

BITCOIN

A Return to Moral Money

Part 3: How Bitcoin Works



1. Types of Nodes
2. Cryptography & Hashing
3. The Blockchain
4. The Lightning Network
5. Running a Node
6. Seed Words

Bitcoin Basics



- Bitcoins are held in bitcoin **wallets***
- **Transactions** are the transfer of bitcoin from one wallet to another; each wallet is identified with a **public key**
- The **blockchain** is a public ledger where transactions are recorded and verified, i.e., wallets determine who owns what using the blockchain
- Bitcoin ownership is confirmed using a **private key** which is used to **sign** transactions
- Signed transactions are broadcast to the network to be confirmed and added to the blockchain
- When you create a wallet, the wallet creates the private key and the mathematically-related public key
- Whenever you initiate a transaction, the wallet will create a *public bitcoin address* from the public key
- These are analogous to an email address (public address) and the password to check your email or send an email (private key)
- The public address can be represented as a QR code
- Here is a public address to one of my wallets:

**As usual, it's a bit more complicated*

Bitcoin Basics



- Bitcoins are held in bitcoin **wallets**
- **Transactions** are the transfer of bitcoin from one wallet to another; each wallet is identified with a **public key**
- The **blockchain** is a public ledger where transactions are recorded and verified, i.e., wallets determine who owns what using the blockchain
- Bitcoin ownership is confirmed using a **private key** which is used to **sign** transactions
- Signed transactions are broadcast to the network to be confirmed and added to the blockchain
- When you create a wallet, the wallet creates the private key and the mathematically-related public key
- Whenever you initiate a transaction, the wallet will create a *public bitcoin address* from the public key
- These are analogous to an email address (public address) and the password to check your email or send an email (private key)

Bitcoin Basics



- Bitcoins are held in bitcoin **wallets**
- **Transactions** are the transfer of bitcoin from one wallet to another; each wallet is identified with a **public key**
- The **blockchain** is a public ledger where transactions are recorded and verified, i.e., wallets determine who owns what using the blockchain
- Bitcoin ownership is confirmed using a **private key** which is used to **sign** transactions
- Signed transactions are broadcast to the network to be confirmed and added to the blockchain
- When you create a wallet, the wallet creates the private key and the mathematically-related public key
- Whenever you initiate a transaction, the wallet will create a *public bitcoin address* from the public key
- These are analogous to an email address (public address) and the password to check your email or send an email (private key)
- The public address can be represented as a QR code
- Here is a public address to one of my wallets:



bc1qyg0fck9g5640dwksff3scvvc50r65zeutpz0r7

**As usual, it's a bit more complicated*

To Receive Bitcoin



YOUR WALLET CREATES A **PRIVATE KEY** AND ASSOCIATED **PUBLIC KEY**

E9873D79C6D87DC0FB6A577863338953213303DA61F20BD67FC233AA33263

FC7492E739D8102d91293098B38A74F0B82901369D937A798E4898D93987C9



A **PUBLIC BITCOIN ADDRESS** IS MATHEMATICALLY DERIVED FROM THE PUBLIC KEY

- The bitcoin address is usually presented as a QR code
- It is **shared** so they can send you funds
- It is your receive address
- It is analogous to your bank account number, but...
- You get a new address for every transaction



SENDER SCANS YOUR QR CODE TO SEND BITCOIN TO YOUR WALLET

To Send Bitcoin



TO SEND BITCOIN, USE YOUR WALLET TO SCAN THE QR CODE FOR THE RECEIPT AND DESIGNATE THE AMOUNT TO SEND



YOUR WALLET SIGNS THE TRANSACTION WITH YOUR PRIVATE KEY AND BROADCASTS THE TRANSACTION TO THE NETWORK



THE NETWORK CONFIRMS THE TRANSACTION IS LEGIT AND REASSIGNS THE COINS TO THE RECEIPT. THE TRANSACTION IS 'SETTLED' WHEN RECORDED ON THE BLOCKCHAIN (~10 MINUTES)



To Send & Receive Bitcoin (Lightning)



1. PRESS **RECEIVE** ON YOUR WALLET
2. **ENTER** THE AMOUNT
3. PRESS **CREATE INVOICE**



- AN ADDRESS AND QR CODE ARE CREATED
- **SHARE** THE ADDRESS OR PRESENT THE QR CODE TO THE SENDER



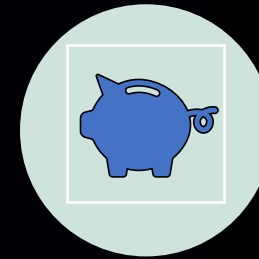
SENDER SCANS YOUR QR CODE TO SEND BITCOIN TO YOUR WALLET INSTANTLY



PRESS **SEND** IN YOUR LIGHTNING WALLET



PASTE INVOICE OR **SCAN** QR CODE



COINS ARE SENT INSTANTLY TO RECEPIENT

Bitcoin Nodes



Bitcoin Nodes



Validating (Full) Nodes

- Independently validate all transactions that occur and have ever occurred on the network (reject bad transactions)
- Independently validate blocks added to the blockchain (reject bad blocks)
- Decentralized consensus
- 10k – 100k full nodes worldwide

Mining Nodes

- Add transactions to blocks
- Add blocks to the blockchain
- Receive mining rewards
- About 100,000 mining nodes worldwide

Lightweight (SPV) Nodes

- Query full nodes to quickly 'validate' transactions and blocks (do not store a copy of the blockchain)
- Used in most cell phone wallets



VALIDATING NODES CONFIRM A TRANSACTION IS LEGIT AND REASSIGNS COINS TO THE RECEIPT. THE TRANSACTION IS 'SETTLED' WHEN RECORDED ON THE BLOCKCHAIN (~10 MINUTES)



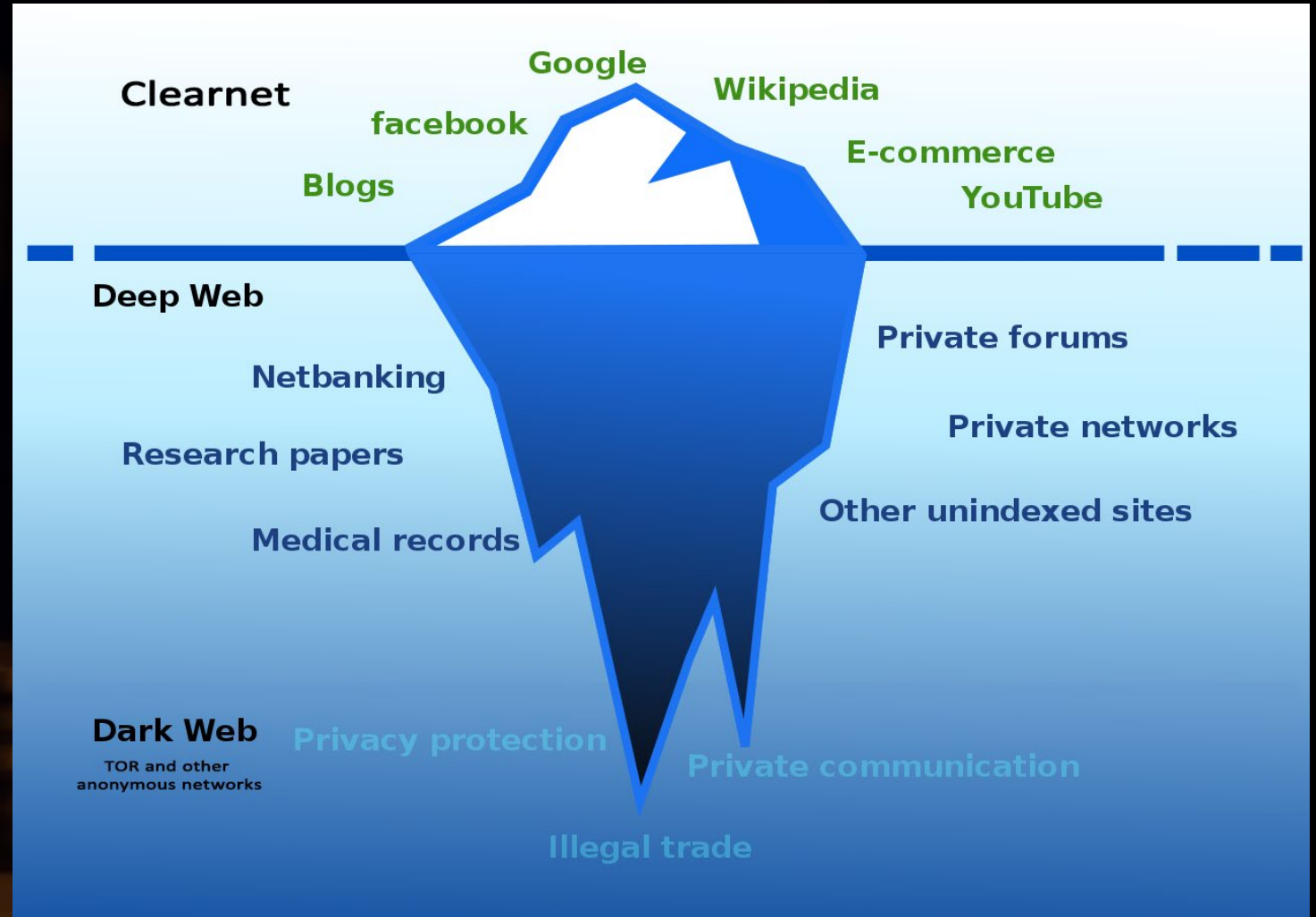
A node is any computer that connects to the Bitcoin network

Bitcoin Nodes



Validating (Full) Nodes

- Independently validate all transactions that occur and have ever occurred on the network (reject bad transactions)
- Independently validate blocks added to the blockchain (reject bad blocks)
- Decentralized consensus
- 10k – 100k full nodes worldwide



Bitcoin Nodes



Validating (Full) Nodes

- Independently validate all transactions that occur and have ever occurred on the network (reject bad transactions)
- Independently validate blocks added to the blockchain (reject bad blocks)
- Decentralized consensus
- 10k – 100k full nodes worldwide

Mining Nodes

- Add transactions to blocks
- Add blocks to the blockchain
- Receive mining rewards
- About 100,000 mining nodes worldwide

Lightweight (SPV) Nodes

- Query full nodes to quickly 'validate' transactions and blocks (do not store a copy of the blockchain)
- Used in most cell phone wallets



A node is any computer that connects to the Bitcoin network

Bitcoin Nodes



Validating (Full) Nodes

- Independently validate all transactions that occur and have ever occurred on the network (reject bad transactions)
- Independently validate blocks added to the blockchain (reject bad blocks)
- Decentralized consensus
- 10k – 100k full nodes worldwide

Mining Nodes

- Add transactions to blocks
- Add blocks to the blockchain
- Receive mining rewards
- About 100,000 mining nodes worldwide

Lightweight (SPV) Nodes

- Query full nodes to quickly 'validate' transactions and blocks (do not store a copy of the blockchain)
- Used in most cell phone wallets



