NEVADA COUNTY
CA

Bitcoin Terminology

Nevada County Bitcoin Meetup
August 17, 2022

Obligatory Disclosures

This is for educational and entertainment purposes only.

This is not investment advice.

We are not financial advisers.

Do your own research prior to purchasing ANY financial instruments.

We DO NOT advocate you purchase bitcoin.

We are here as a resource.

Ultimately, you must decide what is best for yourself.

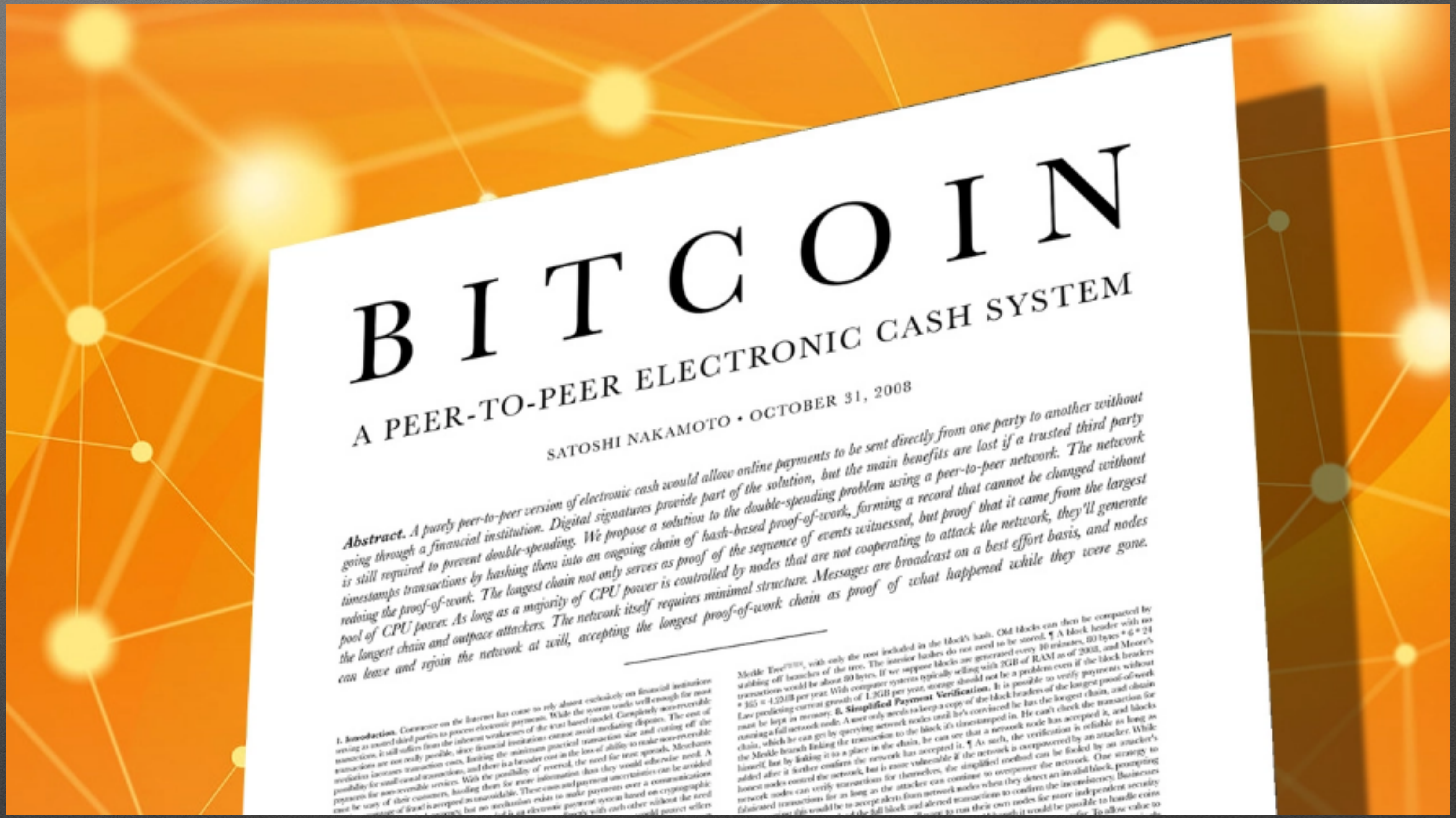
We will not allow discussion of other cryptocurrencies; Make your own group.

