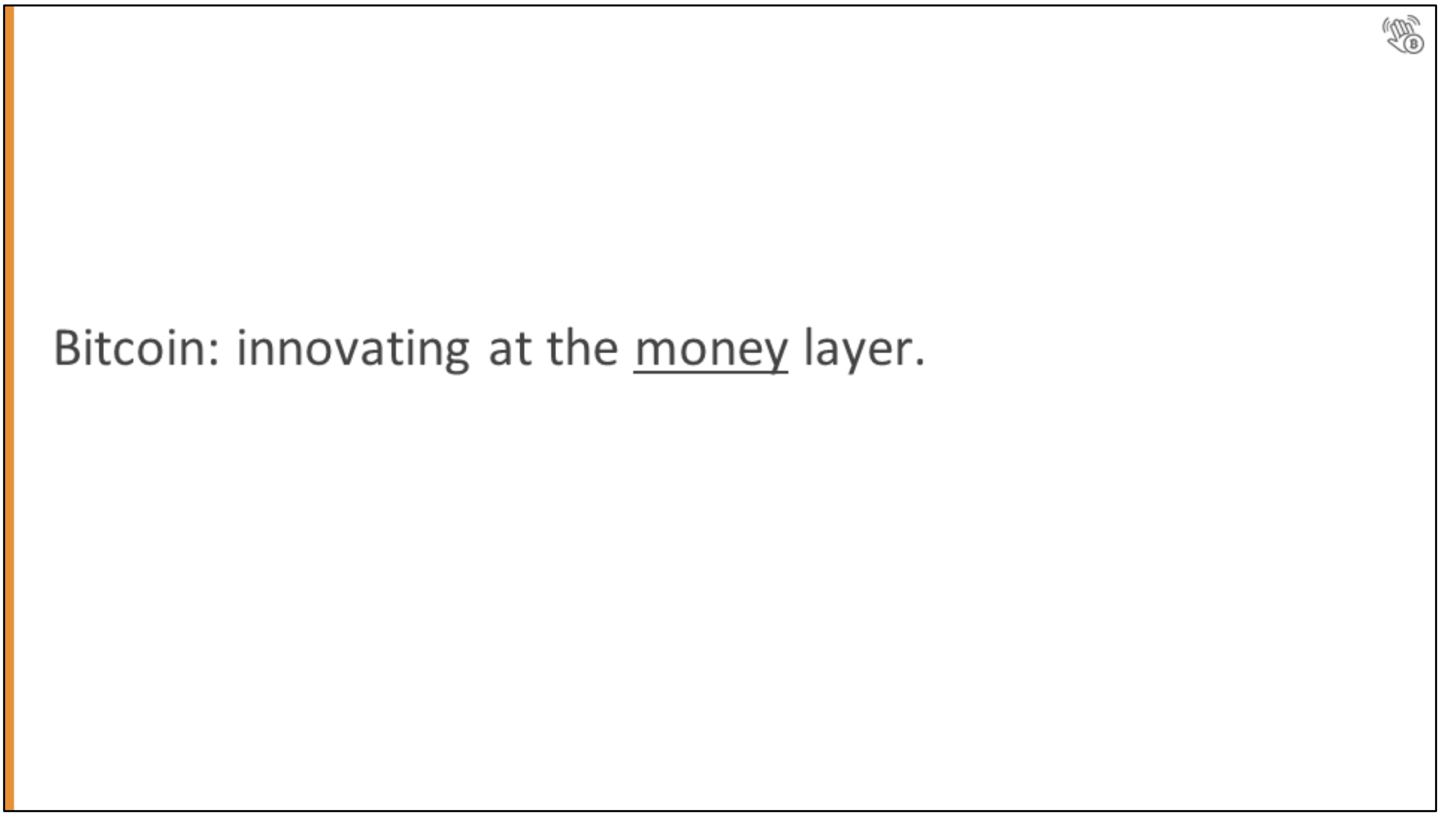
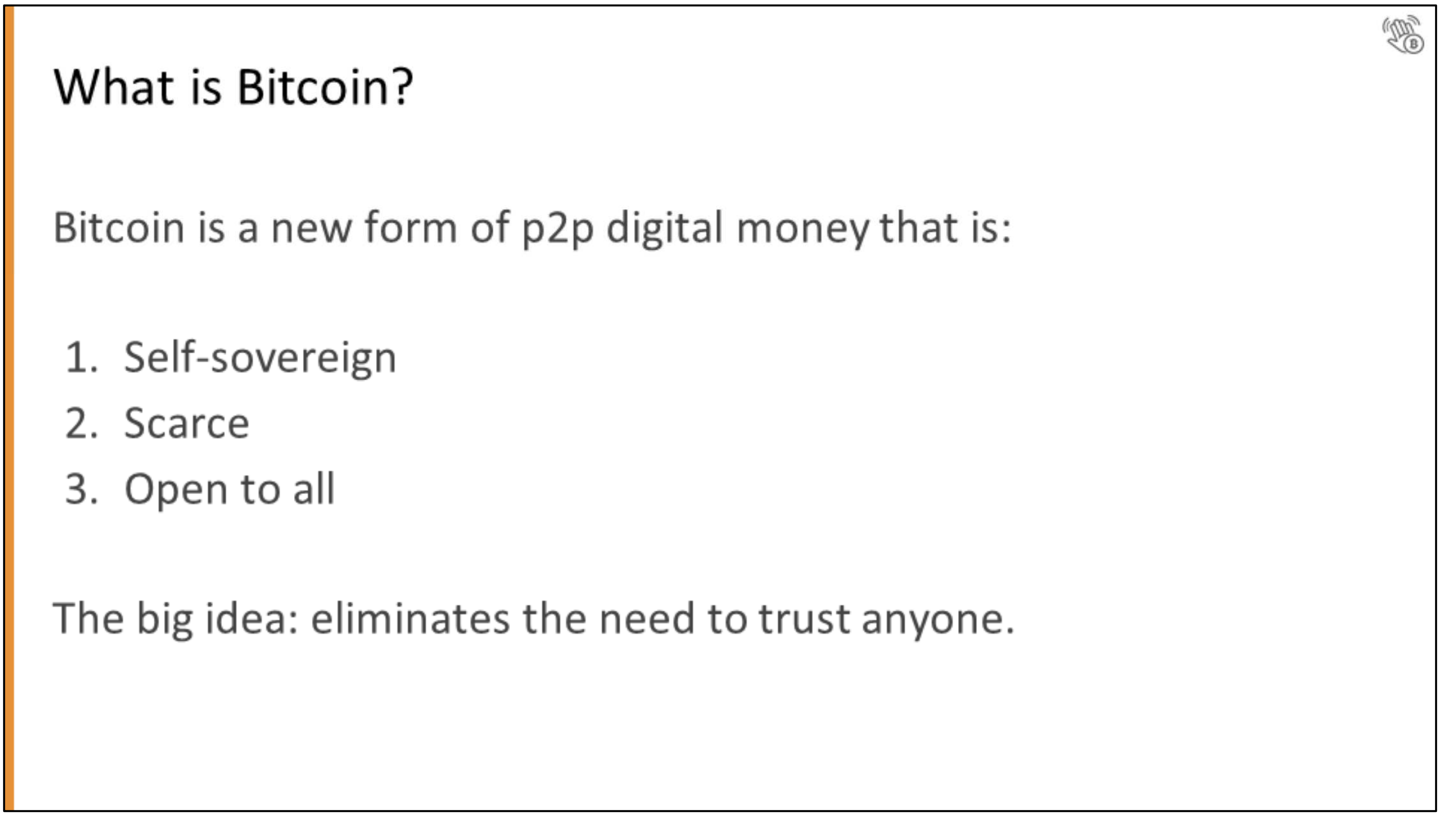


Bitcoin: innovating at the money layer.

And not the payment layer as has been the case with fintech for a generation



What is Bitcoin?

Bitcoin is a new form of p2p digital money that is:

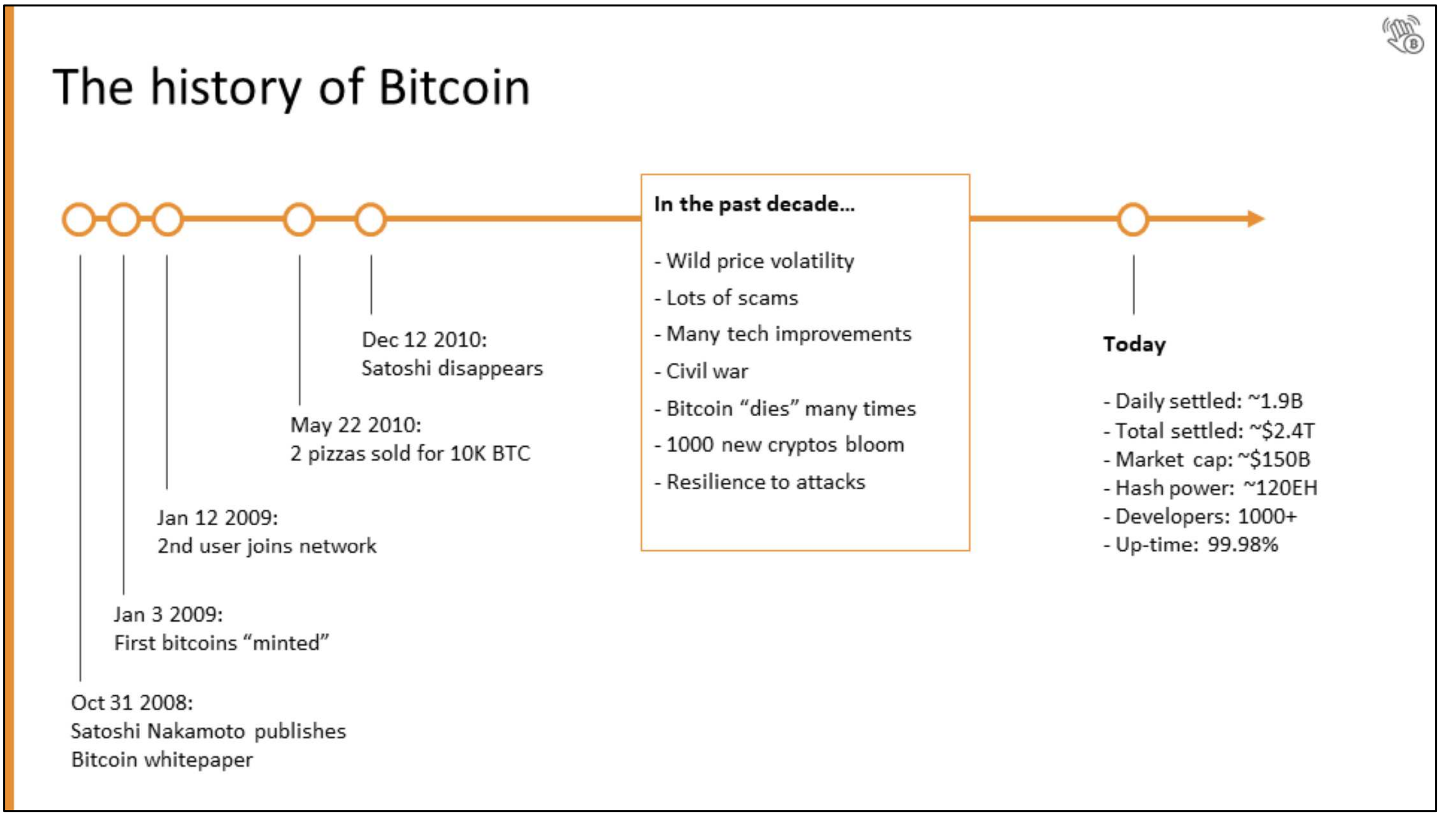
1. Self-sovereign
2. Scarce
3. Open to all

The big idea: eliminates the need to trust anyone.

P2p = “peer to peer” - mention that this is the opposite of client <-> server model, example: music sharing
Trust. Who is the “anyone” we trust today? Banks, government, policy makers.
Another way to think of Bitcoin: as better version of physical cash, for the Internet age (with added benefits, eg. no inflation)
Will come back to dive into each of these properties in more detail later.

RE: eliminates the *NEED* to trust - still have opportunity to choose who to trust (e.g. when incentives align, trust reputable, verifiable actors, etc) it’s the removal of mandatory required trust that is powerful.

How did this even become possible?



The history of Bitcoin

Oct 31 2008:
Satoshi Nakamoto publishes
Bitcoin whitepaper

Jan 3 2009:
First bitcoins "minted"

Jan 12 2009:
2nd user joins network

May 22 2010:
2 pizzas sold for 10K BTC

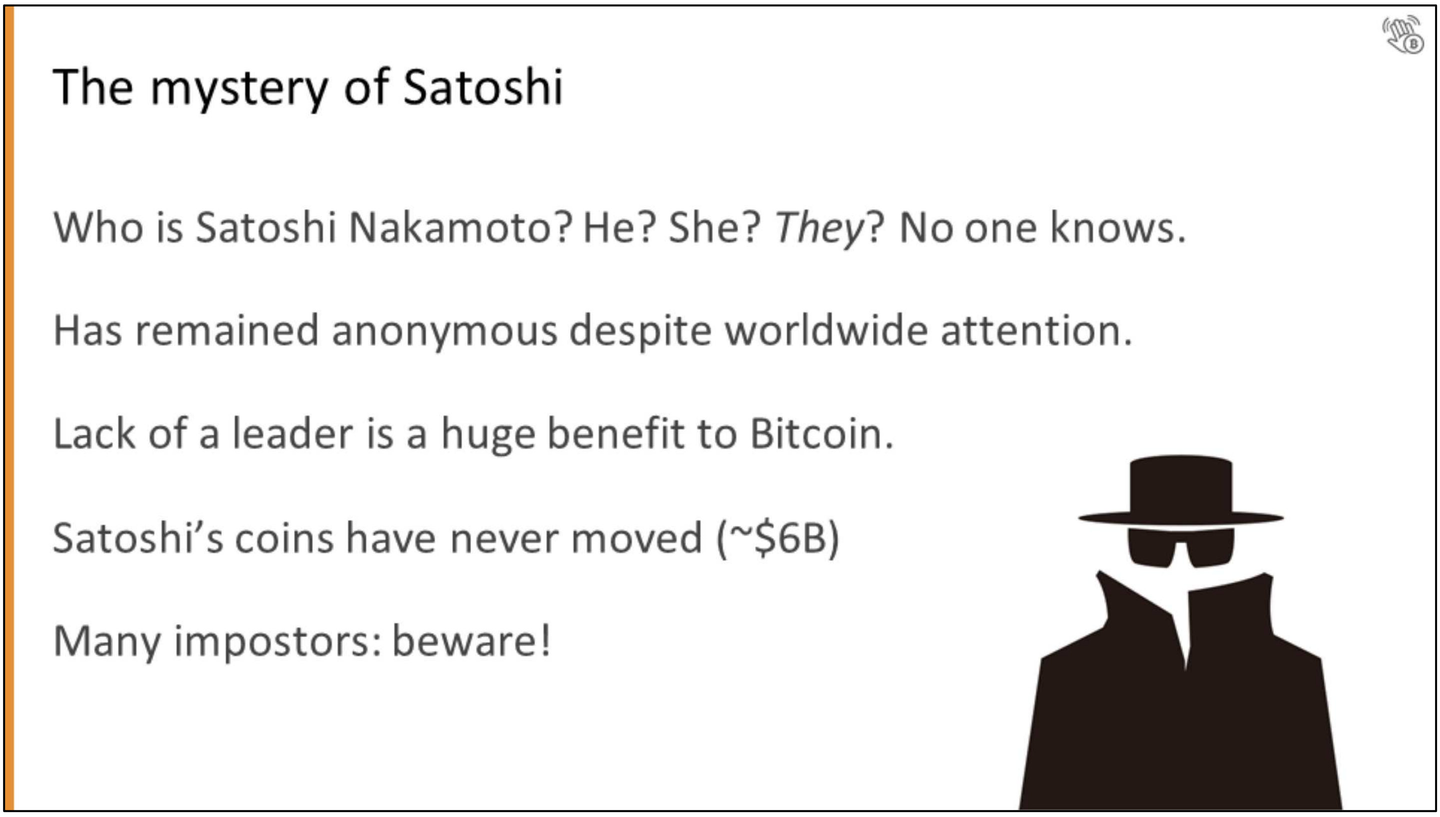
Dec 12 2010:
Satoshi disappears

In the past decade…

- Wild price volatility
- Lots of scams
- Many tech improvements
- Civil war
- Bitcoin "dies" many times
- 1000 new cryptos bloom
- Resilience to attacks

Today

- Daily settled: ~1.9B
- Total settled: ~$2.4T
- Market cap: ~$150B
- Hash power: ~120EH
- Developers: 1000+
- Up-time: 99.98%



The mystery of Satoshi

Who is Satoshi Nakamoto? He? She? *They*? No one knows.