A node is any computer that connects to the Bitcoin network

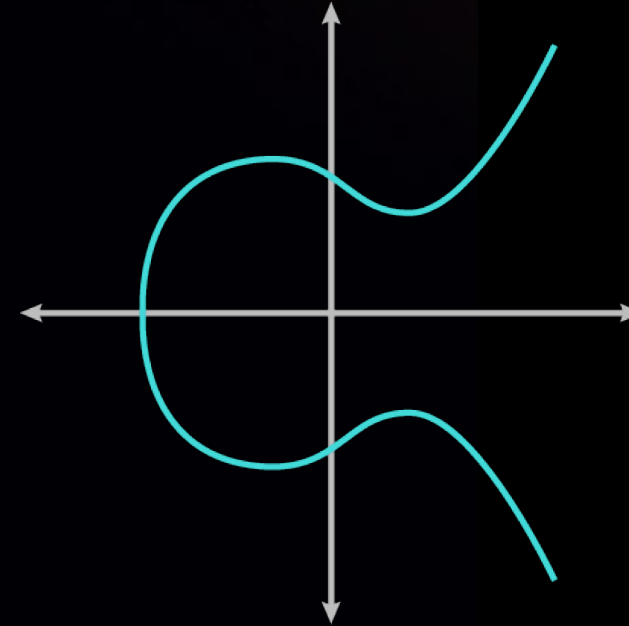
Cryptography & Hashing



Elliptic Curve Cryptography



- The wallet generates the private key using your computer's random number generator
 - *Sometimes, you are asked to provide randomness by wiggling your mouse or rolling dice*
- Bitcoin's private key space is HUGE: $2^{256} = 10^{77}$
 - The universe is believed to have 10^{80} atoms
- The public key is generated from the private key using elliptic curve cryptography; a one-way algorithm
 - *The public key can be derived from the private key, but the private key cannot be derived from the public key*

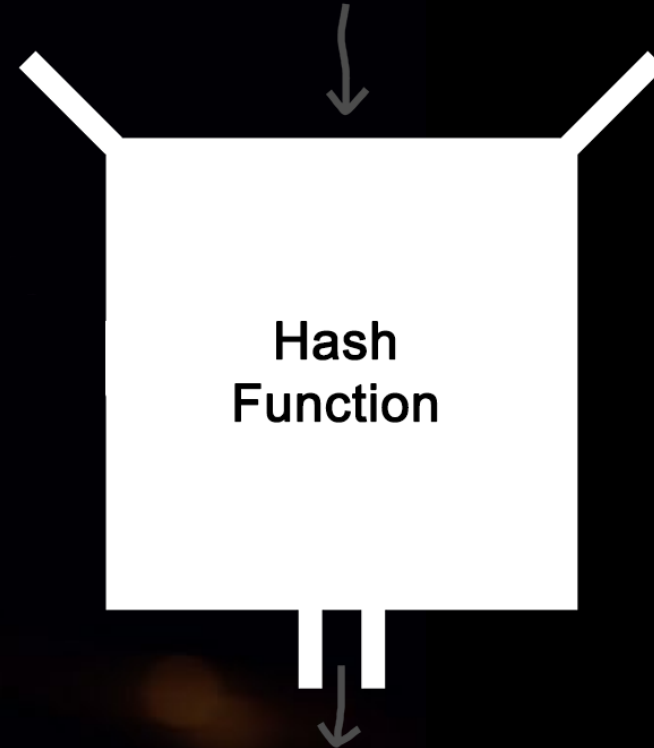


Hashing



- Hashing is a mechanism of converting any string of data into a fixed sized output
- Bitcoin uses SHA256 – a hashing algorithm that produces an output 256 bits long
- No matter how long the input (one letter or a whole movie), the output will always be 256 bits
- The output is unique (like a fingerprint) and can be used to identify the input data

```
01000000018b8abd0508d25087f07fee5fd021e7ec666cfb5e92a99bf5deb18326cec4ed9f000000006b483045
02210085c65501ba621c18763a1d01d3673e24c542ecf3f2f8f3365d272ece0c52f7a50220497ababe3f832bb5
5fd70758357cf572c8d3d20c43e08a1e7fc10666ef6e082a012102834b15b49baf0b19b7645a5522de26a05fdd
4f568669aa5b381e05a646e1c05ffffffff02e9915600000000001976a9142314f60b73a1a6d649052cfc19127ec
ef4e65dd588acddad0700000000001976a914068d92d3c8a1d2797a83cf8c594f0f6b1ea07a1b88ac00000000
```



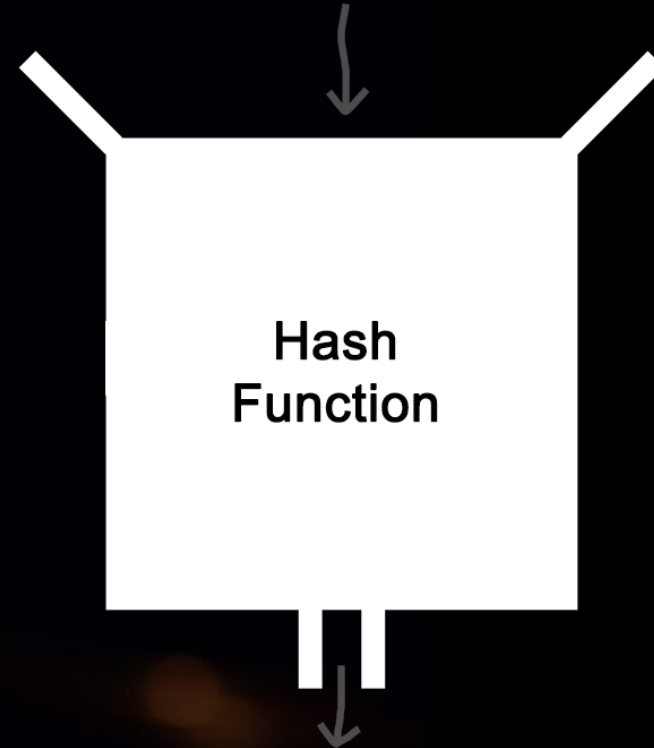
```
4ce18f49ba153a51bcda9bb80d7f978e3de6e81b5fc326f00465464530c052f4
```


Hashing



- Hashing is a mechanism of converting any string of data into a fixed sized output
- Bitcoin uses SHA256 – a hashing algorithm that produces an output 256 bits long
- No matter how long the input (one letter or a whole movie), the output will always be 256 bits
- The output is unique (like a fingerprint) and can be used to identify the input data
- You cannot determine the original data from the result
- The same data always produces the same result
- Different data produces different results

```
01000000018b8abd0508d25087f07fee5fd021e7ec666cfb5e92a99bf5deb18326cec4ed9f000000006b483045
02210085c65501ba621c18763a1d01d3673e24c542ecf3f2f8f3365d272ece0c52f7a50220497ababe3f832bb5
5fd70758357cf572c8d3d20c43e08a1e7fc10666ef6e082a012102834b15b49baf0b19b7645a5522de26a05fdd
4f568669aa5b381e05a646e1c05ffffffff02e9915600000000001976a9142314f60b73a1a6d649052cfc19127ec
ef4e65dd588acddad0700000000001976a914068d92d3c8a1d2797a83cf8c594f0f6b1ea07a1b88ac00000000
```

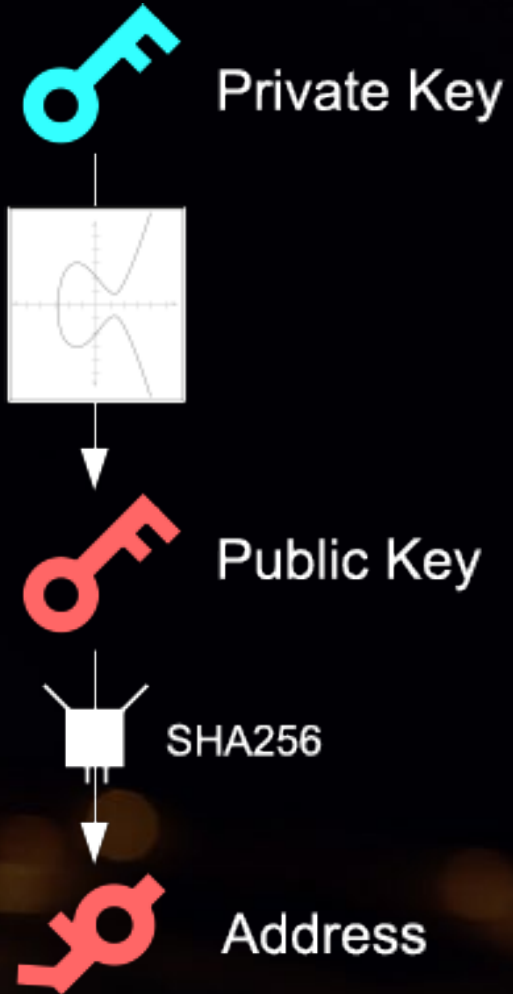


```
4ce18f49ba153a51bcda9bb80d7f978e3de6e81b5fc326f00465464530c052f4
```

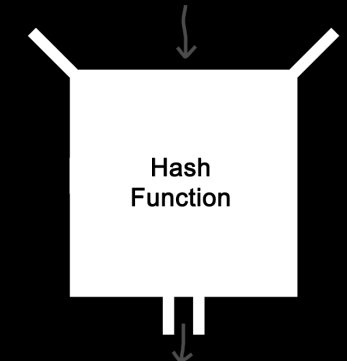
Hashing



- You cannot determine the original data from the result
- The same data always produces the same result
- Different data produces different results
- Bitcoin addresses are derived from the public key by hashing the public key



```
0100000018b8abd0508d2508707fee5fd021e7ec66cfb5e92a99bf5deb18326cec4ed9f000000006b483045
02210085c65501ba621c18763a1d01d3673e24c542ecf3f2f83365d272ece0c527a50220497ababe3f832bb5
5fd70758357cf572c8d3d20c43e08a1e7fc10666ef6e082a012102834b15b49baf0b19b7645a5522de26a05fdd
4f568669aa5b381e05a648e1cd5ffffff02e991560000000000001976a9142314f60b73a1a6d649052cfc19127ec
ef4e65dd58bacddad0700000000001976a914068d92d3c8a1d2797a83cfc8e594f01bb1ea07a1b88ac00000000
```



```
4ce18f49ba153a51bcda9bb80d7f978e3de6e81b5fc326f00465464530c052f4
```

A Hashing Use Case



Imagine....

- The Liberty Champion offers a full scholarship to anyone who solves a very hard Sudoku
- You think you have the solution
- The Champion will not show you the completed puzzle, but they provide a SHA256 hash of the puzzle
- You SHA256 hash your completed puzzle
- If your hash is the same as theirs, you successfully completed the puzzle

			9		2			
	4						5	
		2				3		
2								7
			4	5	6			
6								9
		7				8		
	3						4	
			2		7			

Sudoku

A Hashing Use Case



Imagine....

- The Liberty Champion offers a full scholarship to anyone who solves a very hard Sudoku
- You think you have the solution
- The Champion will not show you the completed puzzle, but they provide a SHA256 hash of the puzzle
- You SHA256 hash your completed puzzle
- If your hash is the same as theirs, you successfully completed the puzzle

		9	2				
4						5	
	2				3		
2			4	5	6		7
6							9
	7					8	
3							4
		2	7				

Data of any length



Hash function

Output of fixed length
(256 bits for SHA256)

1001010100101001...(256)

SHA256



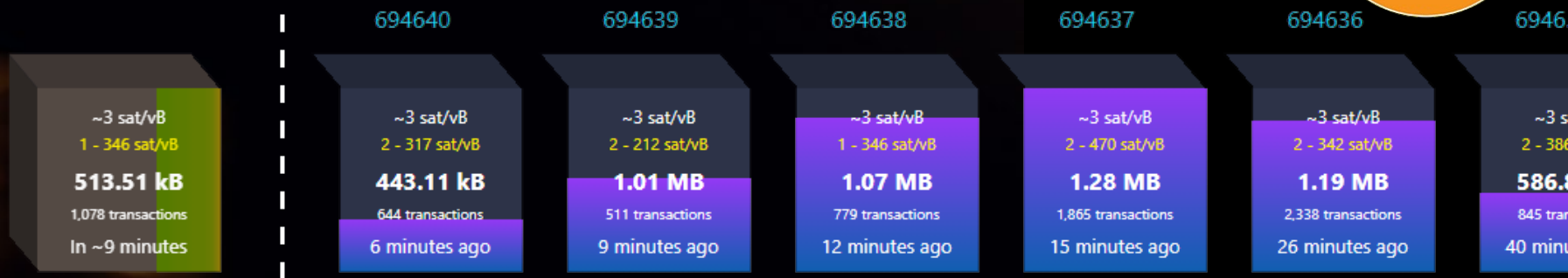
[Play with SHA256](#)