Any current event questions?

General questions welcomed, also!

Refresher: What is Bitcoin?

- Bitcoin is the protocol/network; bitcoin is the currency
- "A peer-to-peer electronic cash system"
- Allows users to transmit value digitally without the use of third party intermediaries
- Secured through cryptography (i.e., math)
- Introduced the world to the "proof-of-work" and "blockchain" concepts
- Hard cap of 21 million bitcoin, which are distributed through the proof-of-work system



BITCOIN

A PEER-TO-PEER ELECTRONIC CASH SYSTEM

SATOSHI NAKAMOTO • OCTOBER 31, 2008

***Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.*

Read the original whitepaper here:
bitcoin.org/bitcoin.pdf

Why is it Important?

- Fixed Supply: No one can change the protocol to increase the supply
- Divisible: Each bitcoin is divisible into 100,000,000 satoshis, or “sats”
- Portable: By remembering 12 words, you can take your bitcoin anywhere
- Verifiable: Anyone with a computer can verify both the supply and every transaction
- Censorship Resistant: No person, government, or business can stop a transaction

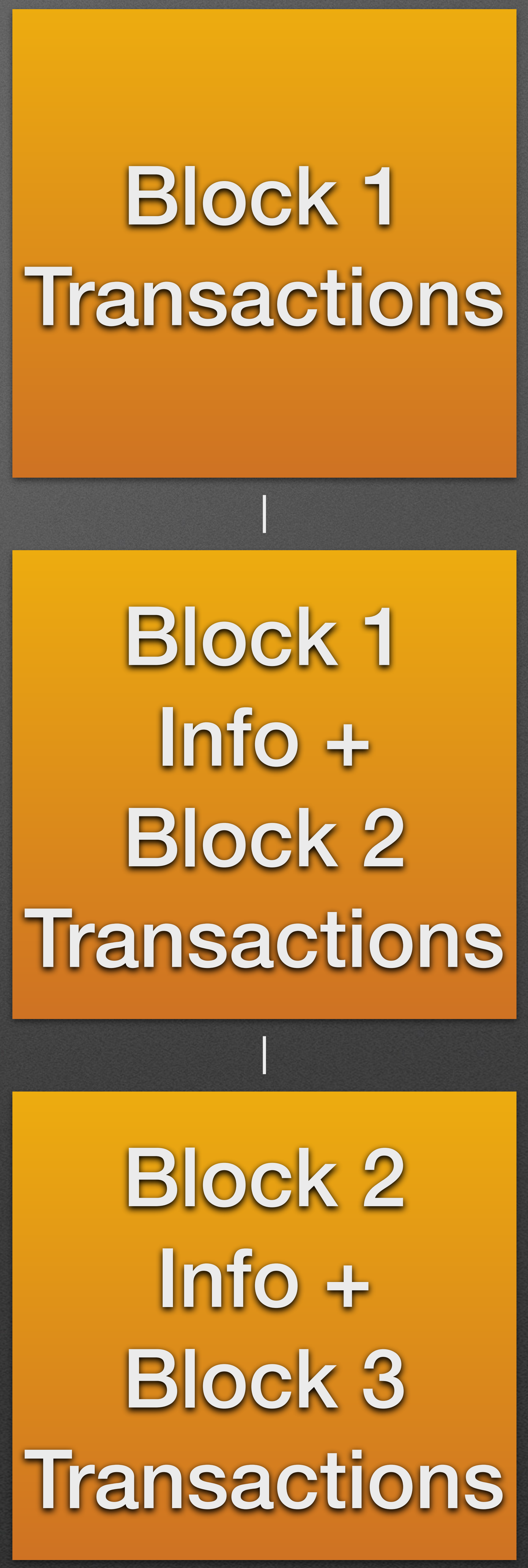
Blockchain

- “Blockchain Technology” was invented with the birth of bitcoin

- A blockchain utilizes the information contained in the last block to build on the chain