Has remained anonymous despite worldwide attention.

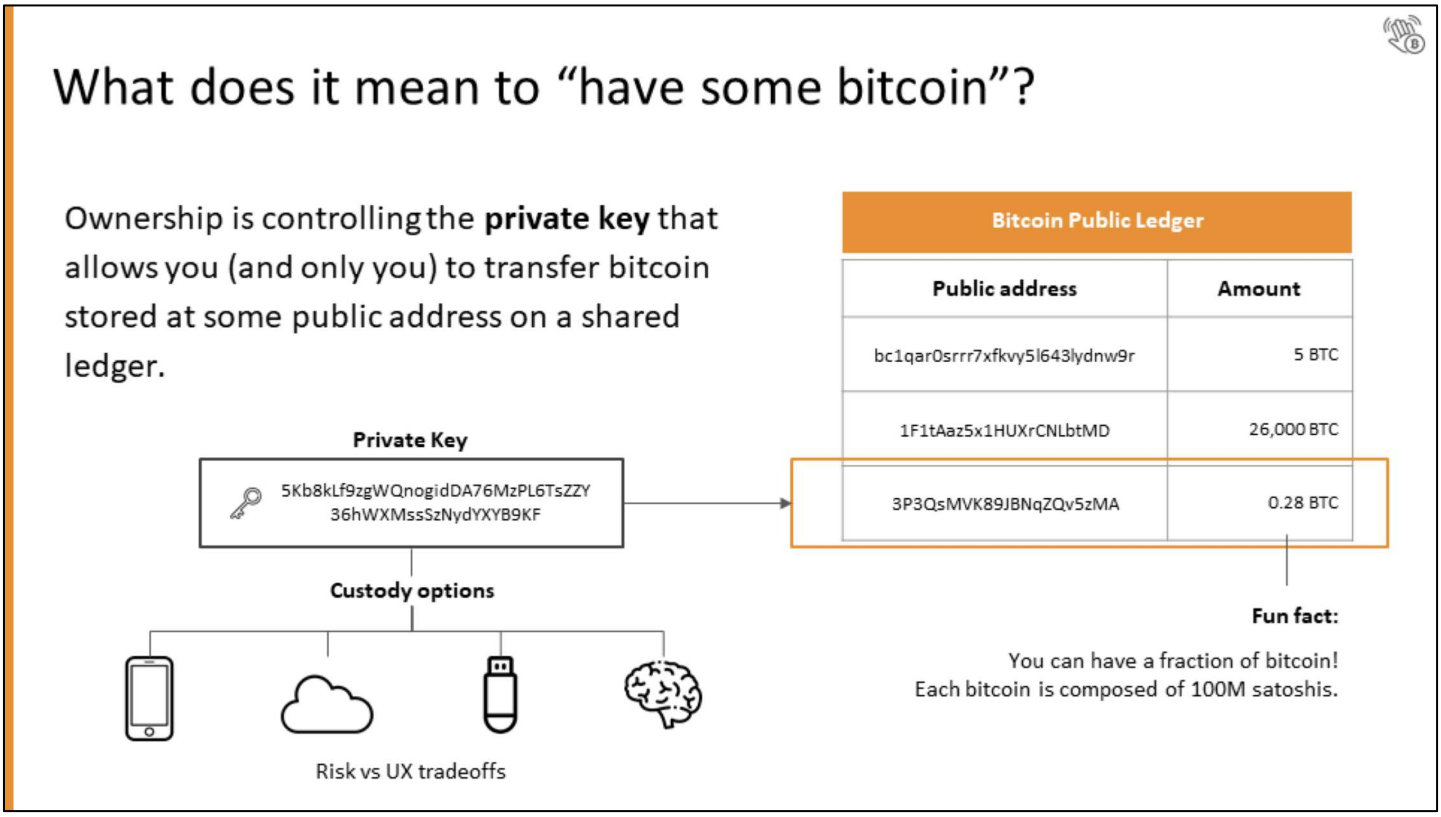
Lack of a leader is a huge benefit to Bitcoin.

Satoshi’s coins have never moved (~$6B)

Many impostors: beware!

Satoshi identity doesn't matter, because with a completely open source system, there's nothing about how it works that isn't completely public.

To appreciate Bitcoin, let’s look under the hood.



What does it mean to "have some bitcoin"?

Ownership is controlling the **private key** that allows you (and only you) to transfer bitcoin stored at some public address on a shared ledger.

Private Key

5Kb8kLf9zgWQnogidDA76MzPL6TsZZY 36hWXMssSzNydYXYB9KF

Custody options

Risk vs UX tradeoffs

Bitcoin Public Ledger

Public address	Amount
bc1qar0srrr7xfkvy5l643lydnw9r	5 BTC
1F1tAaz5x1HUXrCNLbtMD	26,000 BTC
3P3QsMVK89JBNqZQv5zMA	0.28 BTC

Fun fact:

You can have a fraction of bitcoin!
Each bitcoin is composed of 100M satoshis.

- If you're unfamiliar with what a ledger is, just think of this as a simple spreadsheet tracking ownership of coins.
- 2^256 > atoms in universe
- Similar to a $20, if it blows away in the wind, you lose the money. If your priv key is written on a piece of paper that blows away...so there are different custody options

What happens when you send bitcoin?

Amount to send:
3 BTC
To:
3wdpspso3i2
SEND

1 **First, have some bitcoin.**

E.g. You control the private keys to some amount of bitcoin.

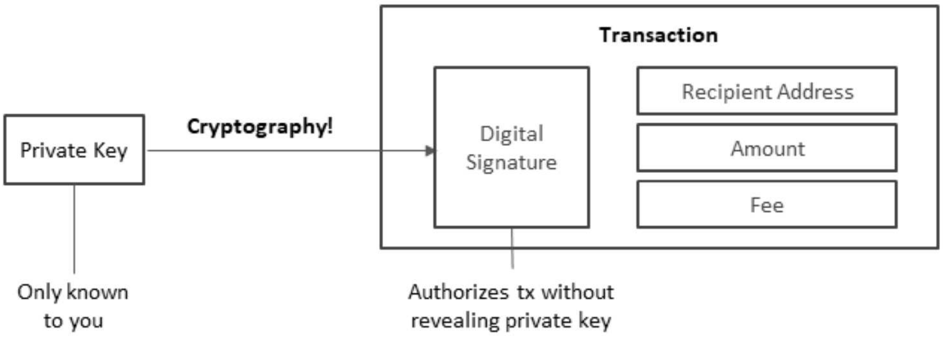
What happens when you send bitcoin?

Amount to send: 3 BTC

To: 3wdpspso3i2

2 **Generate a transaction.**

A digital signature is created using your private key that proves ownership of the coin, allowing them to be transferred.



What happens when you send bitcoin?

Amount to send:

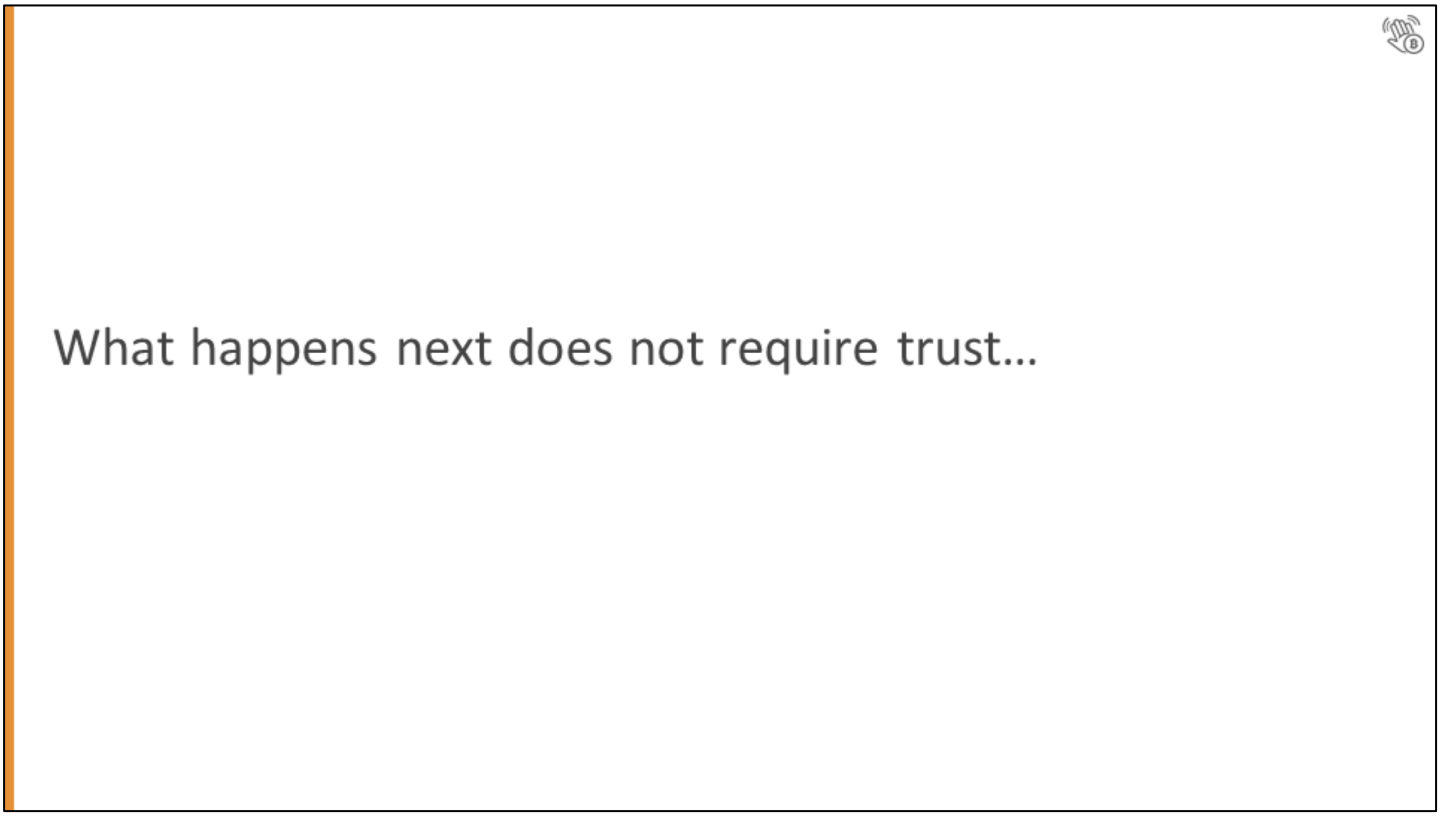
3 BTC

To:

3wdpspso3i2

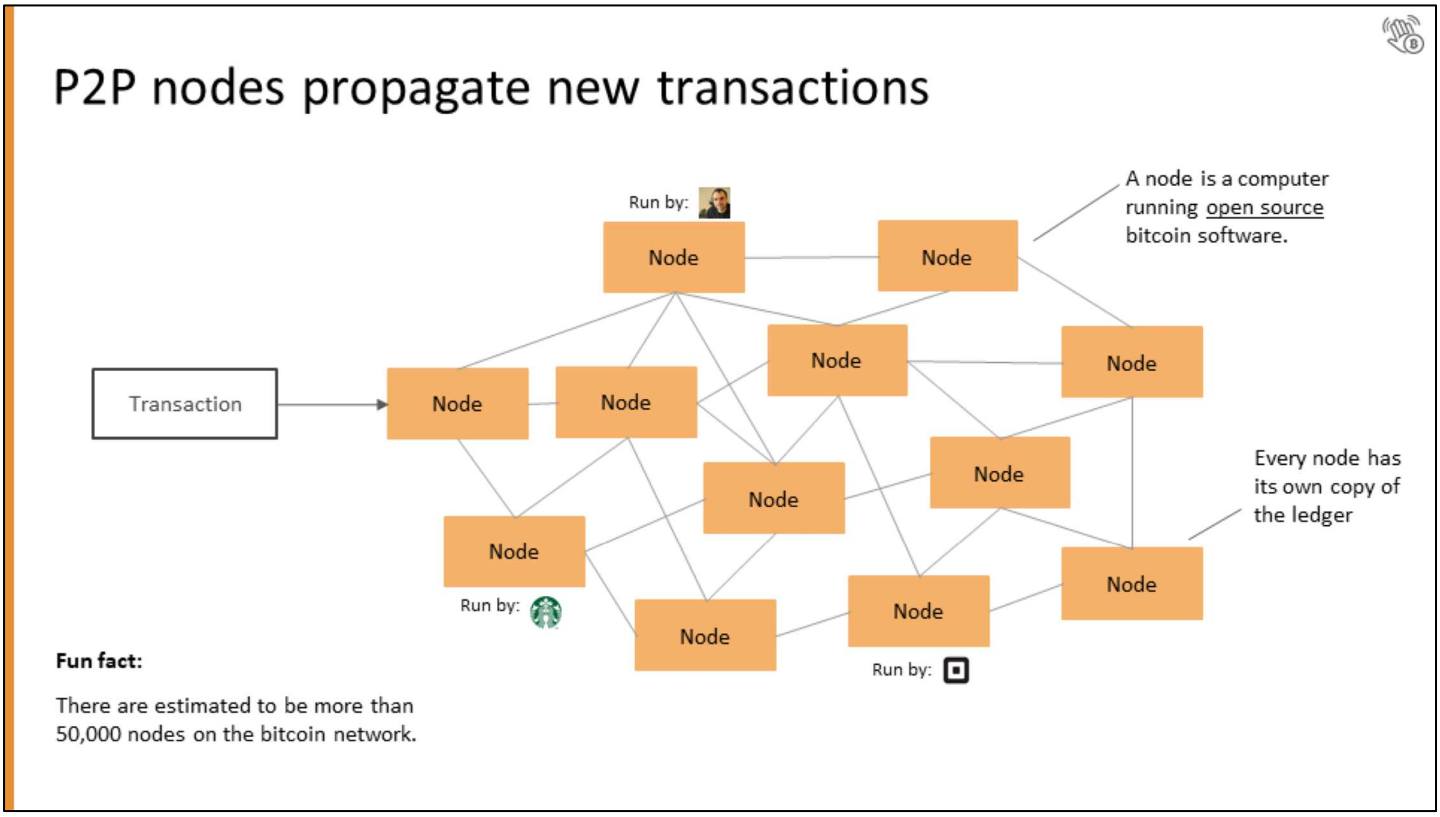
3 **Broadcast the transaction.**

The transaction is sent to the p2p bitcoin network.