The Blockchain



The Blockchain

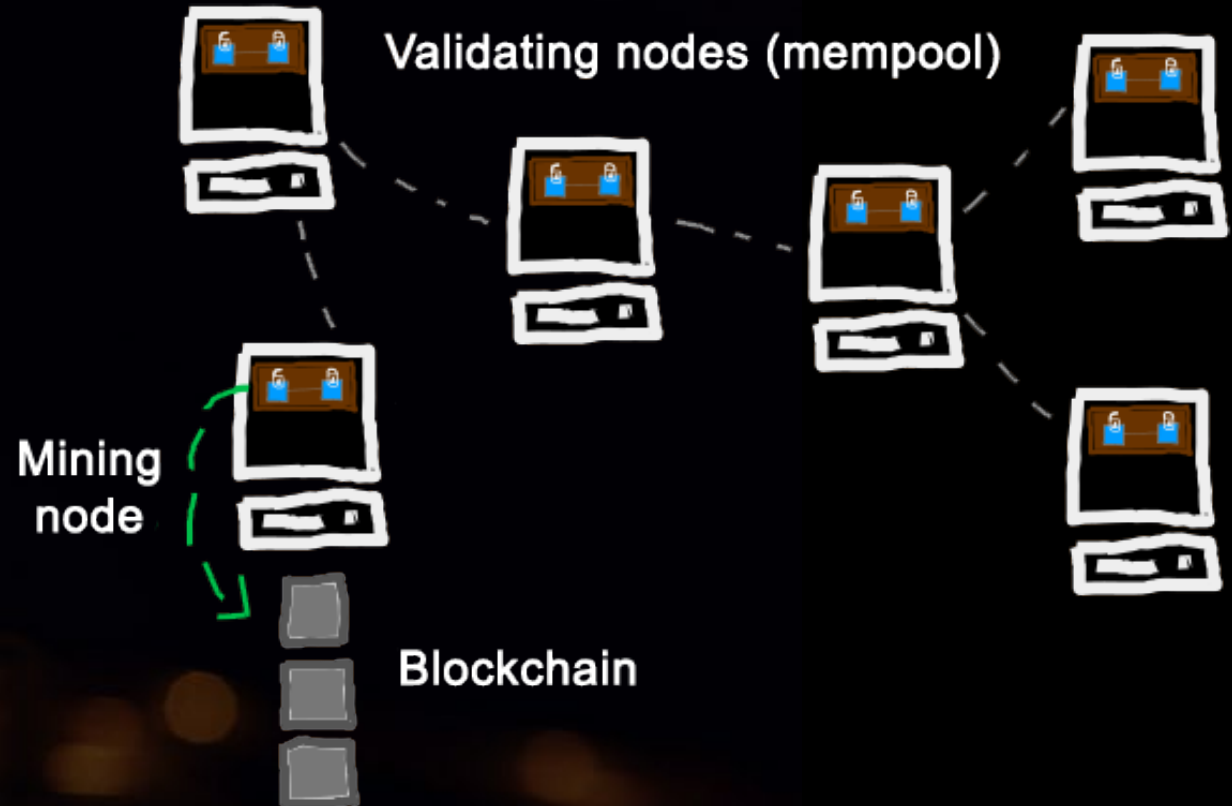


- The blockchain is a public record of transactions
- The blockchain grows one block every 10 minutes (on average)
- Roughly 4,000 transactions can fit in a block

The Blockchain



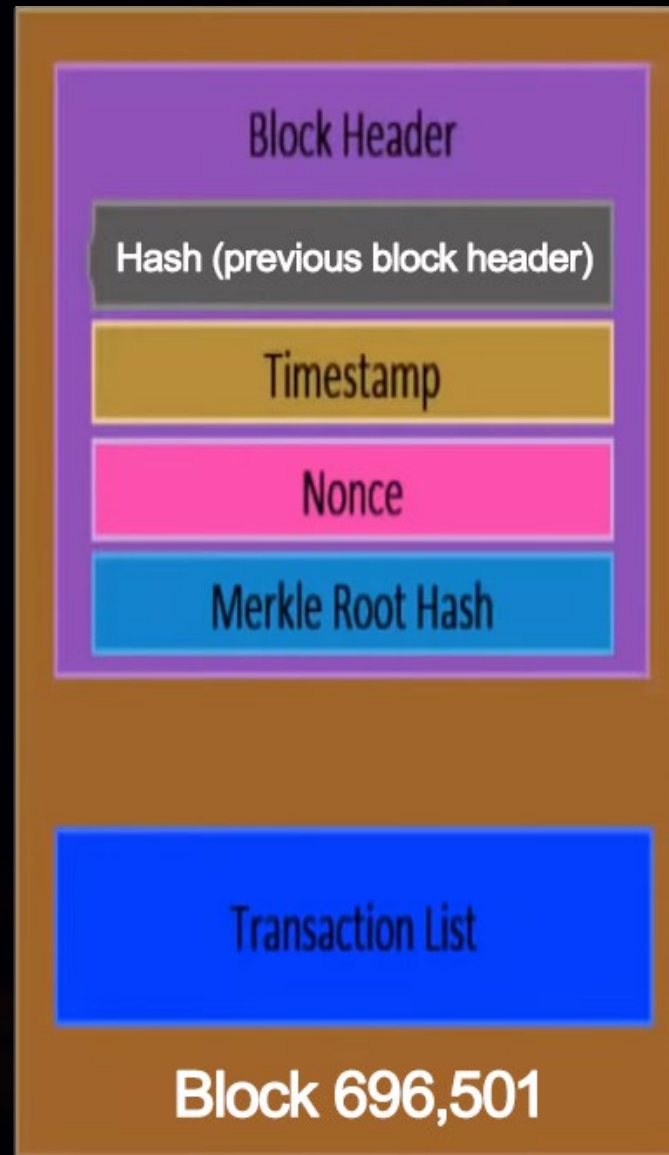
- New transactions are held in a memory pool (mempool) on each full node.
- Miners select transactions from the mempool and place them into a candidate block
- Block size is limited to 1MB (about 4000 transactions)



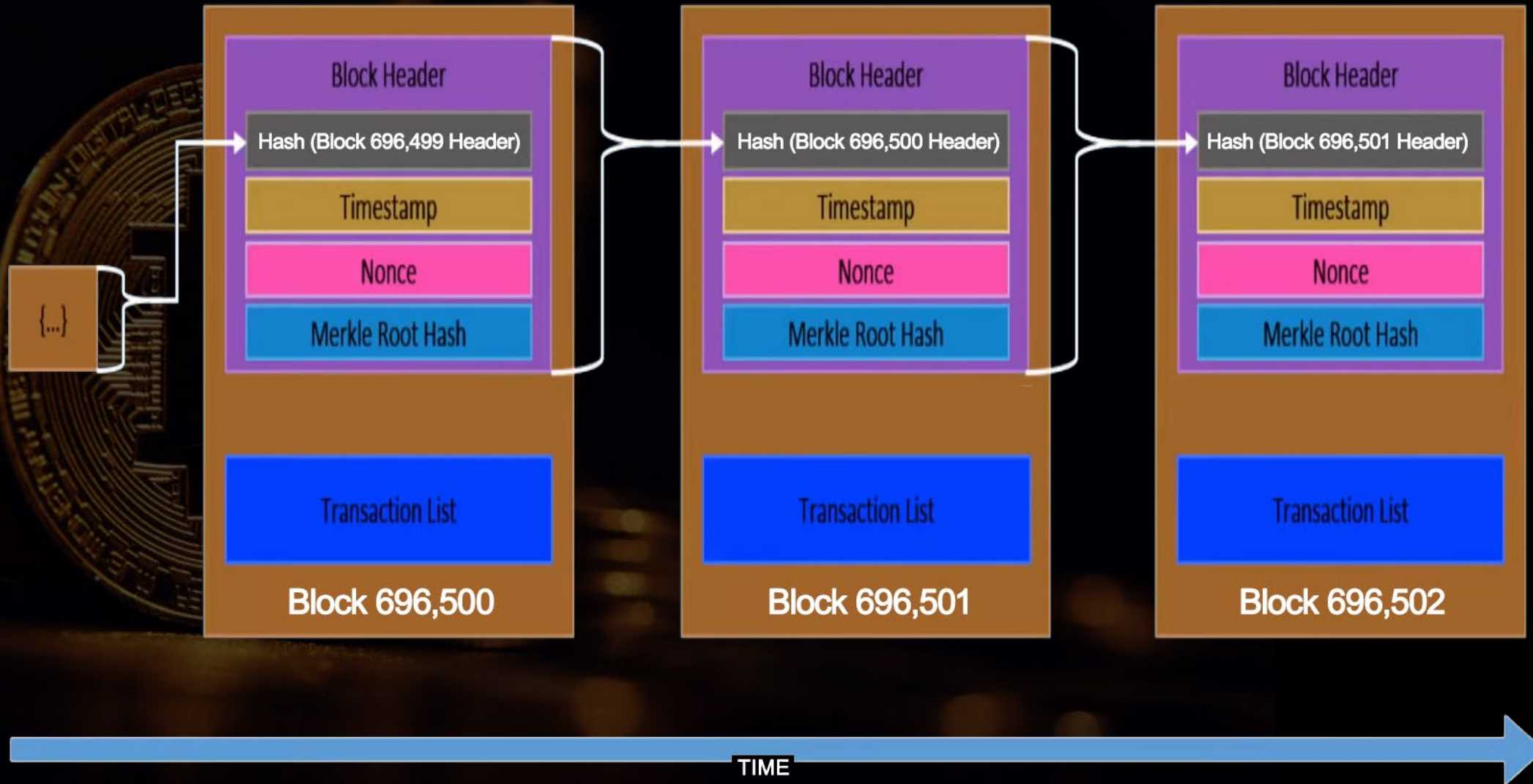
The Blockchain



- New transactions are held in a memory pool (mempool) on each full node.
- Miners select transactions from the mempool and place them into a candidate block
- Block size is limited to 1MB (about 4000 transactions)
- Every block contains
 - List of transactions
 - Merkle tree hash of transactions (compression)
 - Timestamp
 - Nonce (a number N used ONCE) to change the hash output
 - Hash of the *previous block's header*



