Introduction to Bitcoin and how it works

Dr Konstantinos Karasavvas
Blockchain Research Engineer & Lecturer, University of Nicosia
Research Fellow, School of Informatics, Aristotle University

What is it?

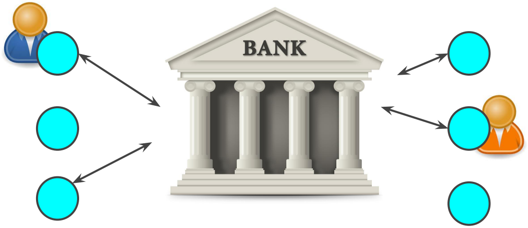
- Digital currencies
  - DigiCash (eCash), e-Gold, Liberty Reserve, ...
- Bitcoin is:
  - **a decentralized digital (crypto-)currency**
  - **a decentralized payment network**
  - **a technology**
    - software
    - a peer-to-peer network/protocol
    - an immutable public transaction ledger (aka blockchain)
    - a proof-of-work algorithm
    - a decentralized trustless platform using elliptic-curve cryptography (PKI)
    - a novel consensus mechanism
- Bitcoin introduced Blockchain technology to the world

Decentralized Digital CryptoCurrency

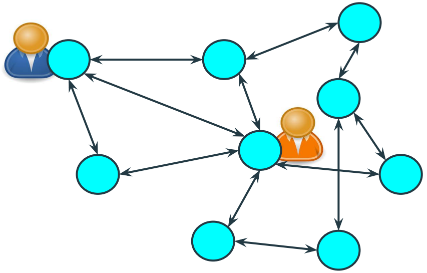
- bank creates/controls currency
- transfer of value via an institution
- higher and inter-institution fees
- 9.00 -15.00 Mon-Fri
- closed security model

- currency is created and distributed algorithmically
- direct transfer of value from A -> B
- no intermediaries and low fees
- global, 24/7, internet connection
- open security model

Centralized

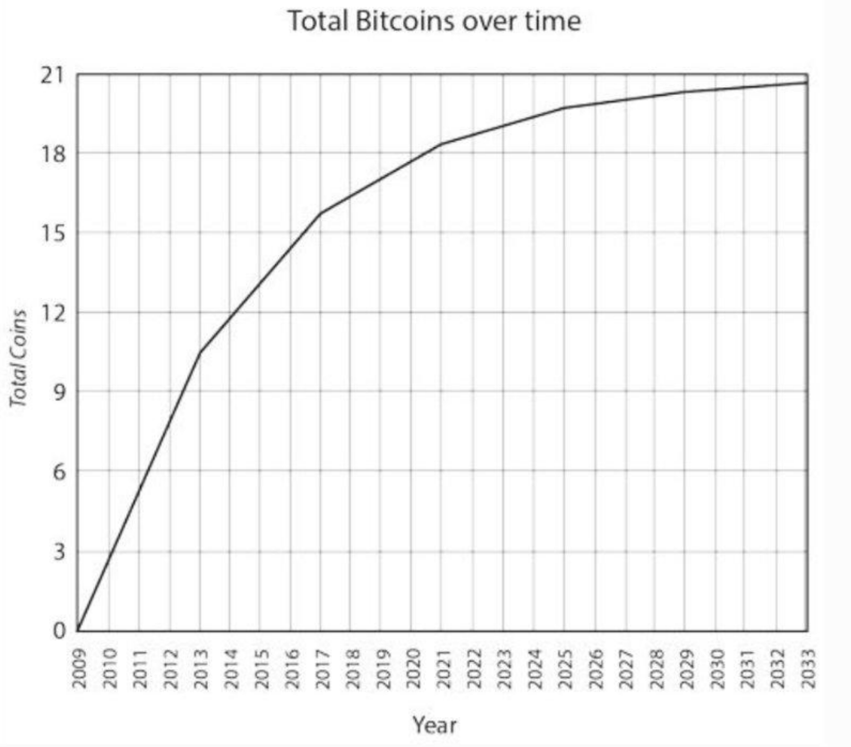


Decentralized



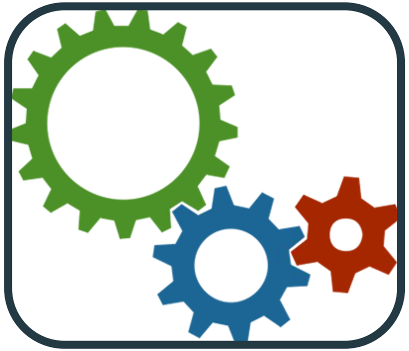
Currency characteristics (fixed supply)

- Bitcoin
  - 21 million
  - issued every ~10 minutes
  - 99% up to ~2036
  - deflationary
- Fiat currency (euro, dollars, etc.)
  - inflationary



Currency characteristics (transparent rules)

- Transparent rules
  - which transactions are valid?
  - how is ownership determined?
  - how are new coins distributed?
- Open source software
  - anyone can verify

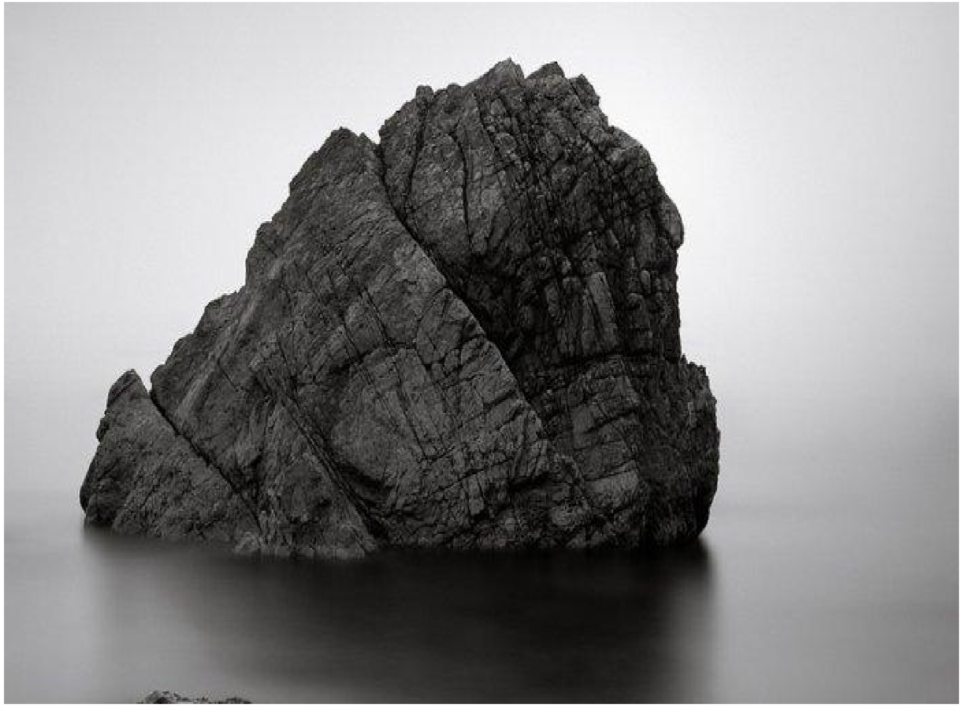


Currency characteristics (consensus-based)

- Valid rule set
  - majority governed
    - valid transactions
    - which transactions occurred
    - …
  - by supporting a specific version

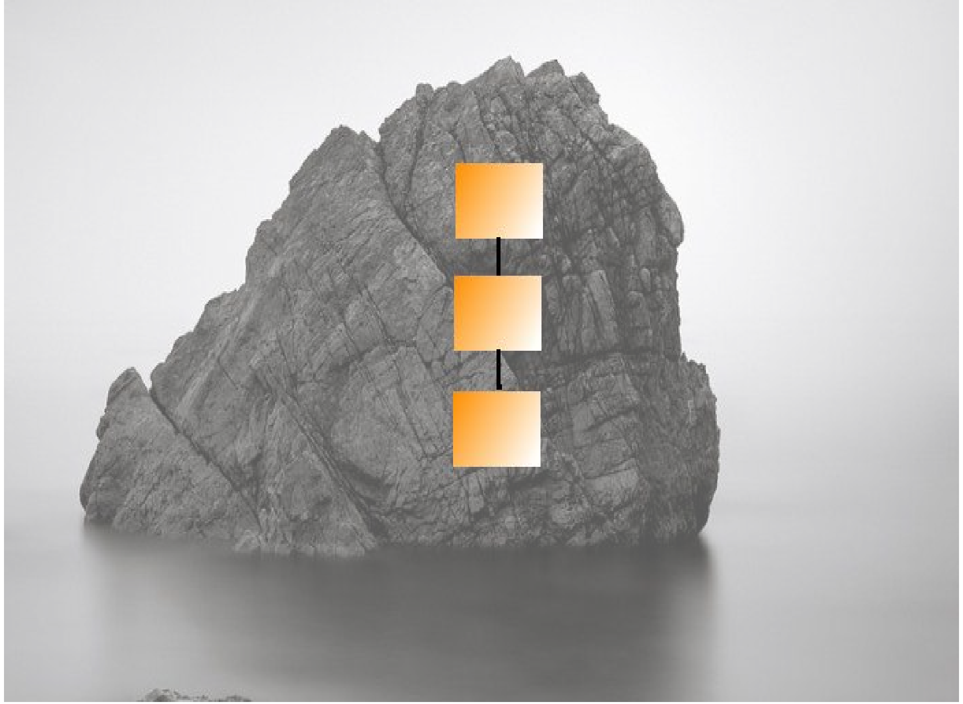
Currency characteristics (tx immutability)

- Immutable tx history / ledger
  - blockchain
    - chain of blocks
    - deeper -> safer



Currency characteristics (tx transparency)

- Public tx history / ledger
  - transparent transactions
  - auditable / verifiable



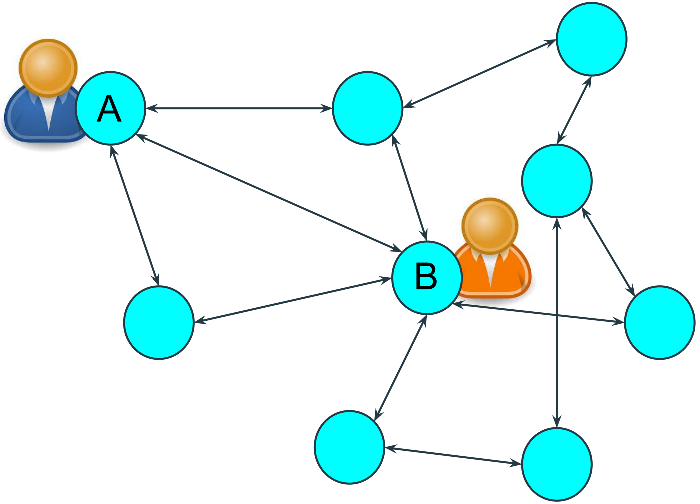
Main attributes

- Decentralized
    - State changes only after majority consensus
- Immutable
    - Append-only; no deletion or modifications allowed (w/o majority consensus)
- Transparent
    - Operations/data are available for all to see and verify
- Open
    - No barriers of entry; anyone can participate
- Secure
    - Strong cryptography ensures integrity of data stored

How it works

- Bird's eye view
  - peer-to-peer network (of)
  - bitcoin nodes (open source software)
  - run and secure the network
  - transaction history (aka blockchain)
    - immutability
    - transparency
- Why run a bitcoin node?
  - volunteerism
  - bitcoin rewards
- Mining
  - secures the network
  - the process of minting new coins

Decentralized



Next: Bitcoin/Blockchain Evolution

Blockchain Technology Evolution

- 2009: **Bitcoin** network was born
- 2010: First *real-value* transaction
- 2011: Silk Road accepts Bitcoin
- 2012
  - Television series ‘The Good Wife’
  - **Litecoin**
- 2013
  - US Financial Crimes Enforcement Network (FINCEN) “guidance report”
  - China bans Bitcoin
- 2014
  - Major online retailers (Overstock) start accepting Bitcoin
  - **Ethereum** (aka Blockchain 2.0)
  - US government auctions 29k Bitcoins
  - UK government classified Bitcoin as asset (no VAT)
- 2015
  - **Hyperledger project** (Linux Foundation)
  - NY Exchange invests in Coinbase
  - ~160.000 merchants accept Bitcoin
- 2016
  - Japan recognises Bitcoin as currency
  - Billions are invested by VCs and ICOs
- 2017
  - Bitcoin surpasses $240 billion in capitalization
  - Cryptocurrencies surpassed $0.5 trillion
  - 1500+ ATMs
  - Blockchain 3.0

- Thousands of blockchain and cryptocurrencies projects
- How disruptive is Blockchain technology?

Next: Use Cases

Bitcoin/Blockchain Applications

- **Remittances**
- **Payments**
- **Bank services for the unbanked**
- **Store of Value**
- **Digital Tokens**
- Decentralized Applications
- Micropayments
- Proof of Existence
- Smart Contracts
- Decentralized Autonomous Organizations
- Internet of Things / Machine to Machine
- Voting / Identity

Remittances

- €600 billion market
  - Western Union (15%)
  - MoneyGram
- High fees
  - depends on location
  - up to 15%
  - more for same day delivery
- Up to same day delivery
- Anywhere there is an agent
- Working hours
  - plus extended hours

Remittances

- €600 billion market
  - Western Union (15%)
  - MoneyGram
- High fees
  - depends on location
  - up to 15%
  - more for same day delivery
- Up to same day delivery
- Anywhere there is an agent
- Working hours
  - plus extended hours

- Cryptocurrencies slowly gains momentum
- Costs cents irrespective of amount
  - In Bitcoin it has been quite high lately
- Takes minutes
  - in practice it is much faster
- Anywhere there is a connected machine
  - Internet (no need for permanent access)
- Anytime
  - 24/7
- No intermediaries, but…
  - bitspark.io
  - rebit.ph
  - bitpesa.co

Making/Receiving Payments

- Online
- Credit cards
  - 2%-6% + small flat rate
- Debit cards
  - 2%-3% + small flat rate
- Paypal
  - 2.9% + $0.30
- Cryptocurrencies
  - none
  - only the sender pays

Making/Receiving Payments

- Online
- Credit cards
  - 2%-6% + small flat rate
- Debit cards
  - 2%-3% + small flat rate
- Paypal
  - 2.9% + $0.30
- Cryptocurrencies
  - none
  - only the sender pays

- Merchants can offer discounts for bitcoin
- Payment Processing
  - Coinbase, BitPay
- Point of Sale
  - Bitcoin PoS (android app)

Making/Receiving Payments

- Online
- Credit cards
  - 2%-6% + small flat rate
- Debit cards
  - 2%-3% + small flat rate
- Paypal
  - 2.9% + $0.30
- Cryptocurrencies
  - none
  - only the sender pays

- Merchants can offer discounts for bitcoin
- Payment Processing
  - Coinbase, BitPay
- Point of Sale
  - Bitcoin PoS (android app)

- Some major companies
  - Overstock
  - Microsoft
  - Dell
  - Expedia
  - Time Inc.
  - DISH Network
  - Newegg
  - Zynga
  - UK’s Theatre Tickets Direct
  - AirBaltic
  - CheepAir
  - …

- Do they keep their bitcoins?
- Can Bitcoin handle demand if widely adopted?

Be your own bank

- Bank services for the unbanked/underbanked
    - payments
    - remittances
    - micro-payments
    - donations
        - UN World Food Programme
    - … using Mobiles

Be your own bank

- Bank services for the unbanked/underbanked
    - payments
    - remittances
    - micro-payments
    - donations
        - UN World Food Programme
    - … using Mobiles

- Bank services for the banked
    - capital controls
    - censorship

Be your own bank

- Bank services for the unbanked/underbanked
  - payments
  - remittances
  - micro-payments
  - donations
    - UN World Food Programme
  - … using Mobiles

- Bank services for the banked
  - capital controls
  - censorship

- Store of value (vs hyper-inflation)
  - gold
  - reserve currencies
  - bitcoin
    - deflationary
    - Latin/South America, China, Russia.