What happens next does not require trust…

Again, not a client/server architecture…compare to Venmo, Cash app, etc.



P2P nodes propagate new transactions

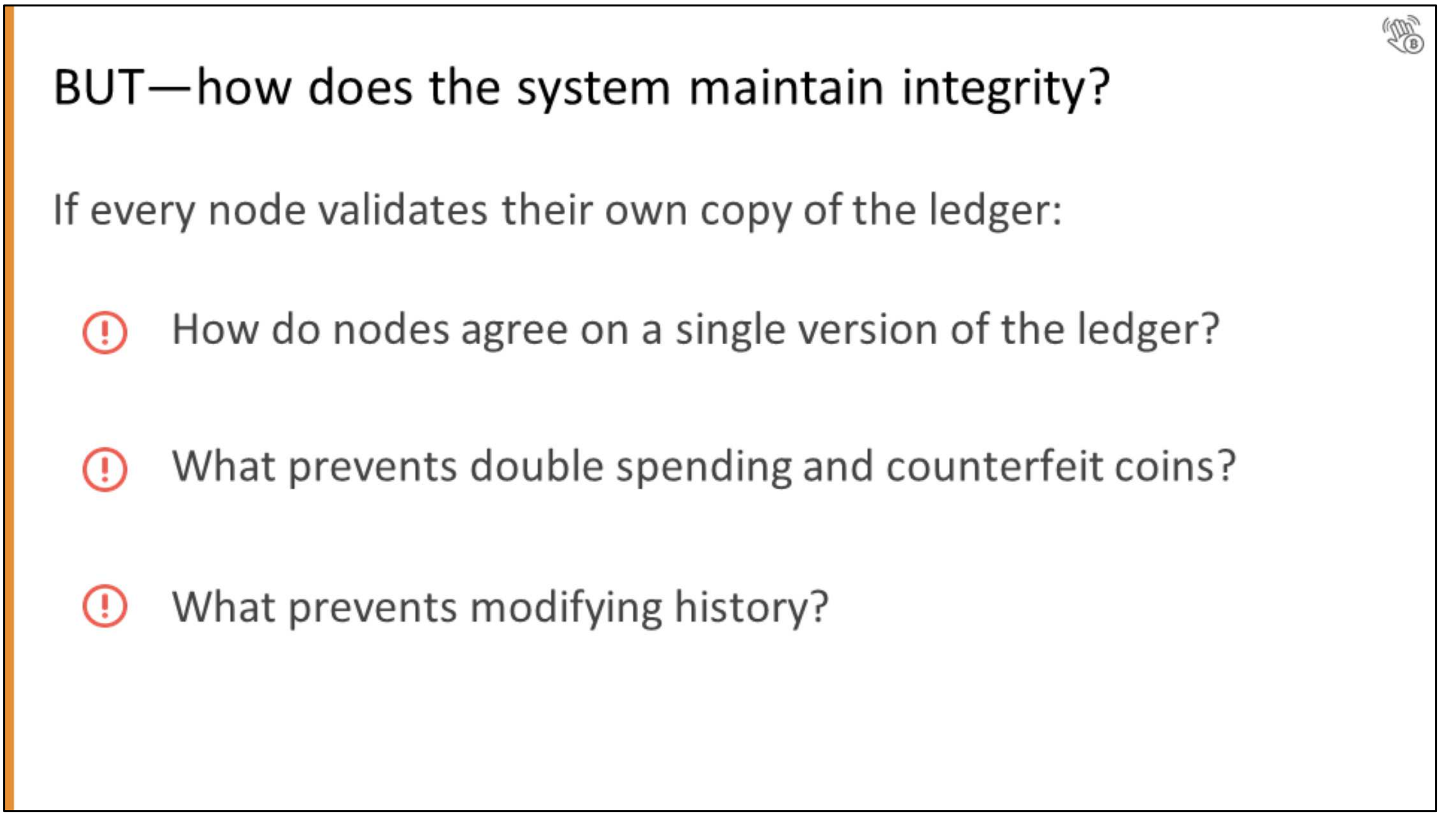
A node is a computer running open source bitcoin software.

Every node has its own copy of the ledger

Fun fact:

There are estimated to be more than 50,000 nodes on the bitcoin network.

why this process doesn't require trust—due to the difference between open source software vs. the closed source software most people are used to. closed source apps or programs on your computer or phone might do nefarious things only it's creators are aware of, not true for open source.



BUT—how does the system maintain integrity?

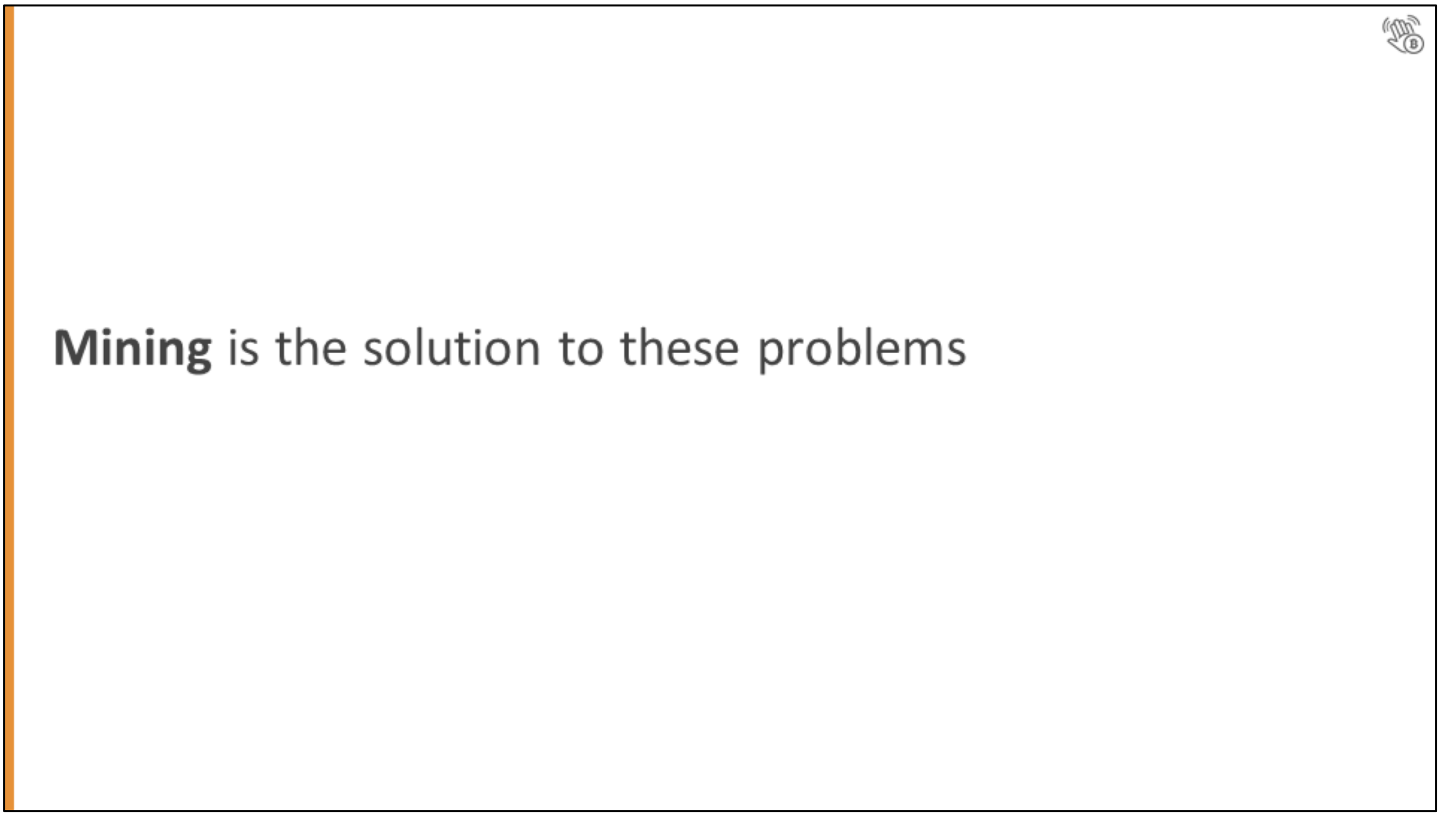
If every node validates their own copy of the ledger:

- How do nodes agree on a single version of the ledger?
- What prevents double spending and counterfeit coins?
- What prevents modifying history?

1. should speak to permissionless entry. anyone can come/go at any point in time, and should not be disadvantaged in any way based on any factor (time entered, amount of hash rate, etc.).

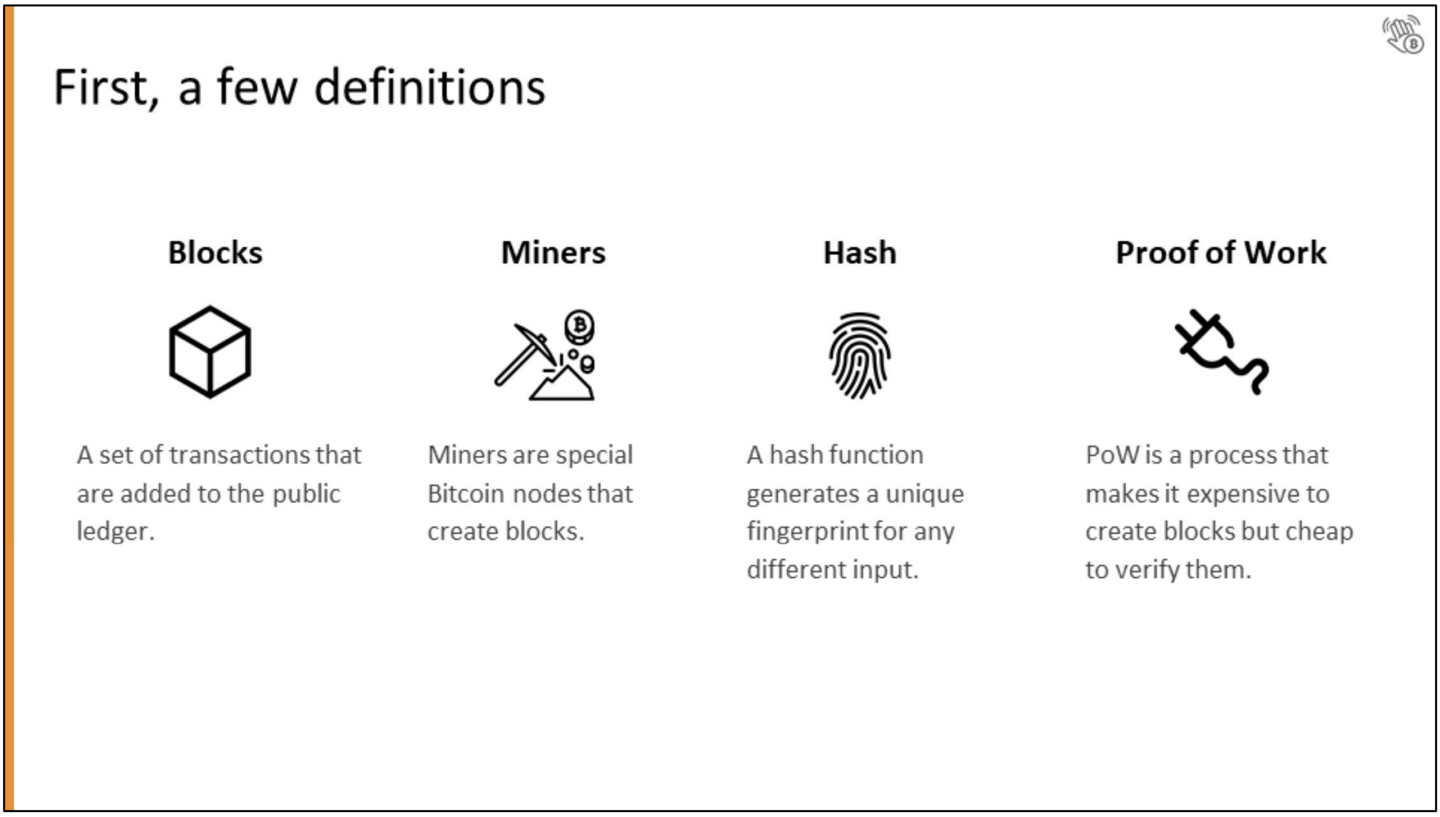
2. randomness is a really hard concept and difficult to produce uniform randomness. it is critical for #1. PoW is a system to create that randomness and create a FAIR SYSTEM.

3. because this is the only method to print money, it is EXTREMELY IMPORTANT to be fair, neutral, and permissionless.



Mining is the solution to these problems

Ask audience, who has heard of bitcoin mining?



First, a few definitions

Blocks

A set of transactions that are added to the public ledger.

