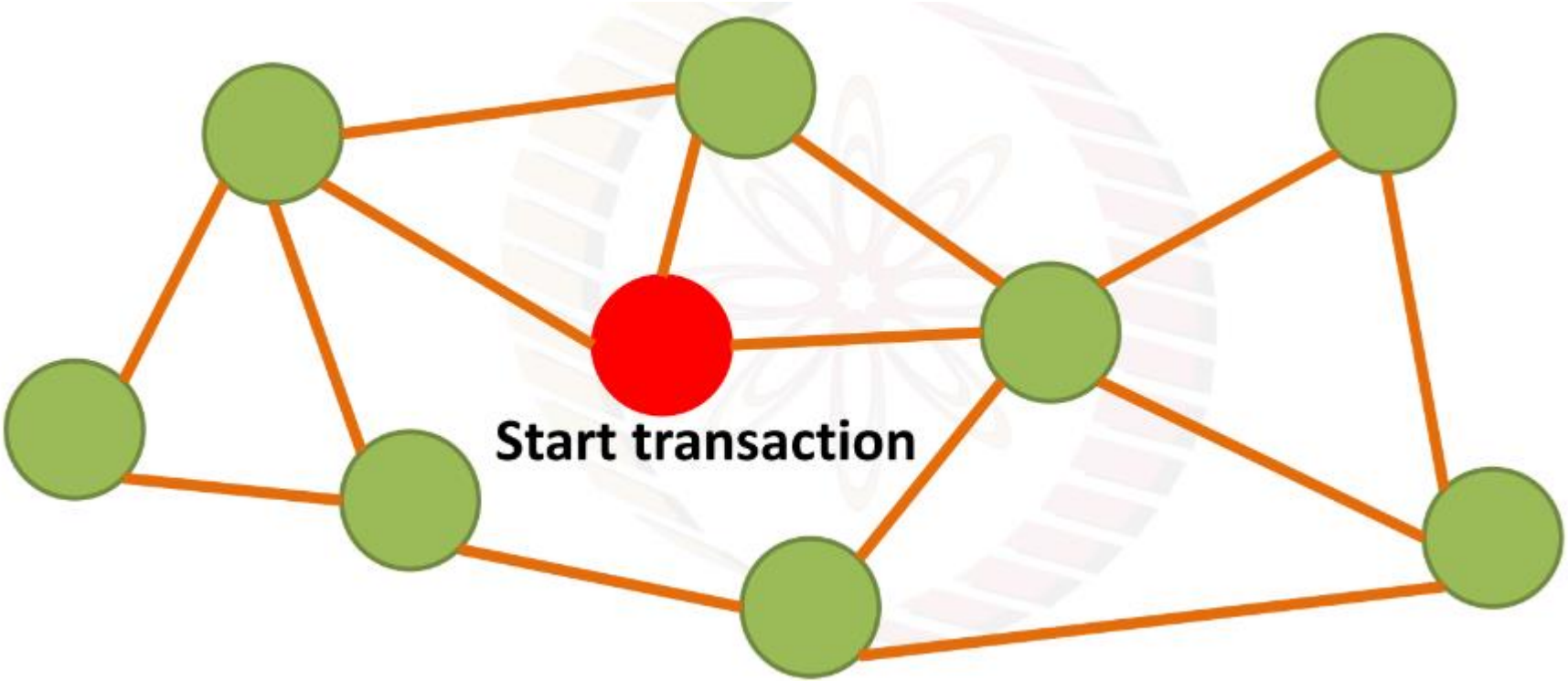
Joining in a Bitcoin P2P Network



Joining in a Bitcoin P2P Network



Joining in a Bitcoin P2P Network



Bitcoin Transaction Format

Bitcoin Transaction Flow

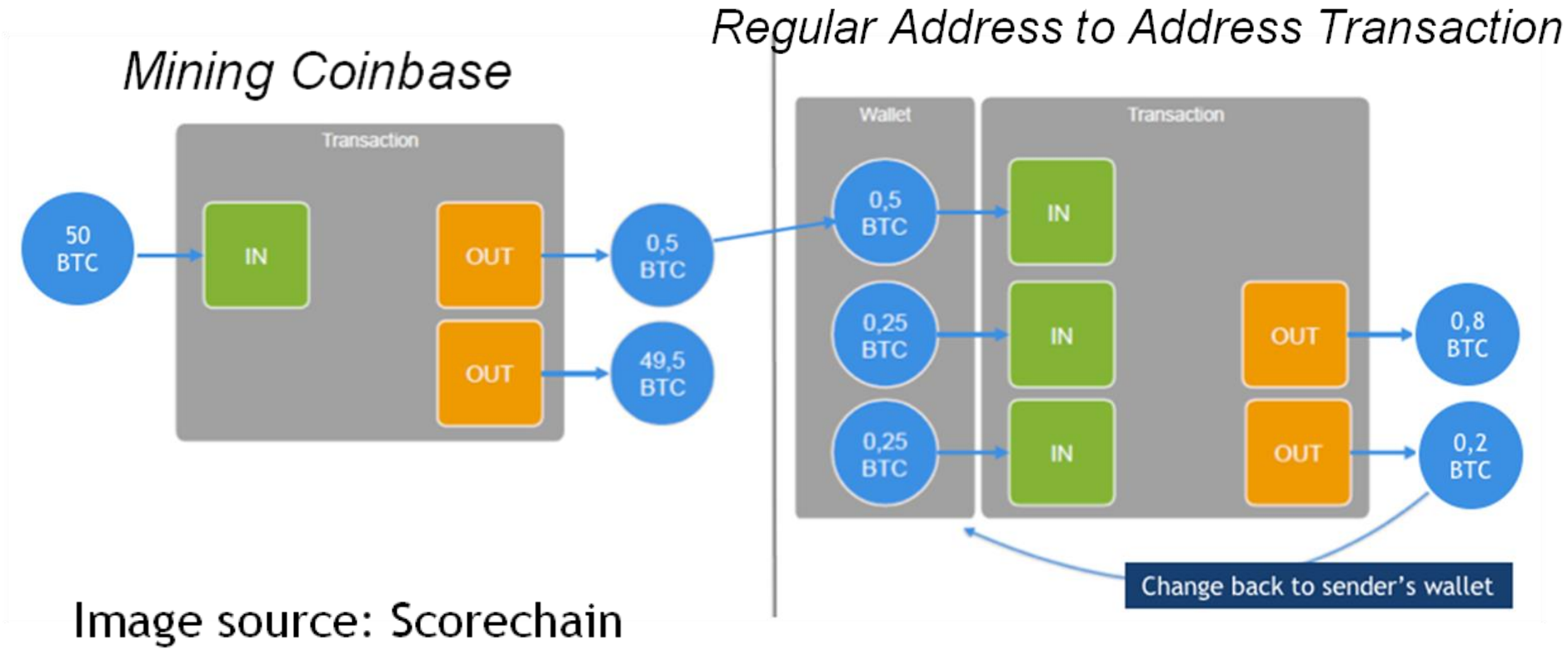
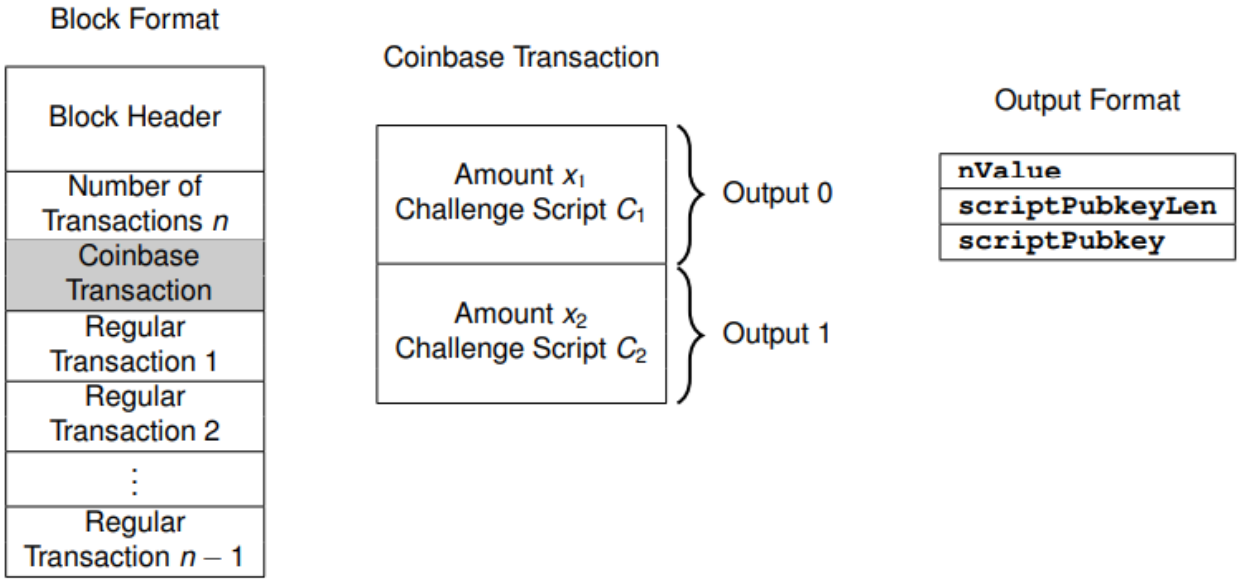


Image source: Scorechain

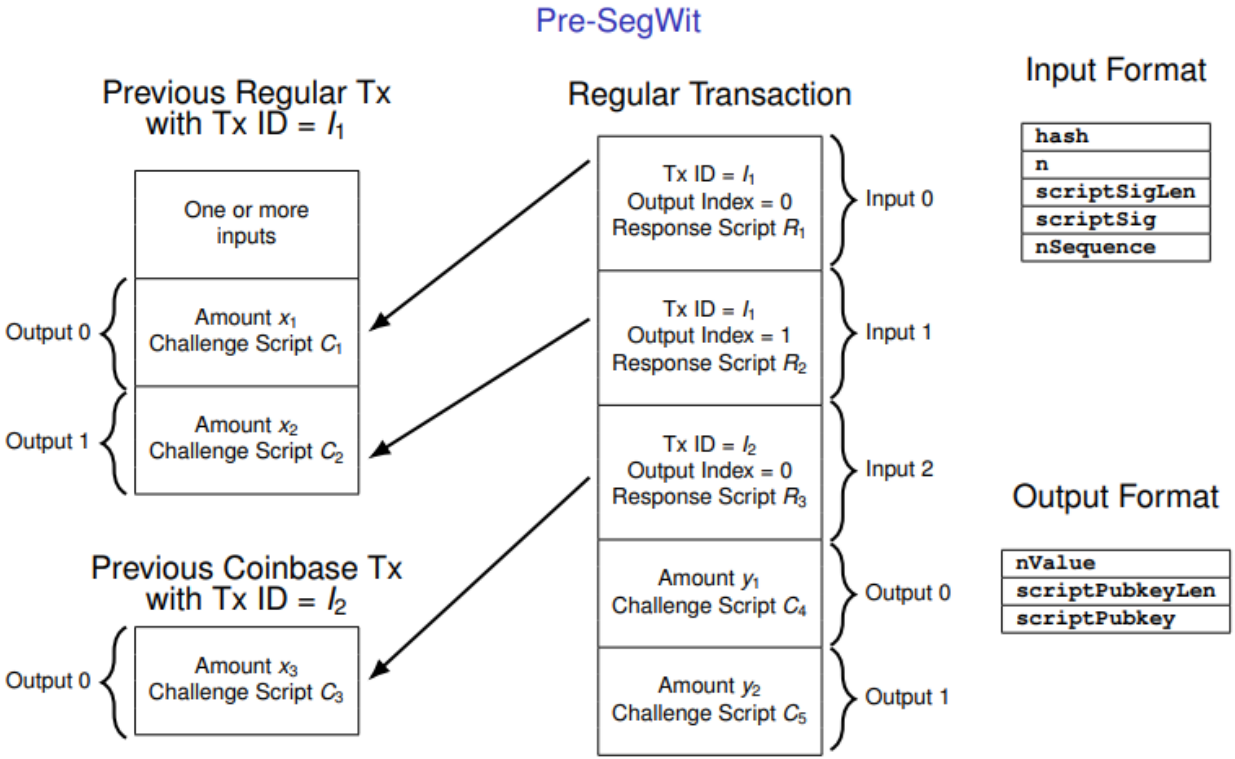
Coinbase Transaction Format

Pre-SegWit



- **`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



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

Bitcoin Transactions

How Bitcoin Transaction Works?