Digital Tokens

- represent/transfer real world value/asset
    - theater tickets
    - consultancy hours
    - authentication mechanism
    - stock markets’ shares
    - new currency
    - car ownership/key, house deeds, …

- open blockchain technology
    - immutability
    - transparency

Digital Tokens

- represent/transfer real world value/asset
  - theater tickets
  - consultancy hours
  - authentication mechanism
  - stock markets’ shares
  - new currency
  - car ownership/key, house deeds, …
- open blockchain technology
  - immutability
  - transparency

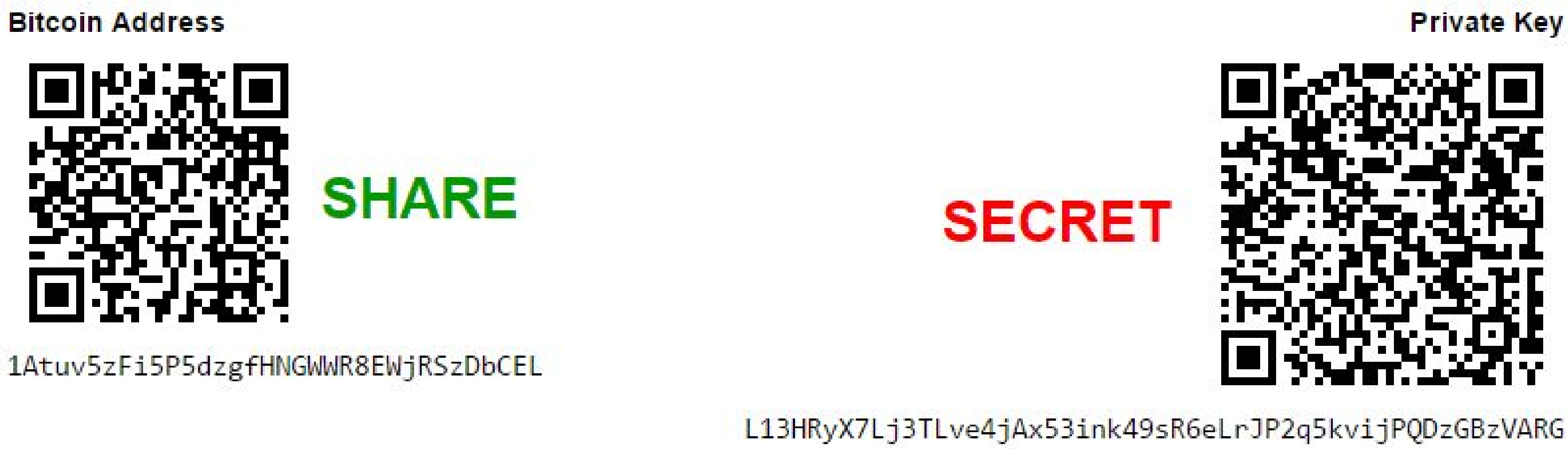
- Swedish National Land Survey (on trial)
  - immutability / transparency
  - automation of selling process
  - less paperwork (months -> days/hours)
  - more secure
- Nasdaq Composite Index
  - pre-IPO trading
  - equity shares on Bitcoin’s blockchain
- LetsTalkBitcoin.com (publishing platform)
  - LTBC token
  - Proof of Participation
  - token-based access
- Steem (social networking with rewards)
- StorJ (decentralized cloud storage)
- FoldingCoin (help scientists cure diseases)
- BitCrystals - Spells of Genesis game
- …

Bitcoin/Blockchain Applications

- **Remittances**
- **Payments**
- **Bank services for the unbanked**
- **Store of Value**
- **Digital Tokens**
- Decentralized Applications
- Micropayments
- Proof of Existence
- Smart Contracts
- Decentralized Autonomous Organizations
- Internet of Things / Machine to Machine
- Voting / Identity

Next: Basic concepts / usage

Basic concepts (Bitcoin address / private key)



Bitcoin Address

1Atuv5zFi5P5dzgfHNGWWR8EWjRSzDbCEL

SHARE

Private Key

SECRET

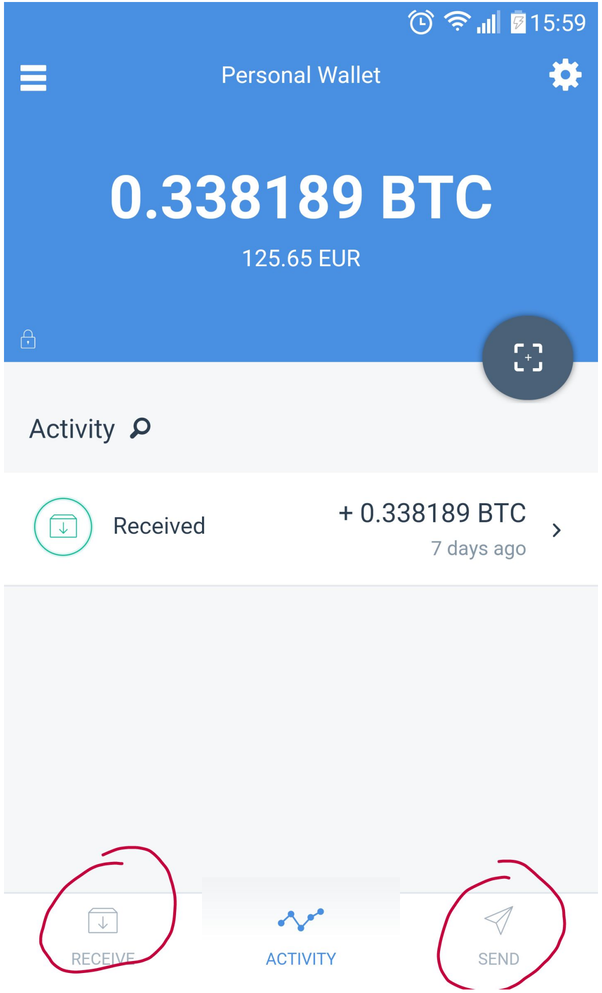
L13HRyX7Lj3TLve4jAx53ink49sR6eLrJP2q5kvijPQDzGBzVARG

Basic concepts (Bitcoin wallets)

- Wallet
  - manages bitcoin addresses (accounts)
  - can send (receive) bitcoins
- Types
  - desktop
  - mobile
  - online/web wallet
  - hardware wallet
- Wallet examples
  - Copay, Mycelium, ...
  - https://bitcoin.org/en/choose-your-wallet

Usage:

- Balance
- Activity
- Receive
- Send



0.338189 BTC

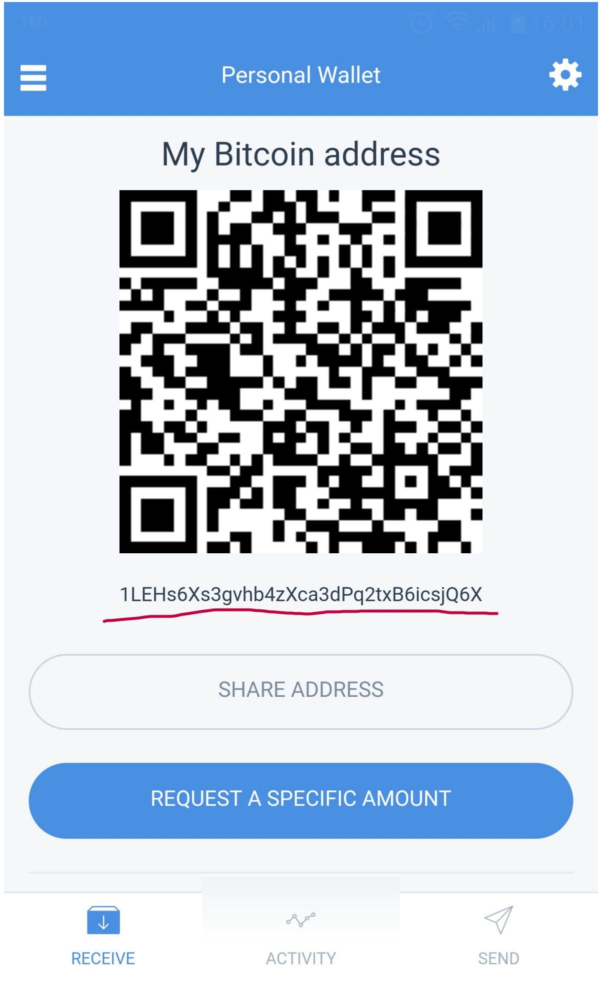
125.65 EUR

Activity

Received + 0.338189 BTC
7 days ago

Usage: receive bitcoins

- Provide address string, or
- QR code

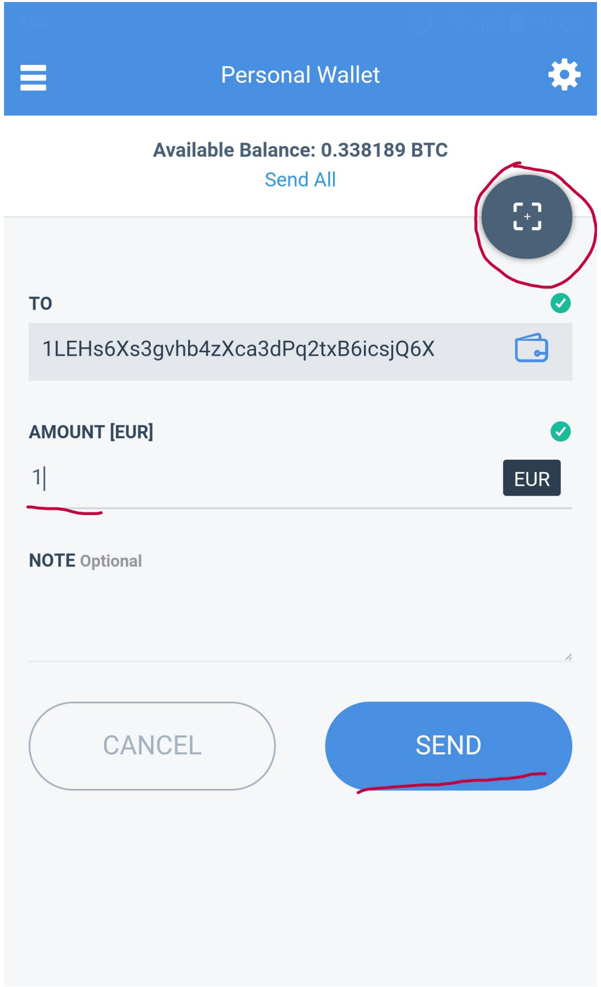


My Bitcoin address

1LEHs6Xs3gvhb4zXca3dPq2txB6icsjQ6X

Usage: send bitcoins

- To: (address / QR code)
- Amount: (in bitcoins or preferred currency)



Available Balance: 0.338189 BTC

TO

1LEHs6Xs3gvhb4zXca3dPq2txB6icsjQ6X

AMOUNT [EUR]

1

How it works

Agenda

The Story of a Transaction

From Transactions to Blocks

Mining

The Story of a Block and Nakamoto Consensus

Basic interaction with a node

Conclusions

The Story of a Transaction

Transaction Basics (1/4)

- Transactions specify the transfer of bitcoin ownership
- Zed transferred 1.5 BTC to 1Alice
- Alice wants to transfer 1 BTC to 1Bob

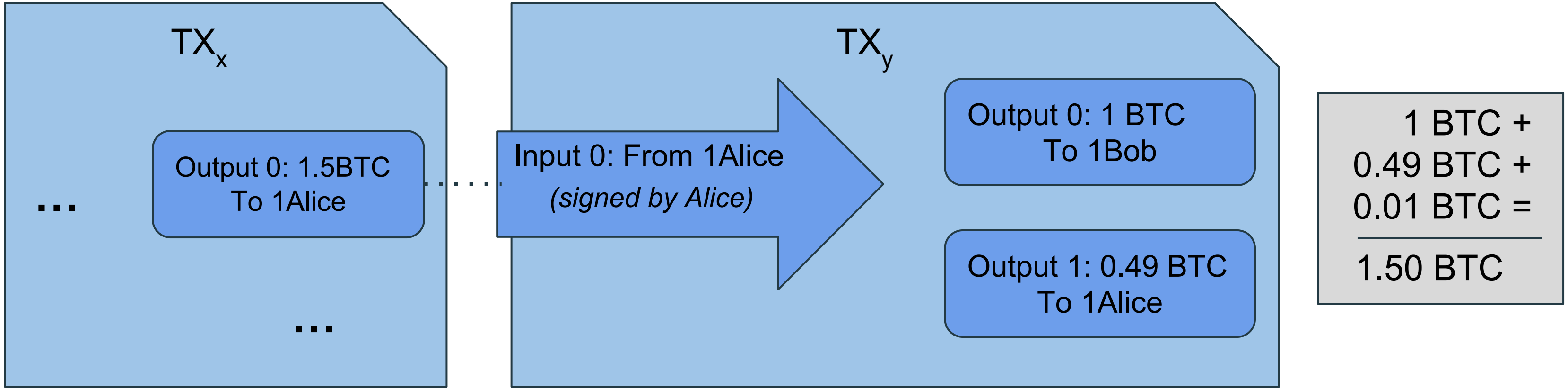
TX_x: 1Zed transfers 1.5 BTC to 1Alice

TX_y: 1Alice transfers 1 BTC to 1Bob

- 1Zed, 1Alice and 1Bob are short for the actual bitcoin addresses
- Alice has to prove that she is the owner of 1Alice
- Bob does not need to do anything

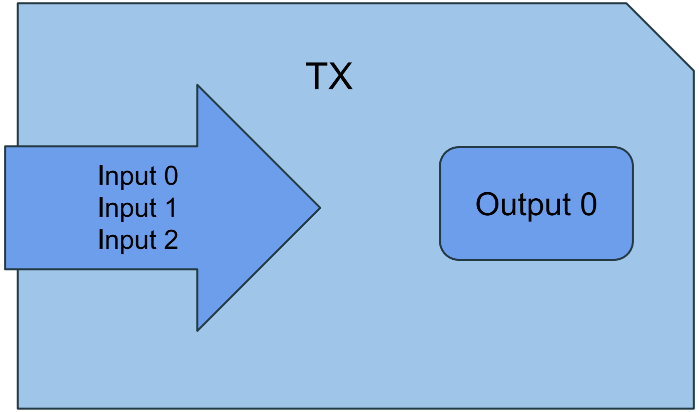
Transaction Basics (2/4)

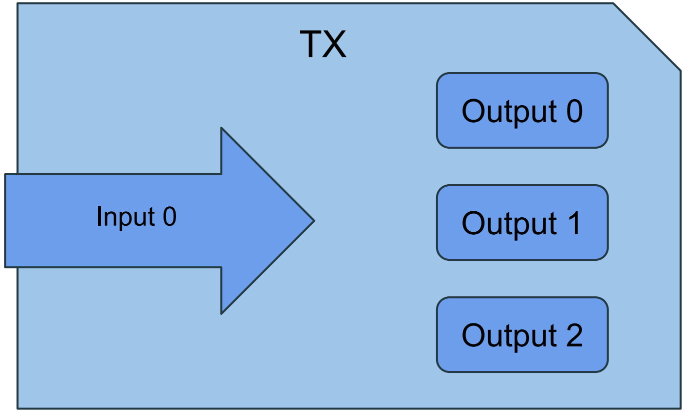
- Transactions can have many inputs and outputs
  - Input; address to get bitcoins from
  - Output; address to send bitcoins to
- When an input is used it is completely consumed
  - all the bitcoins that the TX contained need to be ***spent***.
- Total inputs - total outputs = transaction fee



Transaction Basics (3/4)

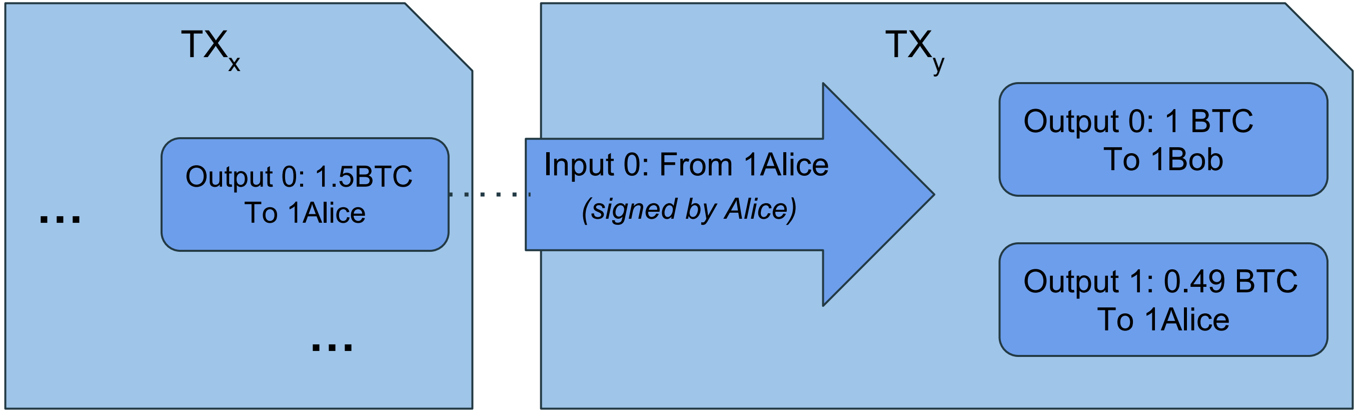
- A typical transaction
  - 1 inputs
  - 2 outputs (1 is *change* to the originating address)
- Other
  - N inputs - 1 output (e.g. aggregation of funds)
  - 1 input - N outputs (e.g. distribution of funds)