Miners

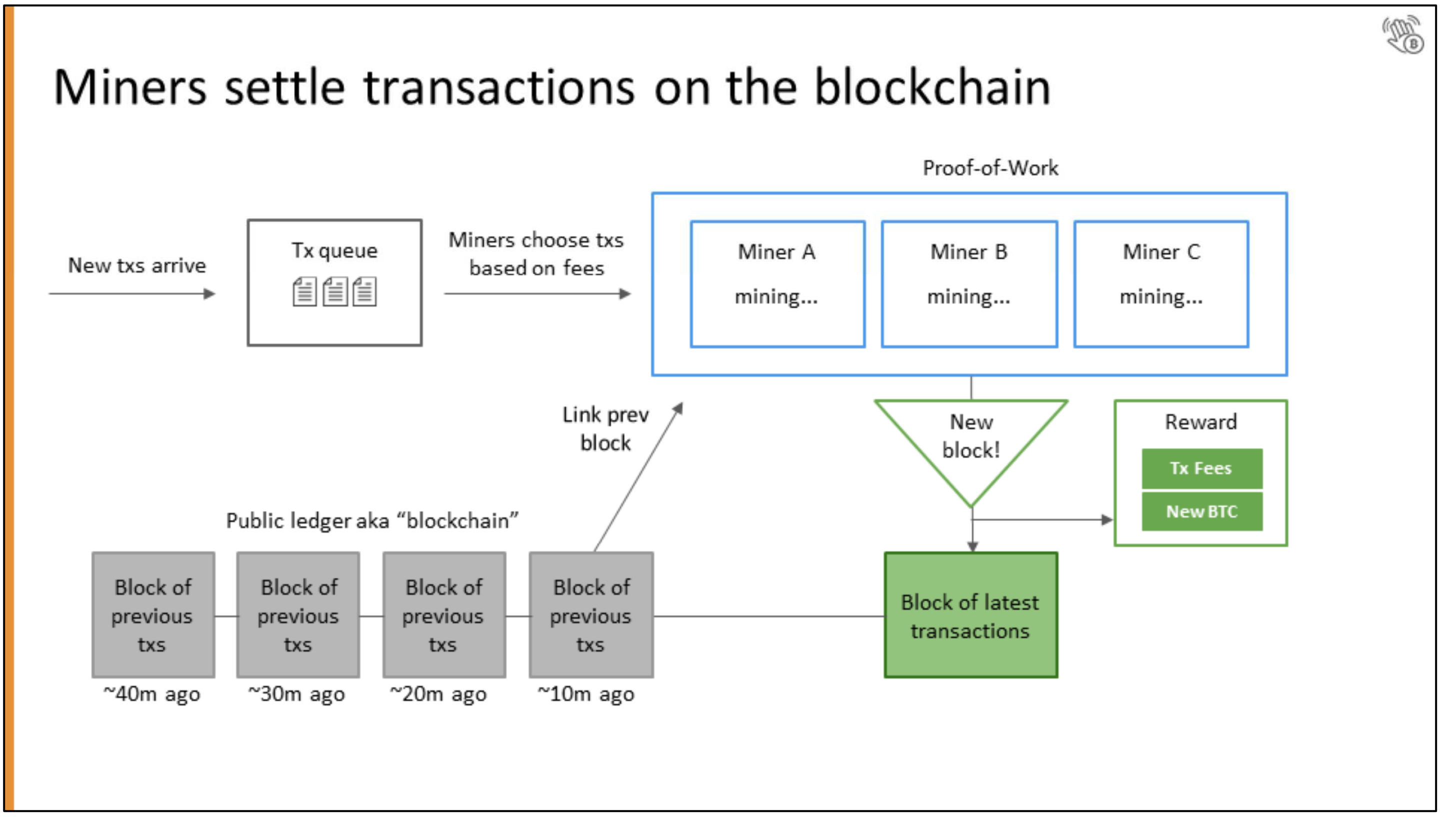
Miners are special Bitcoin nodes that create blocks.

Hash

A hash function generates a unique fingerprint for any different input.

Proof of Work

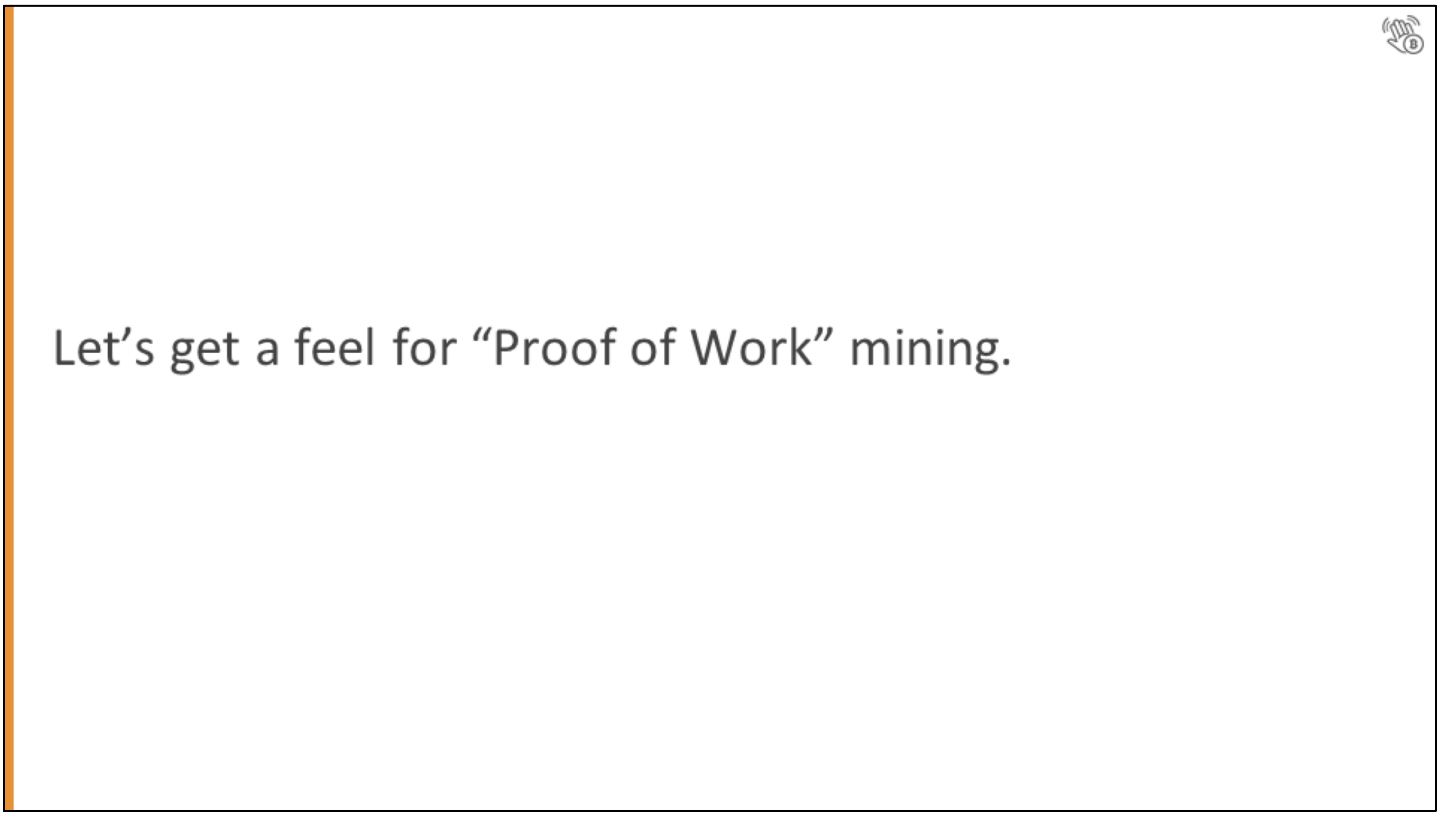
PoW is a process that makes it expensive to create blocks but cheap to verify them.



Miners settle transactions on the blockchain

Critical voiceover:

- A block is valid if all bitcoin protocol rules which include
  - Preventing double spending, by ordering transactions in time **[explicitly refer to this addressing question #2]**
  - Preventing the creation of counterfeit bitcoin **[explicitly refer to this addressing question #4]**
  - The new block *must* link back to previous blocks ensuring the same history of transactions is used **[explicitly refer to this addressing question #3]**



Let’s get a feel for “Proof of Work” mining.

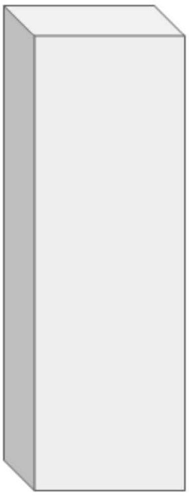
Think of “Proof of Work” as an impenetrable wall

The only way through this wall is over it.

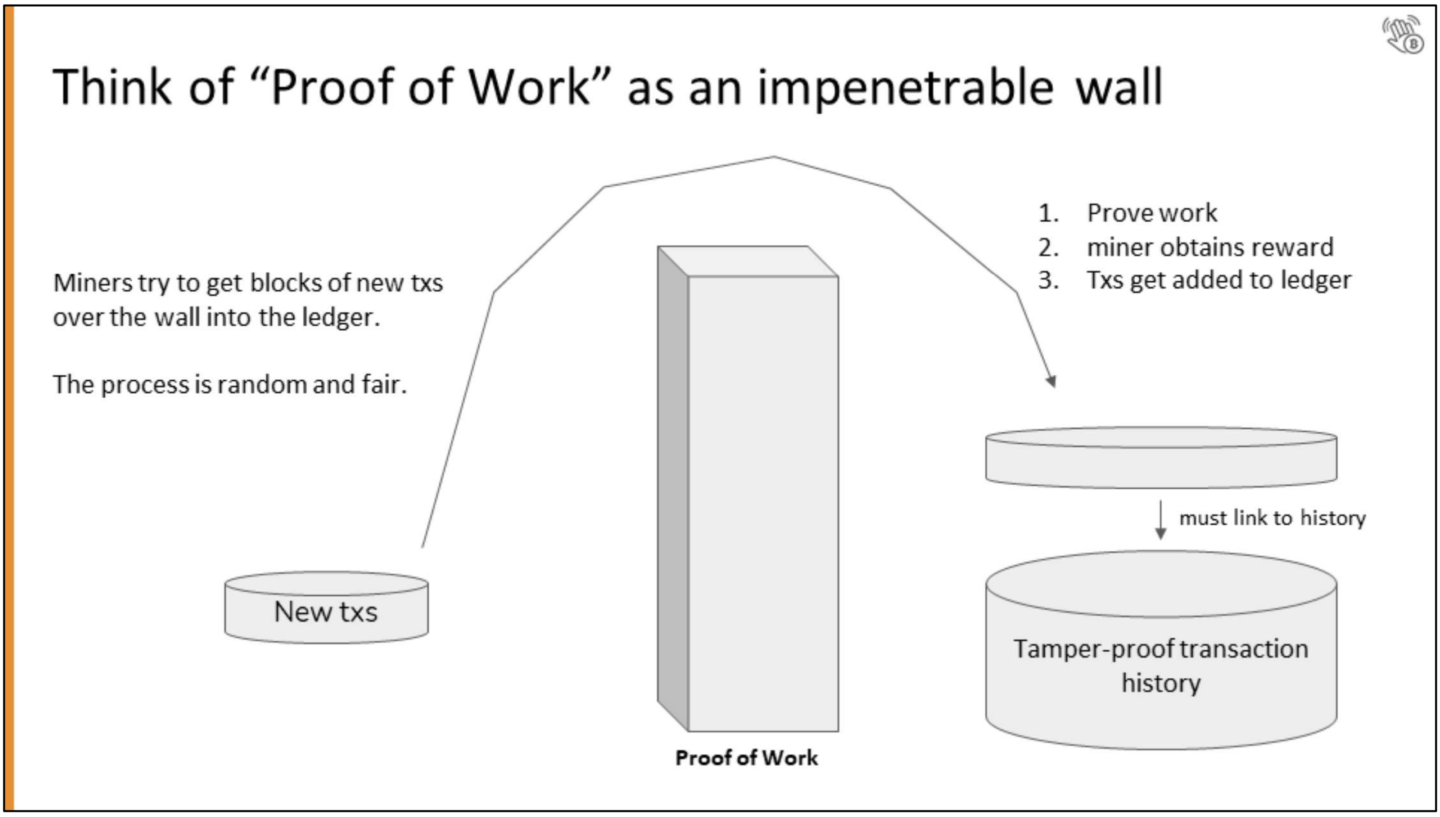
It is very, very hard to overcome it.

Imagine: it requires a gazillion random attempts to succeed!

Getting over is a demonstration (proof) that you expended the required energy (work).



Proof of Work



Think of “Proof of Work” as an impenetrable wall

Miners try to get blocks of new txs over the wall into the ledger.

The process is random and fair.