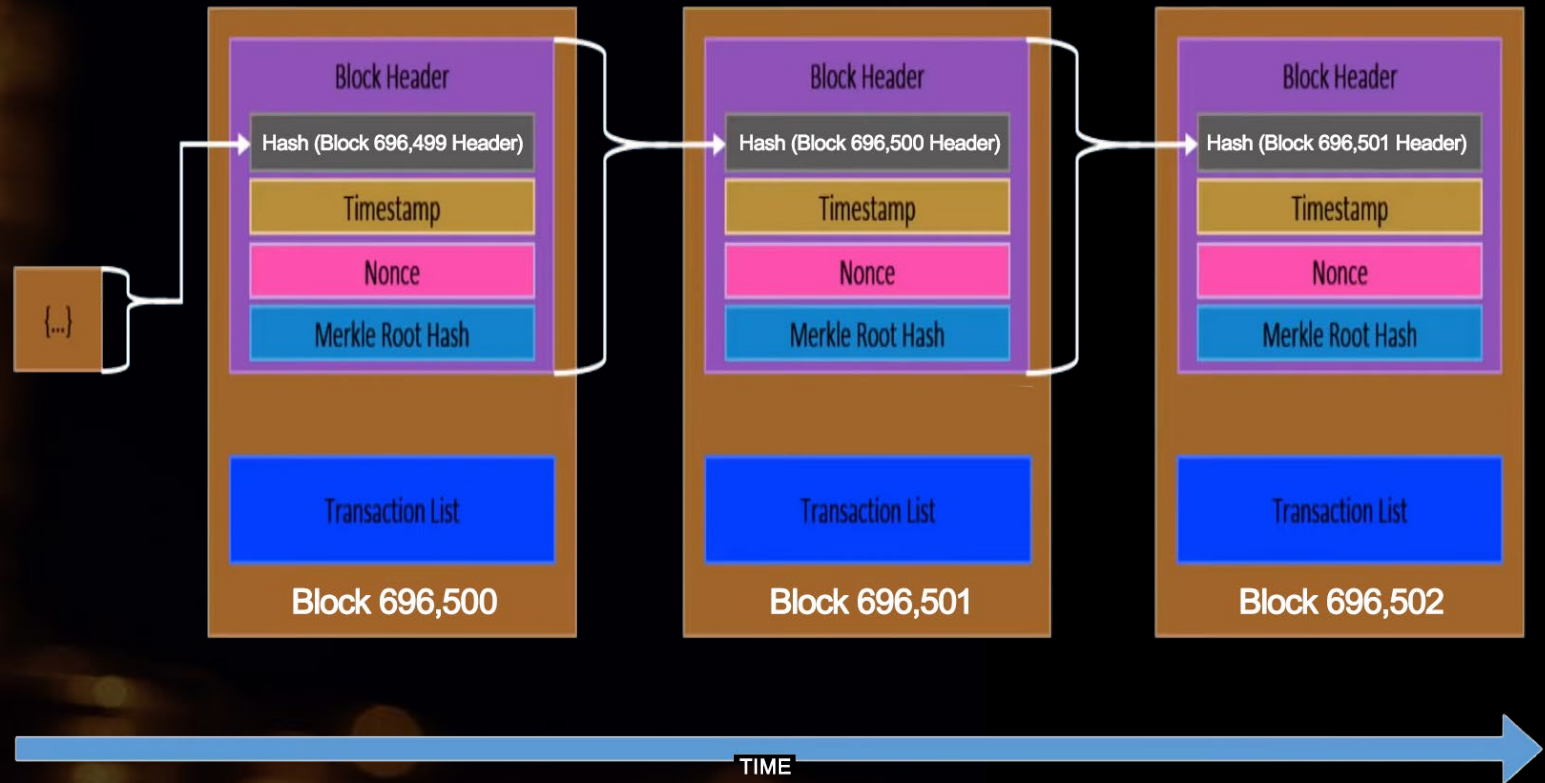
The Blockchain



The Blockchain



- Full nodes keep a complete copy of the blockchain and verify every transaction
- Light (SPV) wallets, e.g. on a cell phone, only keep a copy of the headers
- Complete blockchain = ~ 700 GB
- Headers = ~ 10 MB



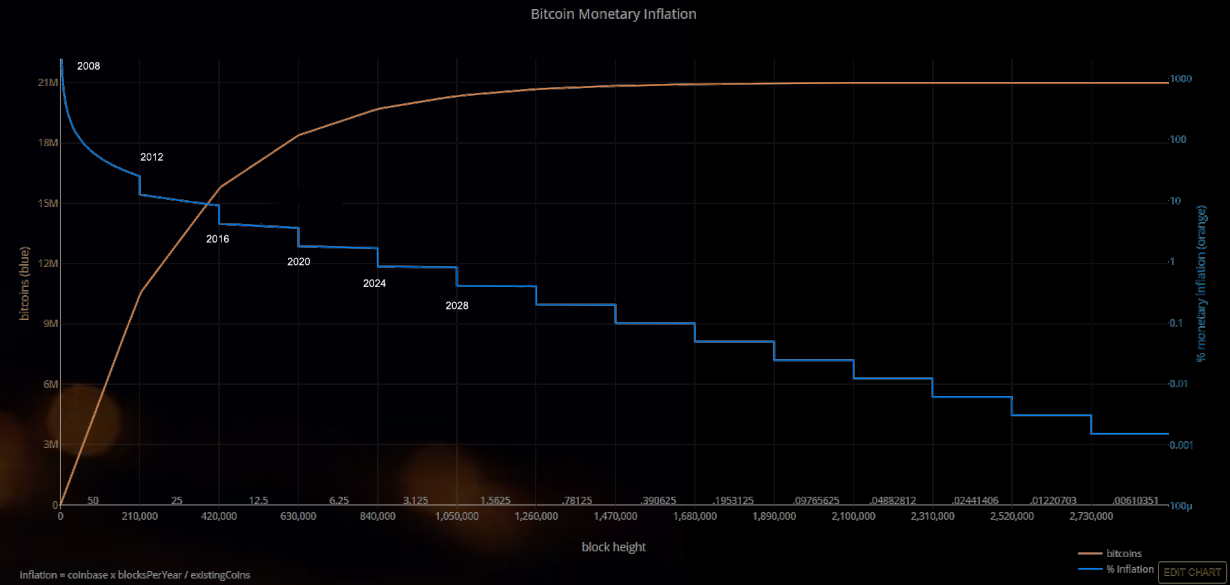
Bitcoin Issuance



<https://mempool.space>



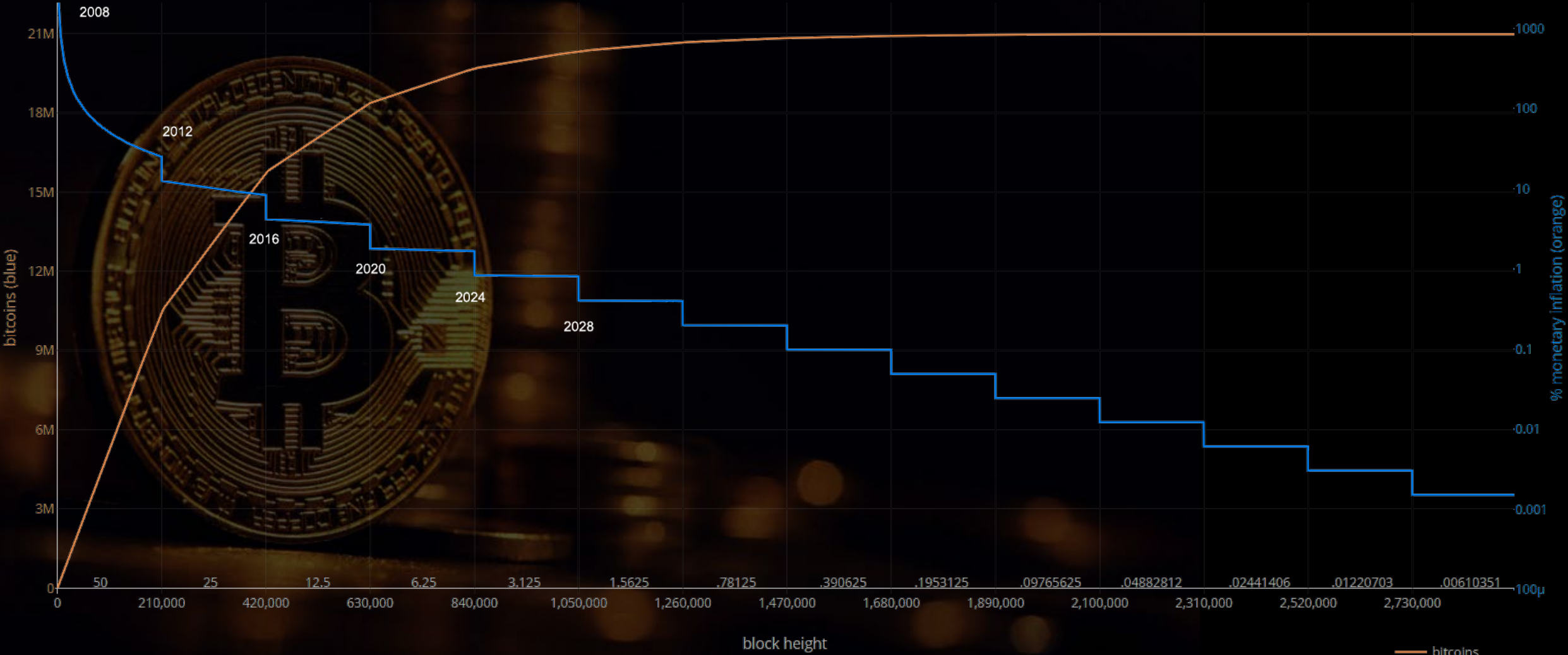
- The first transaction in every block is the coinbase transaction
- New coins are created by this transaction
- New coins are created on a predetermined schedule, with the number of coins created with each block reduced by half every 210,000 blocks
- At 1 block every 10 minutes, halvings occur every four years



Bitcoin Issuance



Bitcoin Monetary Inflation

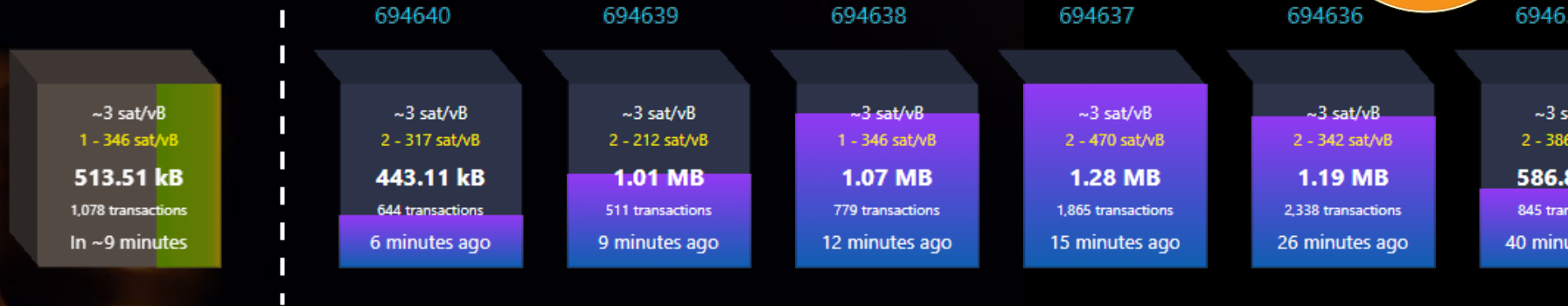


$$\text{inflation} = \frac{\text{coinbase} \times \text{blocksPerYear}}{\text{existingCoins}}$$

Bitcoin Mining



<https://mempool.space>



- New transactions are validated by validating nodes and held in a mempool
- Mining rigs select transactions and place them into a block
- The transaction ID's, the block header, and the previous block header are included in a hash
- Mining rigs race to create a hash with certain properties (a predetermined number of preceding zeros); hash output altered using the *nonce*
- The first mining rig to solve the cryptographic puzzle 'wins' and their block is added to the blockchain – and the miner receives the coinbase reward

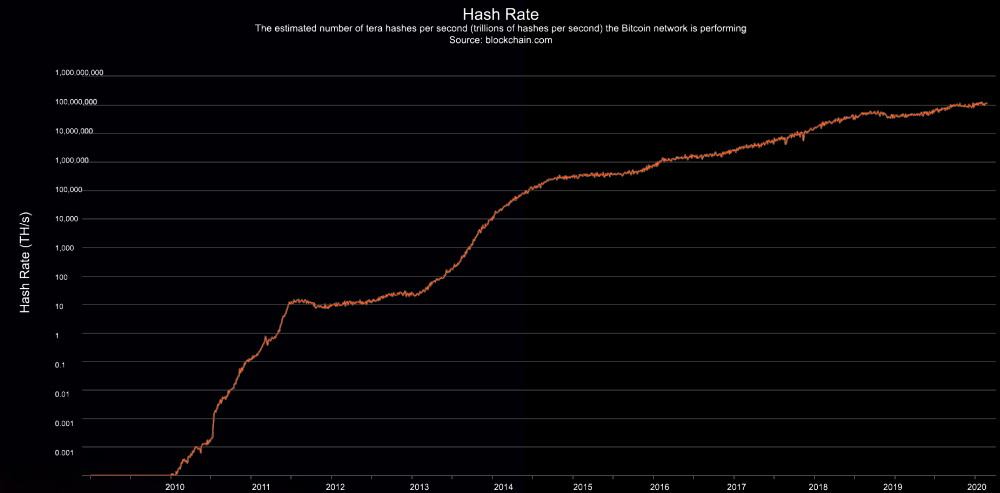
			9	2			
	4					5	
		2				3	
2							7
			4	5	6		
6							9
		7				8	
	3						4
			2	7			