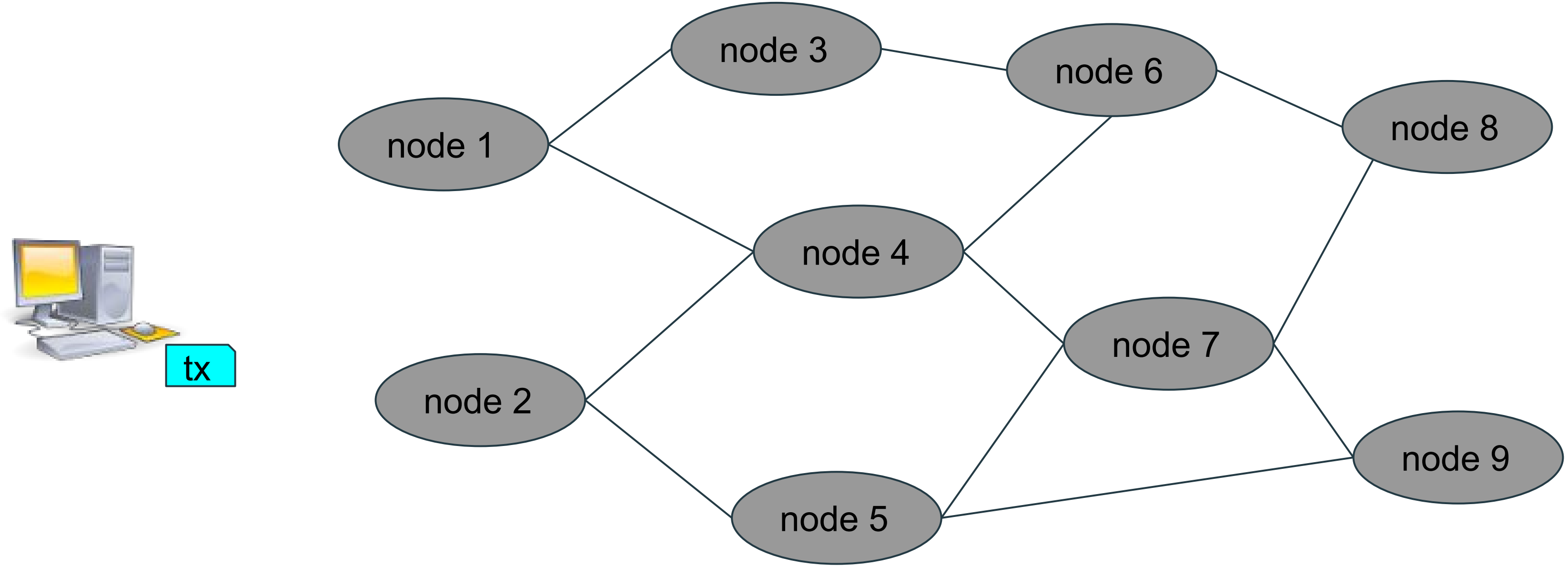


Transaction Basics (4/4)

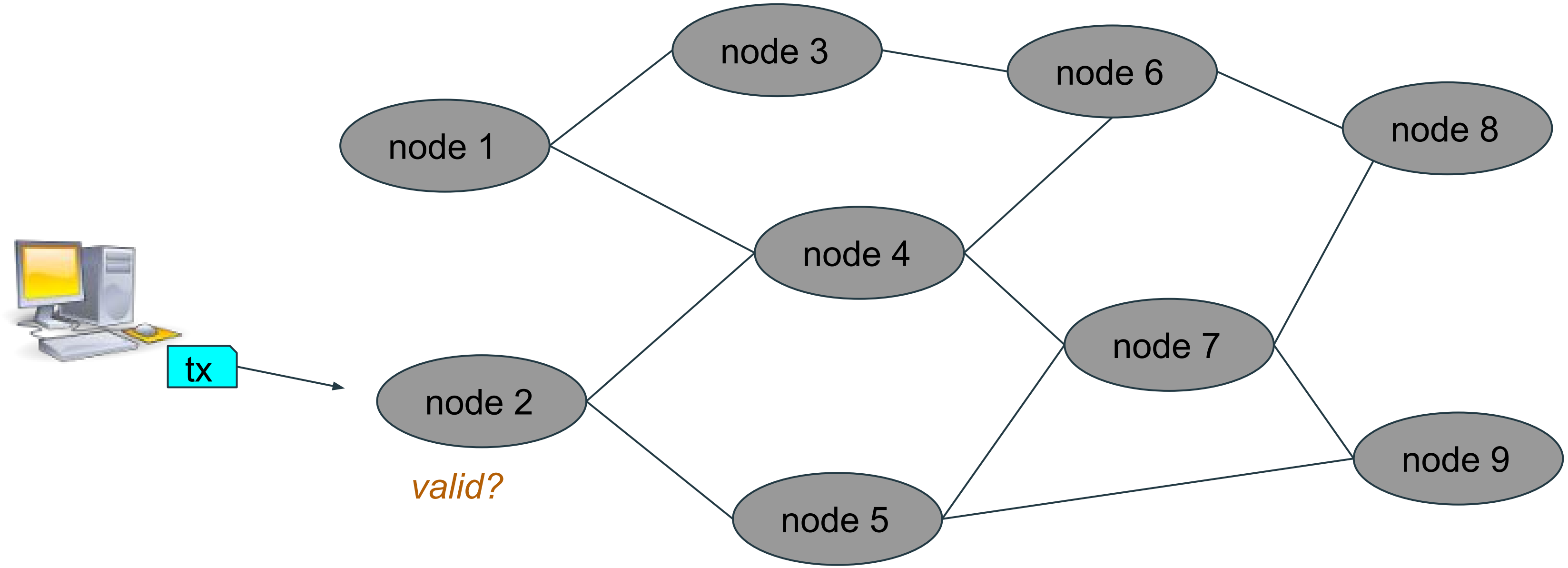
- Alice creates TXy to send 1 BTC to Bob.
- What next?