- Once a block has been added to the chain it can not be edited (immutable)

- If a block is valid, it is provable that each previous block must have been valid as well



Block 1 Transactions

Block 1 Info + Block 2 Transactions

Block 2 Info + Block 3 Transactions

Bitcoin Nodes

- A computer running bitcoin software that stores a copy of the entire blockchain

- Nodes confirm each block contains valid transactions before adding them to the blockchain

  - Thereby acting as the "referees" of the bitcoin network

- Nodes communicate with each other (peer-to-peer) to share new blocks and transactions to keep each node up to date

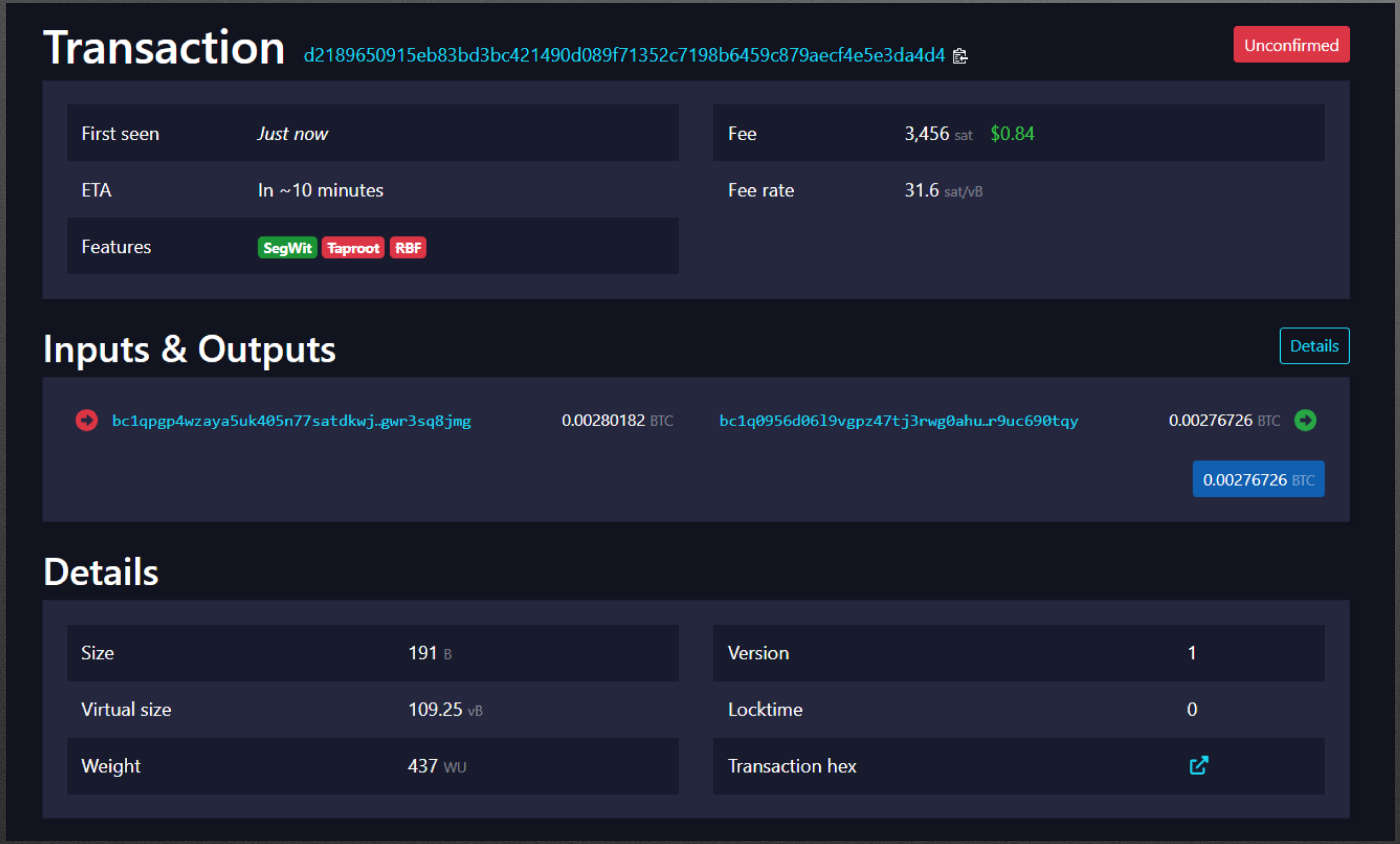
- Can be powered by simple, consumer grade hardware

```
RaspiBlitz v1.6.1  Sh0hansNode
Bitcoin Fullnode + Lightning Network + Tor
------------------------------------------
Refreshed: Sun, 22 Nov 2020 09:47:05 +0200
CPU load 0.60, 0.72, 0.62, temp 54°C 129°F
Free Mem 6929M / 7966M  HDDuse 430G (50%)
SSH admin@192.168.1.17 d30.9MiB u21.8MiB
Web admin --> http://192.168.1.17:3000
bitcoin v0.20.0 mainnet Sync OK 100.00%
Public [redacted] 11 peers

LND 0.11.1-beta wallet 0 sat
0/0 Channels 0 sat 3 peers
Fee Report: 0-0-0 sat (D-W-M)

0271d31eea1bc3498343bc7d9fe1f9bca7842caaaa08e519dae0d89b438e
914d36@nyo7na4kxkozazuu2f3yq5p7bzzh31ptzabkigq7bb5kwbhpj52im
kad.onion:9735
```