Sudoku

Bitcoin Mining



- The race to solve the puzzle is what consumes energy – the competition has produced mining rigs that are extremely powerful (100+ TH/s)
- When miners solve the puzzle, the block is added to the blockchain and they receive new coins as a reward. Some coins are converted to fiat to pay electric bills; the rest are kept or sold for profit
- Bitcoin is programmed to create a new block every 10 minutes on average
- If lots of miners join the network, the difficulty of the puzzle is increased to make sure blocks are not created too quickly
- If lots of miners leave the network, the difficulty of the puzzle is decreased to make sure blocks are not mined too slowly
- This is the *difficulty adjustment*



The “Transaction Chain”



The “Transaction Chain”



- There are in fact ***no coins*** in the bitcoin protocol, only transactions
- There are transaction inputs (to receive “coins”) and transaction outputs (to send “coins”)
- “*Bitcoins*” are nothing more than unspent transaction outputs (UTXOs)
- Every transaction is linked to previous transactions

Transaction format

<u>Input</u>	<u>Output</u>
Previous transaction ID (A previous TX output)	Amount
+	+
Signature (Associated with a private key)	Public Key (Bitcoin Address)
A “bitcoin”	

The “Transaction Chain”



Transaction format

Multiple Inputs & Outputs

Inputs \geq Outputs
Inputs – Outputs = Fees

Inputs

TXID 6, IDX 3, Dsig1
3 BTC

TXID 20, IDX 2, Dsig2
2 BTC

TXID 42, IDX 5, Dsig3
5 BTC

Outputs

Bitcoin Address 1
6 BTC

Bitcoin Address 2
3 BTC

Bitcoin Address 3
0.9 BTC

0.1 BTC

Sender's
Change

Miner's
Fee

The “Transaction Chain”



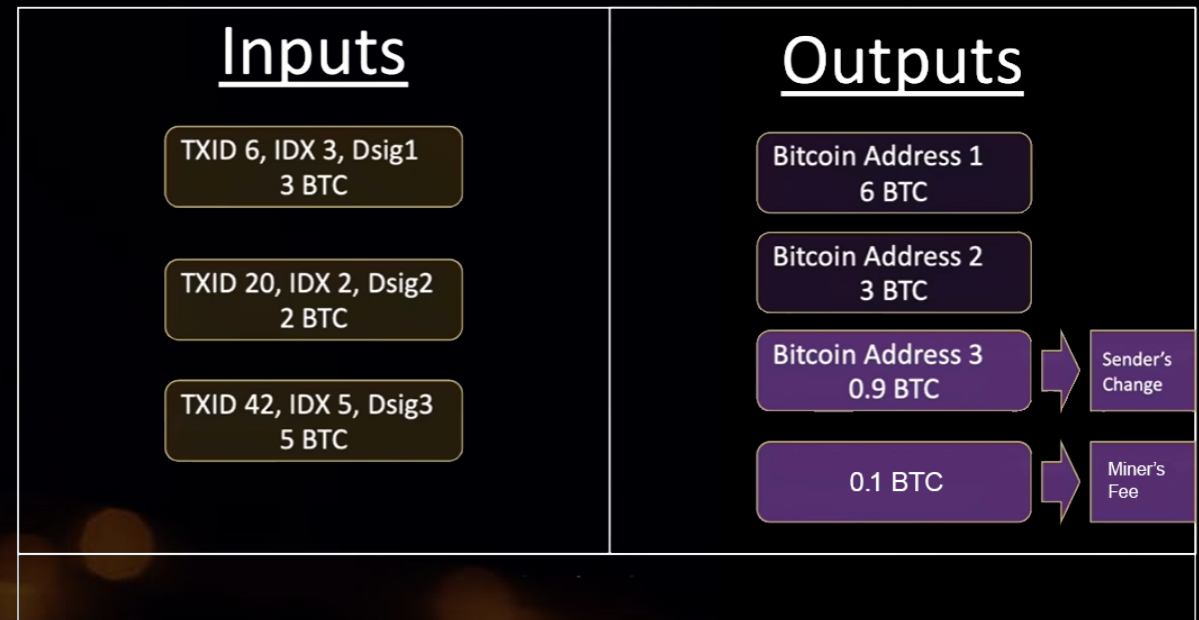
- All transactions are recorded on the blockchain (including UTXOs), but
- A database of UTXOs is stored separately in Bitcoin Core
- This database may also be stored in SPV (light) wallets

Transaction format

Multiple Inputs & Outputs

Inputs \geq Outputs

Inputs – Outputs = Fees



The "Transaction Chain"



Alice wants to send Bob 77k sats

ALICE'S wallet




Public address
from public key

bc1qyg0fck9g5640dwxkff3cvcv50r65zeutpz0r7

- UTXO (10k sats)
- UTXO (75k sats)
- UTXO (5k sats)
- UTXO (20k sats)

Digital signature
from private key

BOB'S wallet



Public address
from public key

bc1qyg0fck9g5640dwxkff3cvcv50r65zeutpz0r7

UTXO (2k sats)

Digital signature
from private key

The "Transaction Chain"



Alice wants to send Bob 77k sats

ALICE'S wallet



Public address
from public key

bc1qyp0fck9g5640dwxkf33cvcv50r65zeutpz0r7

UTXO (10k sats)
UTXO (75k sats)
UTXO (5k sats)
UTXO (20k sats)

Digital signature
from private key

1. Alice scans Bob's public address QR code (derived from his public key)
2. Alice enters the amount, and her wallet selects the UTXOs
3. Her wallet signs the tx with a digital signature (derived from her private key)

BOB'S wallet



Public address
from public key

bc1qyp0fck9g5640dwxkf33cvcv50r65zeutpz0r7

UTXO (2k sats)


Digital signature
from private key

The "Transaction Chain"



Alice wants to send Bob 77k sats

ALICE'S wallet



Public address
from public key


bc1qyg0fck9g5640dwxkff3scvvc50r65zeutpz0r7

UTXO (10k sats)
UTXO (75k sats)
UTXO (5k sats)
UTXO (20k sats)

Digital signature
from private key

1. Alice scans Bob's public address QR code (derived from his public key)
2. Alice enters the amount, and her wallet selects the UTXOs
3. Her wallet signs the tx with a digital signature (derived from her private key)

BOB'S wallet



Public address
from public key

bc1qyg0fck9g5640dwxkff3scvvc50r65zeutpz0r7

UTXO (2k sats)


Digital signature
from private key

The "Transaction Chain"



Alice wants to send Bob 77k sats

ALICE'S wallet



Public address
from public key

bc1qyg0fck9g5640dwxkff3scvvc50r65zeutpz0r7

UTXO (10k sats)
UTXO (75k sats)
UTXO (5k sats)
UTXO (20k sats)


A white-bordered box representing Alice's wallet interface. It contains a QR code on the left and a red key icon with the text "Public address from public key" on the right. Below the QR code is a small alphanumeric string. The bottom half of the box lists four UTXOs with their respective amounts in sats.

Digital signature
from private key

A blue key icon is positioned to the left of the text "Digital signature from private key". The entire text and icon are enclosed in a yellow oval.

1. Alice scans Bob's public address QR code (derived from his public key)
2. Alice enters the amount, and her wallet selects the UTXOs
3. Her wallet signs the tx with a digital signature (derived from her private key)

BOB'S wallet



Public address
from public key

bc1qyg0fck9g5640dwxkff3scvvc50r65zeutpz0r7

UTXO (2k sats)

A white-bordered box representing Bob's wallet interface. It contains a QR code on the left and a red key icon with the text "Public address from public key" on the right. Below the QR code is a small alphanumeric string. The bottom half of the box shows a single UTXO with its amount in sats.


Digital signature
from private key

A blue key icon is positioned to the left of the text "Digital signature from private key".

The "Transaction Chain"



ALICE'S wallet



Public address
from public key

bc1qyg0fck9g5640dwxkff3scvvc50r65zeutpz0r7

UTXO (10k sats)
UTXO (20k sats)
UTXO (3k sats)


Digital signature
from private key

Alice wants to send Bob 77k sats

1. Alice scans Bob's public address QR code (derived from his public key)
2. Alice enters the amount
3. Her wallet signs the tx with a digital signature (derived from her private key)

The 77k sats are sent by creating a new UTXO associated with Bob's wallet and a 'change' UTXO in Alice's wallet

BOB'S wallet



Public address
from public key

bc1qyg0fck9g5640dwxkff3scvvc50r65zeutpz0r7

UTXO (2k sats)
UTXO (77k sats)

Digital signature
from private key

The Lightning Network



The Blockchain



- The blockchain is a public record of transactions
- The blockchain grows one block every 10 minutes (on average)
- Roughly 4,000 transactions can fit in a block
- Therefore, max transaction rate = 6-7 transactions/second