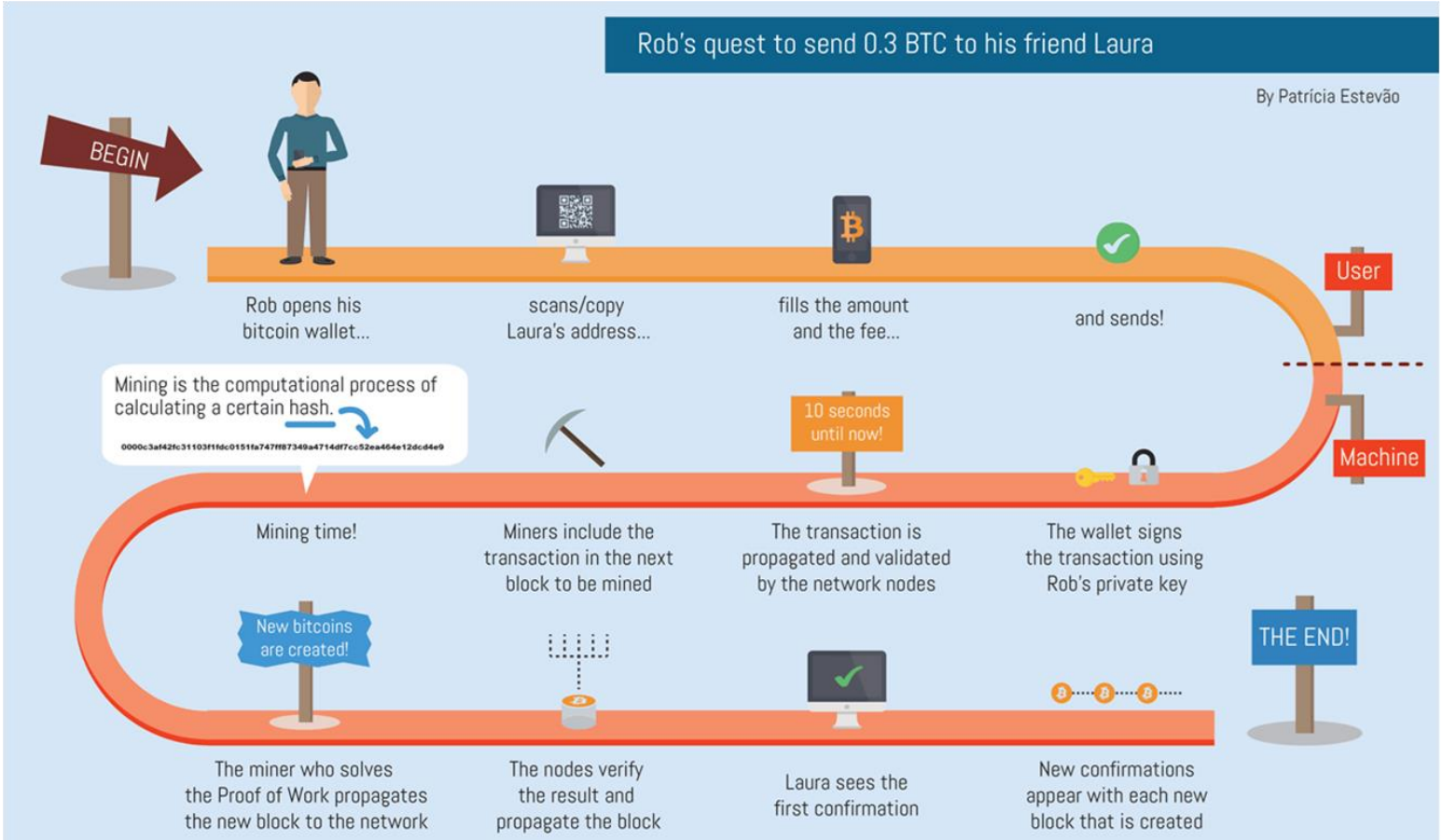
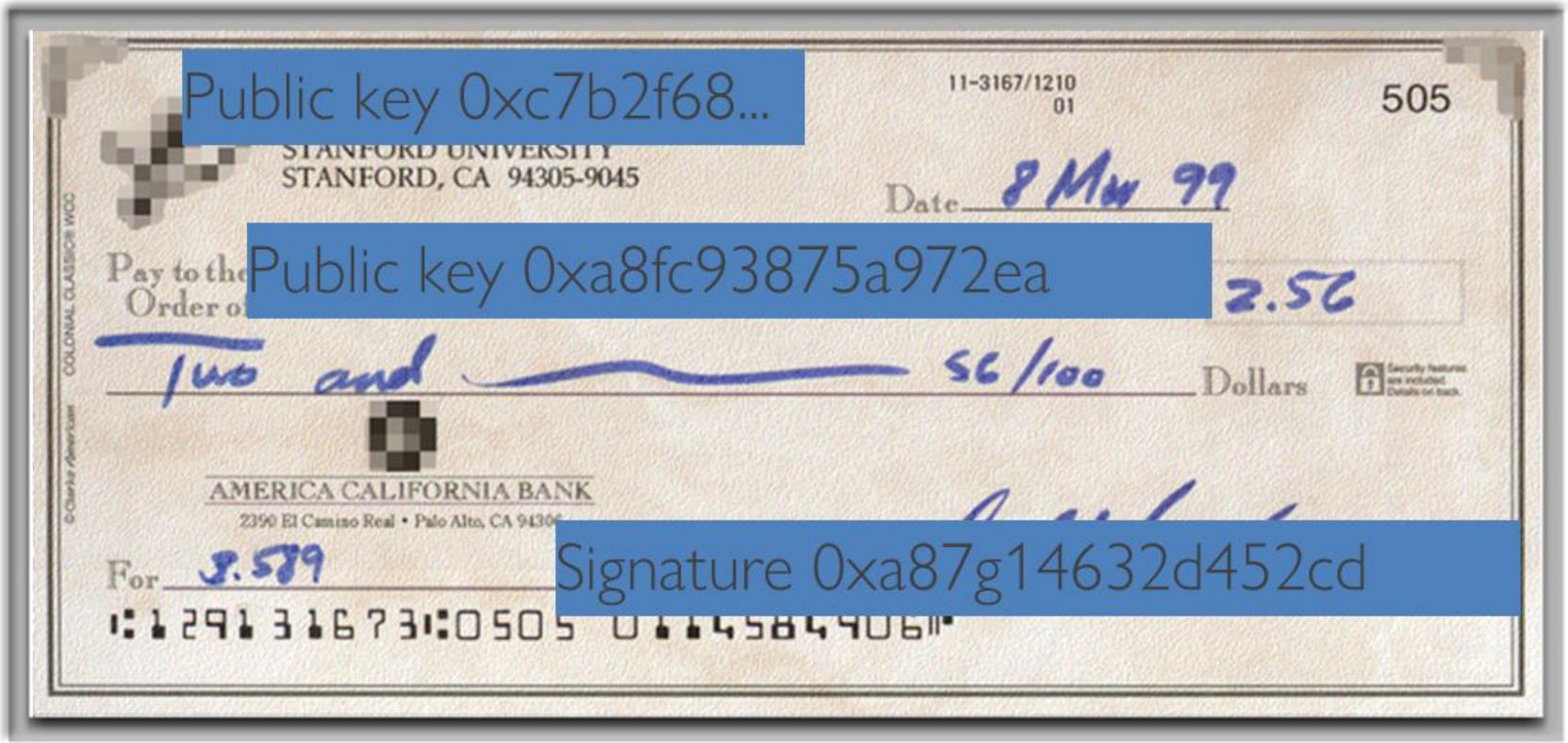


Image source: https://www.weusecoins.com/images/bitcoin-transaction-life-cycle-high-resolution.png