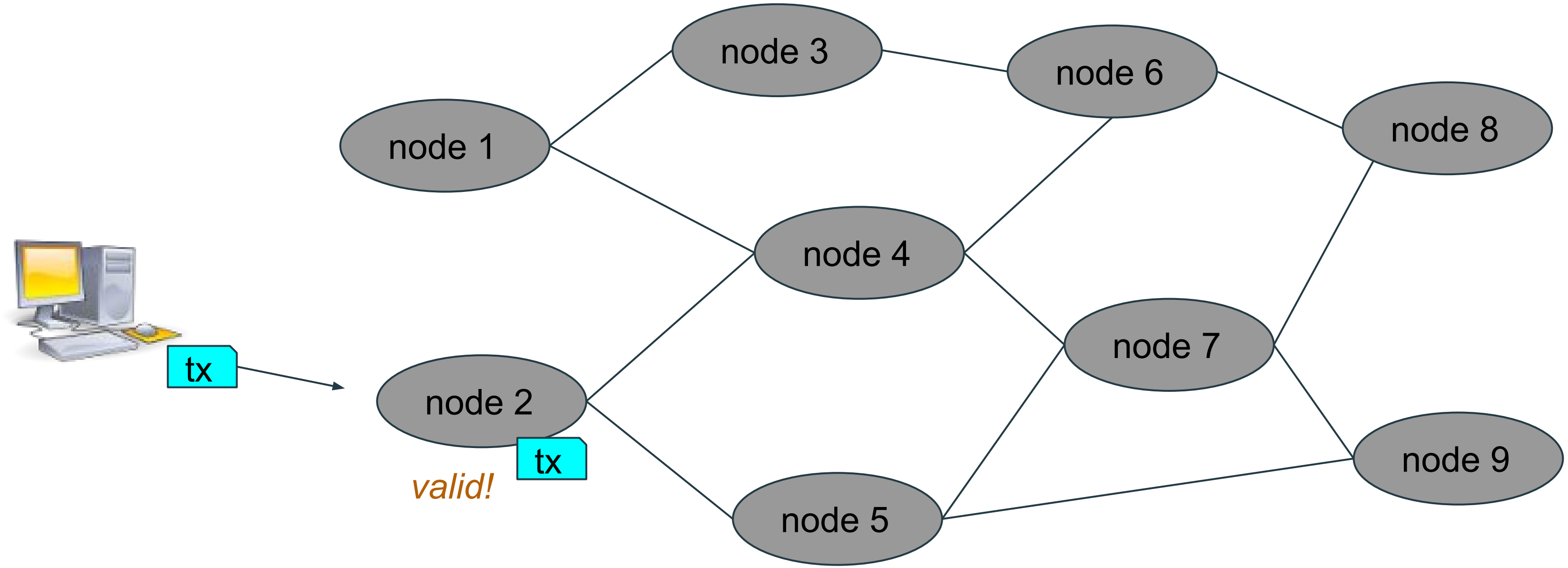
Transaction Network Propagation



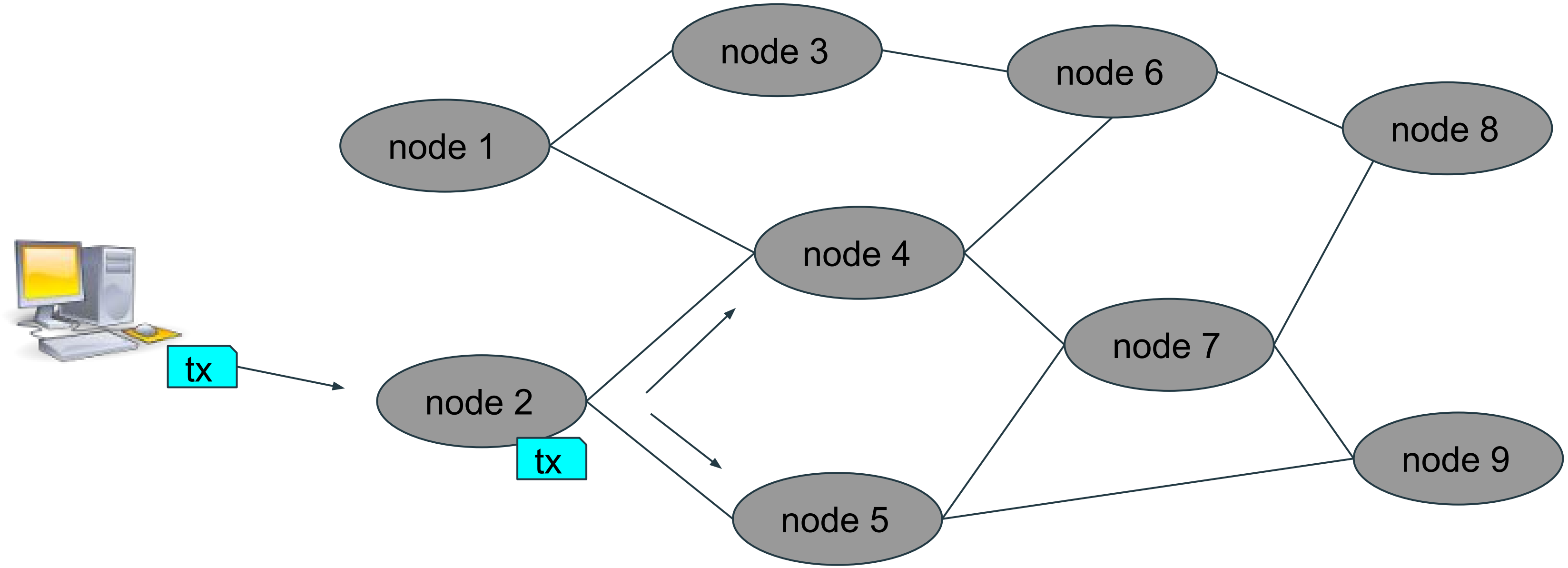
Transaction Network Propagation



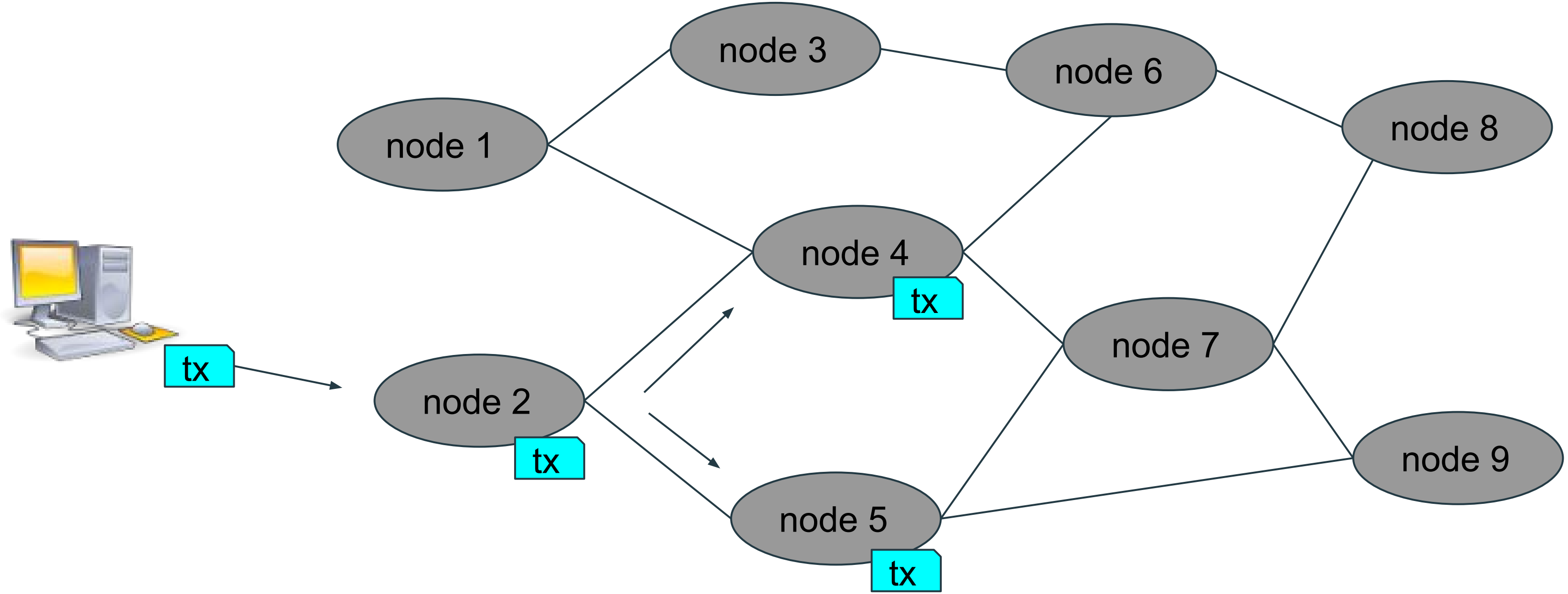
Transaction Network Propagation



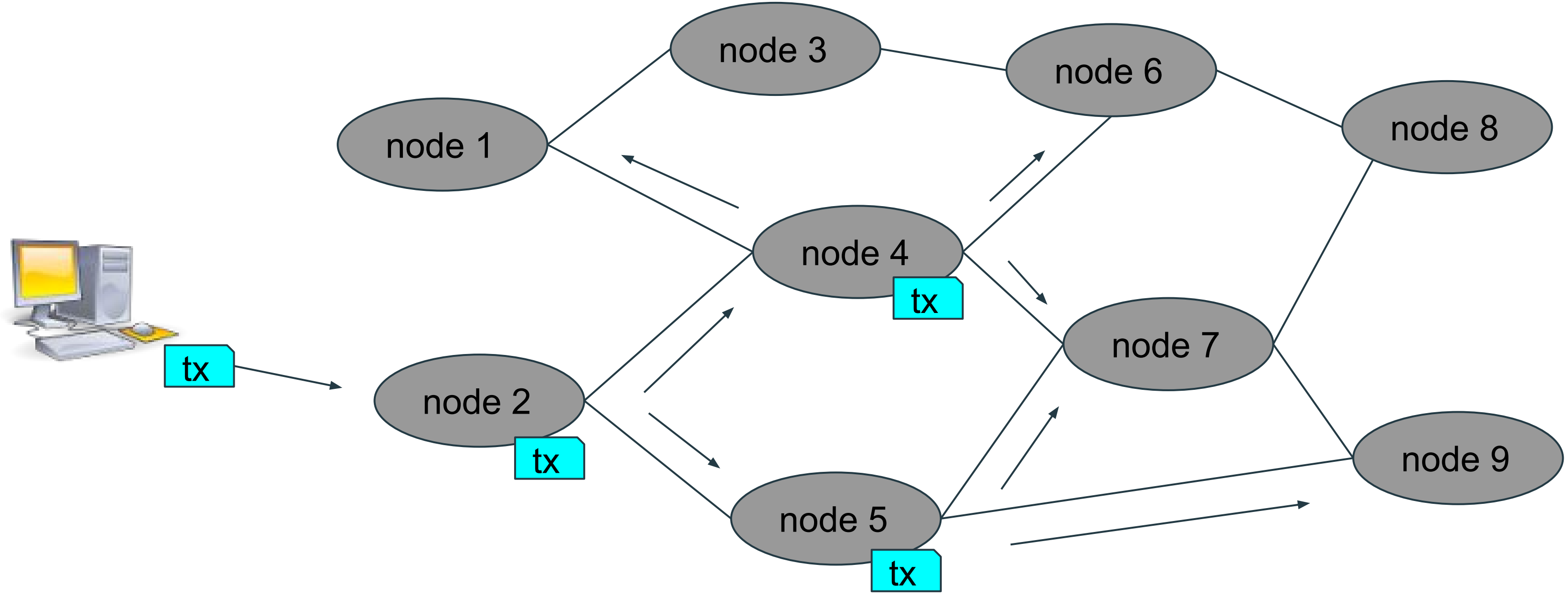
Transaction Network Propagation



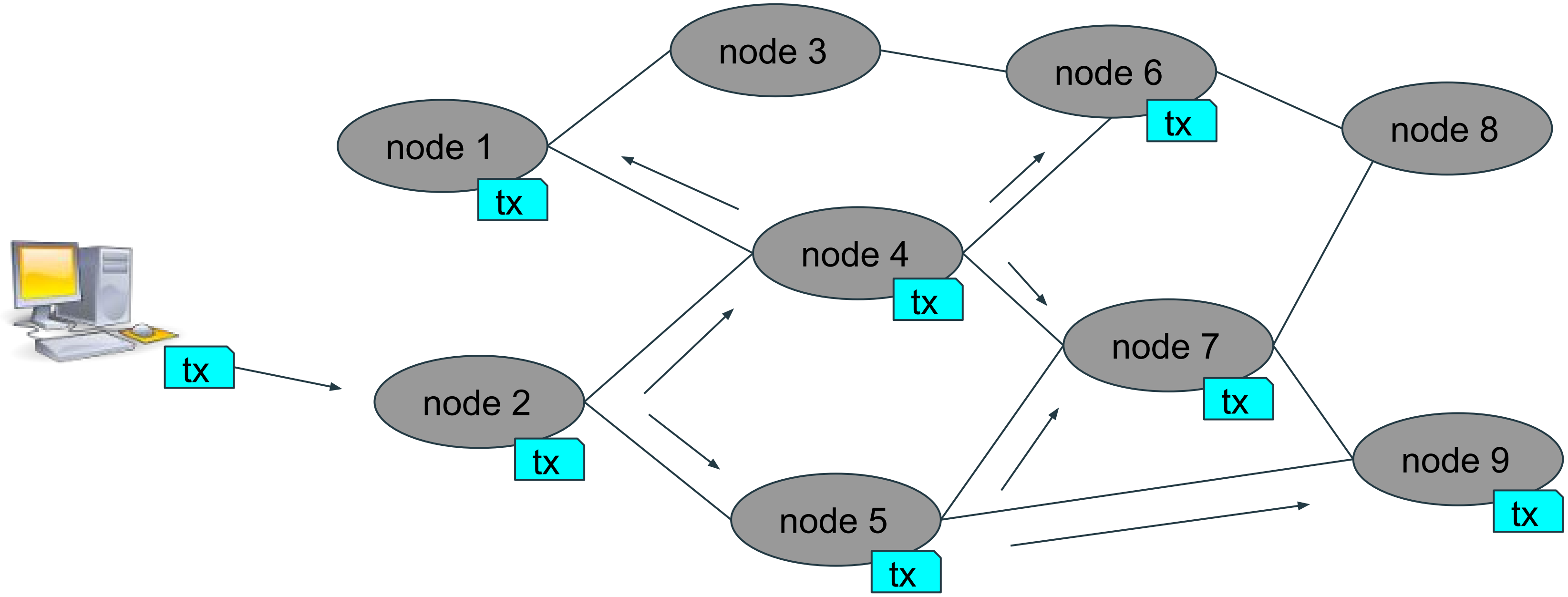
Transaction Network Propagation



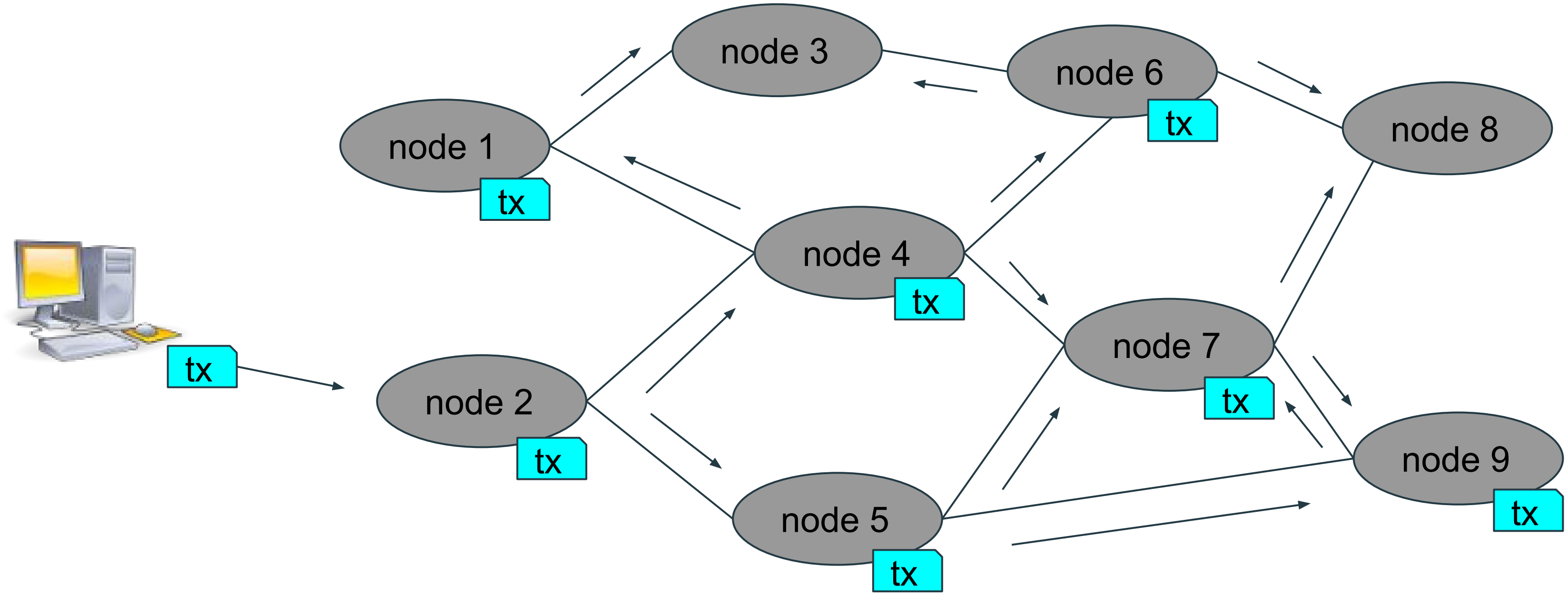
Transaction Network Propagation



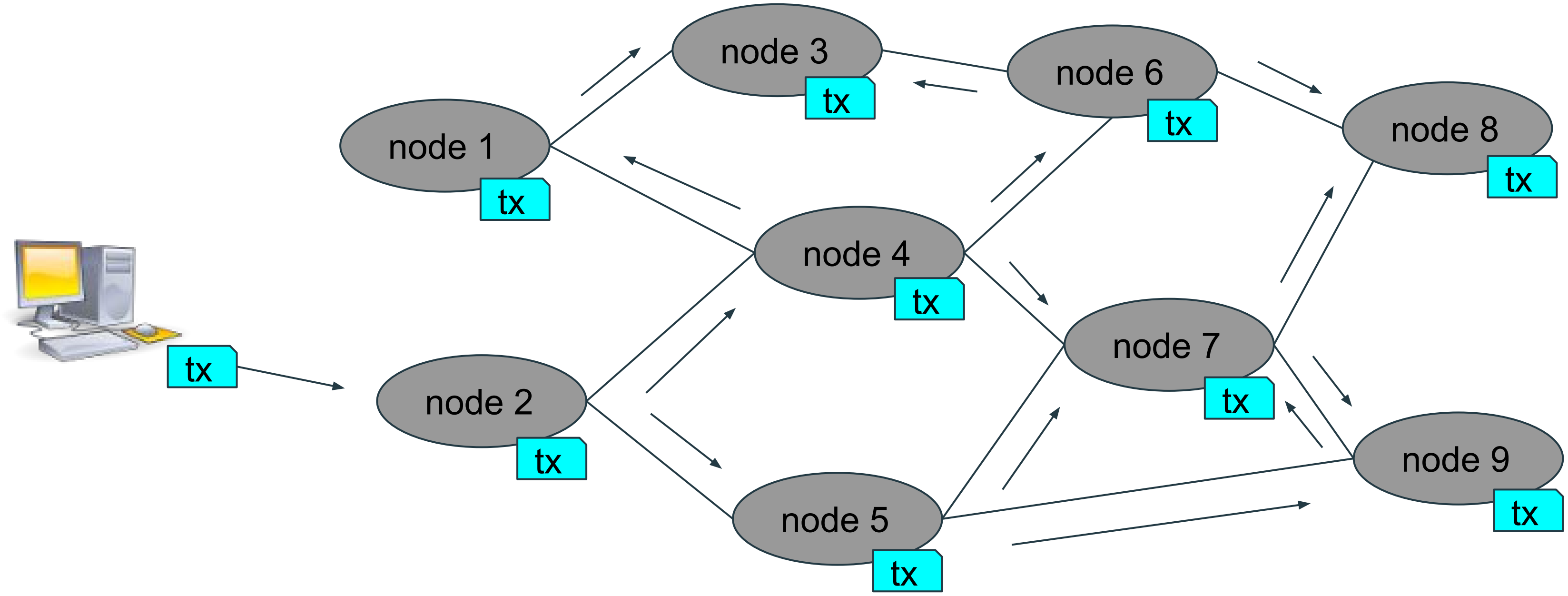
Transaction Network Propagation



Transaction Network Propagation

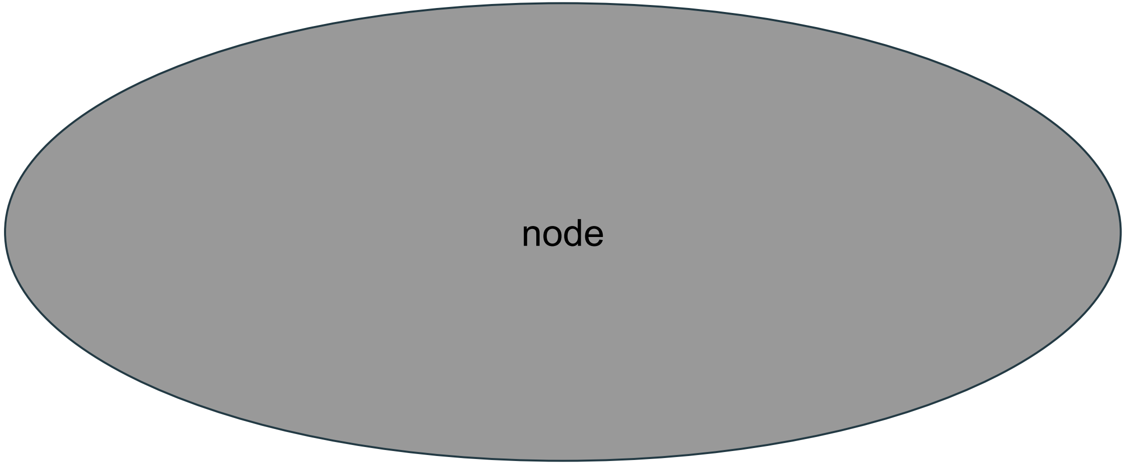


Transaction Network Propagation

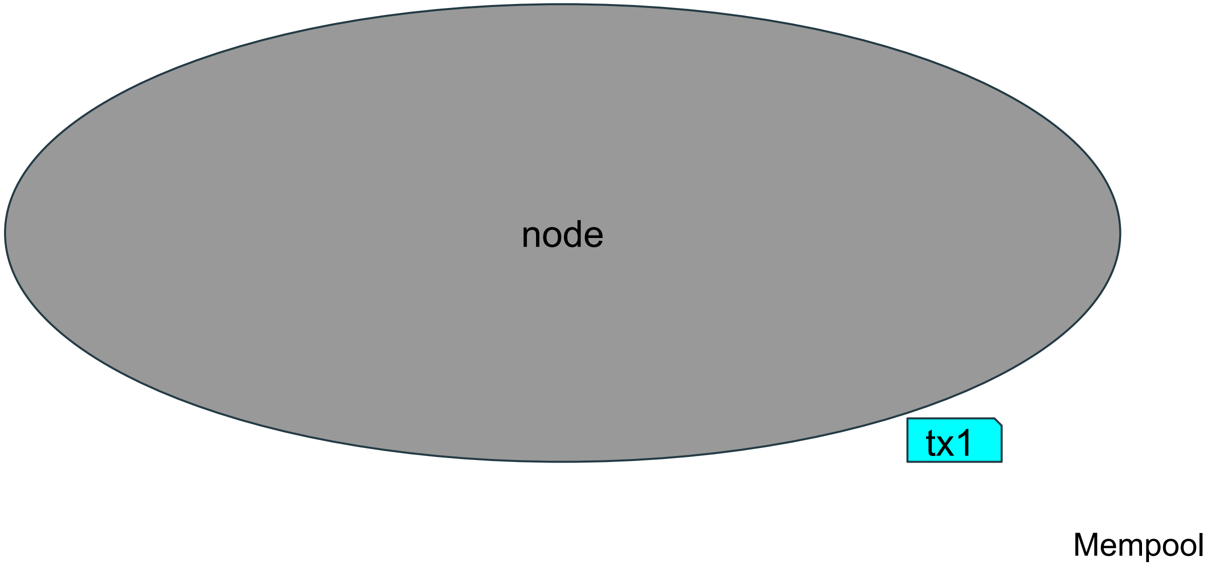


From Transactions to Blocks

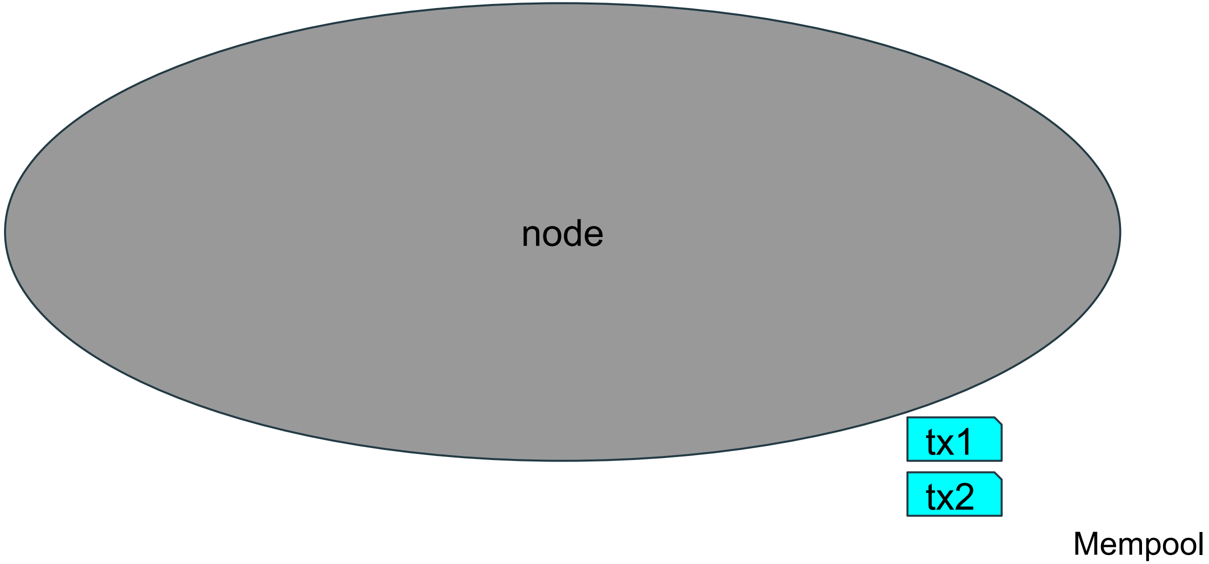
From Transactions to Blocks



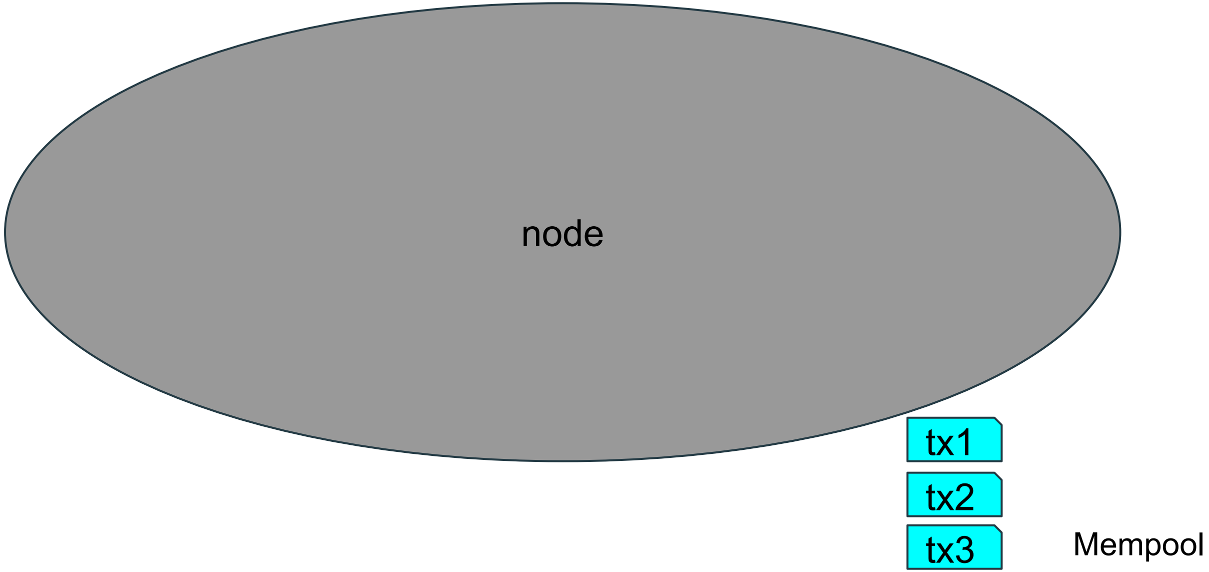
From Transactions to Blocks



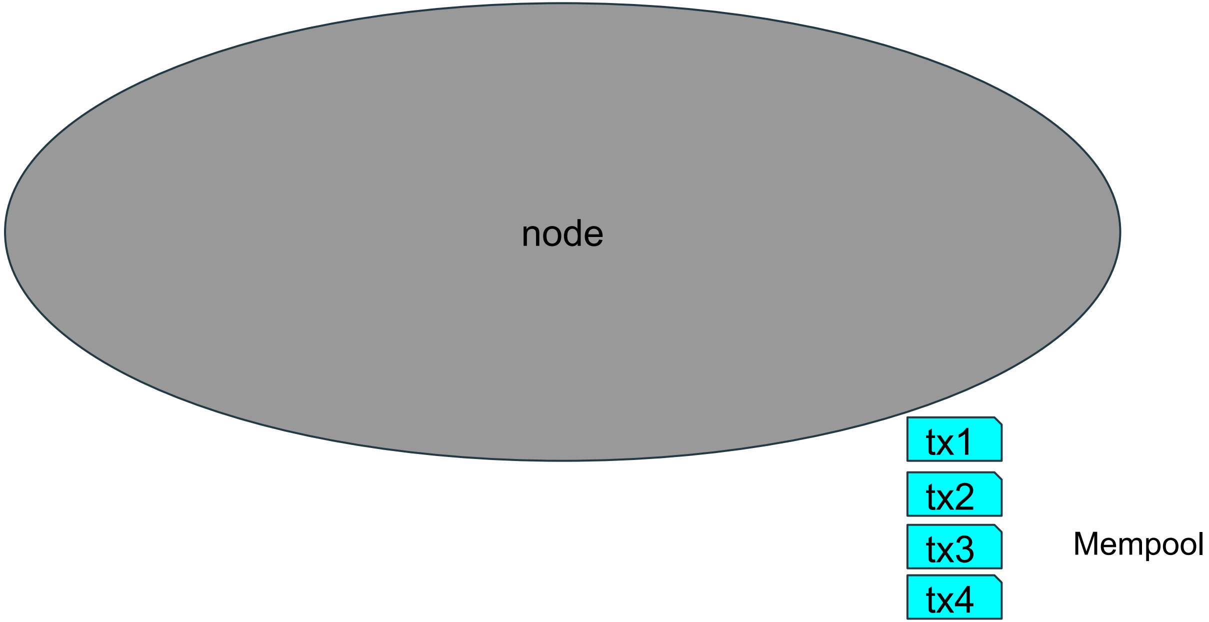
From Transactions to Blocks



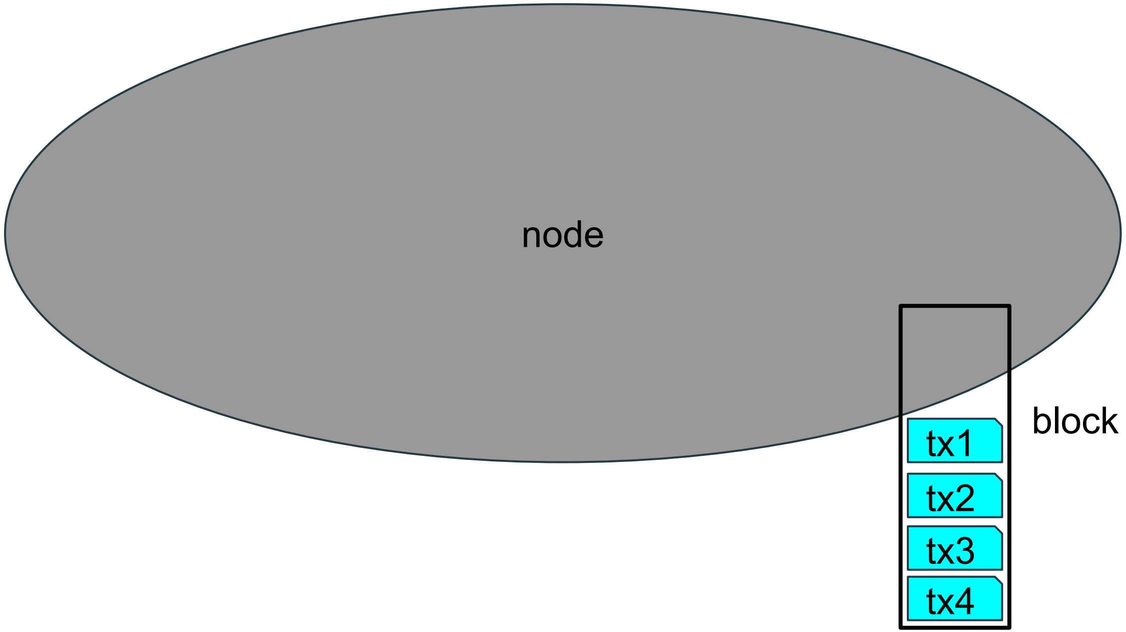
From Transactions to Blocks



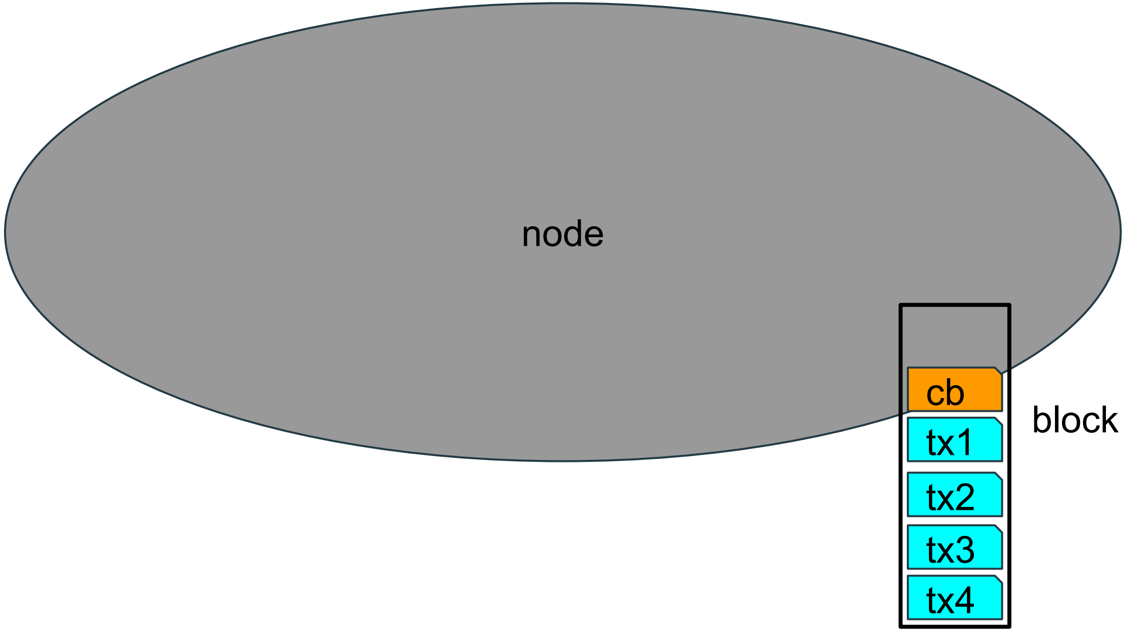
From Transactions to Blocks



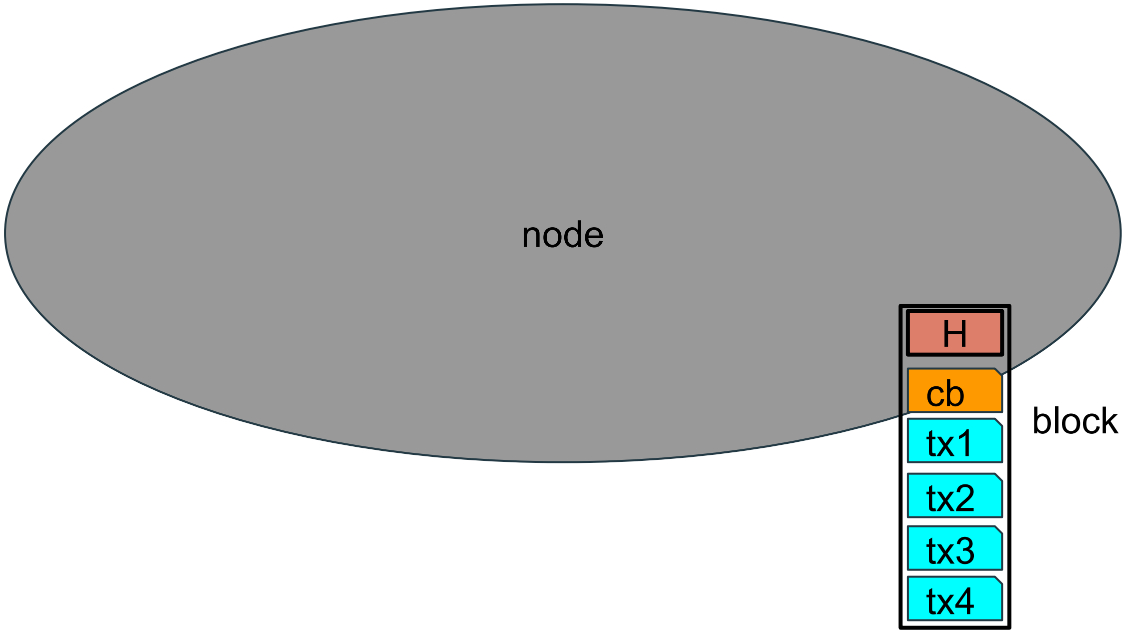
From Transactions to Blocks



From Transactions to Blocks



From Transactions to Blocks



Mining

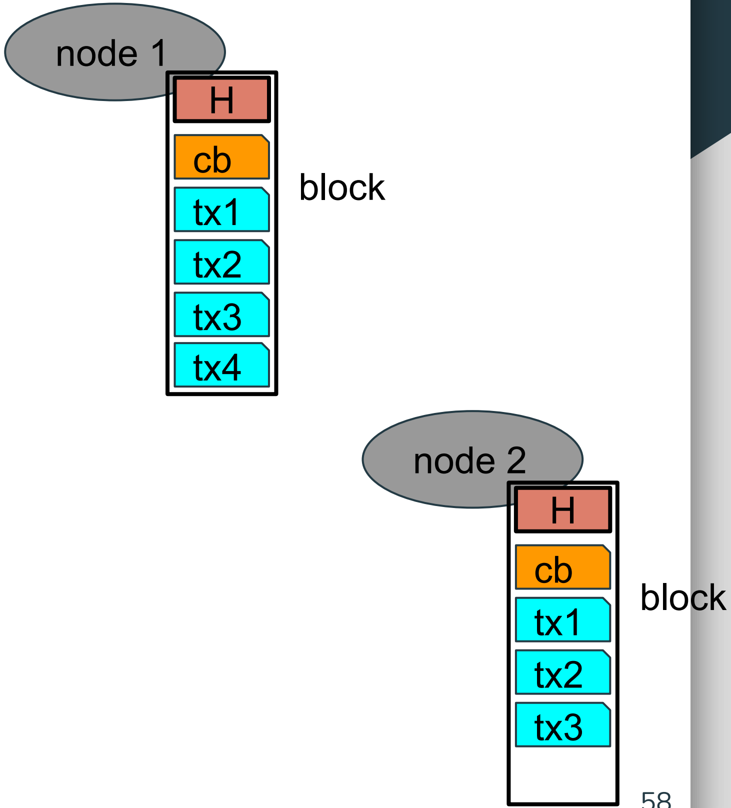
Mining a Block (1/4)

- Multiple nodes will get the transactions