Transactions



Transaction d2189650915eb83bd3bc421490d089f71352c7198b6459c879aecf4e5e3da4d4

Unconfirmed

First seen	*Just now*	Fee	3,456 sat $0.84
ETA	In ~10 minutes	Fee rate	31.6 sat/vB
Features	SegWit Taproot RBF		

Inputs & Outputs

Details

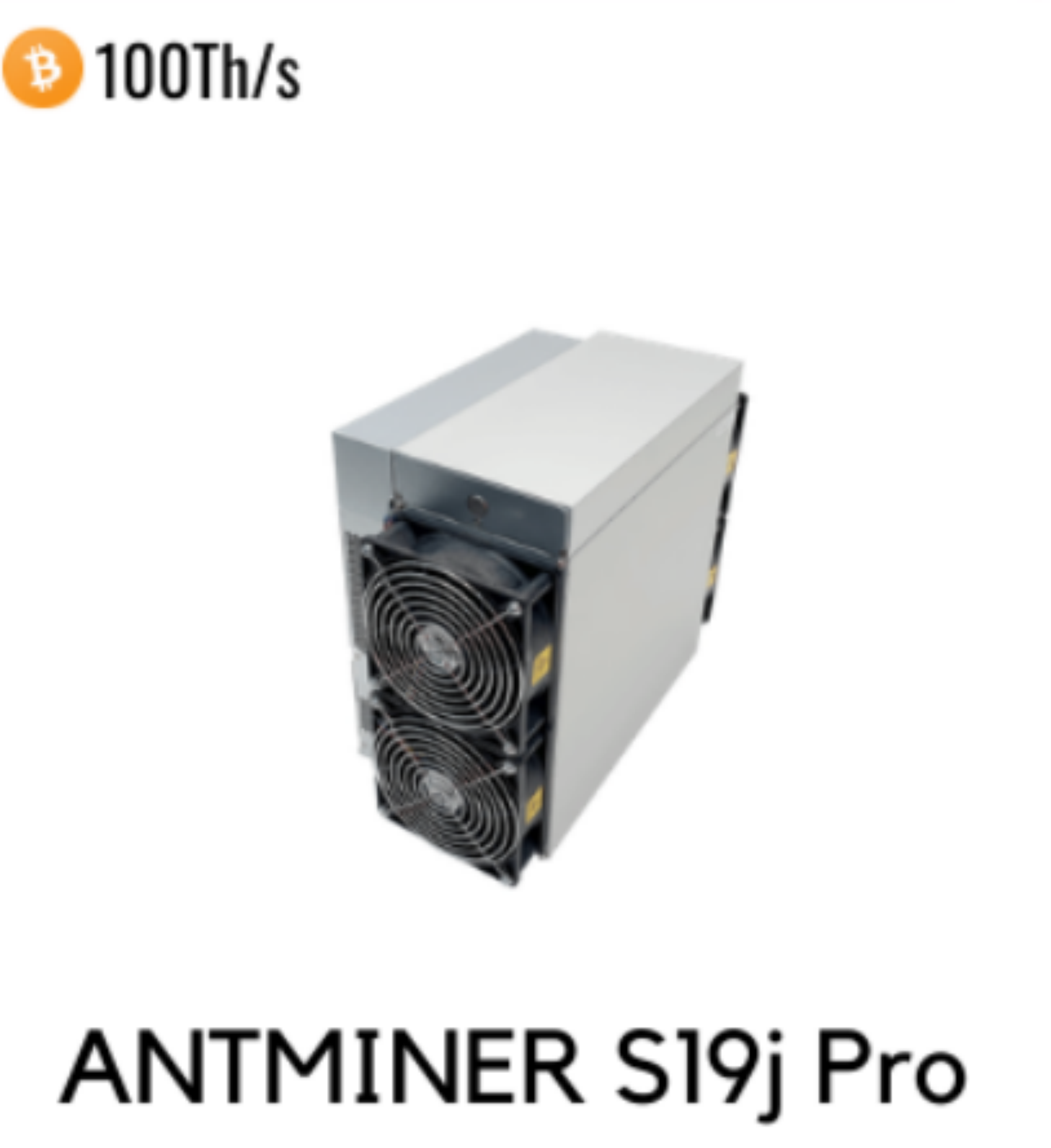
bc1qpgp4wzaya5uk405n77satdkwj…gwr3sq8jmg	0.00280182 BTC	bc1q0956d0619vgpz47tj3rwg0ahu…r9uc690tqy	0.00276726 BTC
			0.00276726 BTC