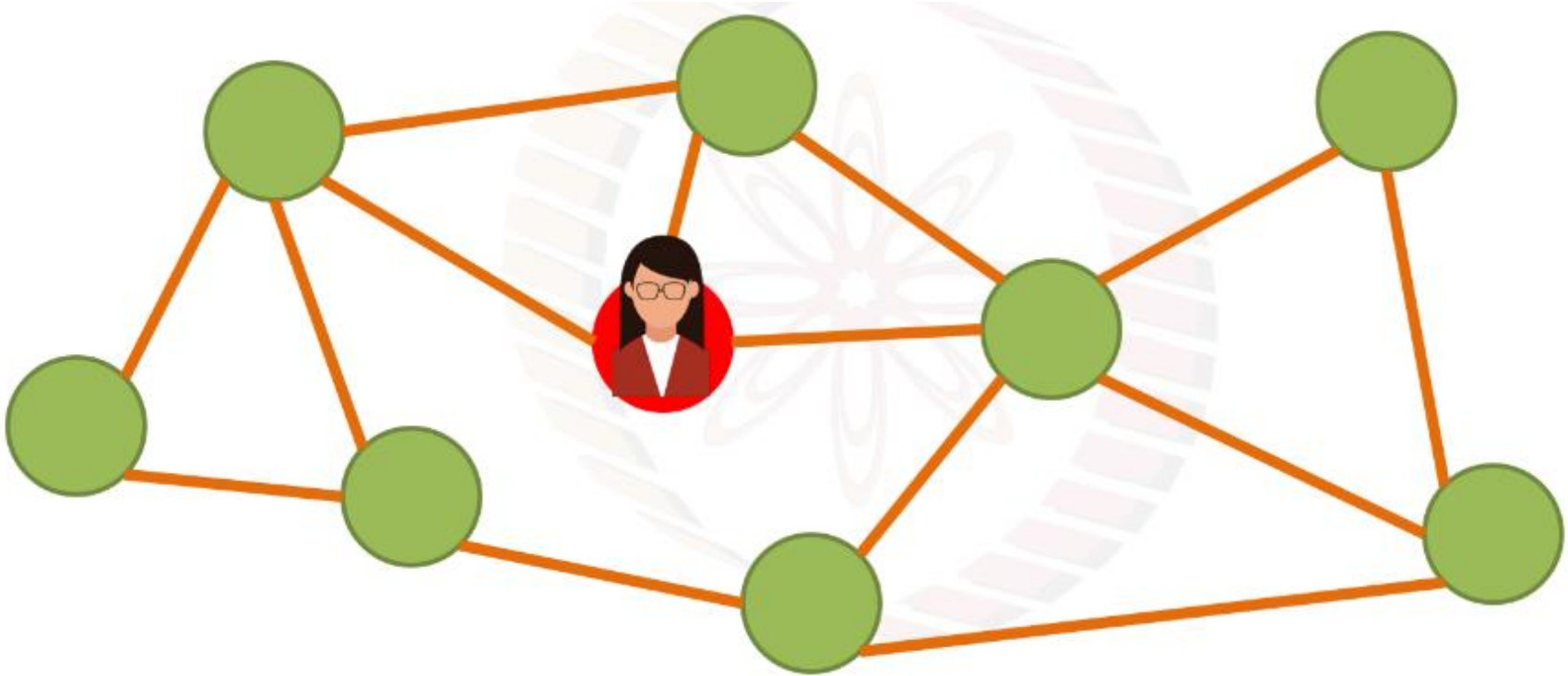
Bitcoin Transactions



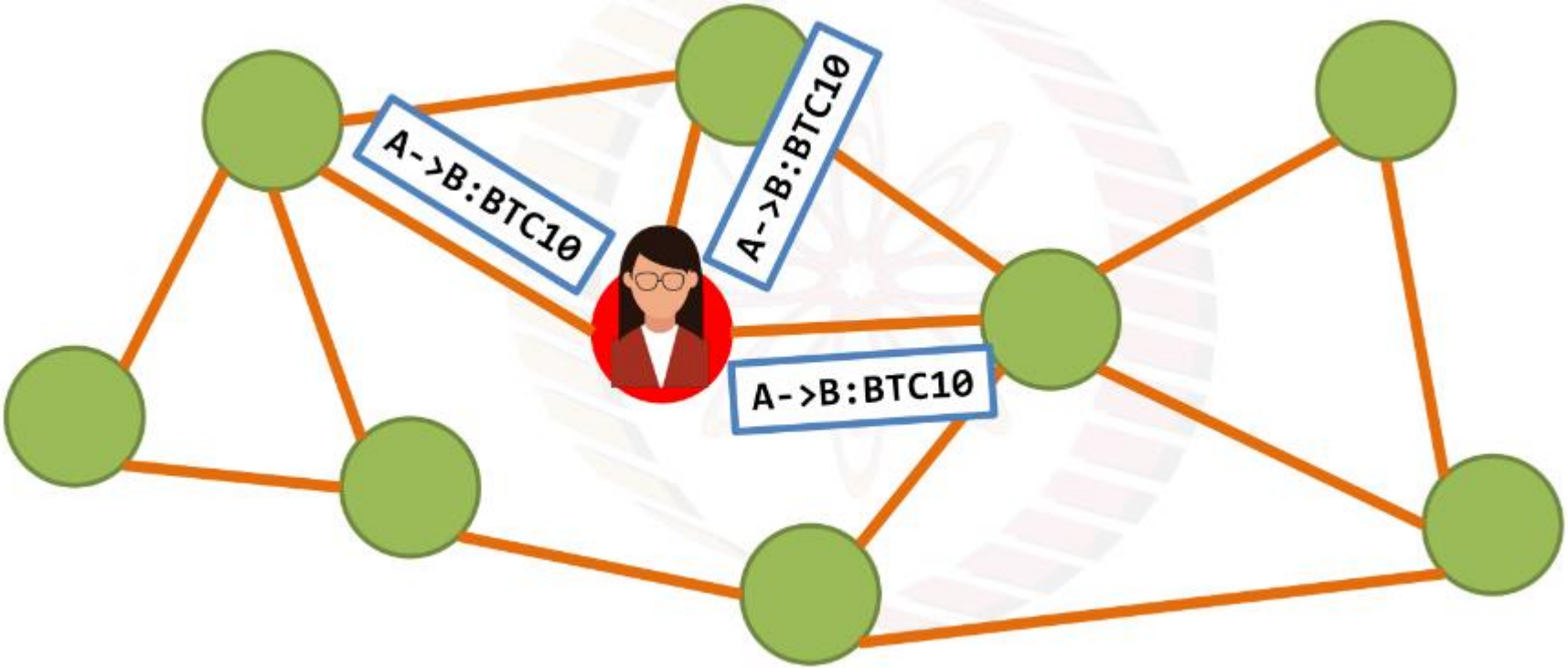
Transaction in a Bitcoin Network

- 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

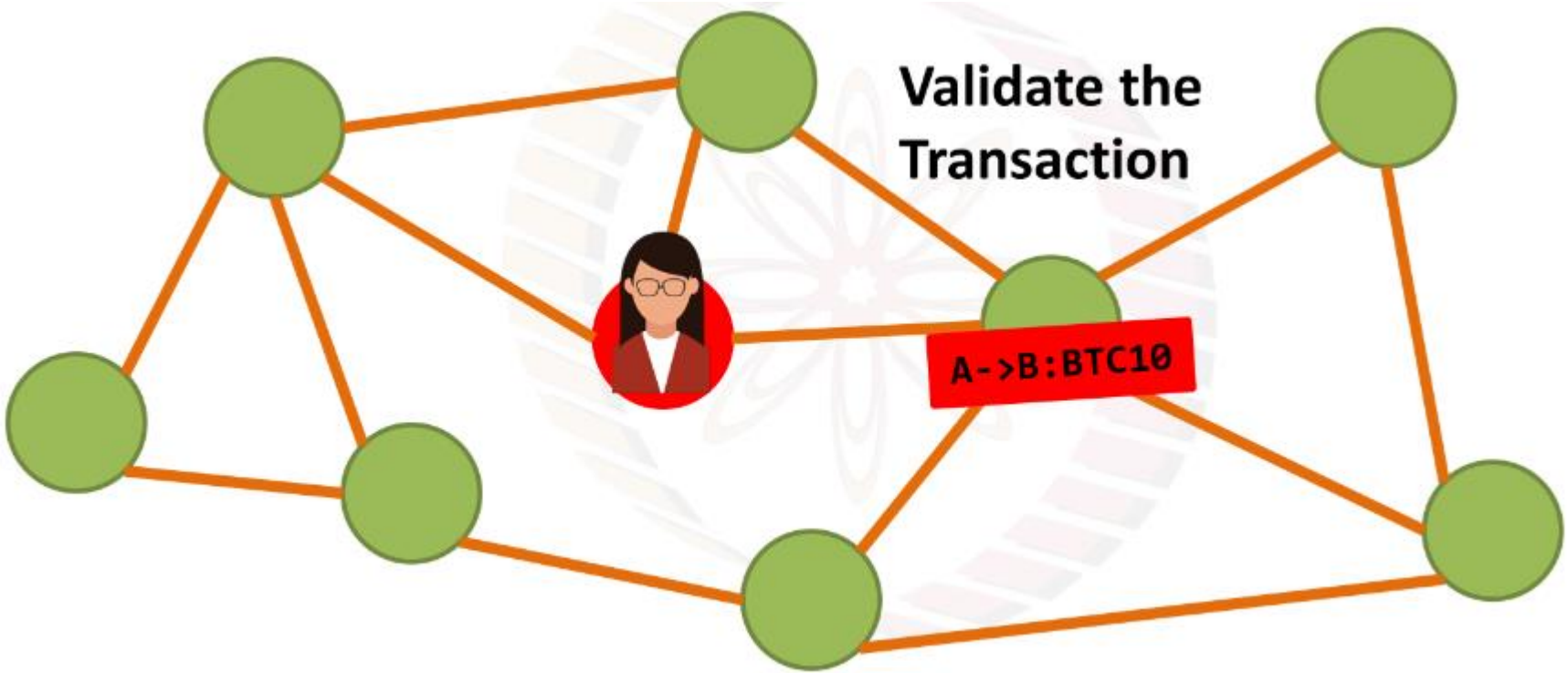
Transaction flooding in a Bitcoin Network



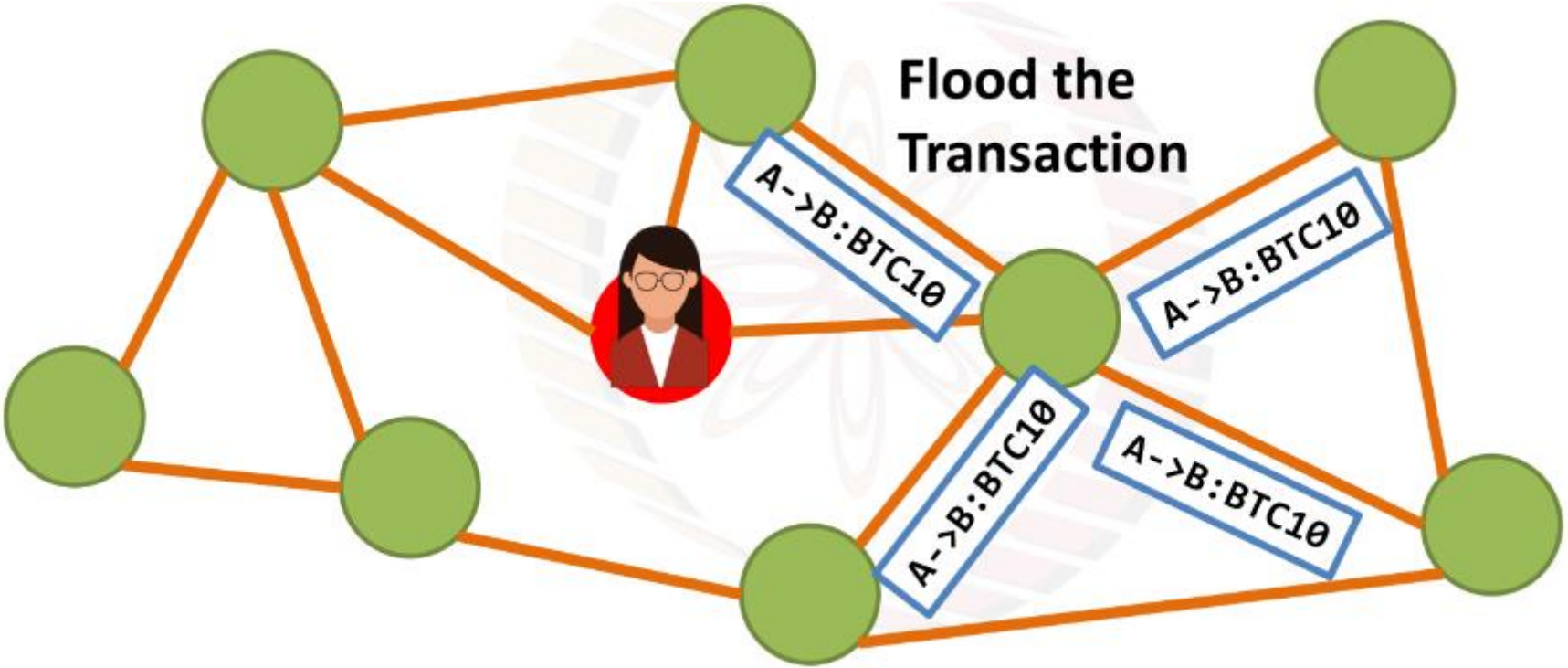
Transaction flooding in a Bitcoin Network