- … and will create new blocks!
  - not identical

How do we avoid spam?

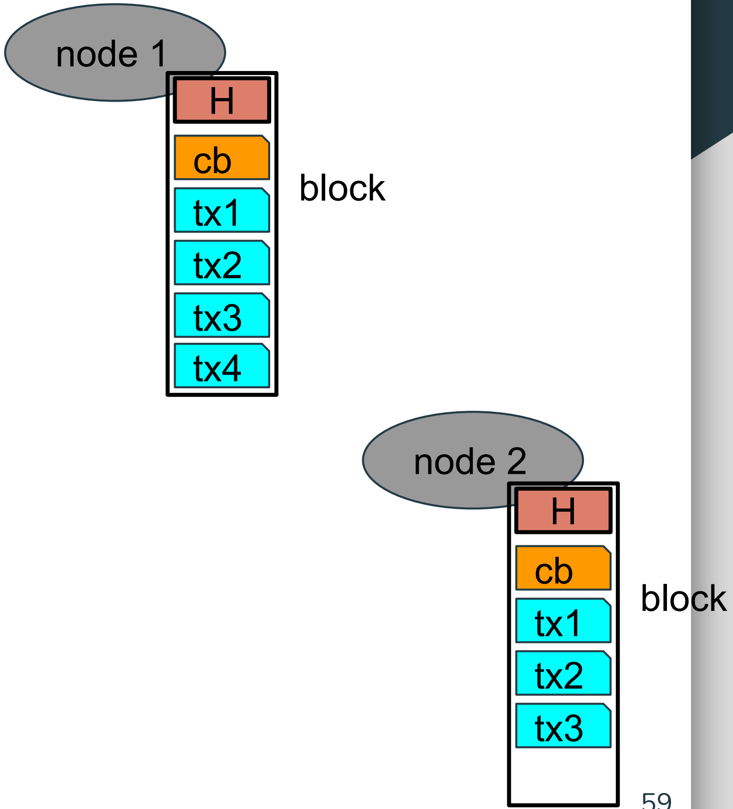
Which blocks are accepted by the network?

- Mining
  - Computational problem
  - Solutions requires work
- Proof-of-Work
  - difficult to calculate
  - trivial to validate



Mining a Block (2/4)

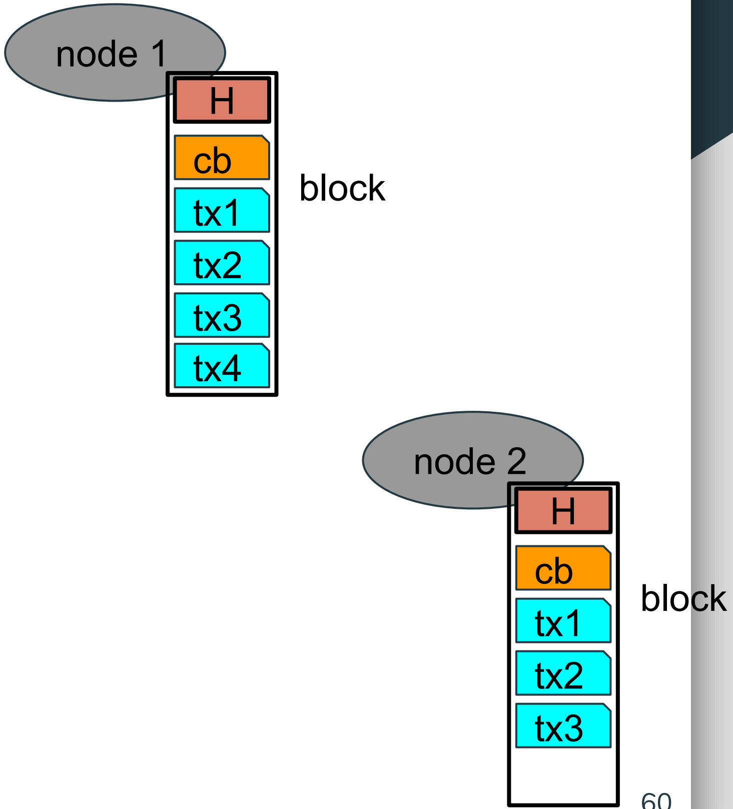
- Bitcoin’s Proof-of-Work puzzle
  - cryptographic hash* of the new block should be less than a given number
  - hash is random and thus it will take several attempts to find a proper hash
  - other nodes can validate with one attempt



* A cryptographic hash function is a hash function that takes an arbitrary block of data and returns a fixed-size bit string, the cryptographic *hash value*, such that any (accidental or intentional) change to the data will also change the hash value significantly.

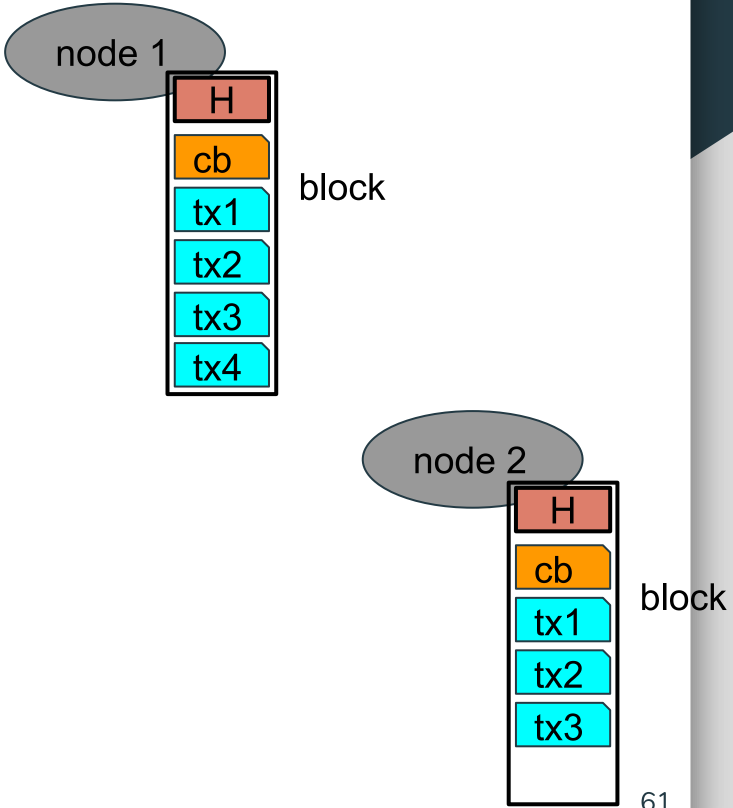
Mining a Block (3/4)

- The puzzle's difficulty automatically adjusts so that it requires approximately 10 minutes to solve
    - following the network's hashrate
- This *difficulty adjustment* happens every 2016 blocks
    - approximately 2 weeks
- The coinbase transaction is added by the miner
    - reward of 12.5 BTC to self
    - if the block is accepted he will get the reward.