1. Prove work
2. miner obtains reward
3. Txs get added to ledger

New txs

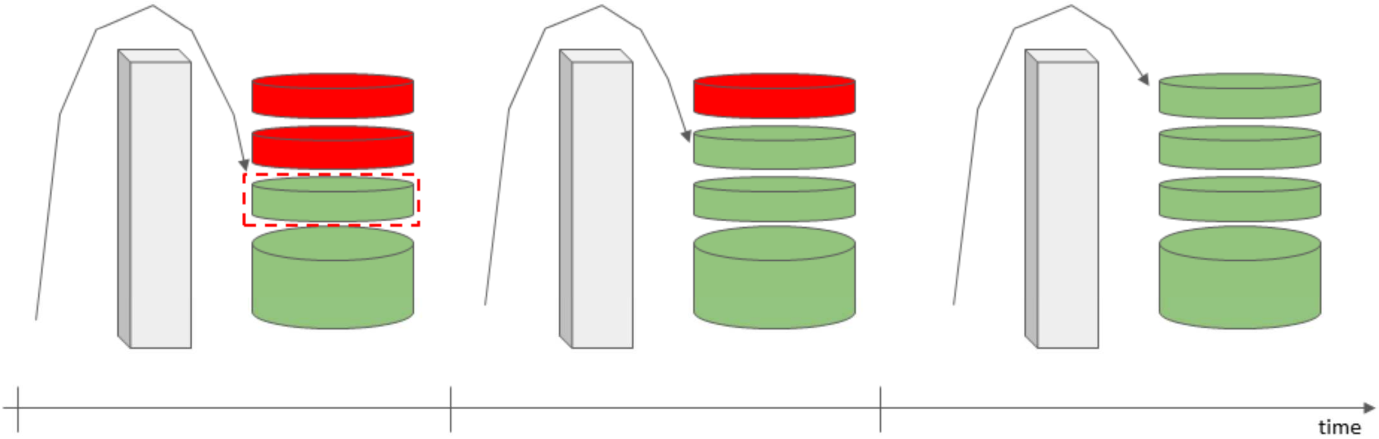
Proof of Work

must link to history

Tamper-proof transaction history

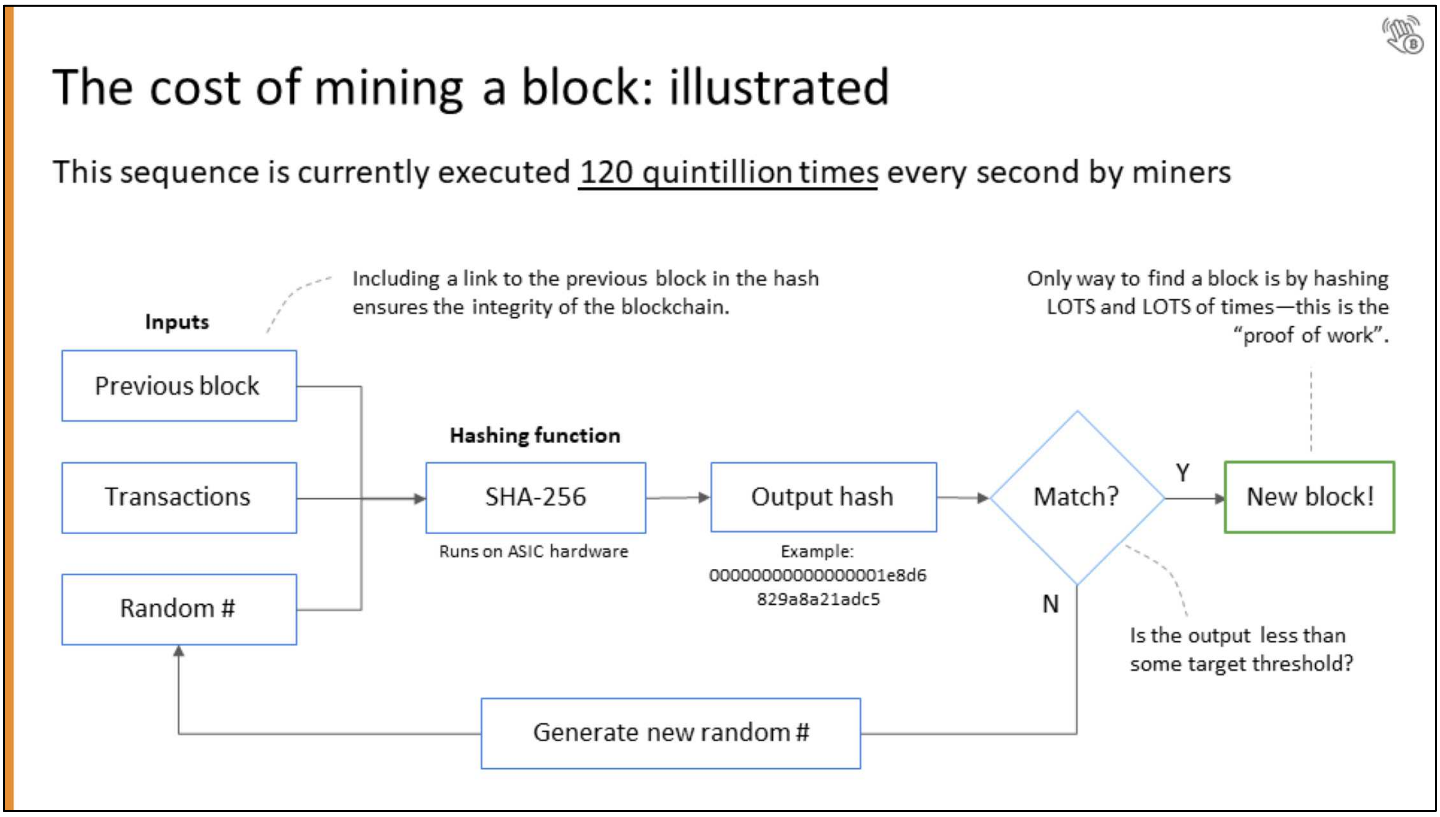
Changing history becomes infeasibly expensive

E.g. making a change 3 periods ago means re-doing work x3



Anyone trying to change history “falls behind” other miners and won’t catch up.

How does it work for real?



The cost of mining a block: illustrated

This sequence is currently executed 120 quintillion times every second by miners

Inputs

Previous block

Transactions

Random #

Including a link to the previous block in the hash ensures the integrity of the blockchain.

Hashing function

SHA-256

Runs on ASIC hardware

Output hash

Example:
00000000000000001e8d6
829a8a21adc5

Match?

Y

N

New block!

Only way to find a block is by hashing LOTS and LOTS of times—this is the "proof of work".

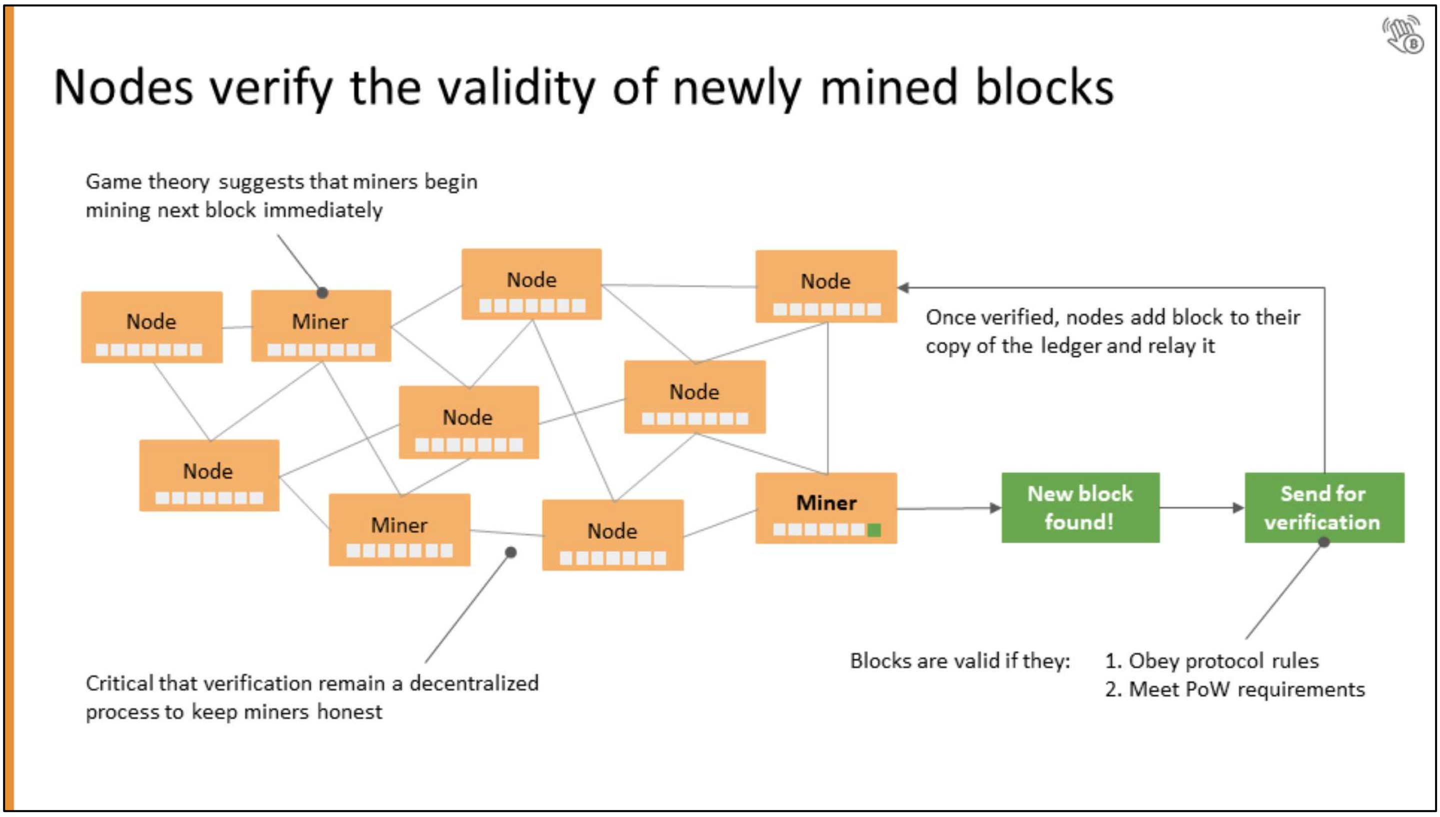
Is the output less than some target threshold?

Generate new random #

- This is what makes it expensive
- And makes it hard to undo past work
- And creates game theory to accept others' work
- Difficulty
- Supply schedule maintained regardless of # miners
- Why do miners spend money to produce new blocks?
  - Each new block mints new bitcoin which the miner receives as compensation.
  - Also, each transaction attaches a fee that goes to the miner as a reward.

- fingerprint; wildly diff output hash; google doc add period ex.

120 quintillion = 120 million trillion hashes per second
By far the biggest "supercomputer" in existence



Nodes verify the validity of newly mined blocks

Game theory suggests that miners begin mining next block immediately

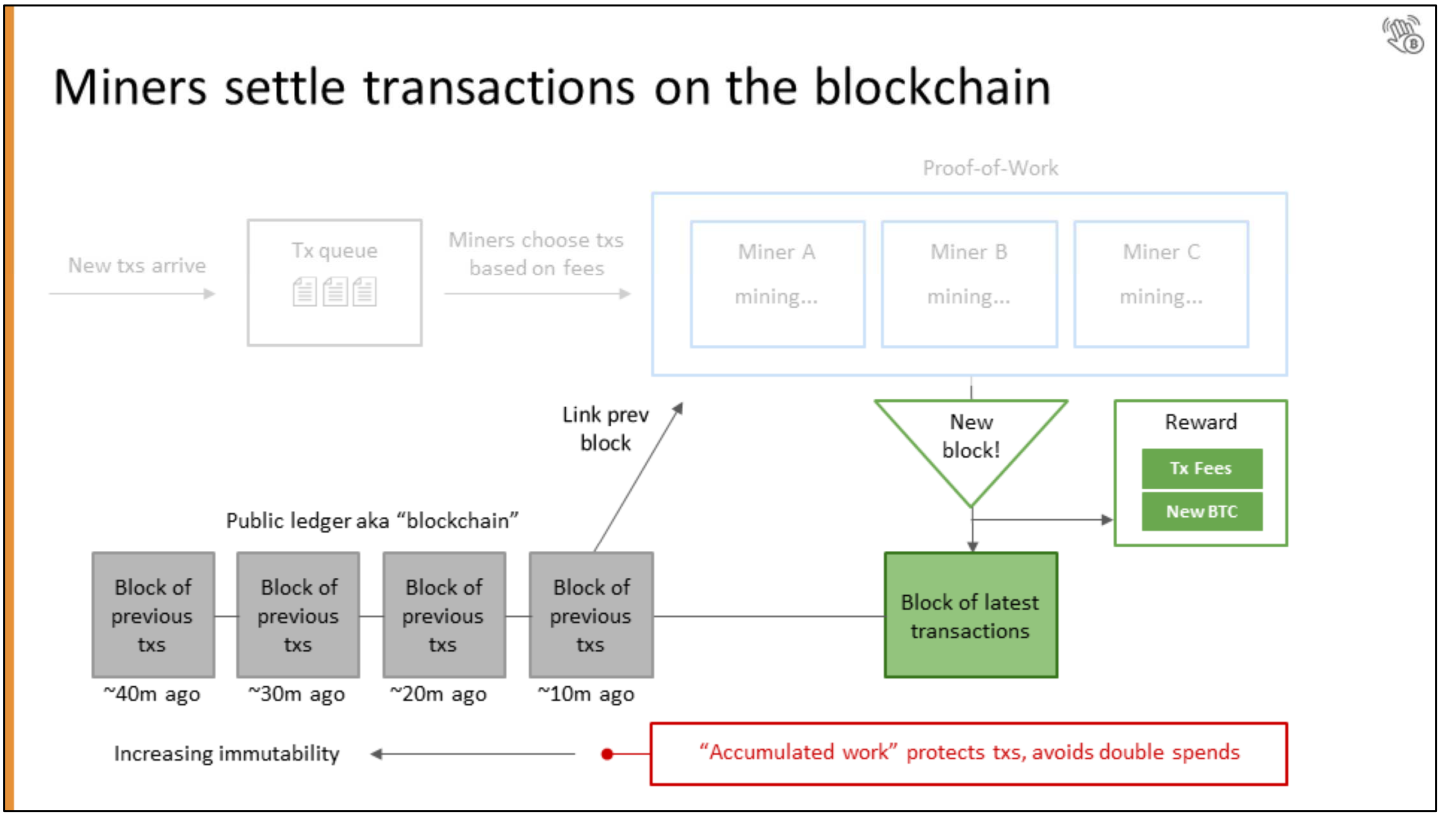
Once verified, nodes add block to their copy of the ledger and relay it

Critical that verification remain a decentralized process to keep miners honest

Blocks are valid if they:

1. Obey protocol rules
2. Meet PoW requirements

- Game theory then suggests that each miner accepts the block and begins attempting to produce the *next* valid block with a new set of transactions
  - The odds of finding a new block doesn't change for a miner, so it isn't like they're "starting over from the beginning" … in fact *each hash* they do is starting over from the beginning
  - If a miner were to ignore a new valid block, and continue attempting to build off of the block they had been, this would create a fork, but the rest of the network would reject their new block once broadcast because it would represent a "shorter chain"
- Similarly, each node in the network verifies the new block is valid and accepts it **[explicitly refer to this addressing question #1]**
  - To emphasize the importance bitcoin puts on allowing anyone to participate, it is possible to run a bitcoin node on a $100 Android phone and audit the entire history of 600k blocks and 500m transactions.



Miners settle transactions on the blockchain

Proof-of-Work

New txs arrive

Tx queue

Miners choose txs based on fees

Miner A mining…

Miner B mining…

Miner C mining…

Link prev block

New block!