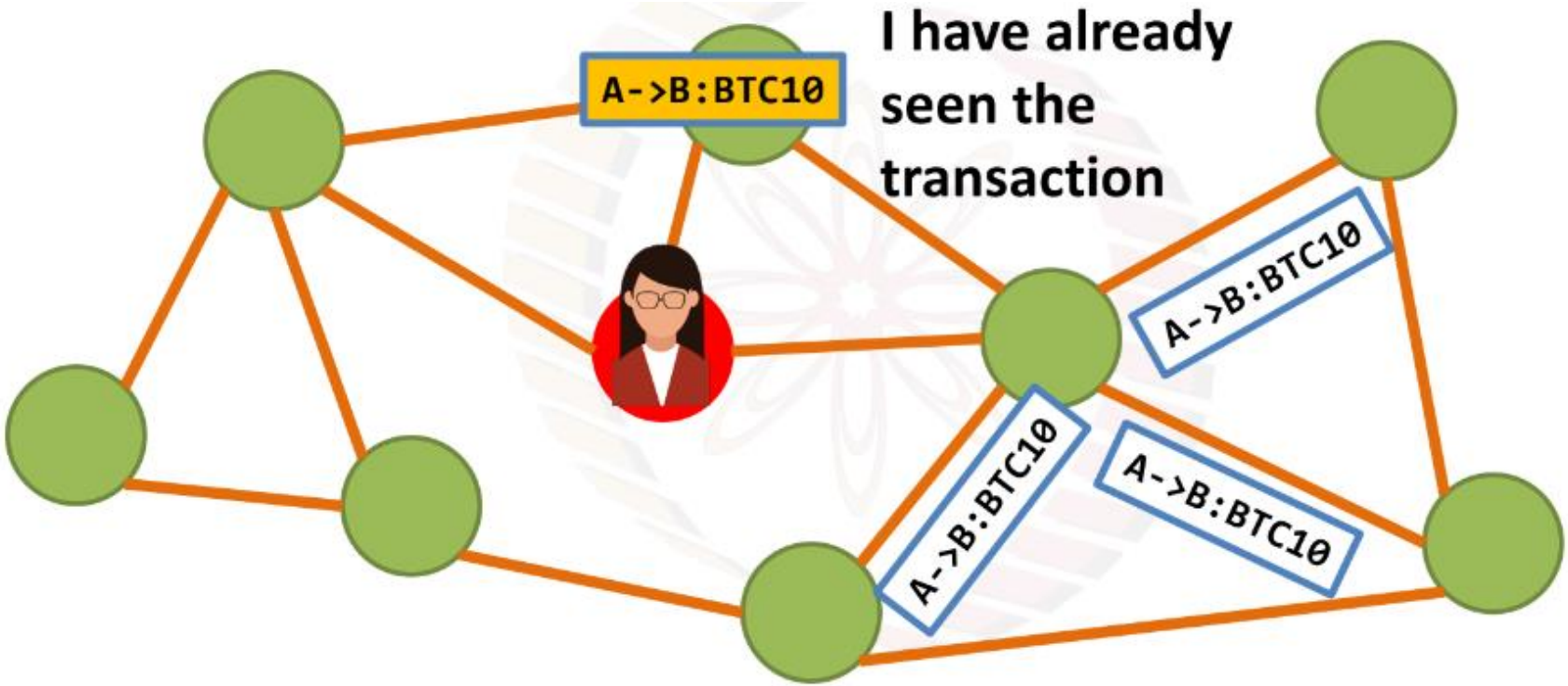
Transaction flooding in a Bitcoin Network



Transaction flooding in a Bitcoin Network



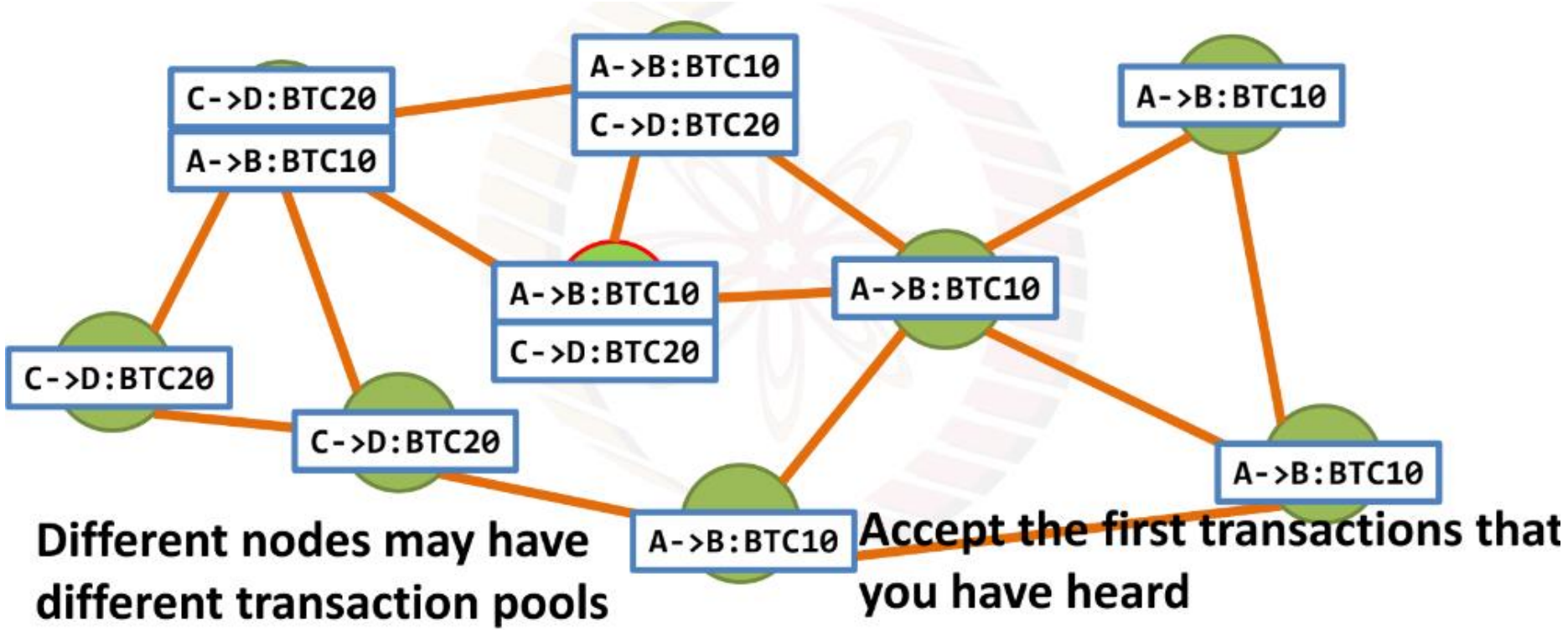
Transaction flooding in a Bitcoin Network



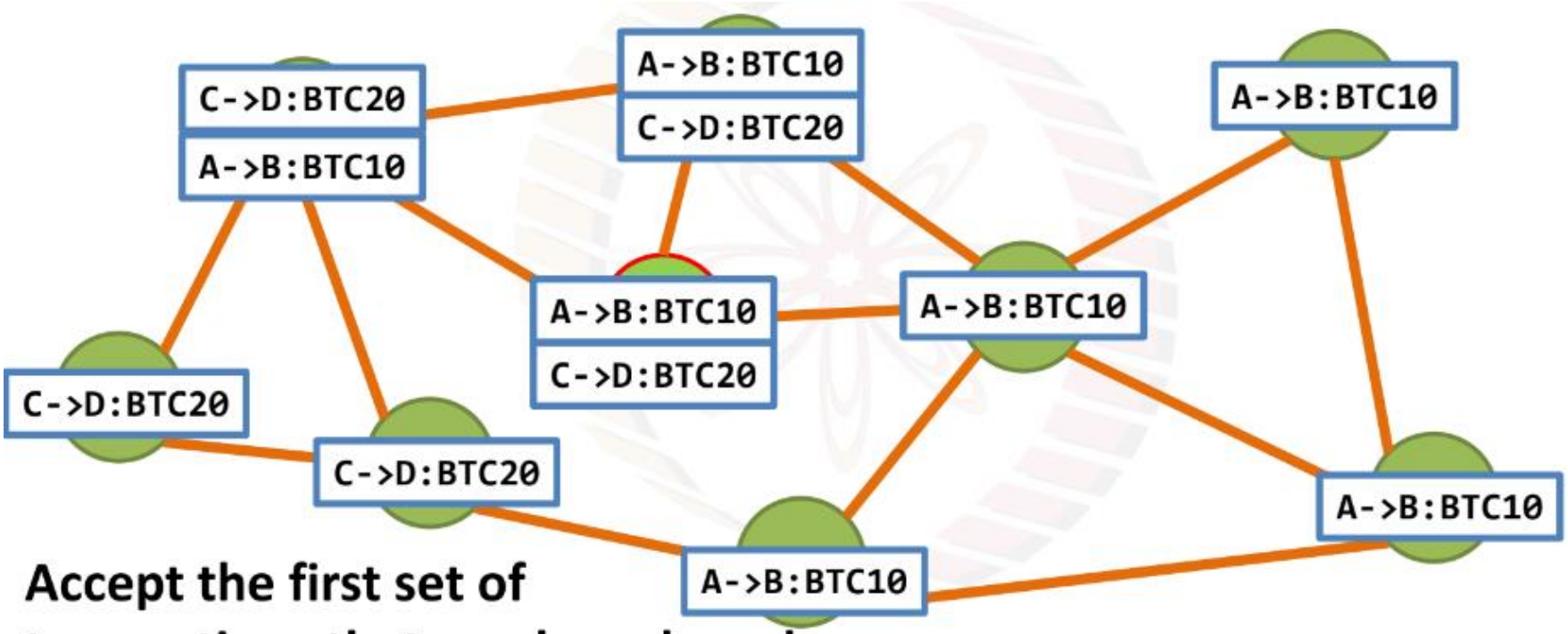
Which transaction should you Relay?