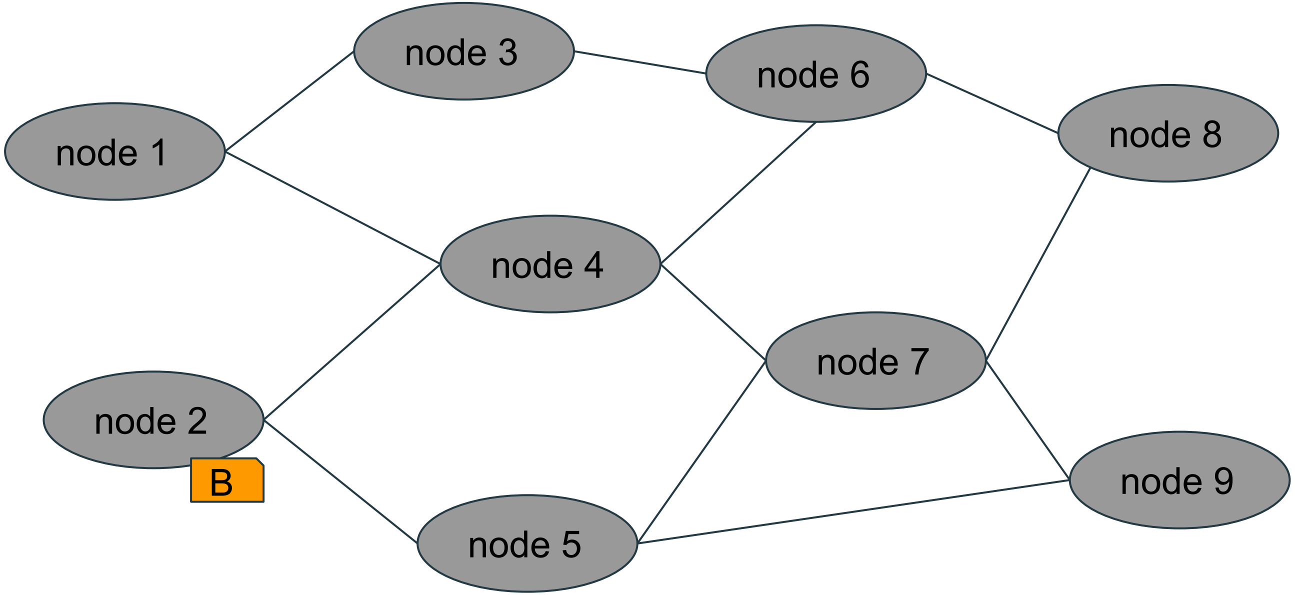
Mining a Block (4/4)

- Reward started at 50 bitcoins
  - It is halved every 210000 blocks
  - approximately 4 years
- All the TXs fees in a block are also awarded to the miner
- The header of a block contains
  - a link to the previously created block