Details

Size	191 B	Version	1
Virtual size	109.25 vB	Locktime	0
Weight	437 WU	Transaction hex	

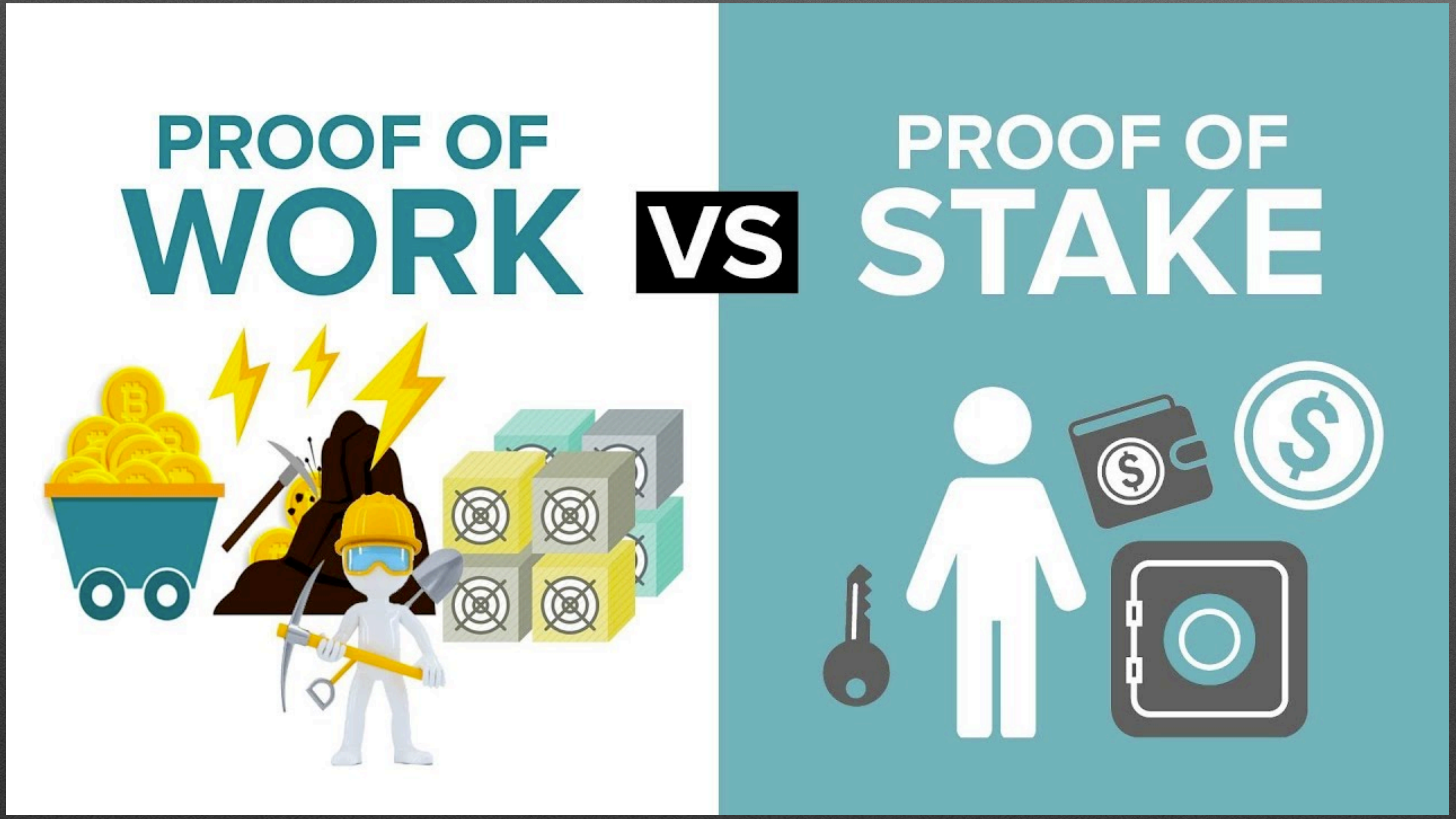
- A “transaction” refers to a transfer of bitcoin from one address to another.
- Each transaction has a "transaction ID" that can be used to look up the transaction details
- A blockchain explorer is a website that can show transaction details by querying the bitcoin blockchain

Bitcoin Mining



- Specialized computers solve complex math problems looking for the "correct answer" to "mint" a block and add it to the blockchain
- Once the correct answer is found, the miner broadcasts proof of the solution to the bitcoin network
- If other miners and node operators agree that the block is valid, it is added to everyones copy of the blockchain
- The miner that found the solution is rewarded with bitcoin and the miners continue searching for the solution to the next block

Proof of Work



- The mining process is referred to as "proof-of-work" because raw computational power (i.e., "work") is required to mint blocks

- The difficulty adjusts and targets an average "block time" of 10 minutes

- The amount of work required to mint a block adjusts automatically every 2016 blocks in response to the amount of computing power participating

- This process is very competitive because there are many computers trying to solve the same problem