- 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

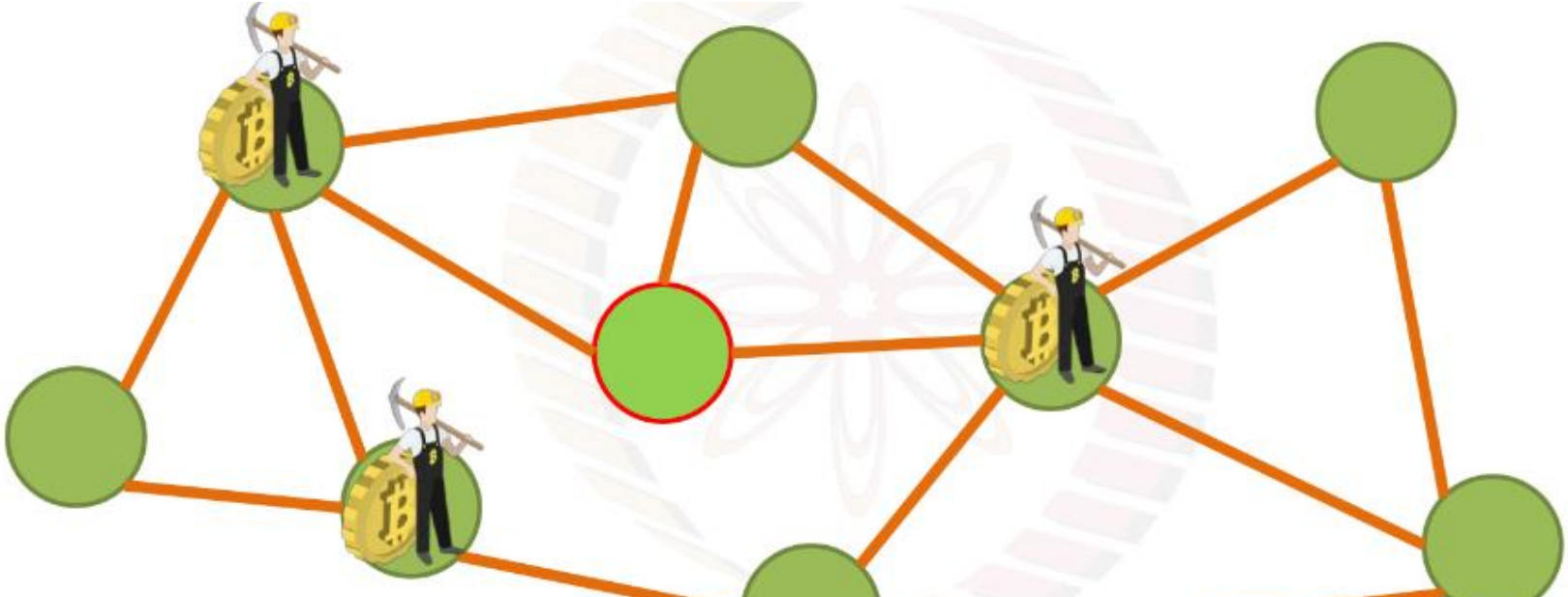
Transaction flooding in a Bitcoin Network



Transaction flooding in a Bitcoin Network



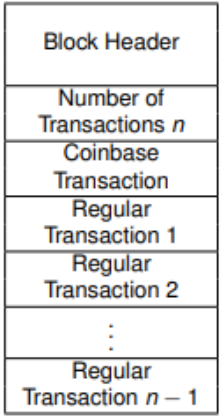
Mining in a Bitcoin Network



Miner collects all the transactions flooded and starts Mining

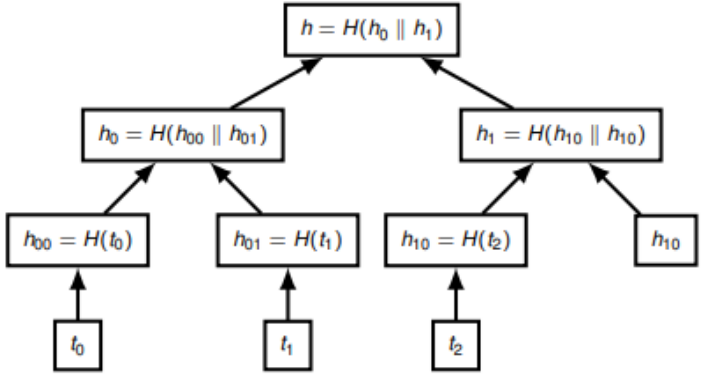
Bitcoin Mining

- 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

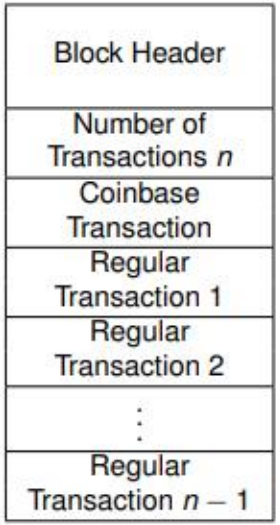


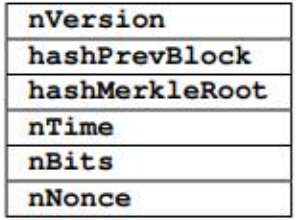
nVersion
hashPrevBlock
hashMerkleRoot
nTime
nBits
nNonce

- **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

$$T = \texttt{0x}\underbrace{00\cdots00}_{\text{16 times}}\underbrace{\texttt{FFFFF}\cdots\texttt{FFFFF}}_{\text{48 times}}$$

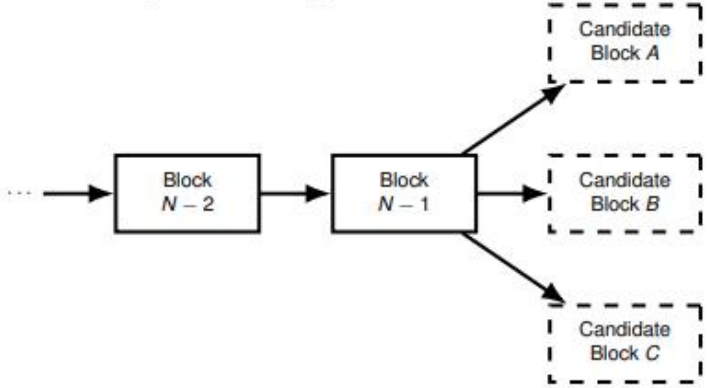
- Miner who can find **nNonce** such that

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

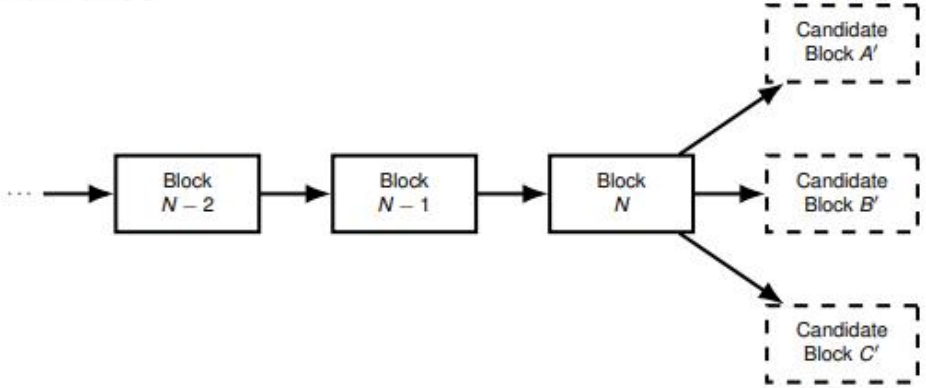
can add a new block

Block Addition Workflow

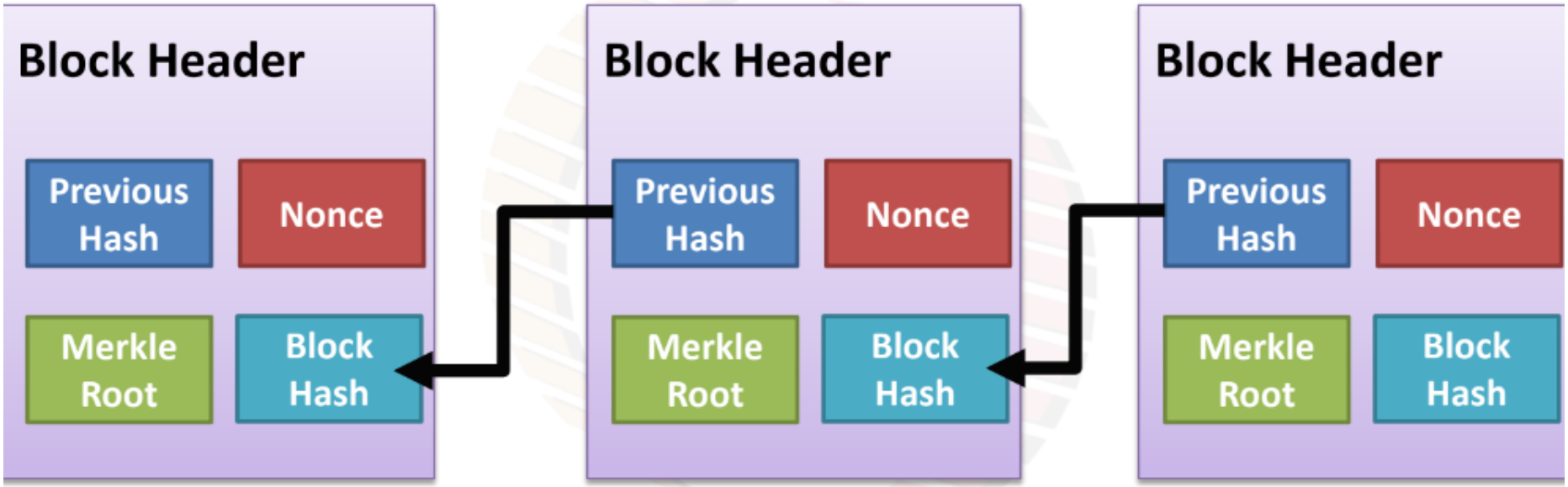
- Nodes broadcast transactions
- Miners accept valid transactions and reject invalid ones (solves double spending)
- Miners try extending the latest block



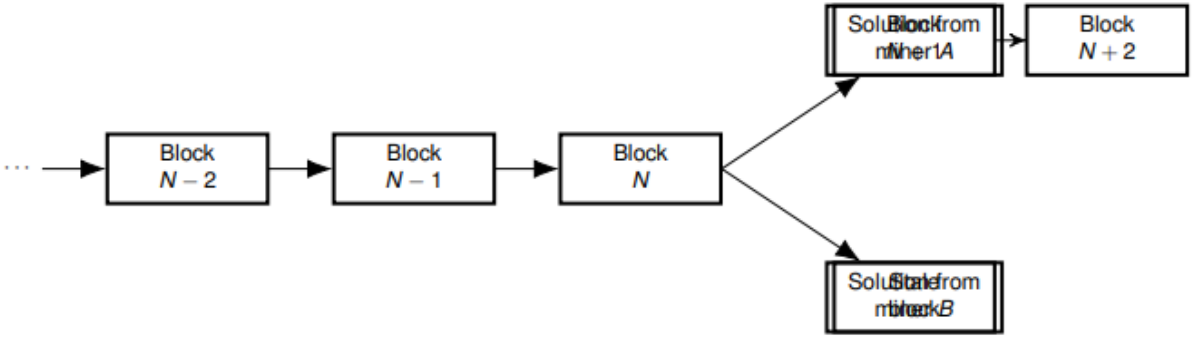
- Miners compete to solve the search puzzle and broadcast solutions
- Unsuccessful miners abandon their current candidate blocks and start work on new ones



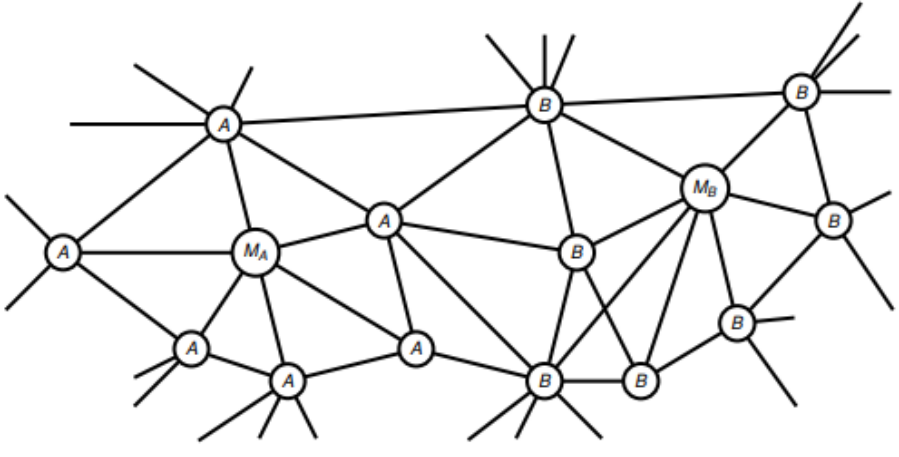
Block Generation Puzzle



Find out the nonce which generates the desired hash (certain zero bits at the prefix - 00000000000000004a2b84f93a285b7a7.....