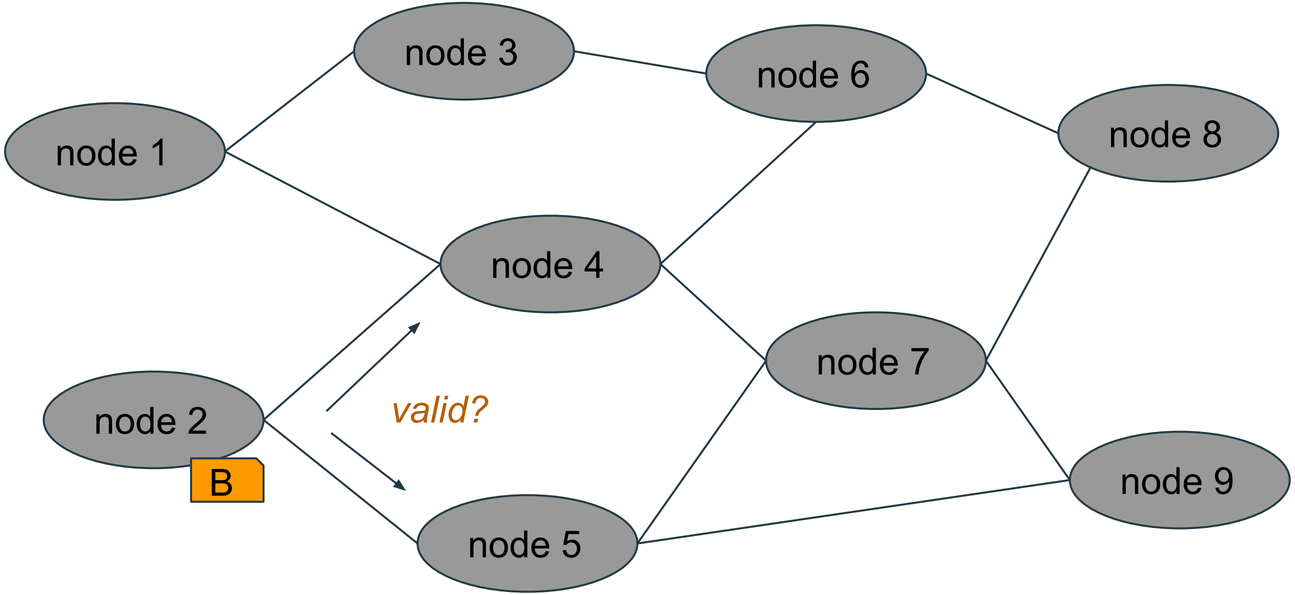


The Story of a Block and Nakamoto Consensus

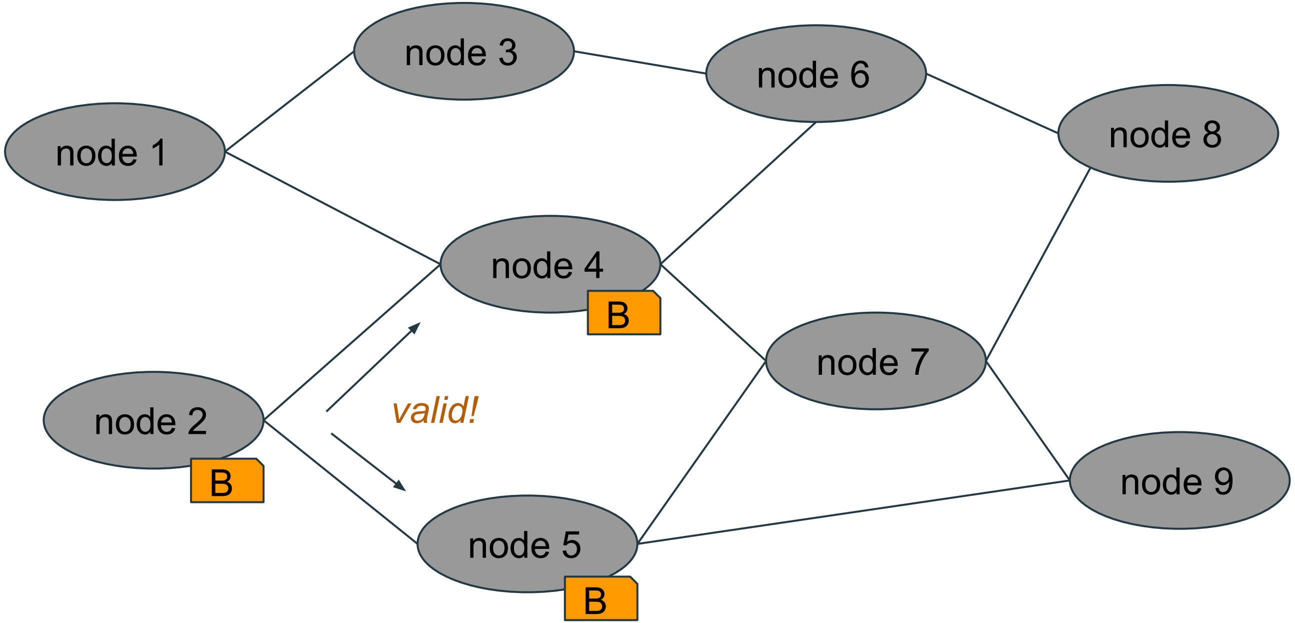
Block Network Propagation



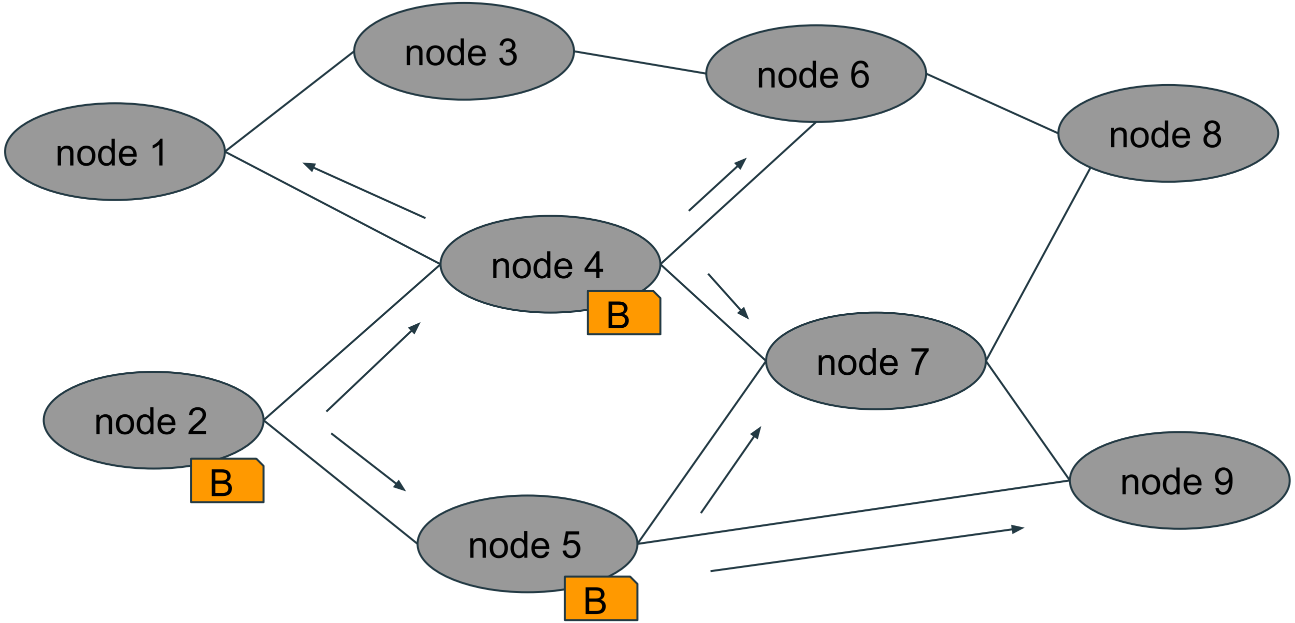
Block Network Propagation



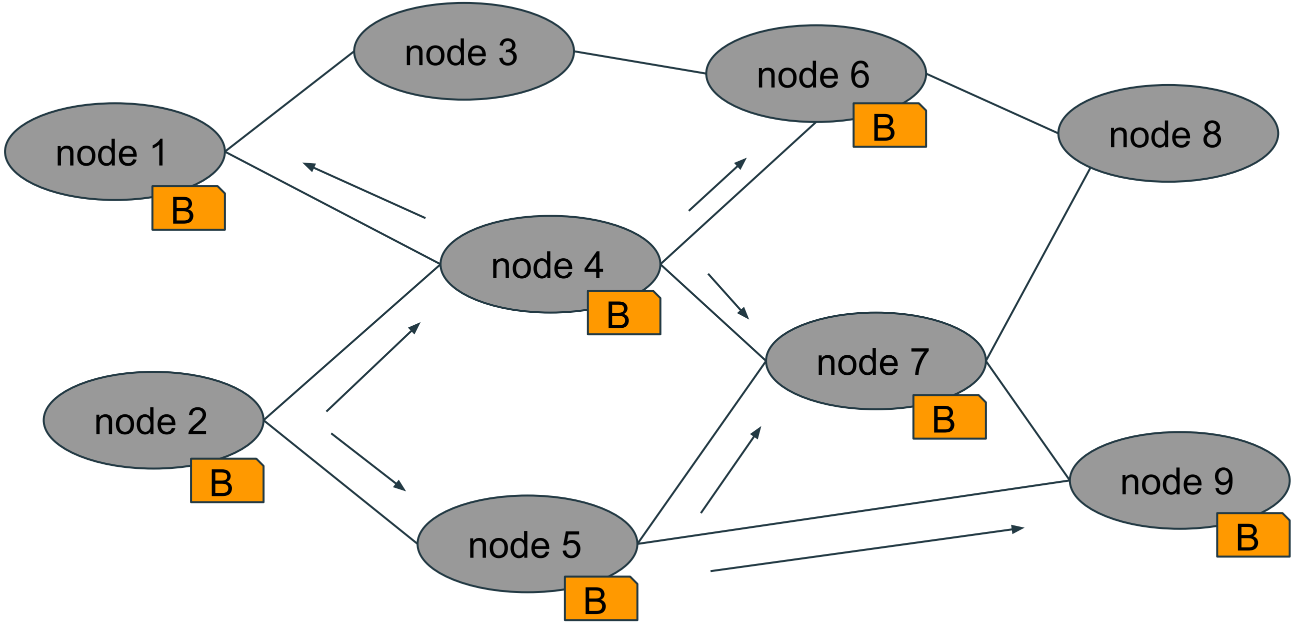
Block Network Propagation



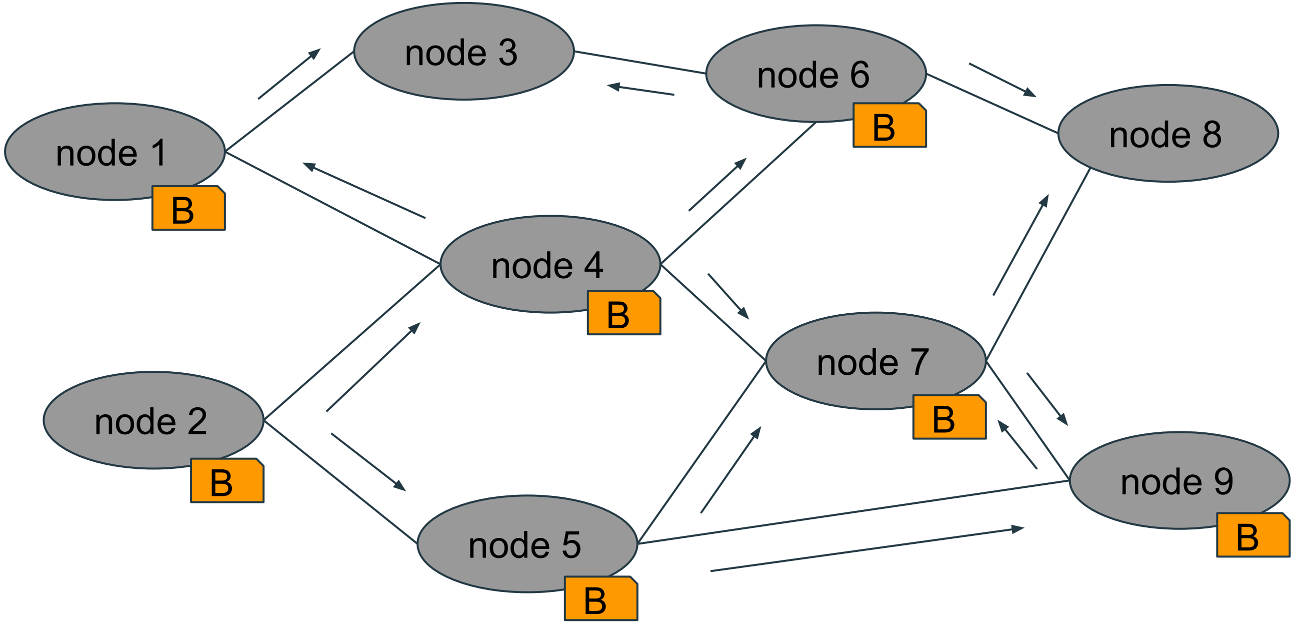
Block Network Propagation



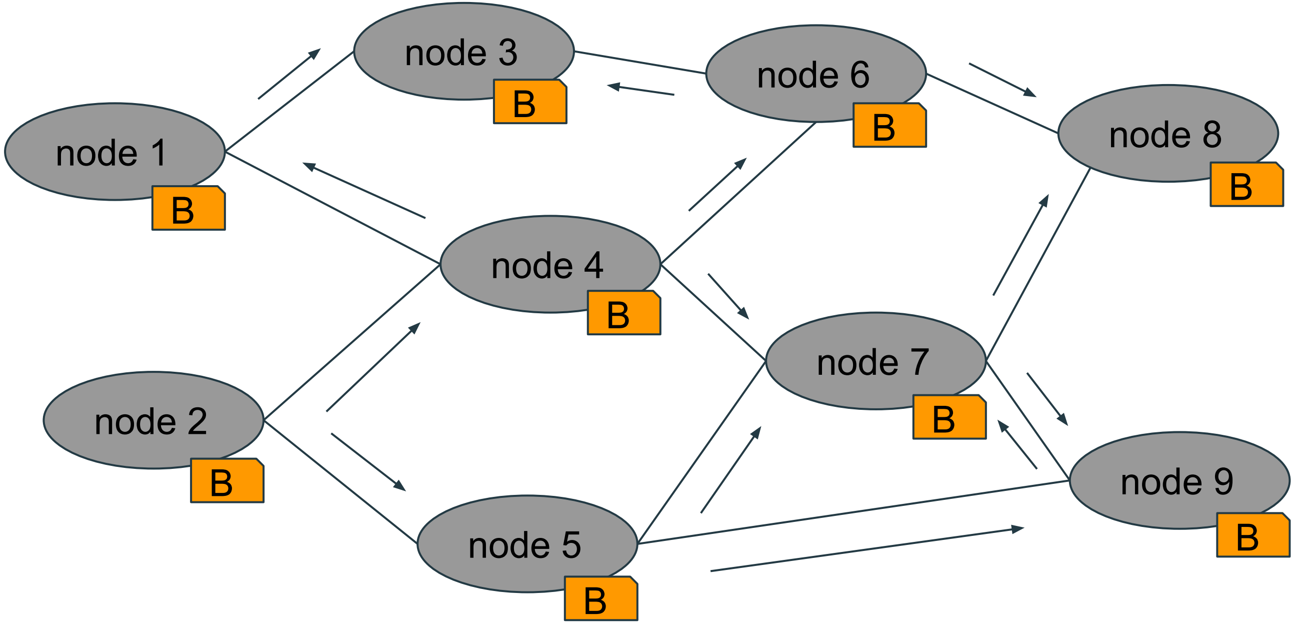
Block Network Propagation



Block Network Propagation



Block Network Propagation

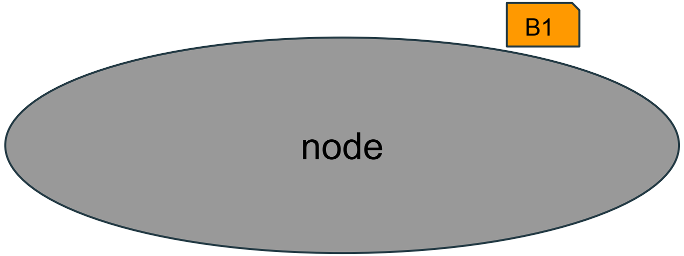


Forming a chain of Blocks (1/3)

- The new block is being added on top of the existing blocks
    - every ~10 minutes

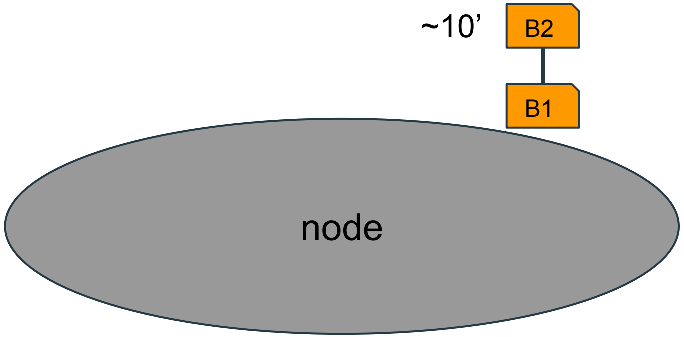
- This occurs on every single node

- Thus the network nodes have the same blocks



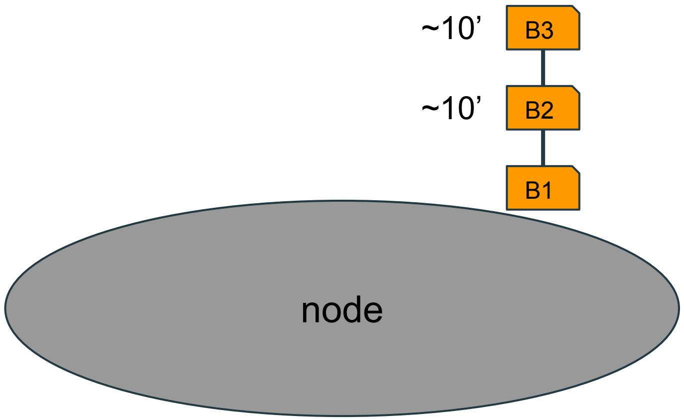
Forming a chain of Blocks (2/3)

- Blocks are linked with cryptographic hashes forming a chain of blocks
    - *Blockchain*.



Forming a chain of Blocks (3/3)

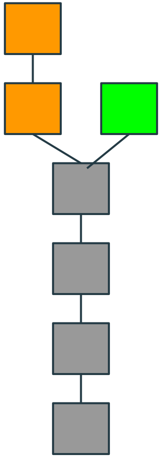
- When B1 is accepted by the network we say that a transaction on that block has one confirmation.
- When B3 is accepted we say that our transaction has 3 confirmations.
- The more confirmations the more final and secure a transaction is.



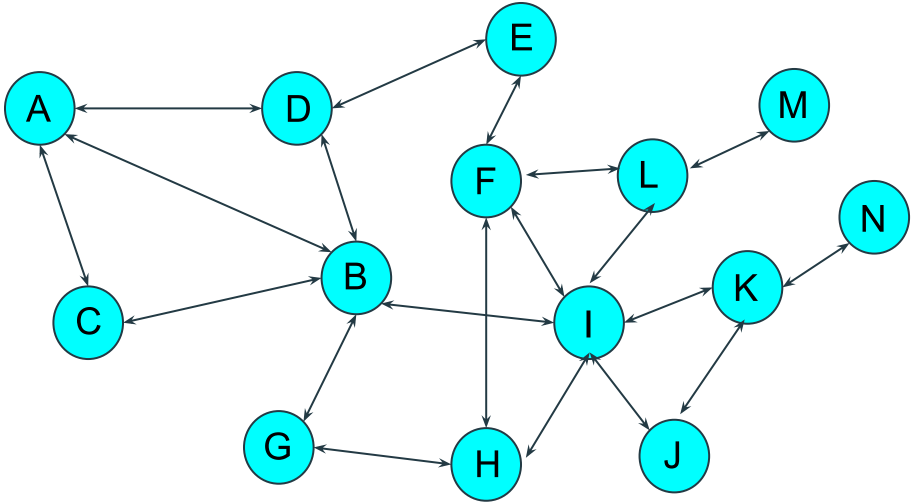
Nakamoto Consensus (1/2)

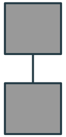
- Nodes receive blocks
  - construct blockchain in isolation
- Nakamoto consensus
  - fundamental contribution
  - how do different nodes come to agreement on what is the current state of the blockchain.
- If two blocks are found by two miners
  - two states
  - nodes continue chain based on the one they received first

- In Nakamoto consensus miners should **follow the longer chain** (the one with the most computation).
  - on next block miners will align and consensus is achieved.

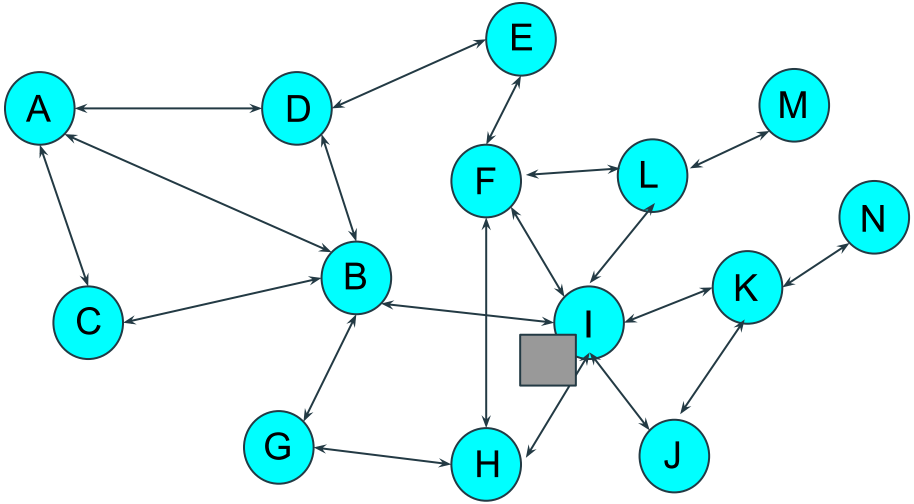


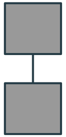
Nakamoto Consensus (2/2)



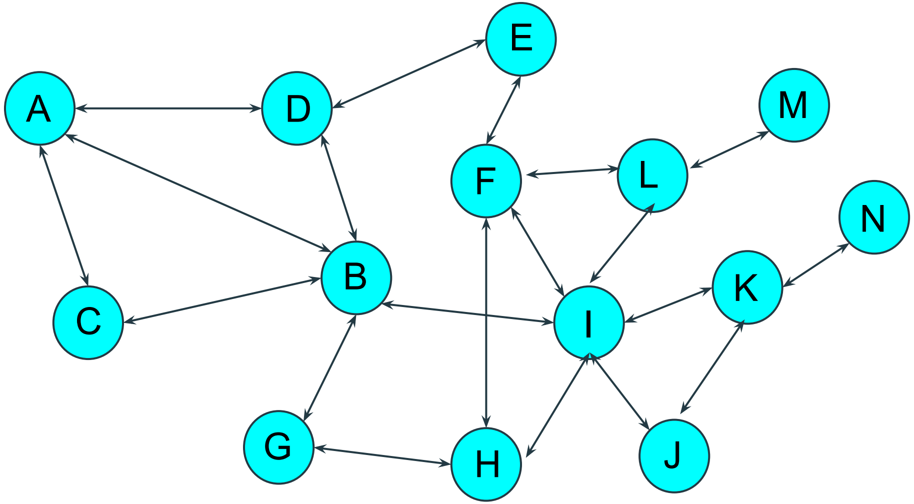


Nakamoto Consensus (2/2)

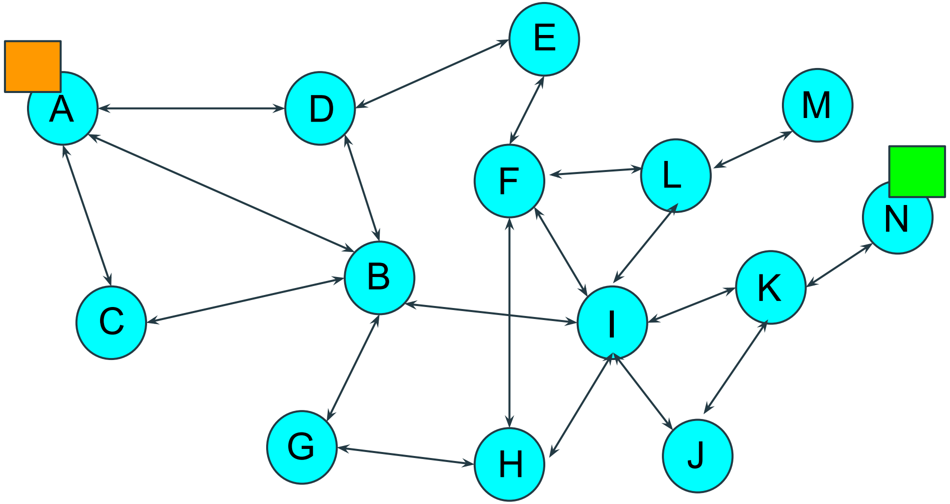




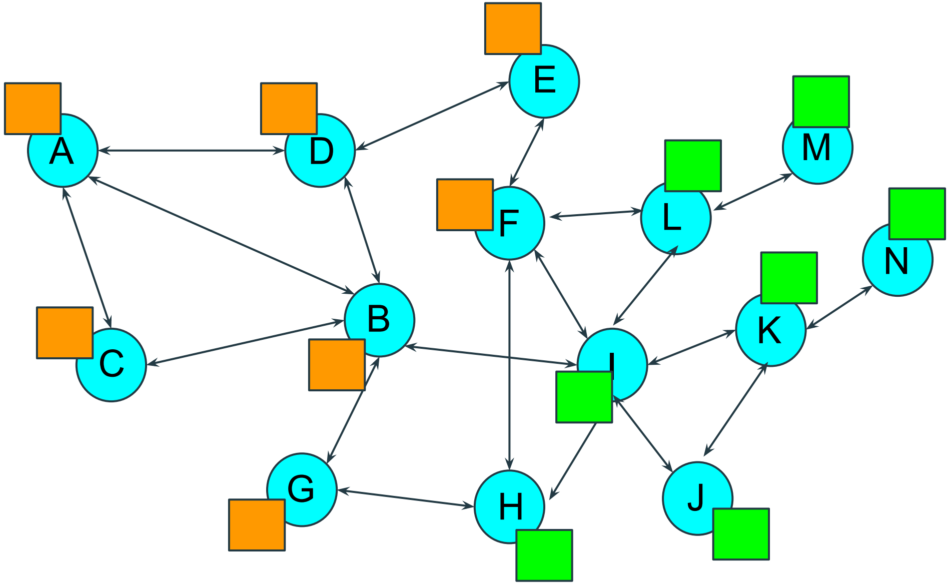
Nakamoto Consensus (2/2)



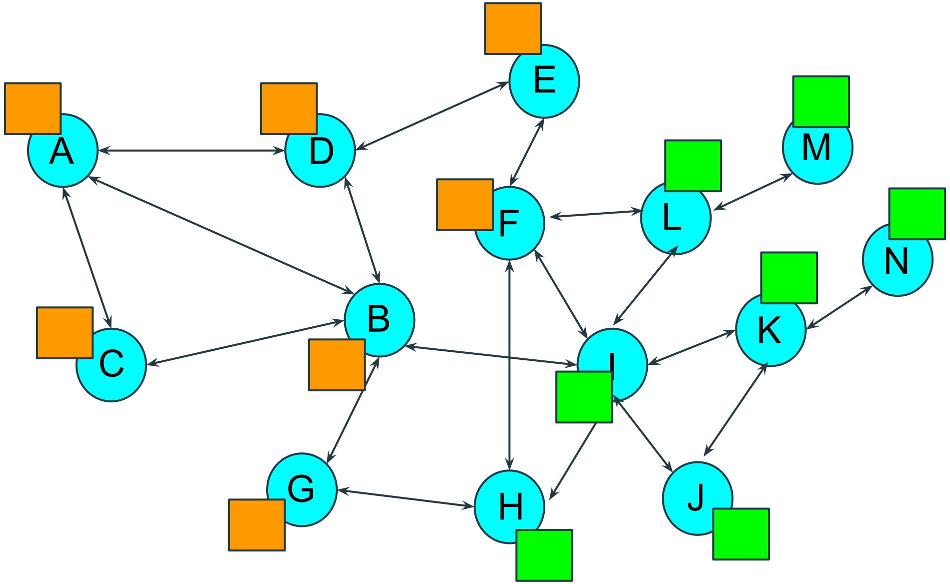
Nakamoto Consensus (2/2)

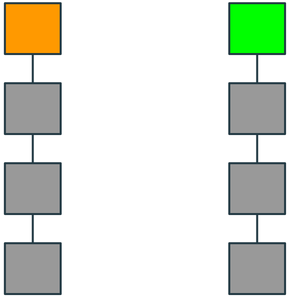


Nakamoto Consensus (2/2)

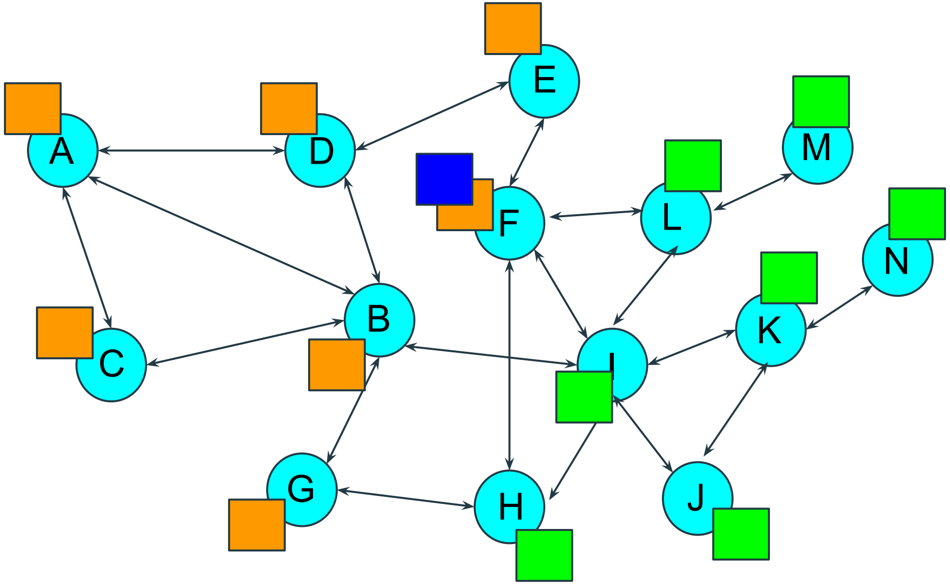


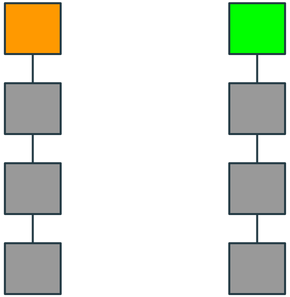
Nakamoto Consensus (2/2)