Reward

Tx Fees

New BTC

Public ledger aka “blockchain”

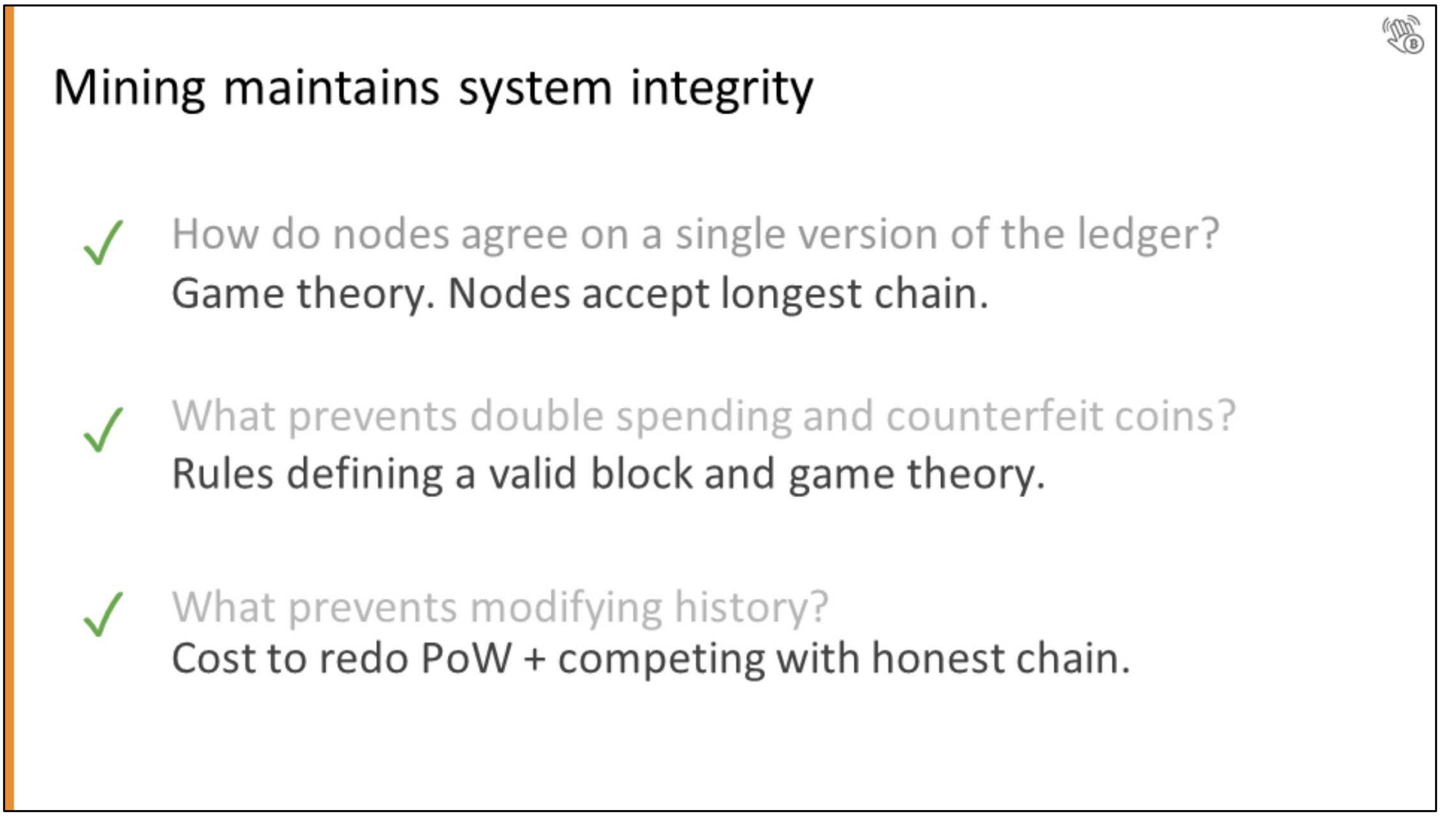
Block of previous txs	Block of previous txs	Block of previous txs	Block of previous txs	Block of latest transactions
~40m ago	~30m ago	~20m ago	~10m ago	

Increasing immutability

“Accumulated work” protects txs, avoids double spends

RECAP

Highlight: block reward, increasing immutability of the ledger



Mining maintains system integrity

- ✓ How do nodes agree on a single version of the ledger?
  Game theory. Nodes accept longest chain.
- ✓ What prevents double spending and counterfeit coins?
  Rules defining a valid block and game theory.
- ✓ What prevents modifying history?
  Cost to redo PoW + competing with honest chain.

single version of ledger ... because each node accepts the longest chain of valid blocks as the valid version of history

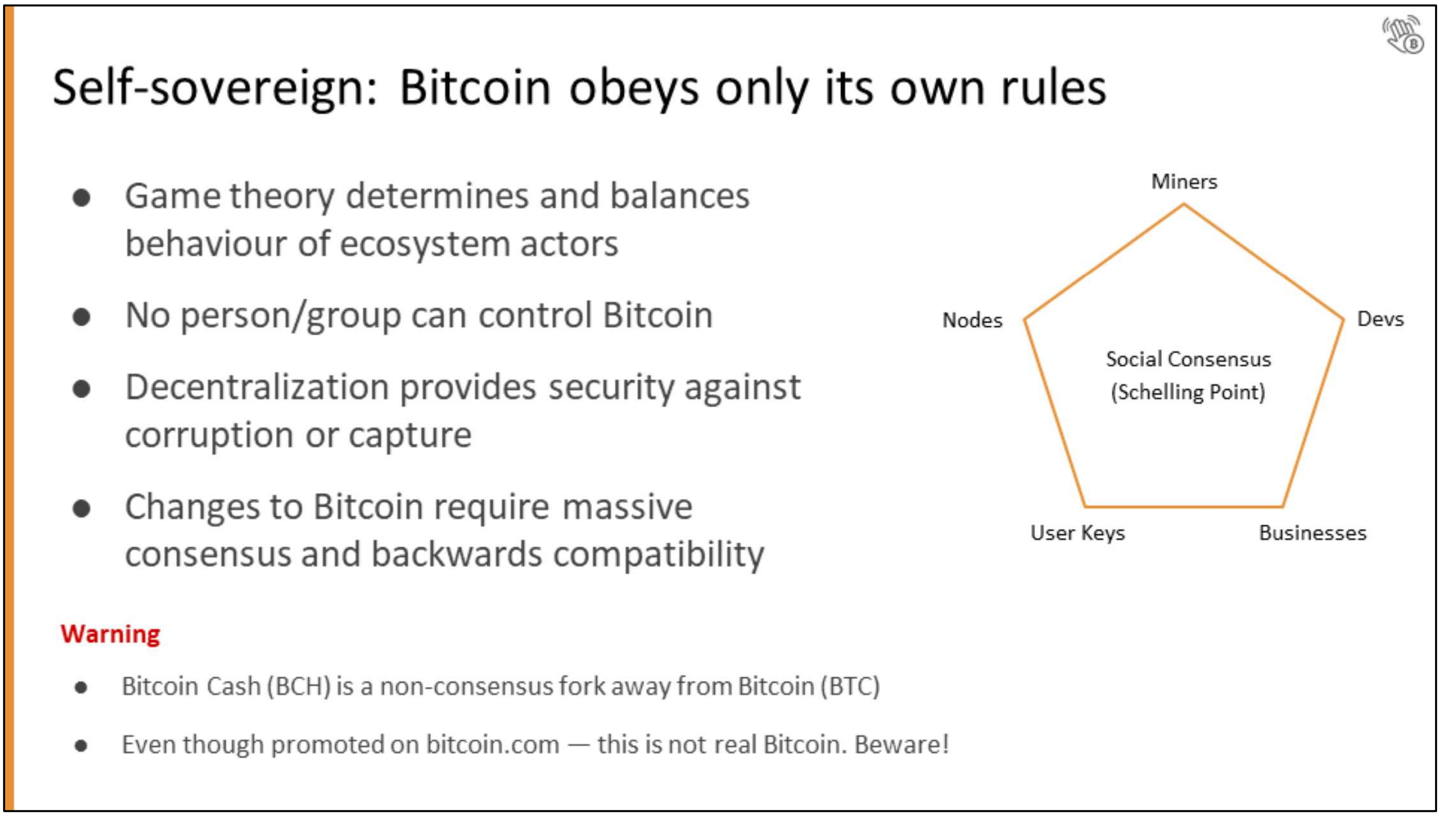
double spending and counterfeit ... to do so would be creation of an invalid block, which miners would reject because they don't want to mine (and spend money) building off of a block they anticipate the rest of the network rejecting. similarly, non-mining nodes would reject as (a) it isn't in their self-interest (only the double spenders) (b) game theory suggests majority will reject

modifying history ... to go back and modify a transaction from, say, last week, would necessitate re-mining 1000+ blocks, which would cost a LOT of money, and, you'd be racing against the rest of the network which would continue to build onto the "valid" chain

Let’s zoom out again.

Bitcoin is a new form of p2p digital money that is:

1. **Self-sovereign**
2. Scarce
3. Open to all



Self-sovereign: Bitcoin obeys only its own rules

- Game theory determines and balances behaviour of ecosystem actors
- No person/group can control Bitcoin
- Decentralization provides security against corruption or capture
- Changes to Bitcoin require massive consensus and backwards compatibility

Miners
Nodes
Devs
Social Consensus
(Schelling Point)
User Keys
Businesses

Warning

- Bitcoin Cash (BCH) is a non-consensus fork away from Bitcoin (BTC)
- Even though promoted on bitcoin.com — this is not real Bitcoin. Beware!

Important hisory: all attempts at ecash prior to bitcoin were shut down, example: https://en.wikipedia.org/wiki/Liberty_dollar_(private_currency)

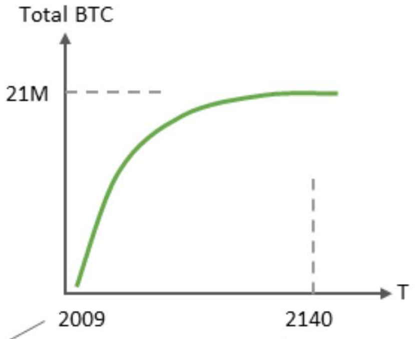
RE: Bitcoin Cash - mere fact that bitcoin.com can be captured by a scam, is testament to the unprecendented freedom of Bitcoin.
RE: Scams in general - lots of greed and misinformation out there. Education and vigilance is important!

Bitcoin is a new form of p2p digital money that is:

1. Self-sovereign
2. **Scarce**
3. Open to all

Digital scarcity: only 21M bitcoins will ever exist (!)

This fixed monetary policy cannot be changed—it is apolitical.



The 21M supply cap is enforced by code, verifiability and social consensus.

Every 4 years the "block reward" to miners drops by half.

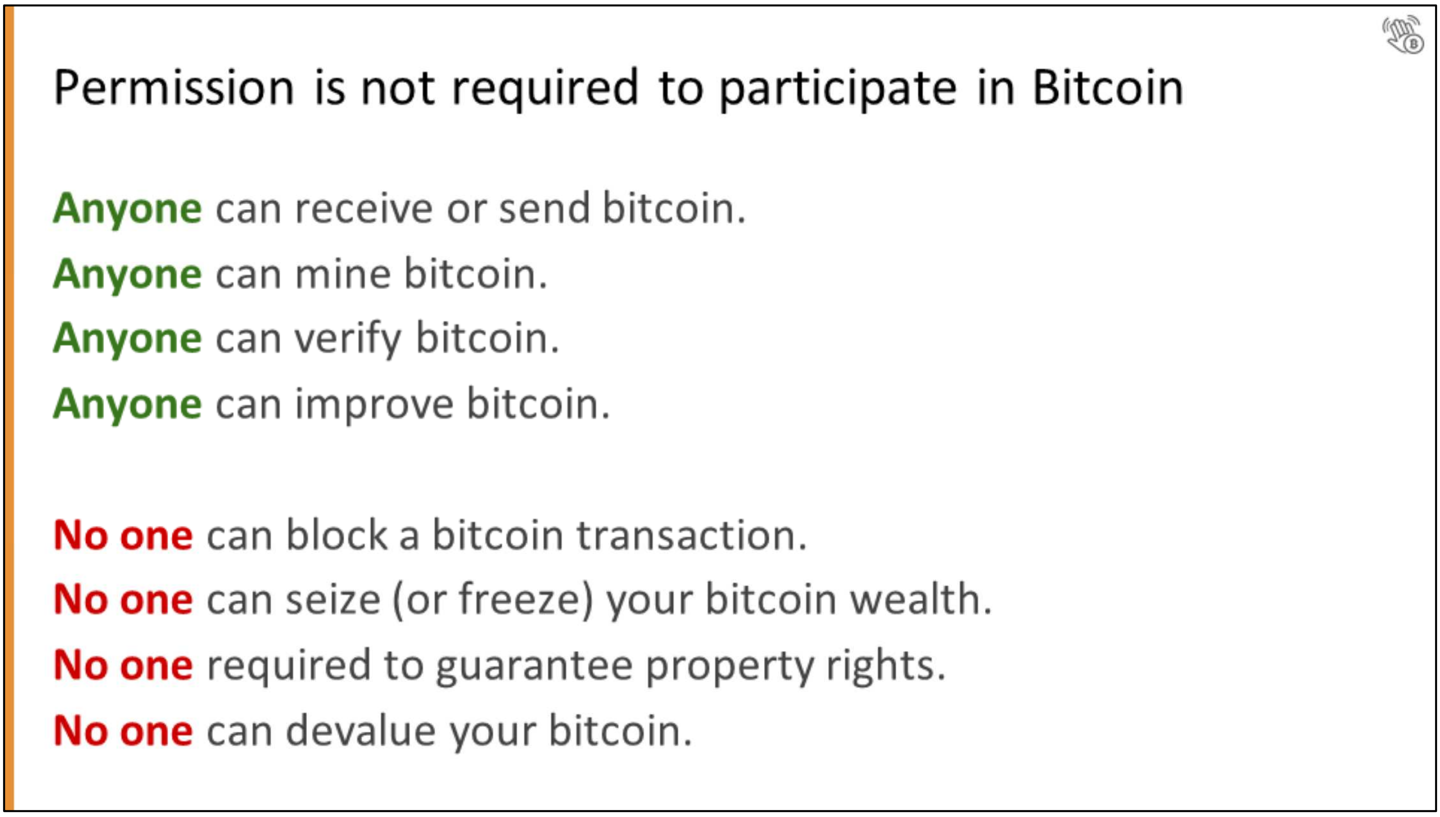
The last new bitcoin will be issued in the year 2140.

Fun facts

- In May block reward drops 12.5→6.25
- 85% of all bitcoins have already been mined
- Up to 4M bitcoins may be lost
- Impossible for every existing millionaire to own a whole bitcoin
- 0.28 BTC is sufficient to be in the top 1% of holders

Bitcoin is a new form of p2p digital money that is:

1. Self-sovereign
2. Scarce
3. **Open to all**



Permission is not required to participate in Bitcoin

Anyone can receive or send bitcoin.

Anyone can mine bitcoin.

Anyone can verify bitcoin.

Anyone can improve bitcoin.