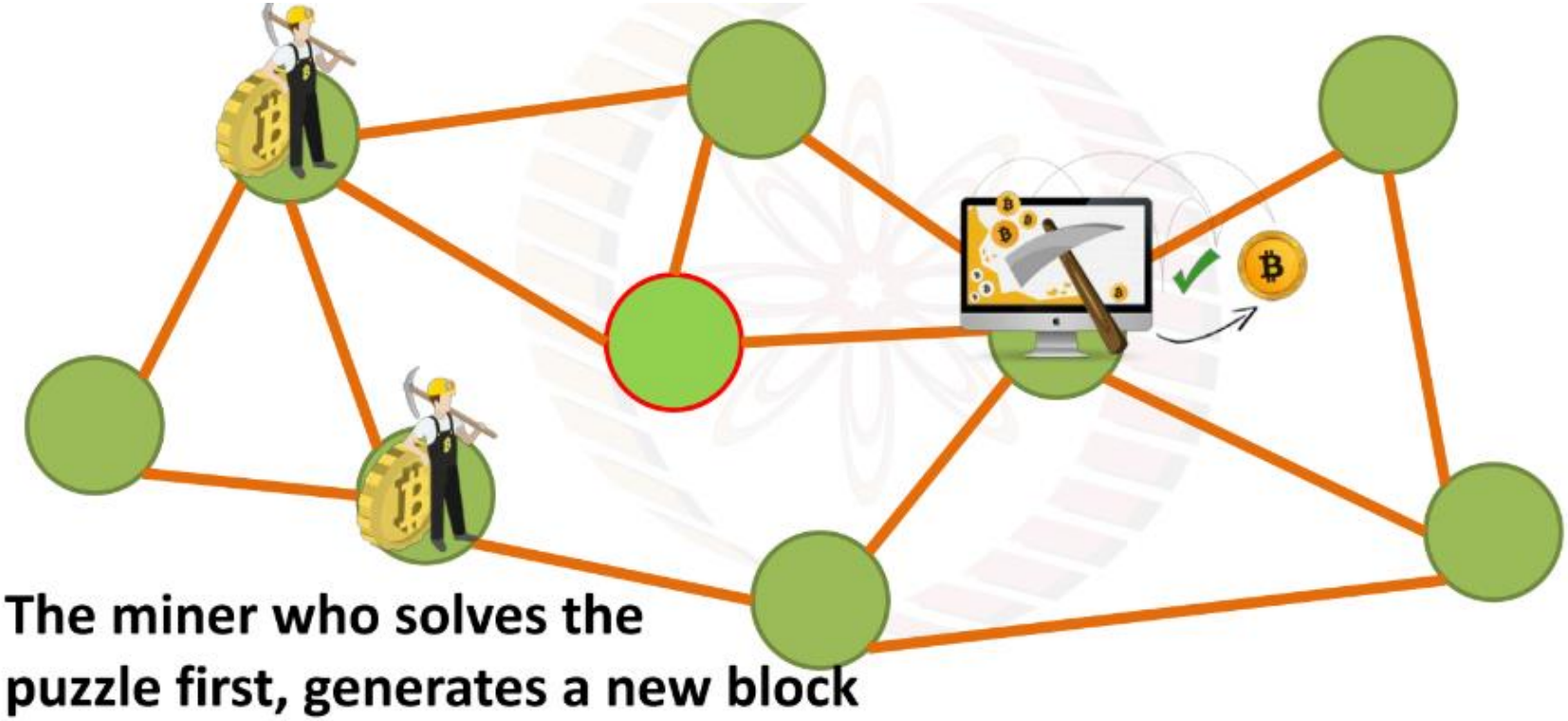
- Both miners will broadcast their solution on the network
- Nodes will accept the first solution they hear and reject others



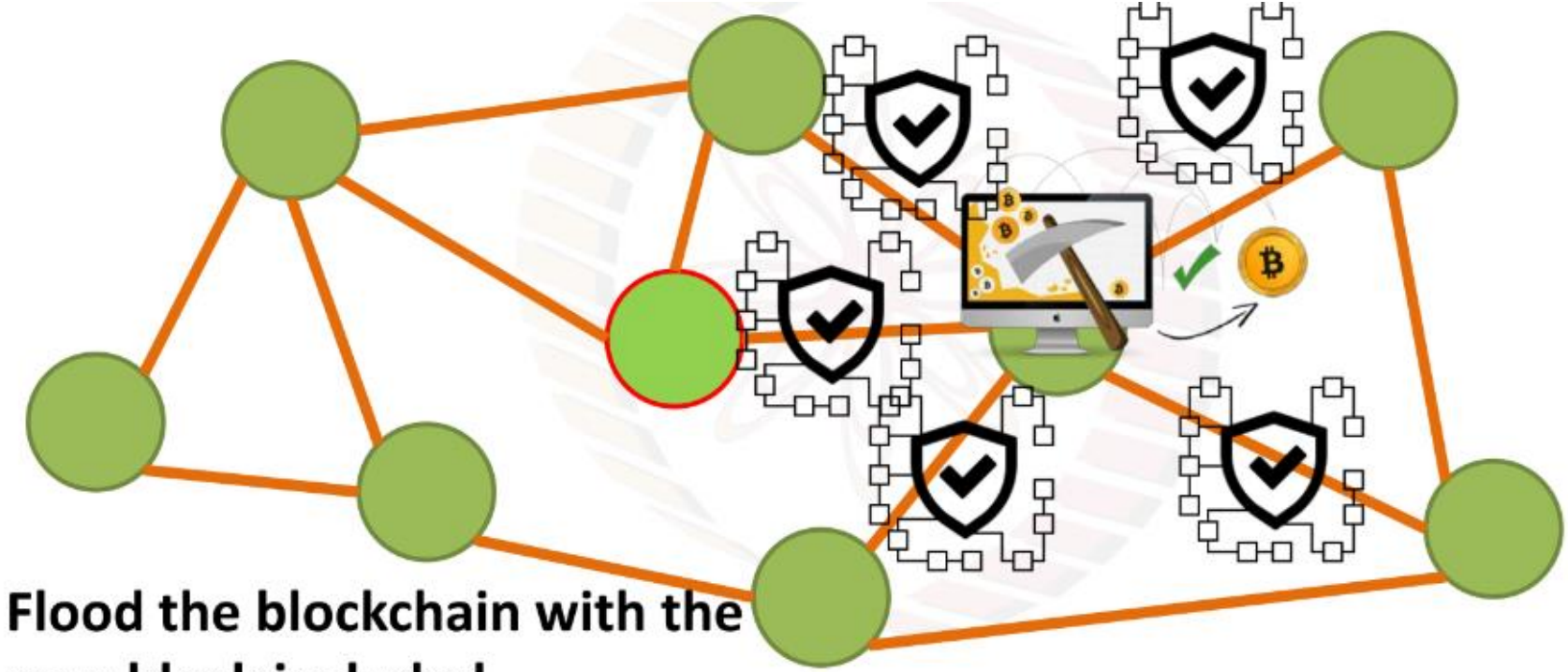
- Nodes always switch to the longest chain they hear
- Eventually the network will converge and achieve consensus