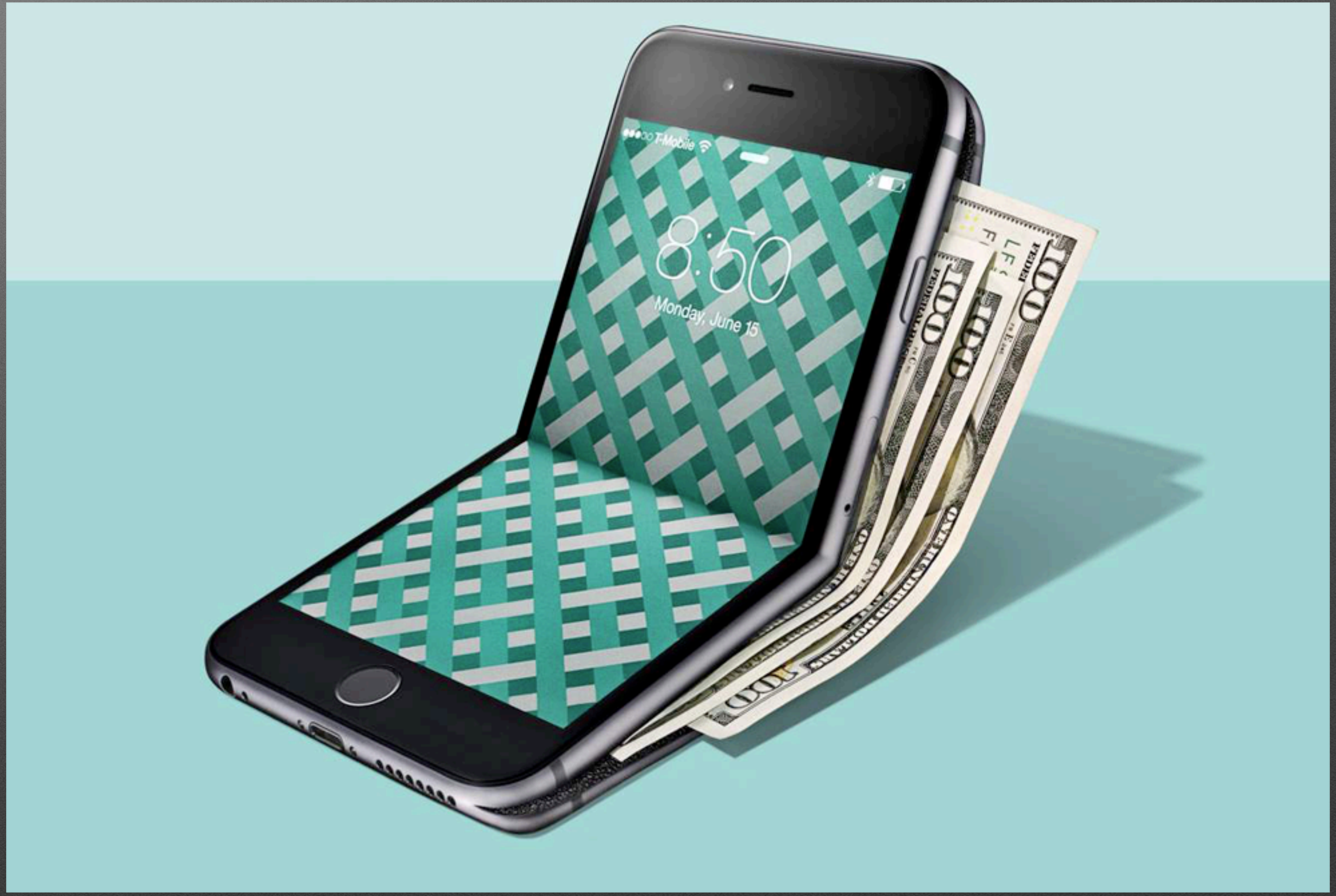
Wallets

- Wallets are software for your computer or phone

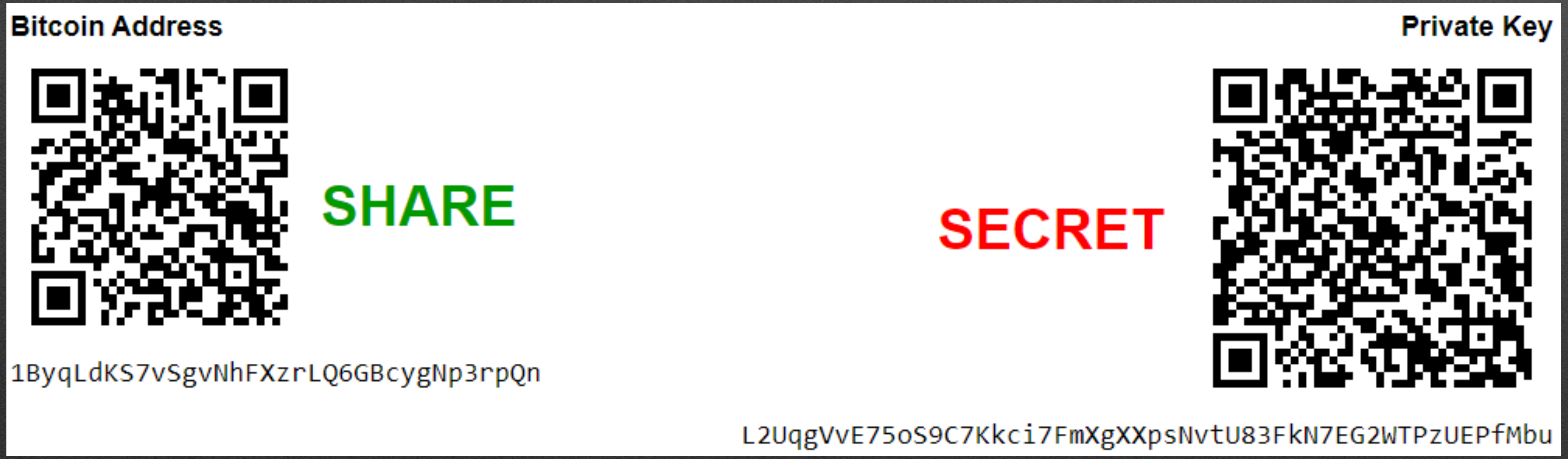
- Wallets allow bitcoin to be received and spent

- Most of the technical aspects of the wallet are done behind the scenes

- Wallets can be open or closed source



How Do Bitcoin Wallets Work? (cont'd)



Bitcoin Address

SHARE

1ByqLdKS7vSgvNhFXzrLQ6GBcygNp3rpQn

Private Key

SECRET

L2UqgVvE75oS9C7Kkci7FmXgXXpsNvtU83FkN7EG2WTPzUEPfMbu

Real key pair generated at bitaddress.com

- What is a private/public key pair?
  - Key pairs are generated together through cryptography and are mathematically related
  - Public key is viewable on the blockchain
  - Private key is only known by the owner of the key pair
  - Private key allows owner prove ownership of public key (e.g., create, sign, and transmit a bitcoin transaction)

Custodial Bitcoin Storage

Pros

- Easy to set up an account with ID
- Link bank or debit card to purchase bitcoin
- Help line should you forget your password

Cons

- A "trusted" custodian holds your private keys and can send bitcoin on your behalf
- Risk of hacks, regulatory changes, business defaults

Self-Custody Solutions

Pros:

- Different ways to store your bitcoin by having your own wallet
- Less subject to regulatory capture/seizure
- Ability to anonymize transactions/balances

Cons:

- There is no help line to call if you lose your backups