The Blockchain



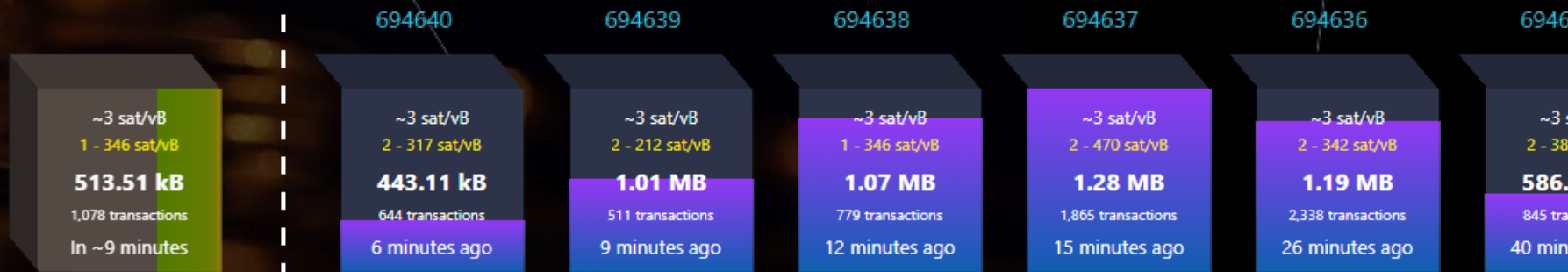
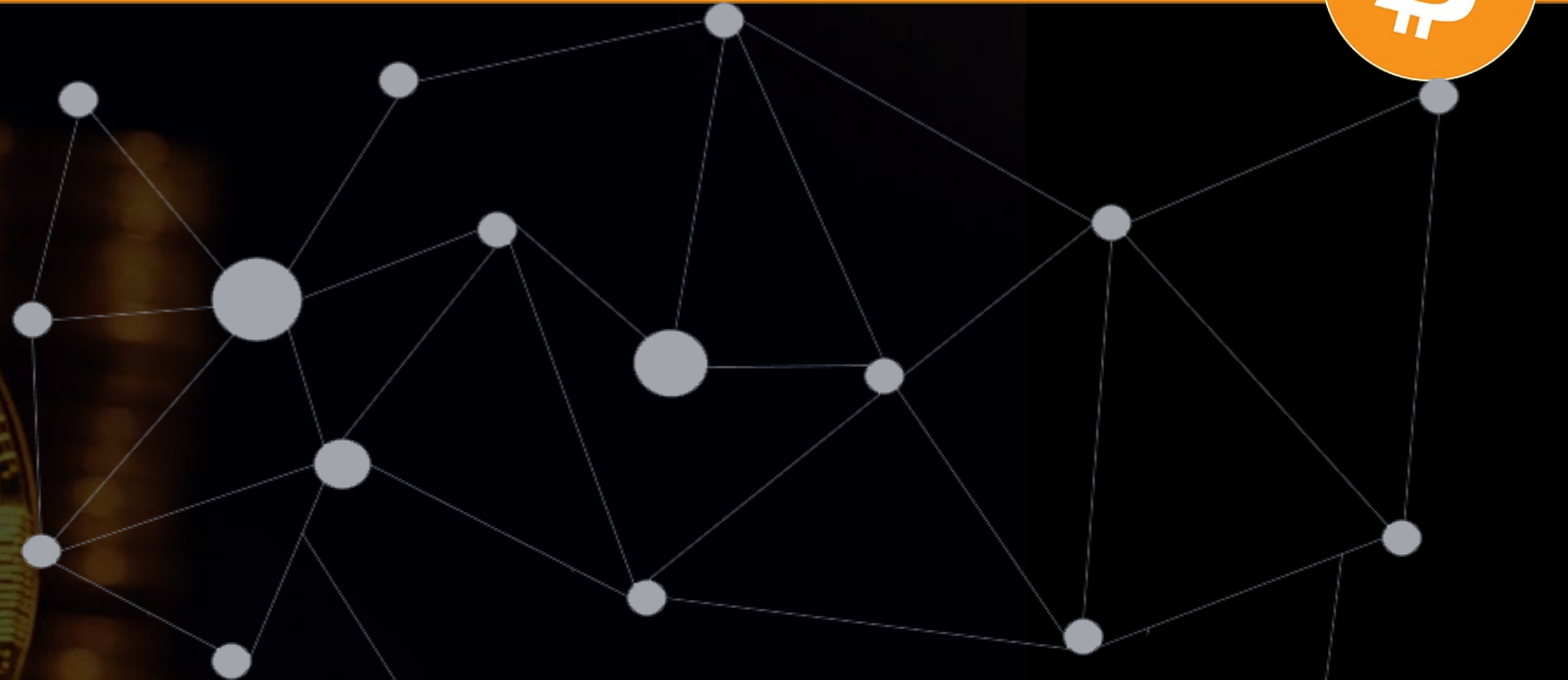
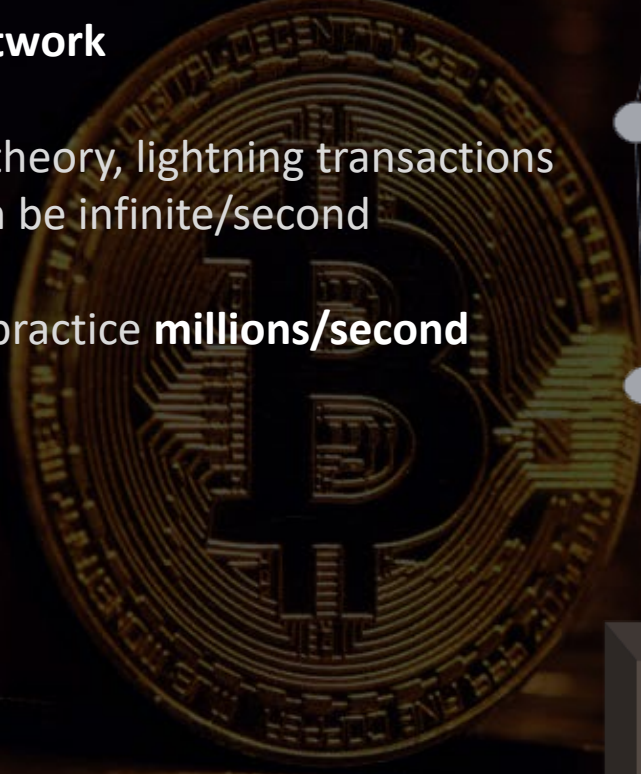
- The blockchain is a public record of transactions
- The blockchain grows one block every 10 minutes (on average)
- Roughly 4,000 transactions can fit in a block
- Therefore, max transaction rate = 6-7 transactions/second

VISA can do 65,000 transactions/second

The Lightning Network



- The speed of Bitcoin is accelerated by a second-layer solution called the **LIGHTNING network**
- In theory, lightning transactions can be infinite/second
- In practice **millions/second**



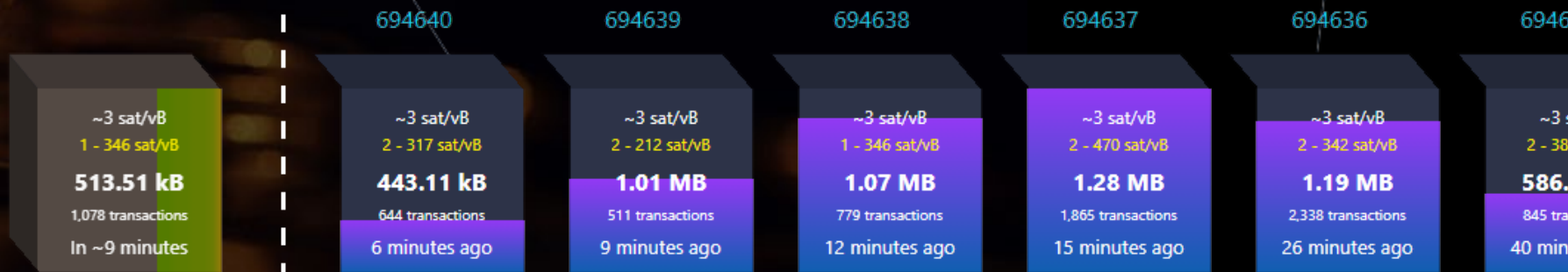
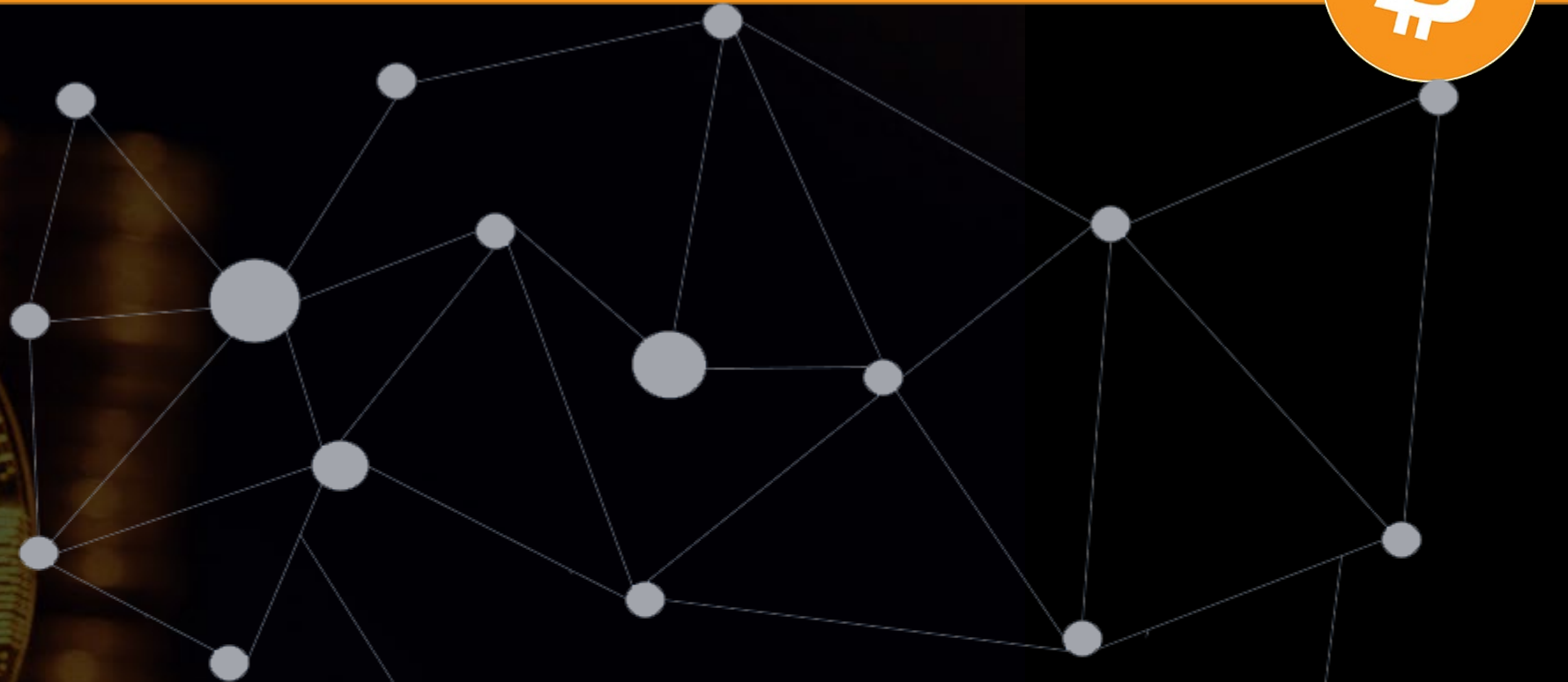
The Lightning Network



- The speed of Bitcoin is accelerated by a second-layer solution called the **LIGHTNING network**
- In theory, lightning transactions can be infinite/second
- In practice **millions/second**
- **Lightning wallets** make use of this off-chain network

My Favorites:

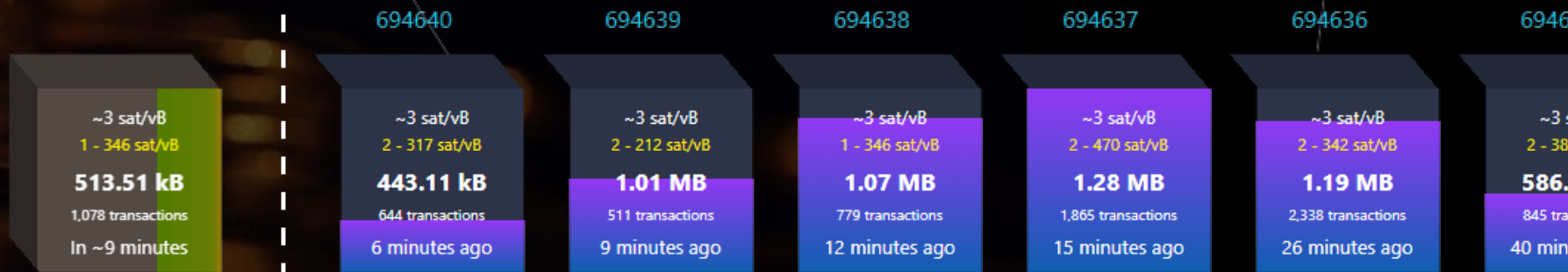
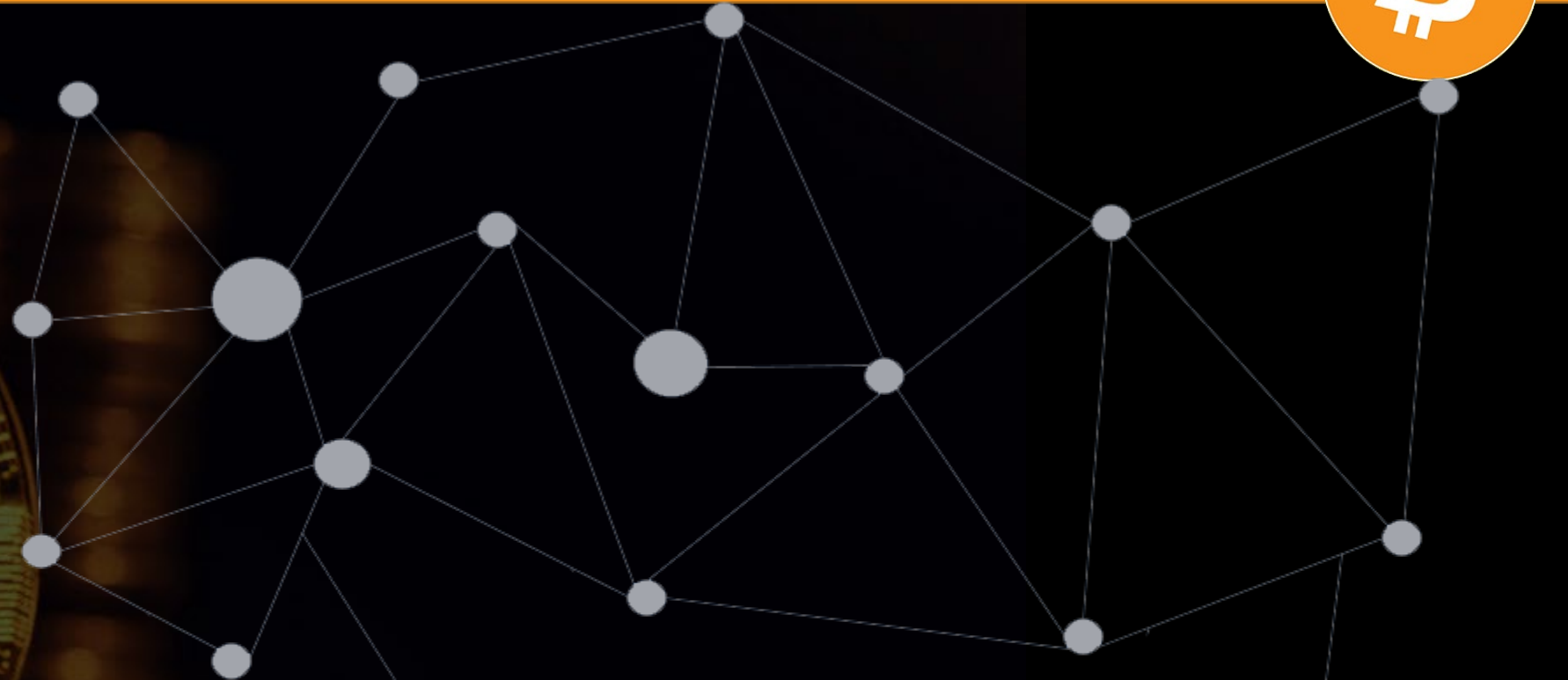
- Wallet of Satoshi
- Aqua wallet
- Strike
- Cash App