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

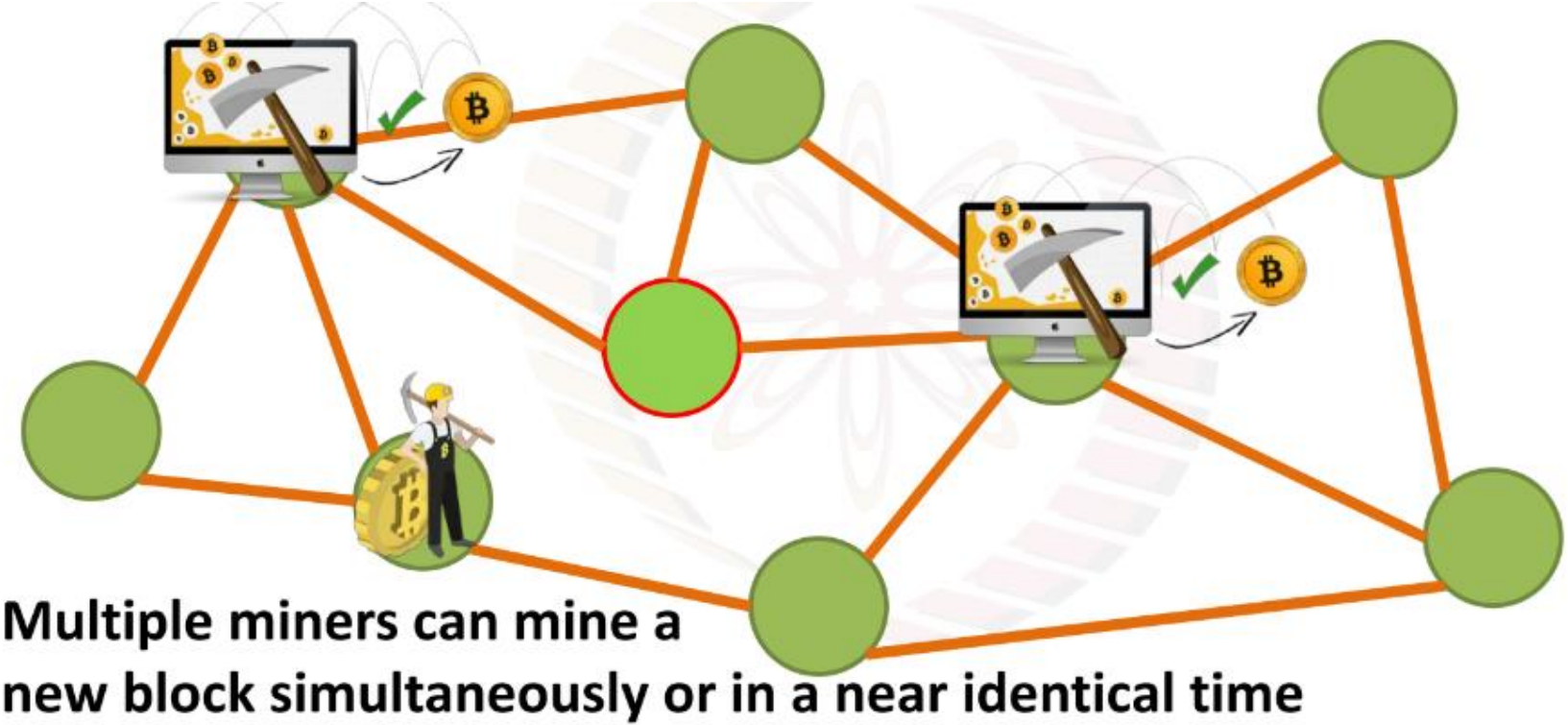
Block Generation



Block Flooding



Block Propagation



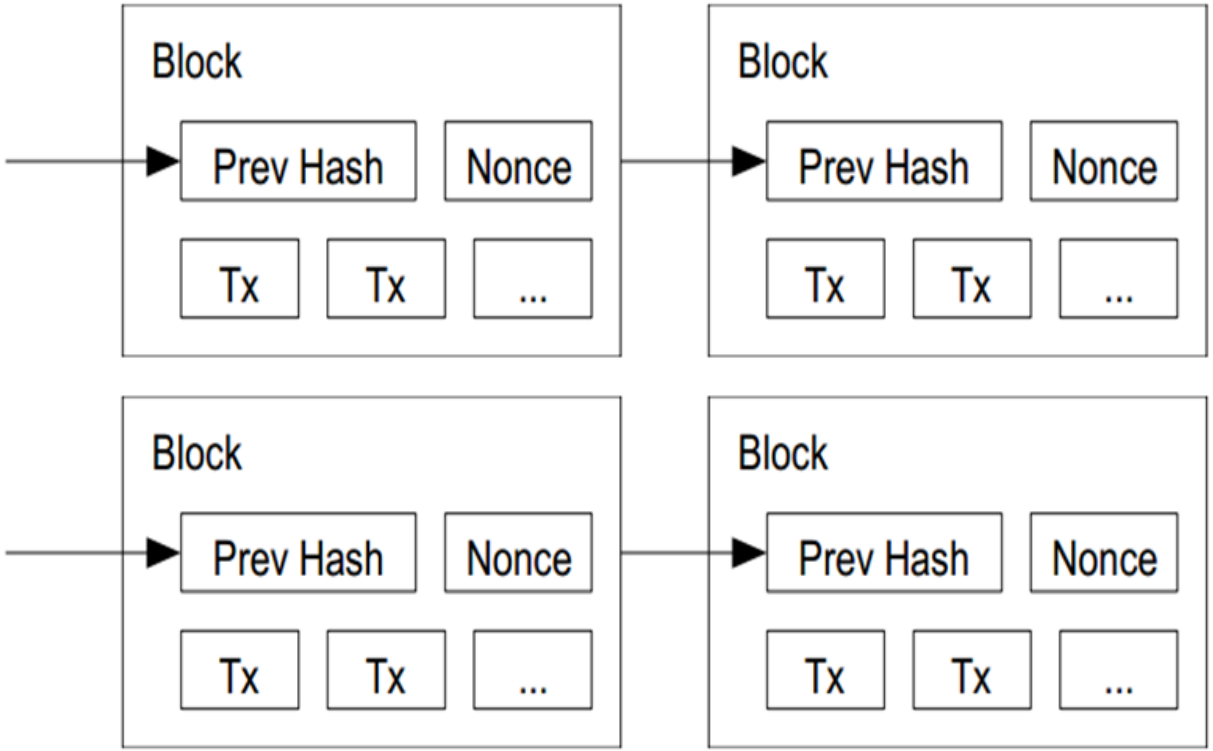
Tie Breaking

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

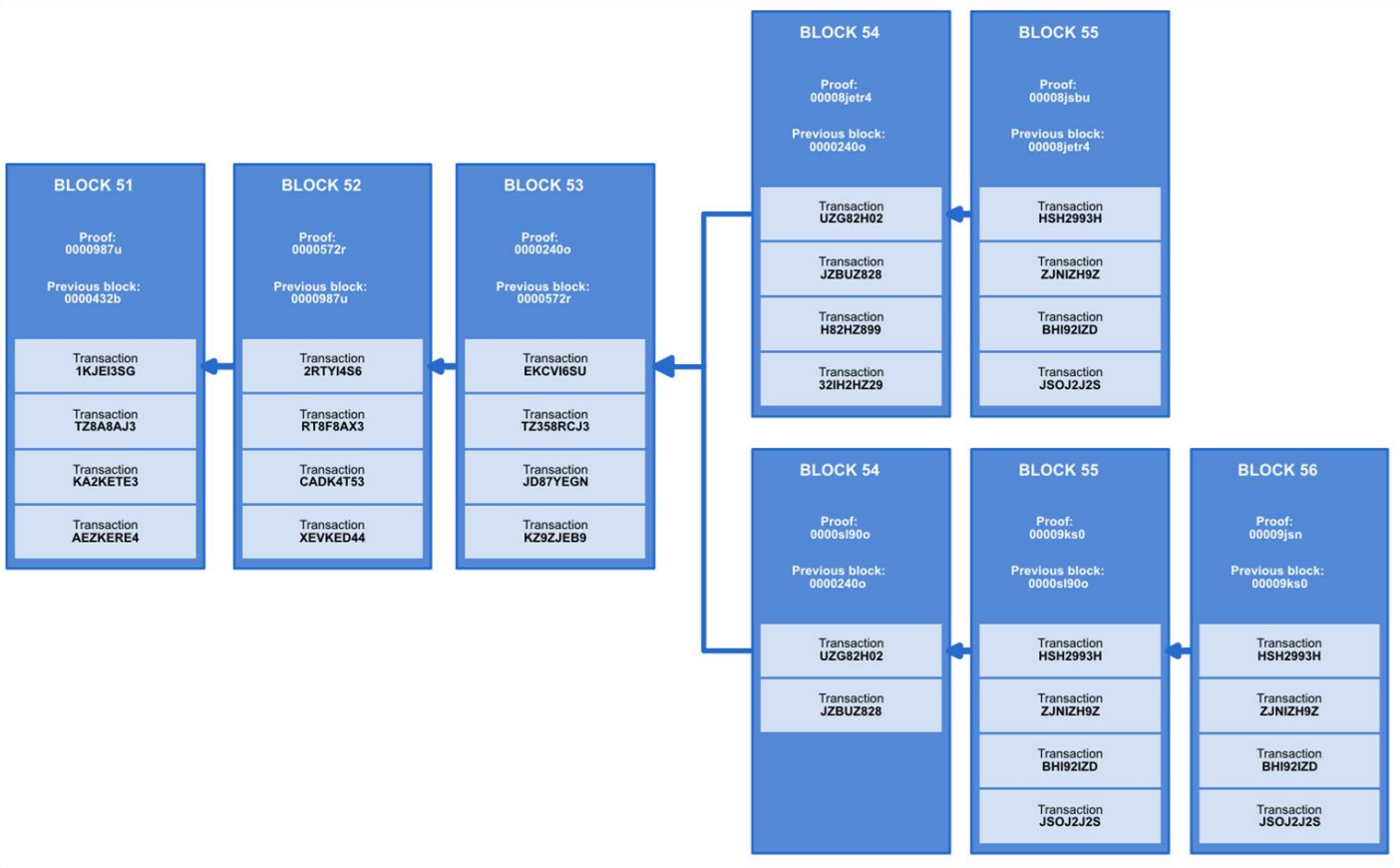
Two nodes may find a correct block simultaneously.

– Keep both and work on the first one

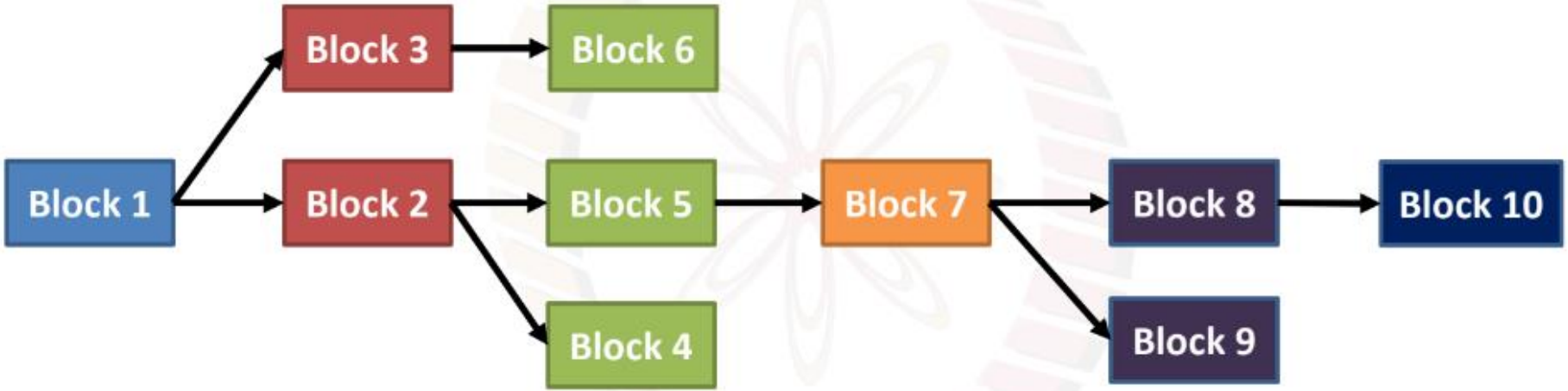
– If one grows longer than the other, take the longer one