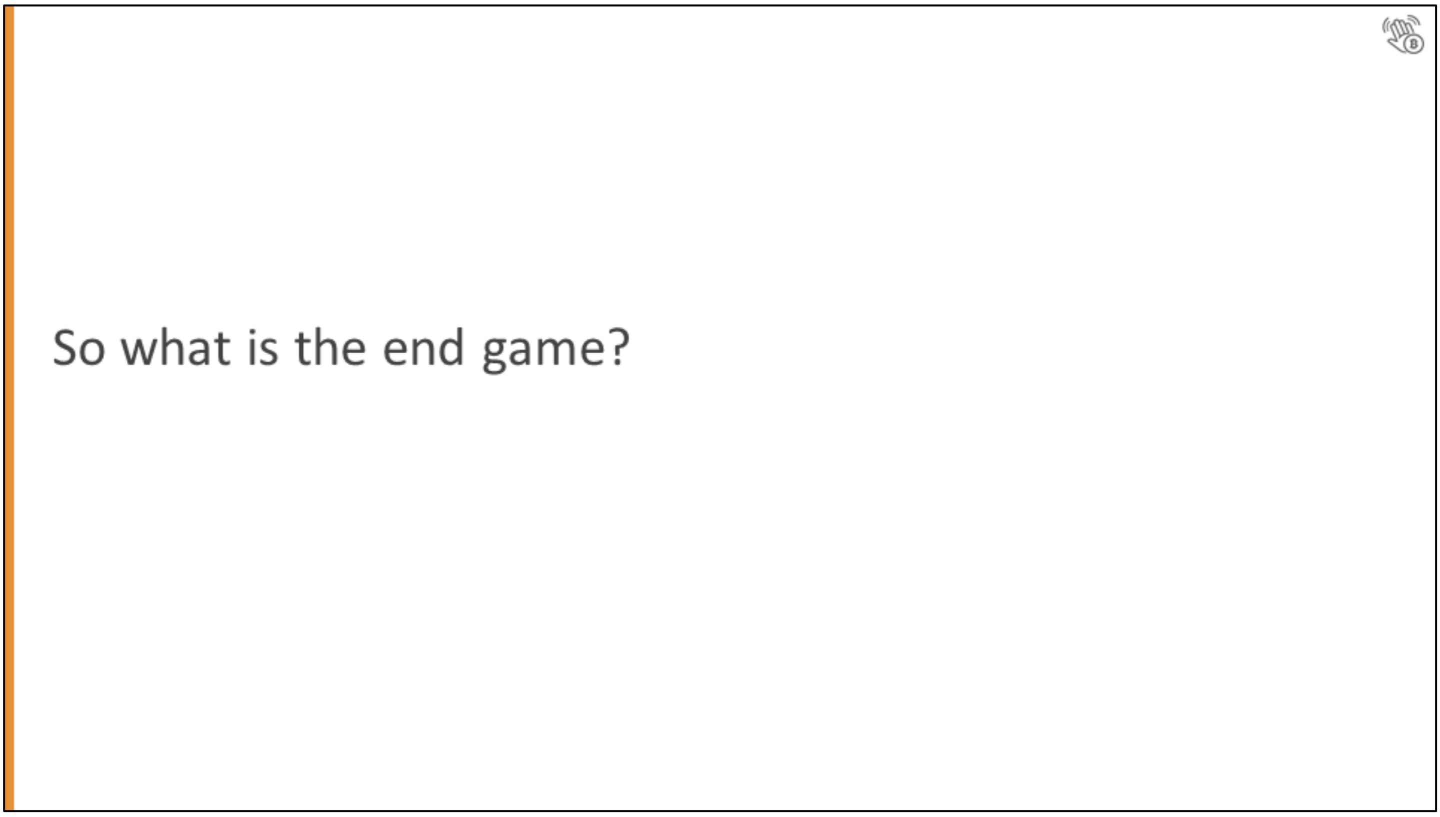
No one can block a bitcoin transaction.

No one can seize (or freeze) your bitcoin wealth.

No one required to guarantee property rights.

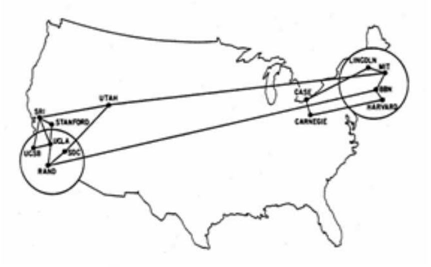
No one can devalue your bitcoin.

you don't have to apply for an account, fax in forms to some institution, etc. you just need to pick a number!



So what is the end game?

New protocols take time to mature



1970

Netscape - [Version 2.01]
File Edit View Go Bookmarks Options Directory Window Help
Location:
What's New! What's Cool! Handbook Net Search Net Directory Software
NETSCAPE

Netscape Navigator (TM)
Version 2.01
Copyright © 1994-1995 Netscape Communications Corporation, All rights reserved.

This software is subject to the license agreement set forth in the license. Please read and agree to all terms before using this software.

Report any problems through the feedback page.

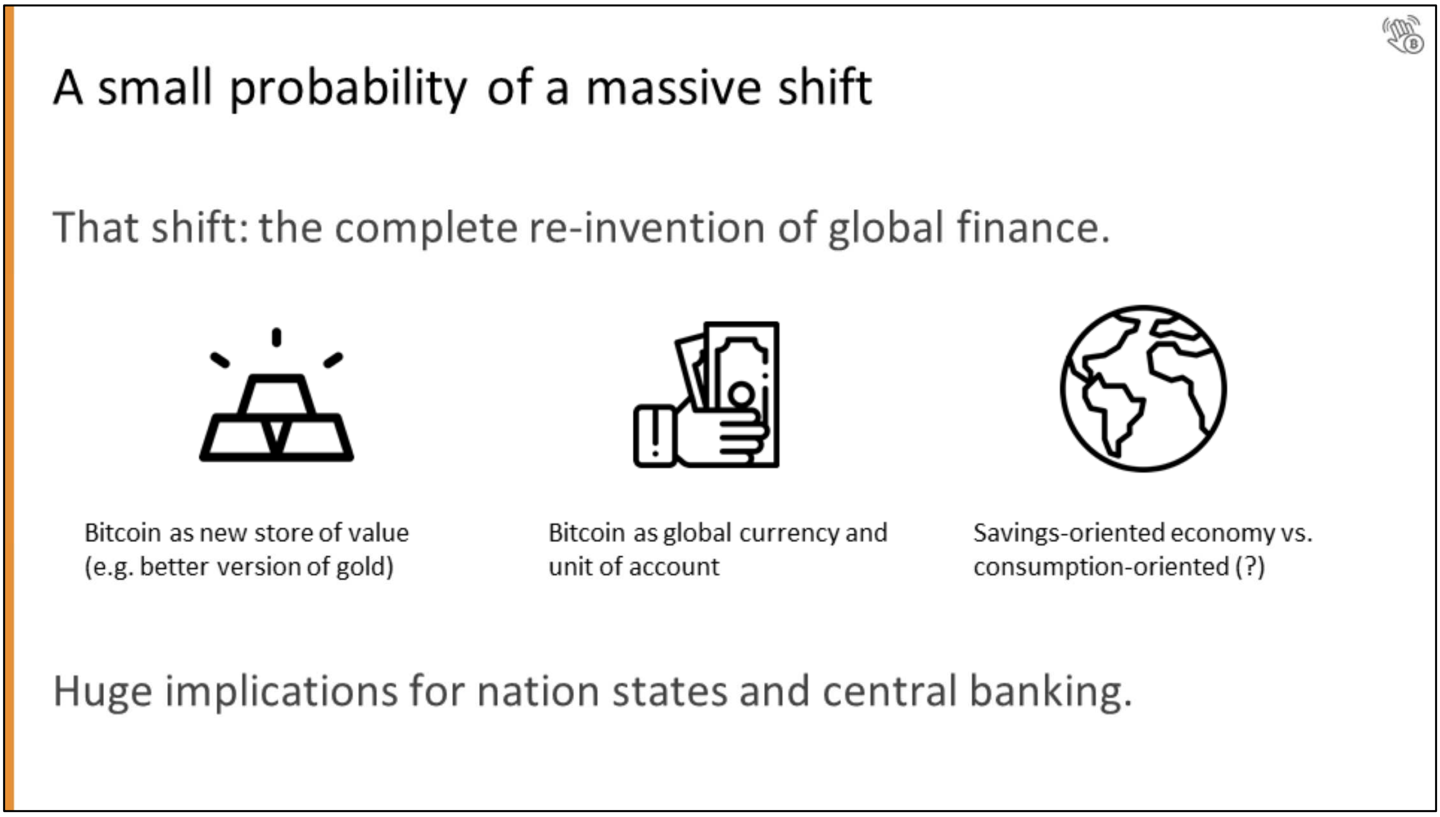
Netscape Communications, Netscape, Netscape Navigator and the Netscape Communications logo are trademarks of Netscape Communications Corporation.

Contains Java™ software developed by Sun Microsystems, Inc.
Copyright © 1992-1995 Sun Microsystems, Inc. All Rights Reserved.

1995

2020

Speak to big areas that still need a lot of improvement: UX. Scaling. Security. Privacy. Volatility. Tax regulation.



A small probability of a massive shift

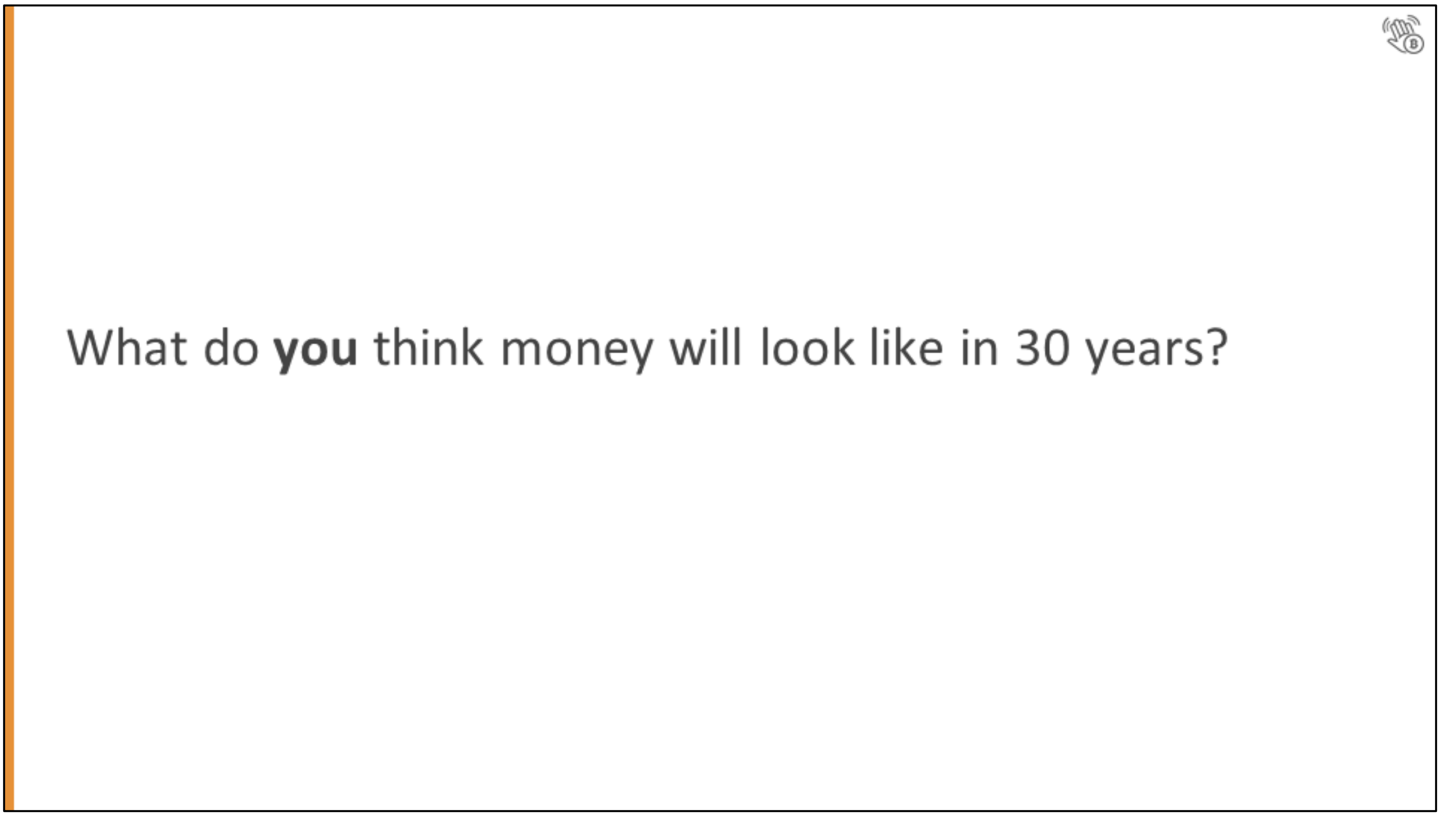
That shift: the complete re-invention of global finance.

Bitcoin as new store of value
(e.g. better version of gold)

Bitcoin as global currency and
unit of account

Savings-oriented economy vs.
consumption-oriented (?)