The Lightning Network



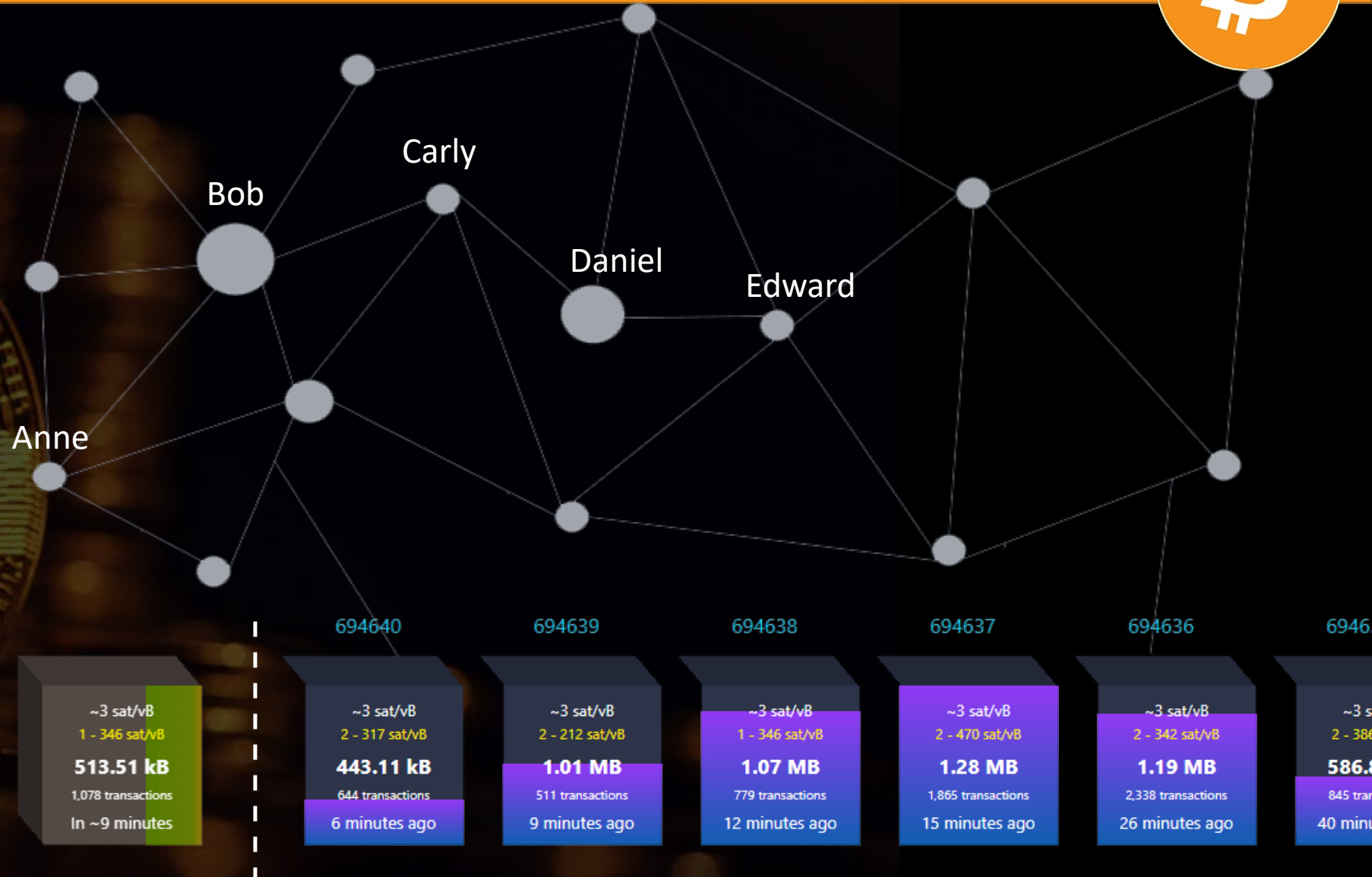
- Lightning nodes are run by individuals, like bitcoin nodes
- Payment channels are created between nodes
- Bitcoin payments can be sent across these channels extremely fast (seconds)
- A direct channel not required for buyer and seller; payments can be routed through intermediate nodes



The Lightning Network



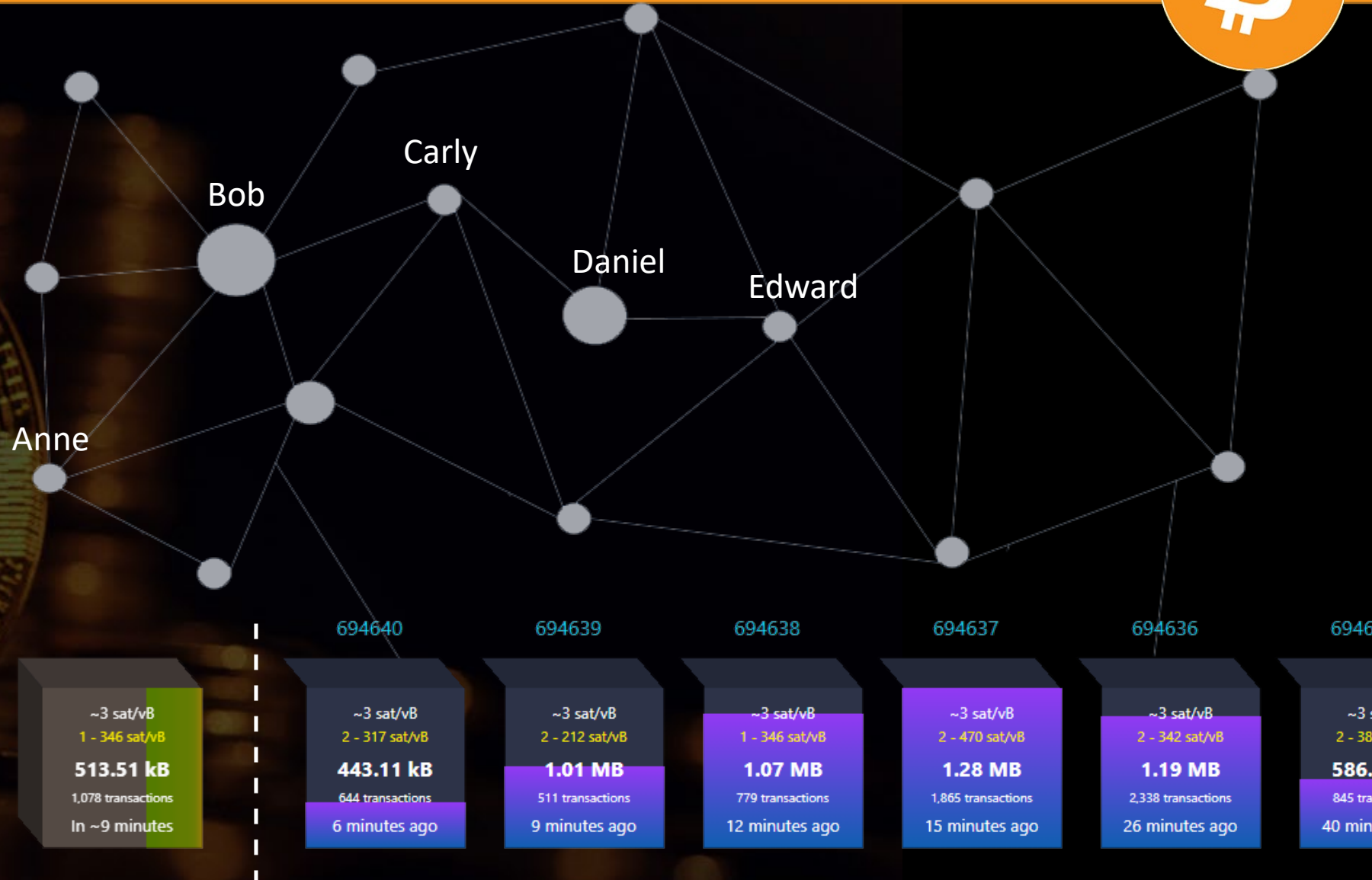
- Lightning nodes are run by individuals, like bitcoin nodes
- Payment channels are created between nodes
- Bitcoin payments can be sent across these channels extremely fast (seconds)
- A direct channel not required for buyer and seller; payments can be routed through intermediate nodes



The Lightning Network



- As Bitcoin adoption increases, it's likely that most daily transactions will be done on second layer solutions
- Main chain transactions might be reserved for nation state or global bank settlements



Running Your Own Bitcoin Node



<https://mempool.space>

Running Your Own Bitcoin Node



- To run your own full (validating) node, you only need to download and install **Bitcoin Core** on any computer
- Best practices:
 - Use a **dedicated computer** that is online 24/7/365
 - Use **Linux** operating system
- A single-board **Raspberry Pi** is ideal
- **1 TB hard drive** (minimum) to hold the entire blockchain
- **Third-party** hardware & applications available to make it easier!



Running Your Own Bitcoin Node



www.mynodebtc.com

mynode

Core Services

Bitcoin Running	Height: 697753 Peers: 21 Difficulty: 1.78e+13 Mempool Size: 0.203 MB Version: v0.21.1	Lightning Running	On-chain Balance: 53,472 Lightning Balance: 2,489,604 Peers: 5 Channels: 5 Version: v0.12.1
---------------------------	---	-----------------------------	---

Apps

RTL Lightning Wallet	Electrum Server Running	BTCPay Server Merchant Tool	Mempool Mempool Viewer	LND Hub BlueWallet Backend
RTL Disable	Info Disable	BTCPay Server Disable	Mempool Disable	LND Hub Disable
Explorer BTC RPC Explorer	Dojo Mixing Tool	Whirlpool Mixing Tool	JoininBox JoinMarket Mixing	Thunderhub Lightning Wallet
Explorer Disable	Enable	Enable	Info	Enable

Windows taskbar: File Explorer, Chrome, Firefox, mynode, Telegram, Word, Excel, Outlook, Premiere Pro, Photoshop, OBS, Teams, PowerToys



Running Your Own Bitcoin Node



www.umbrel.com

Good afternoon, BRB.