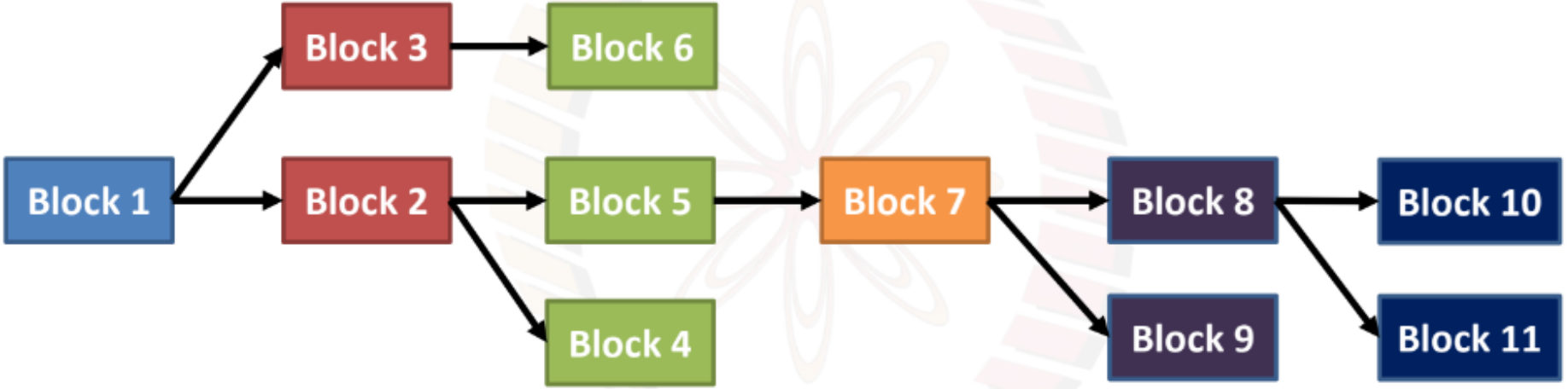
Forks


BLOCK 51
Proof:
0000987u
Previous block:
0000432b
Transaction
1KJEI3SG
Transaction
TZ8A8AJ3
Transaction
KA2KETE3
Transaction
AEZKERE4
BLOCK 52
Proof:
0000572r
Previous block:
0000987u
Transaction
2RTYI4S6
Transaction
RT8F8AX3
Transaction
CADK4T53
Transaction
XEVKED44
BLOCK 53
Proof:
0000240o
Previous block:
0000572r
Transaction
EKCVI6SU
Transaction
TZ358RCJ3
Transaction
JD87YEGN
Transaction
KZ9ZJEB9
BLOCK 54
Proof:
00008jetr4
Previous block:
0000240o
Transaction
UZG82H02
Transaction
JZBUZ828
Transaction
H82HZ899
Transaction
32IH2HZ29
BLOCK 55
Proof:
00008jsbu
Previous block:
00008jetr4
Transaction
HSH2993H
Transaction
ZJNIZH9Z
Transaction
BHI92IZD
Transaction
JSOJ2J2S
BLOCK 54
Proof:
0000sl90o
Previous block:
0000240o
Transaction
UZG82H02
Transaction
JZBUZ828
BLOCK 55
Proof:
00009ks0
Previous block:
0000sl90o
Transaction
HSH2993H
Transaction
ZJNIZH9Z
Transaction
BHI92IZD
Transaction
JSOJ2J2S
BLOCK 56
Proof:
00009jsn
Previous block:
00009ks0
Transaction
HSH2993H
Transaction
ZJNIZH9Z
Transaction
BHI92IZD
Transaction
JSOJ2J2S

Block Propagation - Accept the Longest Chain



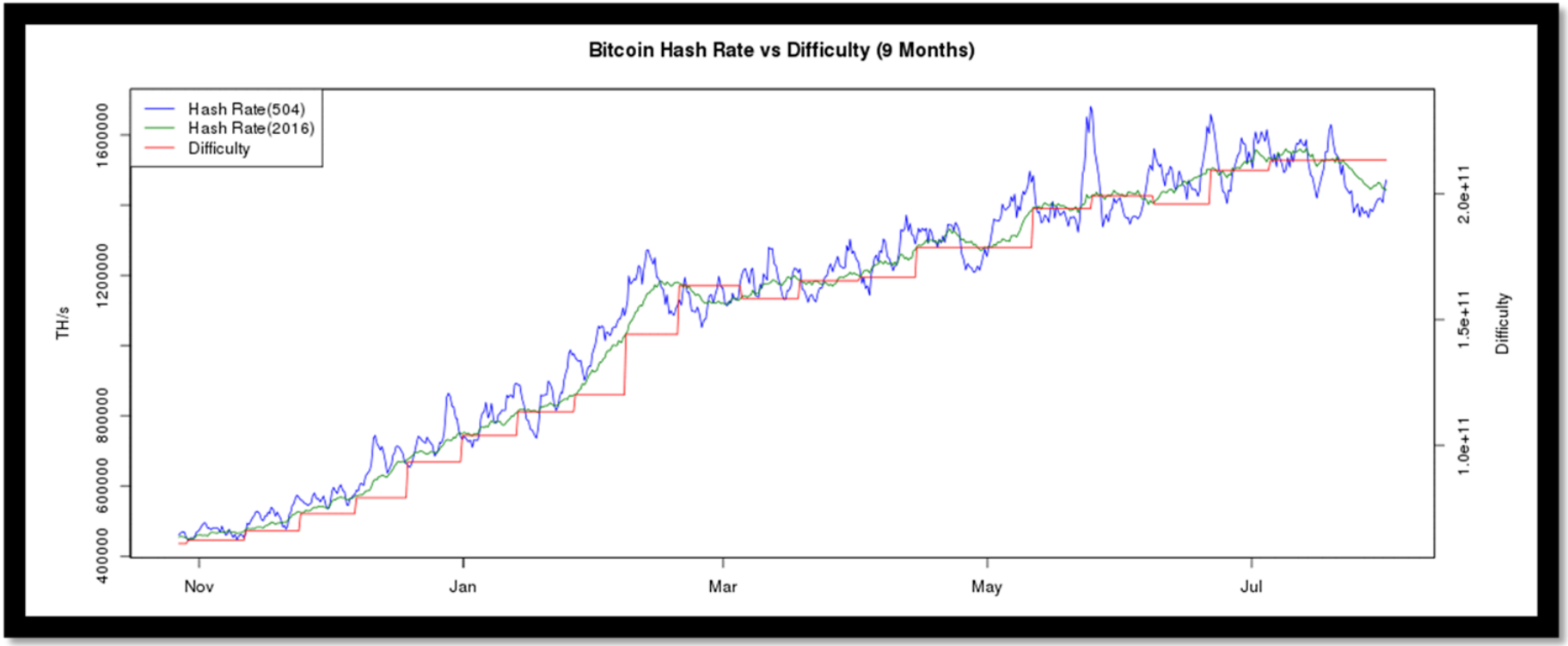
Block Propagation - Accept one of the Longest Chain



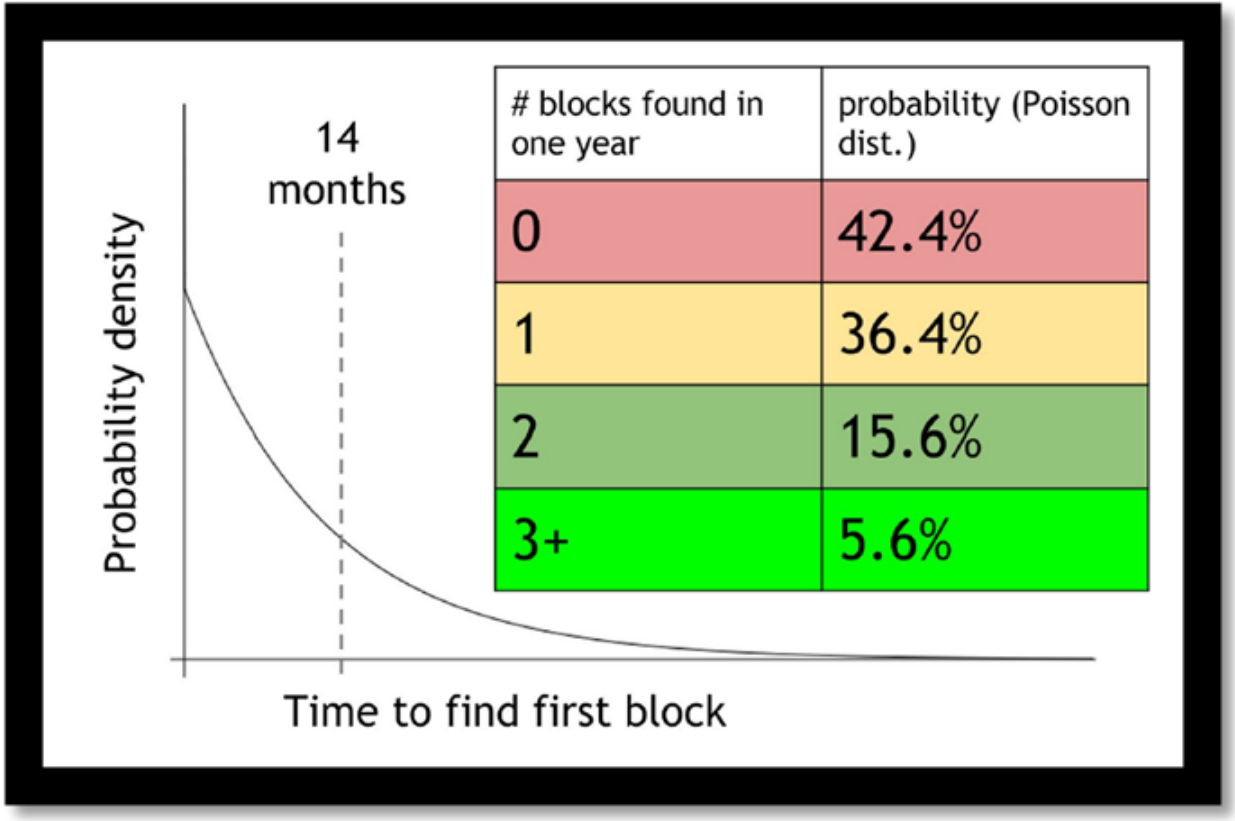
Which Block to Relay?

- 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



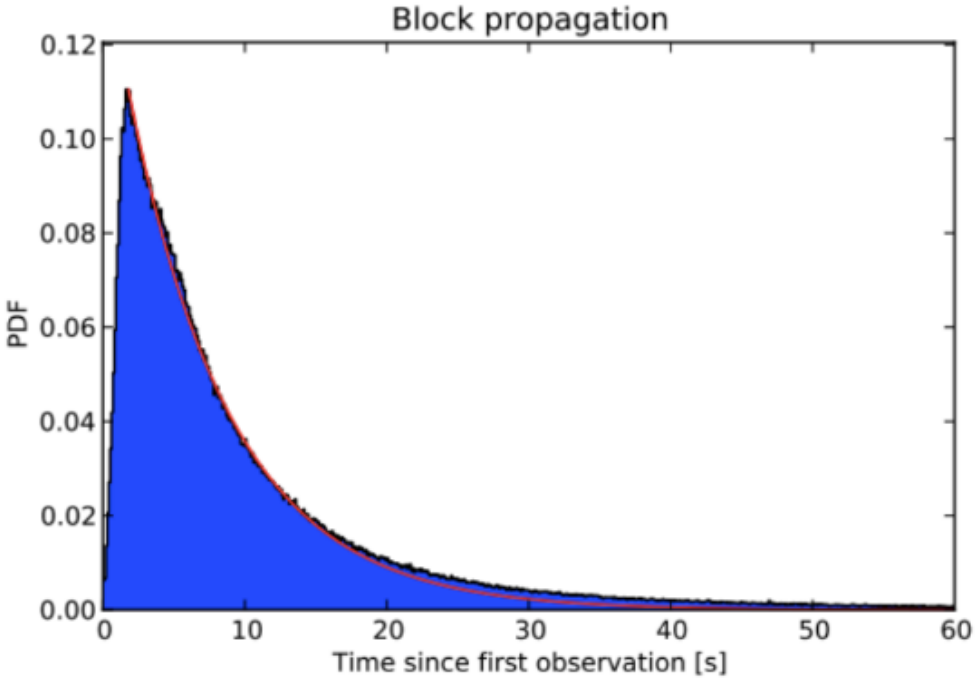
Mining Pools



# blocks found in one year	probability (Poisson dist.)
0	42.4%
1	36.4%
2	15.6%
3+	5.6%

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