- More difficult than storing your bitcoin IOU’s on an exchange

Non-Custodial Storage

- A "wallet" refers to the combination of a public/private key pair
  - Paper wallets
  - Web wallets
  - Mobile wallets
  - Hardware wallets

Hot vs. Cold Wallets

- A "hot wallet" refers to a wallet that is connected to the internet (e.g., a mobile wallet)
    - Increased risk of loss due to viruses, hacks, or mistakes
- A "cold wallet" refers to a wallet that is not connected to the internet (only connects to the internet when making transactions)
    - Generally a safer way to hold bitcoin

Cold Storage

- Refers to a wallet that rarely, if ever, is connected to the internet
- The most secure option for long term storage
- There are various approaches to accomplish this

How to Procure Bitcoin?

- Centralized exchanges
  - Cash App
  - Strike
- Peer-to-peer exchanges
  - Bisq
  - HodlHodl
- Friends!

Suggested reading/listening

“The Words we Use in Bitcoin”

By DerGigi, read by Guy Swann

“It can’t be said often enough: Bitcoin is confusing. However, it’s not complicated like a Rube Goldberg machine is complicated. It’s just very foreign and thus very misunderstood—it is a completely new thing. ‘There’s nothing to relate it to,’ as Satoshi put it in one of his posts."

-Gigi, “The Words we Use in Bitcoin”

Questions?
Suggestions?
Discussions?

Thank you all for coming by.
We enjoy sharing this information.
Make sure to follow us on Meetup or on Twitter:
@NevCoBTC