Live Usage			Bitcoin Node		mempool	
CPU 69%	Memory 4.94 GB	Storage 848 GB	Connections 12 peers	Mempool 233.1 MB	No priority 2 sat/vB	Low priority 9 sat/vB
			Hashrate 780 EH/s	Blockchain size 700.7 GB	Medium priority 11 sat/vB	High priority 12 sat/vB

Bitcoin Node, BlueWallet Lightni..., BTCPay Server, Electrs, Lightning Node, Lightning Terminal, mempool, Ride The Lightning

Search Ctrl+K



Wallets, Keys & Seeds



Wallets, Keys, & Seeds



- The simplest wallet is a device that stores your private key
- A software wallet is software that generates a private key, a public key, bitcoin addresses, and talks to the bitcoin network

Types of Wallets

1. **Brain wallet** – private key stored in your head (not recommended)
2. **Paper wallet** – private key stored on paper
3. **Desktop wallet** – private key stored on your computer
4. **Mobile Wallet** – private key stored on your phone
5. **Hardware wallet** – private key stored on specialized hardware

Bitcoin Wallets



- The simplest wallet is a device that stores your private key
- A software wallet is software that generates a private key, a public key, bitcoin addresses, and talks to the bitcoin network

Types of Wallets

1. **Brain wallet** – private key stored in your head (not recommended)
2. **Paper wallet** – private key stored on paper
3. **Desktop wallet** – private key stored on your computer
4. **Mobile Wallet** – private key stored on your phone
5. **Hardware wallet** – private key stored on specialized hardware

Custodial wallet = someone else stores your seed words (i.e, private key)

“Not your keys, not your coins!”

Bitcoin Wallets



- The simplest wallet is a device that stores your private key
- A software wallet is software that generates a private key, a public key, bitcoin addresses, and talks to the bitcoin network

Types of Wallets

1. **Brain wallet** – private key stored in your head (not recommended)
2. **Paper wallet** – private key stored on paper
3. **Desktop wallet** – private key stored on your computer
4. **Mobile Wallet** – private key stored on your phone
5. **Hardware wallet** – private key stored on specialized hardware

Custodial wallet = someone else stores your seed words (i.e, private key)

“Not your keys, not your coins!”

Hot wallet = a wallet connected to the internet

Cold wallet = a wallet that never connects to the internet (safest)



My favorites:

Types of Wallets

Seedsigner



1. **Brain wallet** – private key stored in your head (not recommended)

2. **Paper wallet** – private key stored on paper (cold wallet)

Sparrow wallet



3. **Desktop wallet** – private key stored on your computer (hot wallet)

Blue wallet



4. **Mobile Wallet** – private key stored on your phone (hot wallet)

Coldcard



5. **Hardware wallet** – private key stored on specialized hardware (cold wallet)

Private Key



- Your wallet generates a private key. **You never see it.**
 - 110100101110010100000101001010001100101011010010100101000100101001010100....(256 bits)
 - E9873D79C6D87DC0FB6A577863338953213303DA61F20BD67FC233AA33262
- To make backup easier, your wallet's private key is converted to a series of words (usually 12 or 24) known as your **seed words (or seed phrase)**
- You write down the seed words with **pencil/pen and paper** – NEVER ELECTRONICALLY (don't even take a picture of it) and store it in a safe place, like you would diamonds or gold coins
- Whoever has access to your seed words has access to your coins
- If you lose your seed words, you lose your coins
- If your wallet is lost or destroyed, you can **recover** your coins using the seed words

Seed Words



- Your wallet generates a private key. *You never see it.*
 - 110100101110010100000101001010001100101011010010100101000100101001010100....(256 bits)
 - E9873D79C6D87DC0FB6A577863338953213303DA61F20BD67FC233AA33262
- To make backup easier, your wallet's private key is converted to a series of words (usually 12 or 24) known as your **seed words (or seed phrase)**
- You write down the seed words with **pencil/pen and paper** – NEVER ELECTRONICALLY (don't even take a picture of it) and store it in a safe place, like you would diamonds or gold coins
- Whoever has access to your seed words has access to your coins
- If you lose your seed words, you lose your coins
- If your wallet is lost or destroyed, you can **recover** your coins using the seed words

1. spot
2. chimney
3. energy
4. lift
5. rugged
6. season
7. mystery
8. airplane
9. jungle
10. silence
11. tool
12. energy

Seed Words



- Your wallet generates a private key. *You never see it.*
 - 110100101110010100000101001010001100101011010010100101000100101001010100....(256 bits)
 - E9873D79C6D87DC0FB6A577863338953213303DA61F20BD67FC233AA33262
 - To make backup easier, your wallet's private key is converted to a series of words (usually 12 or 24) known as your *seed words (or seed phrase)*
 - You write down the seed words with **pencil/pen and paper** – NEVER ELECTRONICALLY (don't even take a picture of it) and store it in a safe place, like you would diamonds or gold coins
 - Whoever has access to your seed words has *access to your coins*
 - If you lose your seed words, you *lose your coins*
 - If your wallet is lost or destroyed, you can *recover* your coins using the seed words
1. spot
 2. chimney
 3. energy
 4. lift
 5. rugged
 6. season
 7. mystery
 8. airplane
 9. jungle
 10. silence
 11. tool
 12. energy

Seed Words



- Your wallet generates a private key.
 - 110100101110010100000101001010001100101011010010100101000100101001010100....(128 or 256 bits)
- Your wallet converts the private key into seed (12 or 24) words.

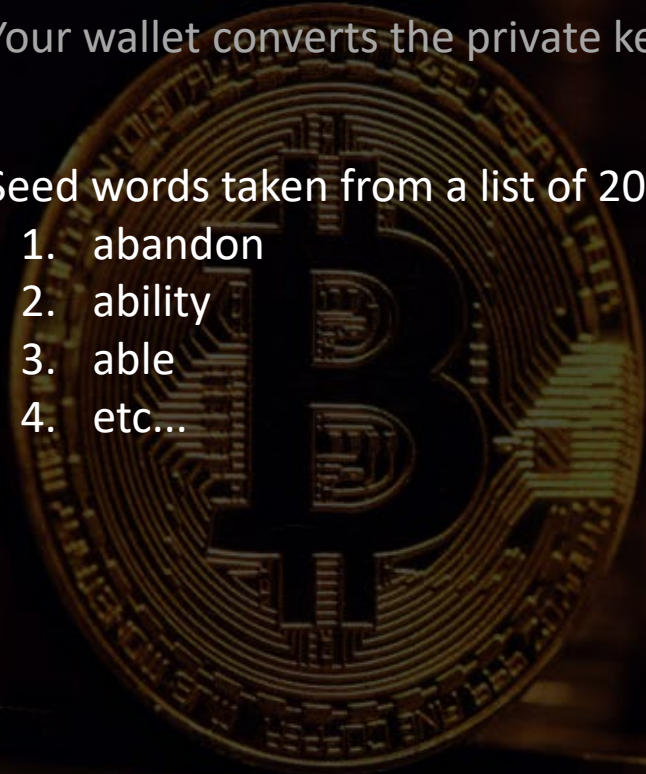
1. spot
2. chimney
3. energy
4. lift
5. rugged
6. season
7. mystery
8. airplane
9. jungle
10. silence
11. tool
12. energy



Seed Words



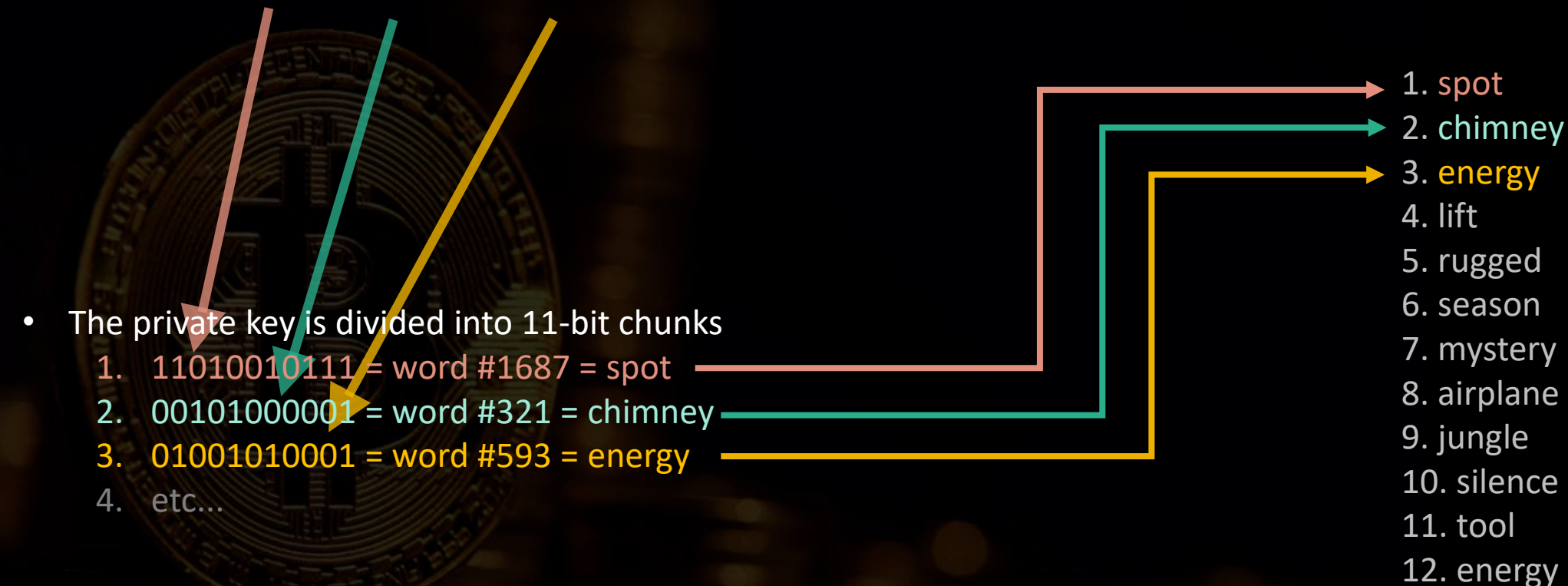
- Your wallet generates a private key.
 - 110100101110010100000101001010001100101011010010100101000100101001010100....(128 or 256 bits)
- Your wallet converts the private key into seed (12 or 24) words.
- Seed words taken from a list of 2048 English words (called BIP39 word list)
 1. abandon
 2. ability
 3. able
 4. etc...
 5. rugged
 6. season
 7. mystery
 8. airplane
 9. jungle
 10. silence
 11. tool
 12. energy



Seed Words



- Your wallet generates a private key.
 - 110100101110010100000101001010001100101011010010100101000100101001010100...(128 or 256 bits)



- The private key is divided into 11-bit chunks
 - 11010010111 = word #1687 = spot
 - 00101000001 = word #321 = chimney
 - 01001010001 = word #593 = energy
 - etc...
- Seed words taken from a list of 2048 English words (called [BIP39](#) word list)
 - abandon
 - ability
 - able
 - etc...

Bitcoin Energy Use



Bitcoin Energy Use



- The world produces 167,617 TWh of electricity annually
- The world consumes 117,098 TWh of electricity annually
 - = 50,520 TWh of electricity *wasted* annually
- Bitcoin consumes 79 TWh of electricity annually
- The amount of electricity *wasted* annually is **639x greater** than what Bitcoin consumes
- 56% of Bitcoin is electricity supplied by renewable energy
- Most Bitcoin mining is done with excess energy rather than energy *produced for mining*

MORE INFO...