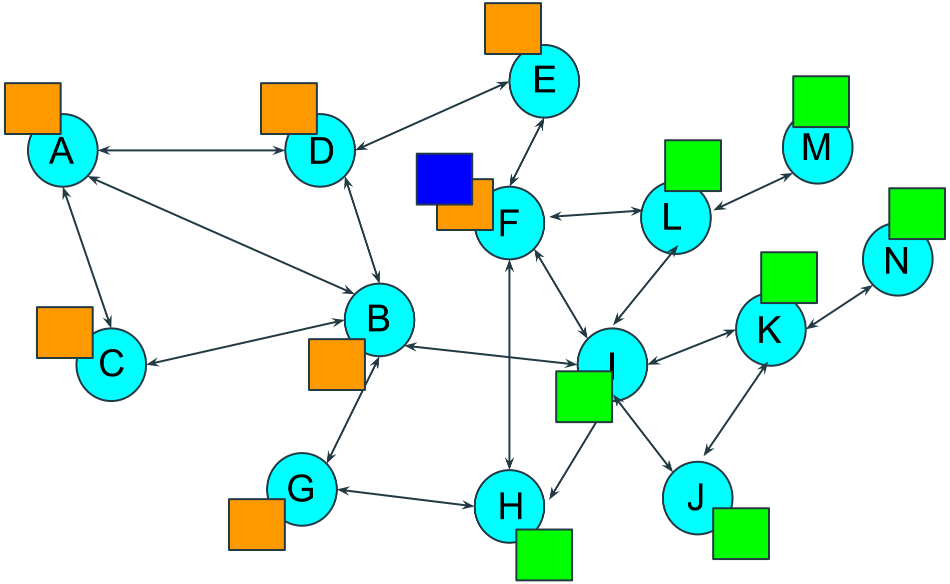


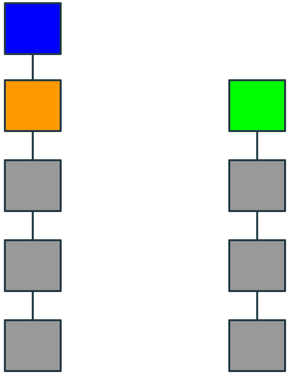
Nakamoto Consensus (2/2)



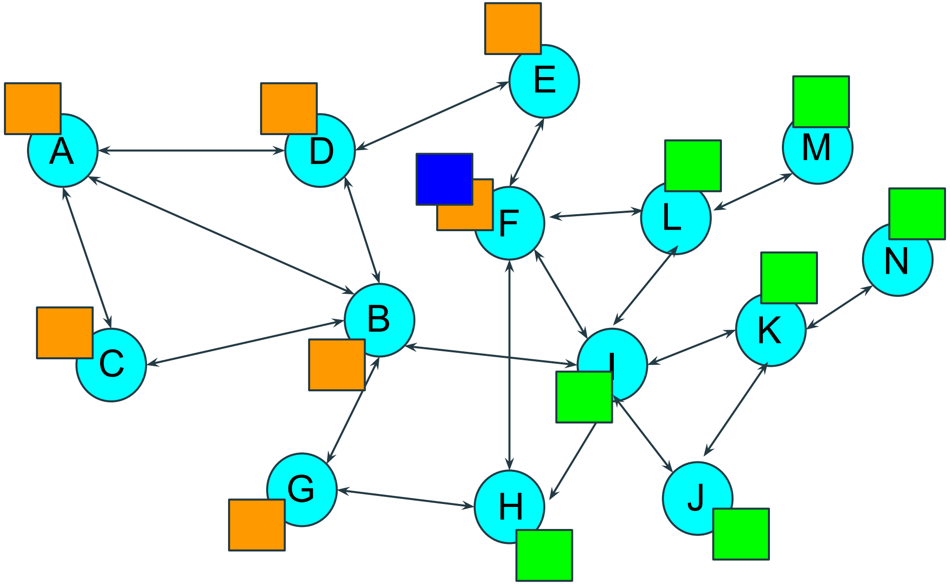


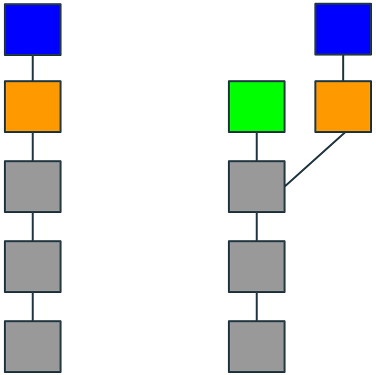
Nakamoto Consensus (2/2)



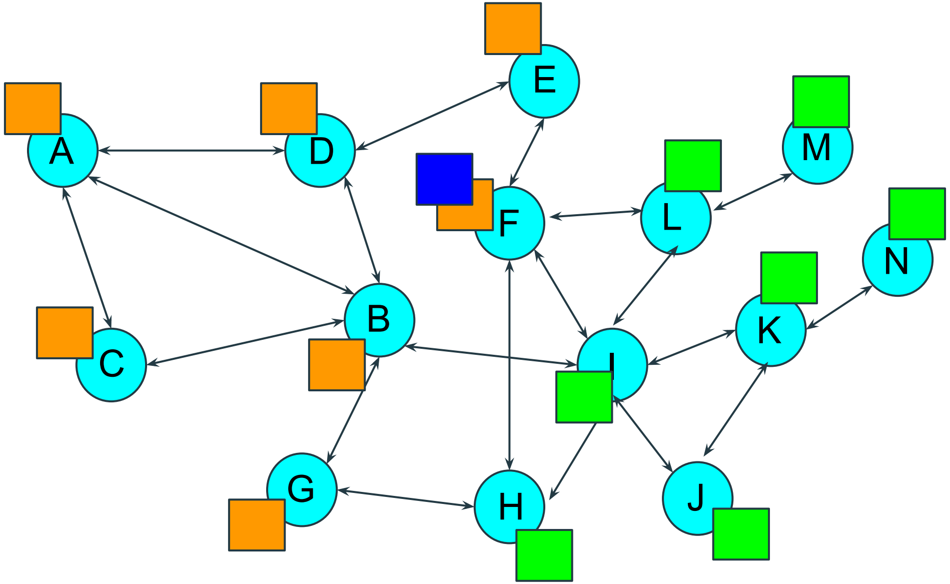


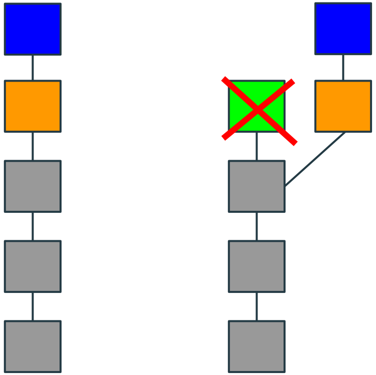
Nakamoto Consensus (2/2)





Nakamoto Consensus (2/2)



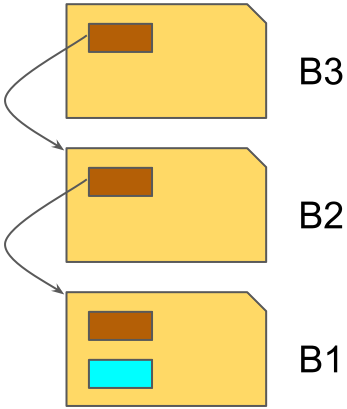


Blockchain and Trust (1/2)

- Blocks are linked together
  - hash of the previous block header

- If a Tx in B1 is tampered with it will be detected immediately by peers
  - since the hash of B1 will change

- An attacker will need to re-create all blocks
  - computationally infeasible
  - 51% attack

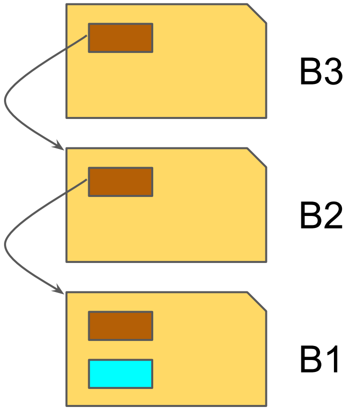


Blockchain and Trust (2/2)

- The block will be rejected and the attack will fail
  - since all peers have a copy of the blockchain they can detect tampering.

- When all hashes match across the whole chain all participants (nodes) know that they can trust their records, i.e. the system.

- Blockchain and Nakamoto Consensus achieve **trustless** interaction between participants.



Basic interaction with a node

Bitcoin software

The Bitcoin software includes several executables, one providing the core functionality and the other utility tools:

bitcoind:

The daemon server provides full peer functionality; includes a wallet. It provides a JSON-RPC API to talk to the node (ports: mainnet: 8332, testnet: 18332).

bitcoin-cli:

Provides a command-line interface to *talk* to the daemon server

bitcoin-qt:

Provides a graphical user interface to the Bitcoin peer and wallet (subset of the API as part of GUI but also provides a console for all calls)

bitcoin-tx:

Allows to create, parse or modify transactions

JSON-RPC API Calls (1/2)

```
$ ./bitcoin-cli help

$ ./bitcoin-cli getblockcount
1128802

$ ./bitcoin-cli getbalance
1.51815479

$ ./bitcoin-cli getnewaddress
mvBGdiYC8jLumpJ142ghePYuY8kecQgeqS

$ ./bitcoin-cli encryptwallet MyPaSsWoRd
wallet encrypted; Bitcoin server stopping, restart
to run with encrypted wallet. The keypool has been
flushed, you need to make a new backup.

$ ./bitcoin-cli walletpassphrase MyPaSsWoRd 120

$ ./bitcoin-cli backupwallet wallet.backup

$ ./bitcoin-cli importwallet wallet.backup
```

```
$ ./bitcoin-cli getinfo
{
  "version": 130100,
  "protocolversion": 70014,
  "walletversion": 130000,
  "balance": 1.51815479,
  "blocks": 1142660,
  "timeoffset": 0,
  "connections": 8,
  "proxy": "",
  "difficulty": 4898.829455242267,
  "testnet": true,
  "keypoololdest": 1480065505,
  "keypoolsize": 100,
  "paytxfee": 0.00000000,
  "relayfee": 0.00001000,
  "errors": ""
}
```

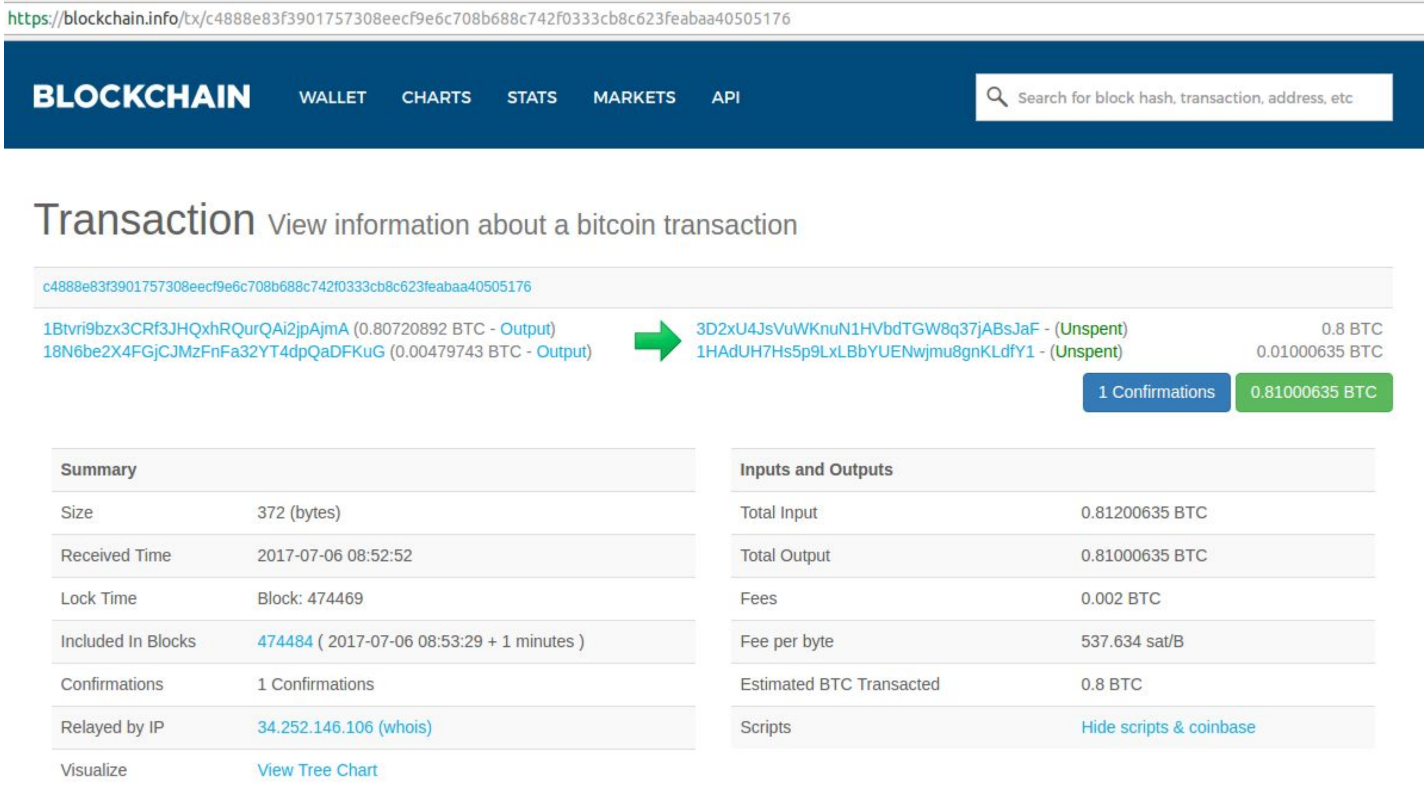
JSON-RPC API Calls (2/2)

```
$ ./bitcoin-cli sendtoaddress mvBGdiYC8jLumpJ142ghePYuY8kecQgeqS 0.01
Ff8322626c21c5bdfa1d27f75a55a1cb1d3b764bb34063f64b38f0803c370c08

$ ./bitcoin-cli listunspent 2
[
 {
    "txid": "30d98980c56a139438f0c969ca30d4be2c7f865d098b905362263c5daca2afa7",
    "vout": 0,
    "address": "mgs9DLttzvWFkZ46YLSNKSZbgSNiMNUsdJ",
    "amount": 1.01452015,
    "confirmations": 20183,
    ...
  }
  ...
]
$ ./bitcoin-cli listaccounts
{
  "": -1.01483854,
  ...
}

$ ./bitcoin-cli getaddressesbyaccount “”
[ “mvBGdiYC8jLumpJ142ghePYuY8kecQgeqS”, ... ]
```

Blockchain Explorer: Transaction Example



https://blockchain.info/tx/c4888e83f3901757308eecf9e6c708b688c742f0333cb8c623feabaa40505176

Transaction View information about a bitcoin transaction

c4888e83f3901757308eecf9e6c708b688c742f0333cb8c623feabaa40505176

1Btvri9bzx3CRf3JHQxhRQurQAi2jpAjmA (0.80720892 BTC - Output)
18N6be2X4FGjCJMzFnFa32YT4dpQaDFKuG (0.00479743 BTC - Output)

3D2xU4JsVuWKnuN1HVbdTGW8q37jABsJaF - (Unspent) 0.8 BTC
1HAdUH7Hs5p9LxLBbYUENwjmu8gnKLdfY1 - (Unspent) 0.01000635 BTC

1 Confirmations 0.81000635 BTC

Summary	
Size	372 (bytes)
Received Time	2017-07-06 08:52:52
Lock Time	Block: 474469
Included In Blocks	474484 (2017-07-06 08:53:29 + 1 minutes)
Confirmations	1 Confirmations
Relayed by IP	34.252.146.106 (whois)
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	0.81200635 BTC
Total Output	0.81000635 BTC
Fees	0.002 BTC
Fee per byte	537.634 sat/B
Estimated BTC Transacted	0.8 BTC
Scripts	Hide scripts & coinbase

Greek Community

- Bitcoin and Blockchain Tech Meetup (Thessaloniki)
    - **http://www.meetup.com/BlockchainGreece-1/**

- Bitcoin and Blockchain Tech Meetup (Athens)
    - http://www.meetup.com/BlockchainGreece-0/
- Bitcointalk forum (Greek section)
    - https://bitcointalk.org/gr
- Blog
    - http://www.bitcoin-gr.org/
- Facebook
    - https://www.facebook.com/groups/bitcoin.gr/?fref=ts
- Slack
    - https://bitcoingreece.herokuapp.com
- https://weacceptbitcoin.gr/

Questions ?

Website:	**www.kkarasavvas.com**
Linkedin:	https://www.linkedin.com/in/kkarasavvas
Twitter:	@kkarasavvas
Email:	kkarasavvas@gmail.com
Bitrated:	https://www.bitrated.com/kostas
Keybase:	https://keybase.io/kkarasavvas