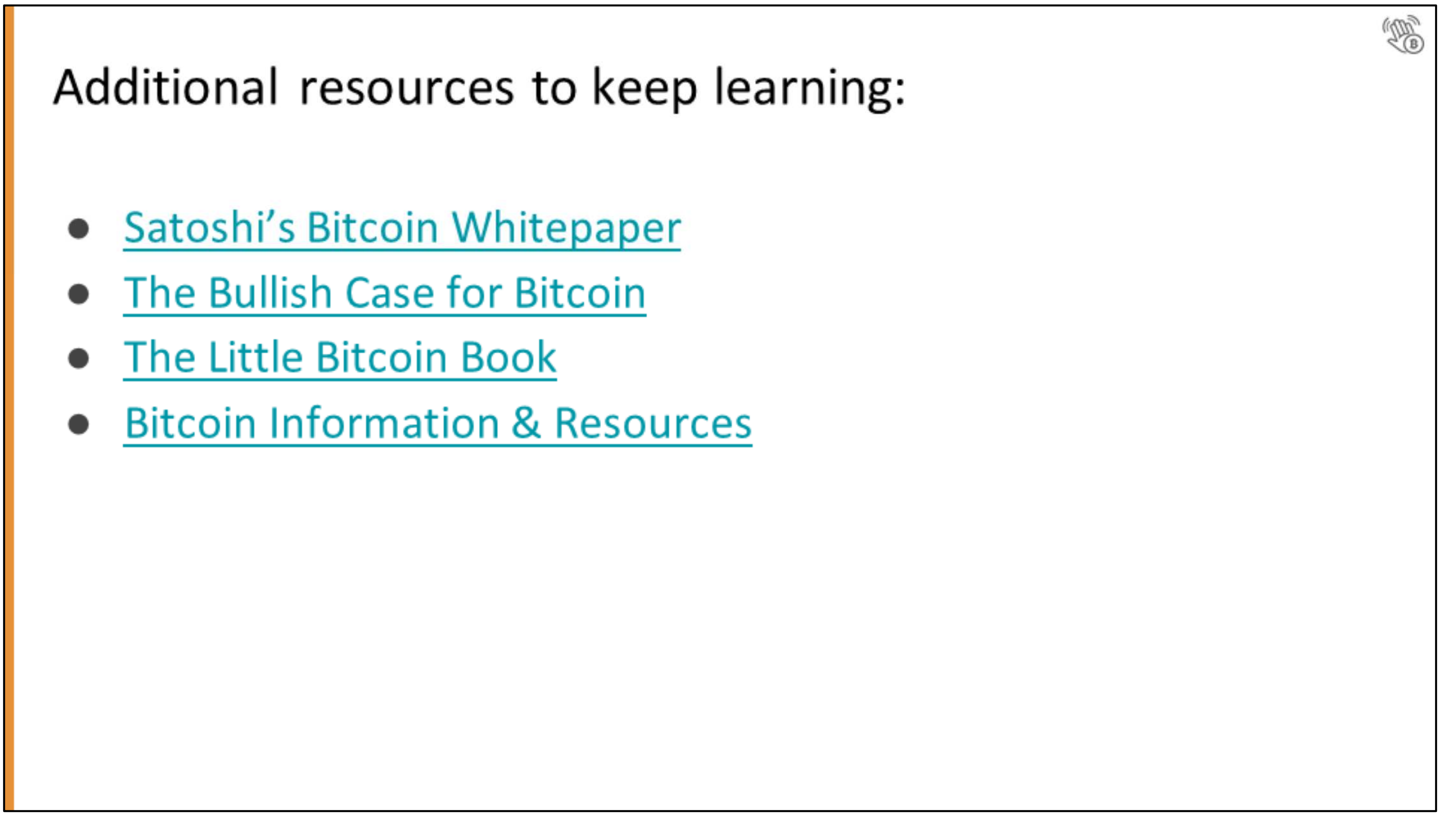
Huge implications for nation states and central banking.



What do **you** think money will look like in 30 years?

Thank you.

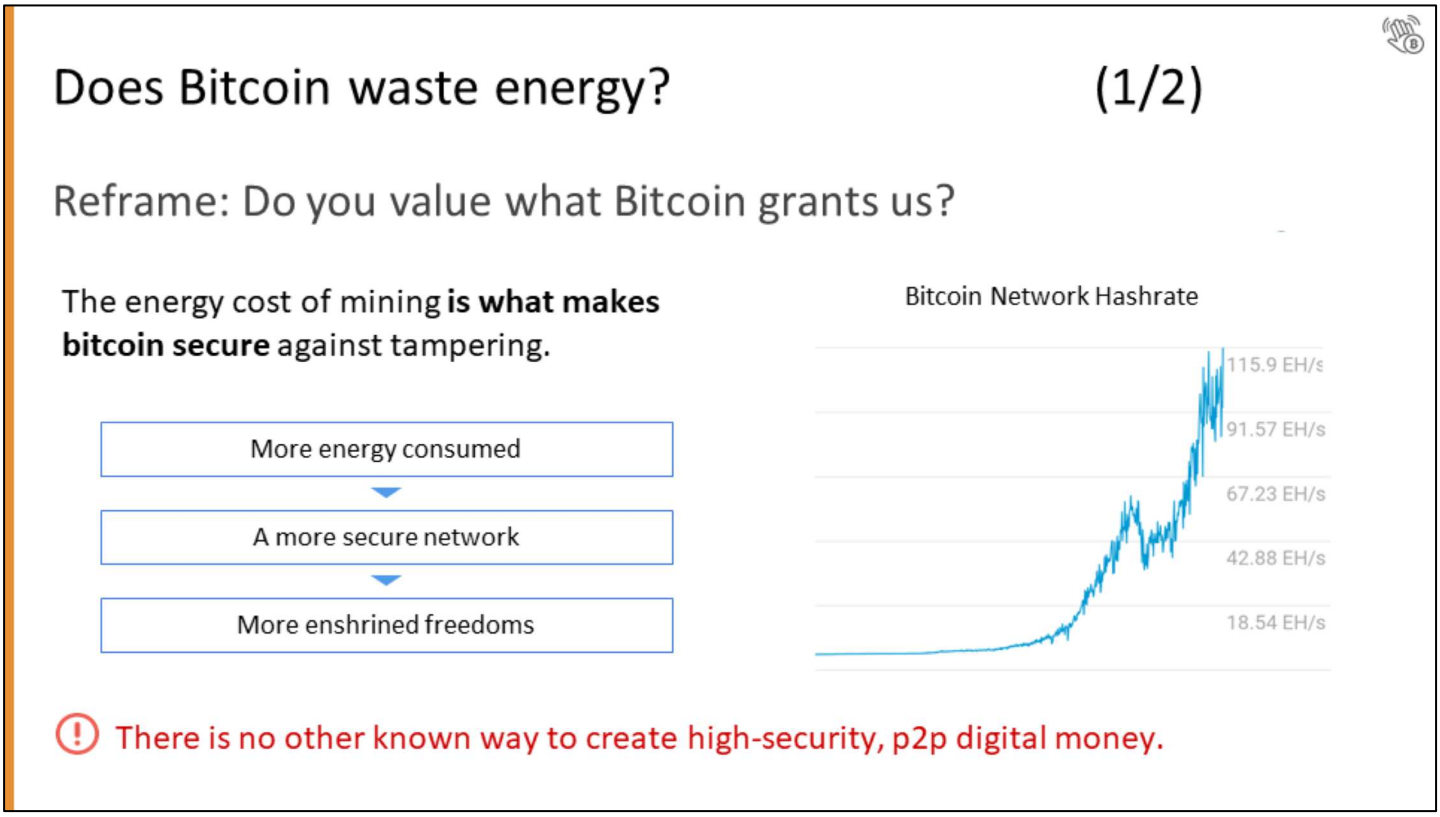
http://hellobitco.in @hello_bitcoin llo-bitcoin



Additional resources to keep learning:

- Satoshi’s Bitcoin Whitepaper
- The Bullish Case for Bitcoin
- The Little Bitcoin Book
- Bitcoin Information & Resources

Appendix: Additional Q&A



Does Bitcoin waste energy? (1/2)

Reframe: Do you value what Bitcoin grants us?

The energy cost of mining **is what makes bitcoin secure** against tampering.

More energy consumed

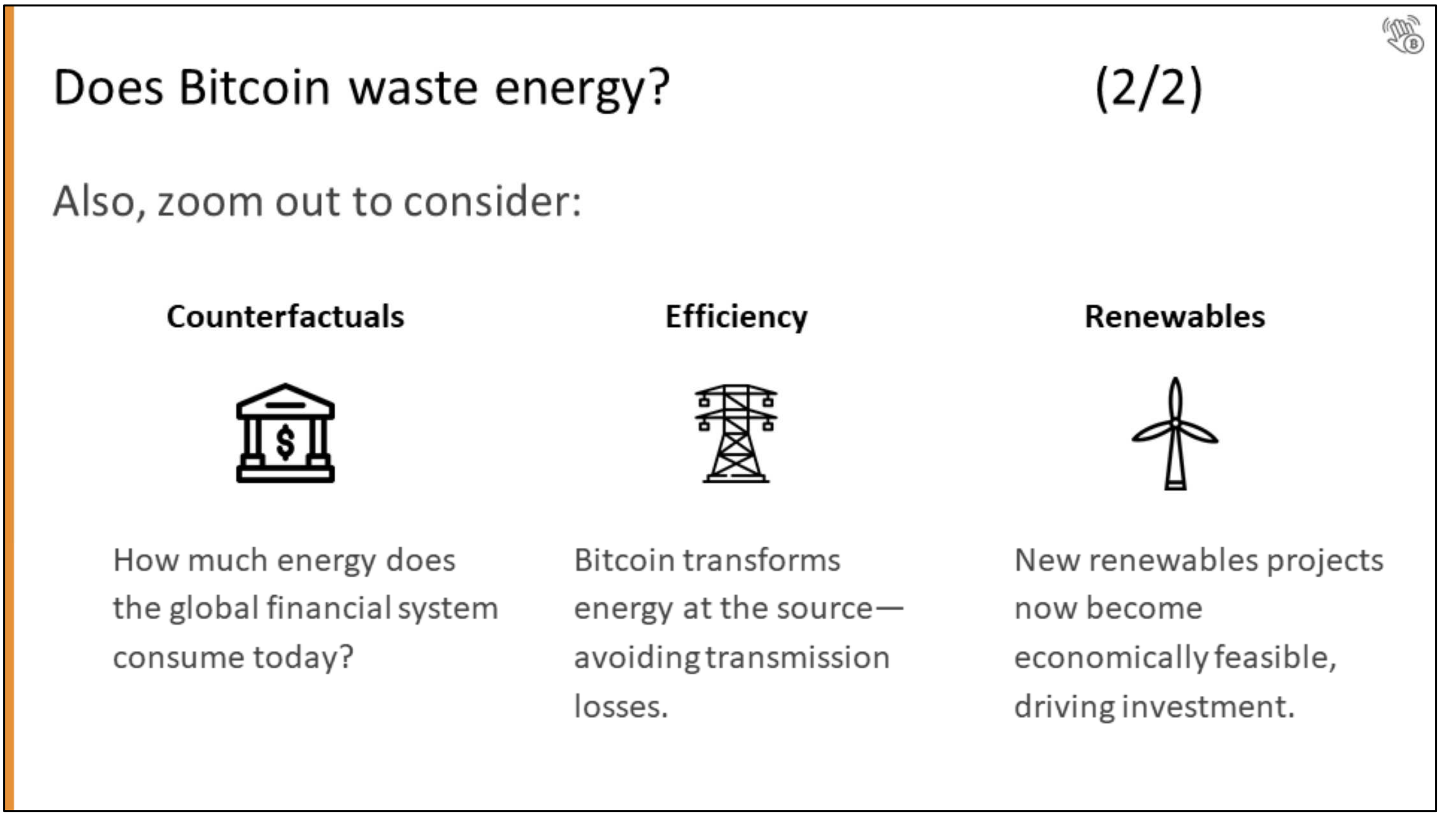
A more secure network

More enshrined freedoms

Bitcoin Network Hashrate

115.9 EH/s
91.57 EH/s
67.23 EH/s
42.88 EH/s
18.54 EH/s

ⓘ There is no other known way to create high-security, p2p digital money.



Does Bitcoin waste energy? (2/2)

Also, zoom out to consider:

Counterfactuals

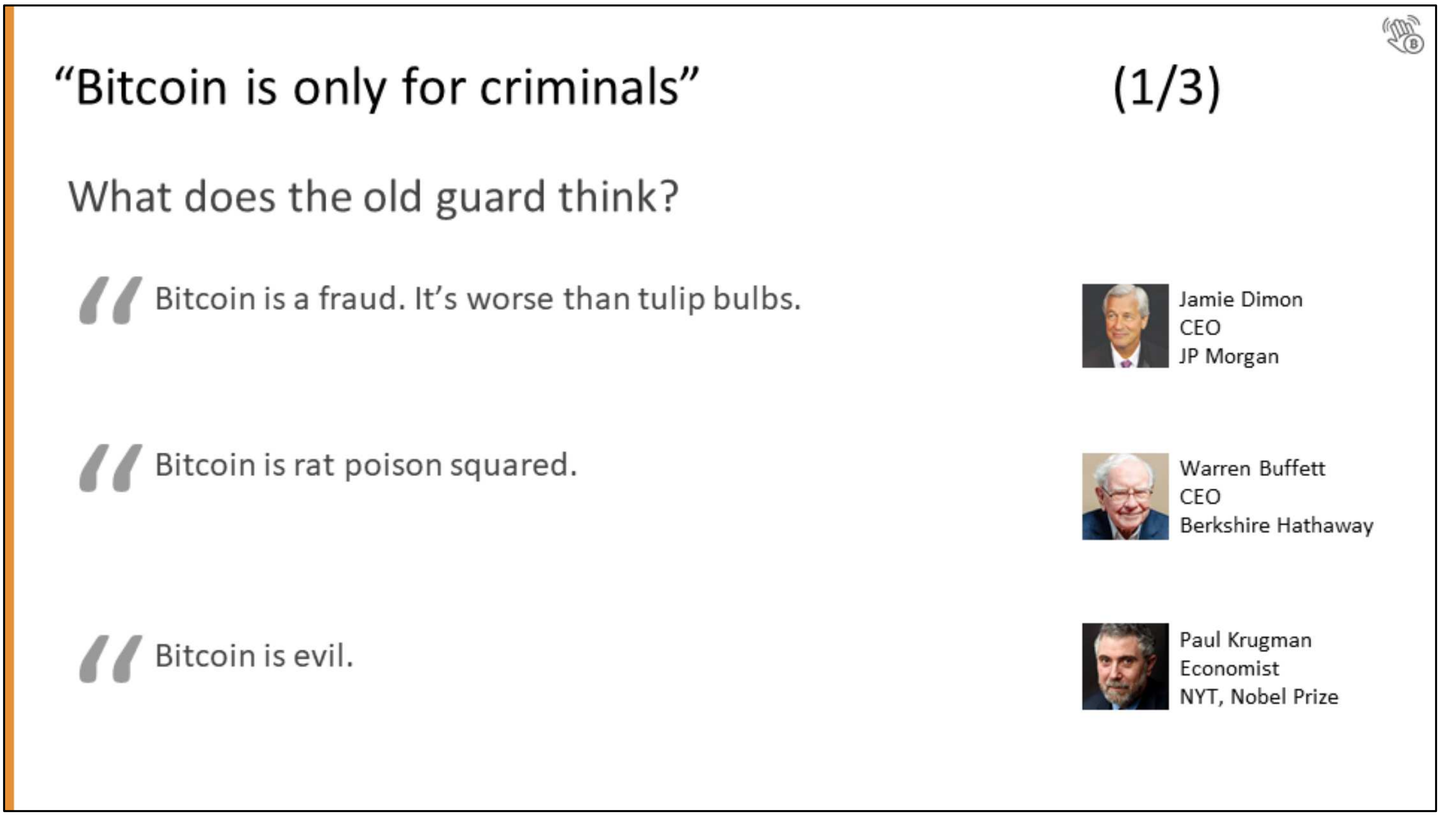
How much energy does the global financial system consume today?

Efficiency

Bitcoin transforms energy at the source—avoiding transmission losses.

Renewables

New renewables projects now become economically feasible, driving investment.



“Bitcoin is only for criminals” (1/3)

What does the old guard think?

“ Bitcoin is a fraud. It’s worse than tulip bulbs.

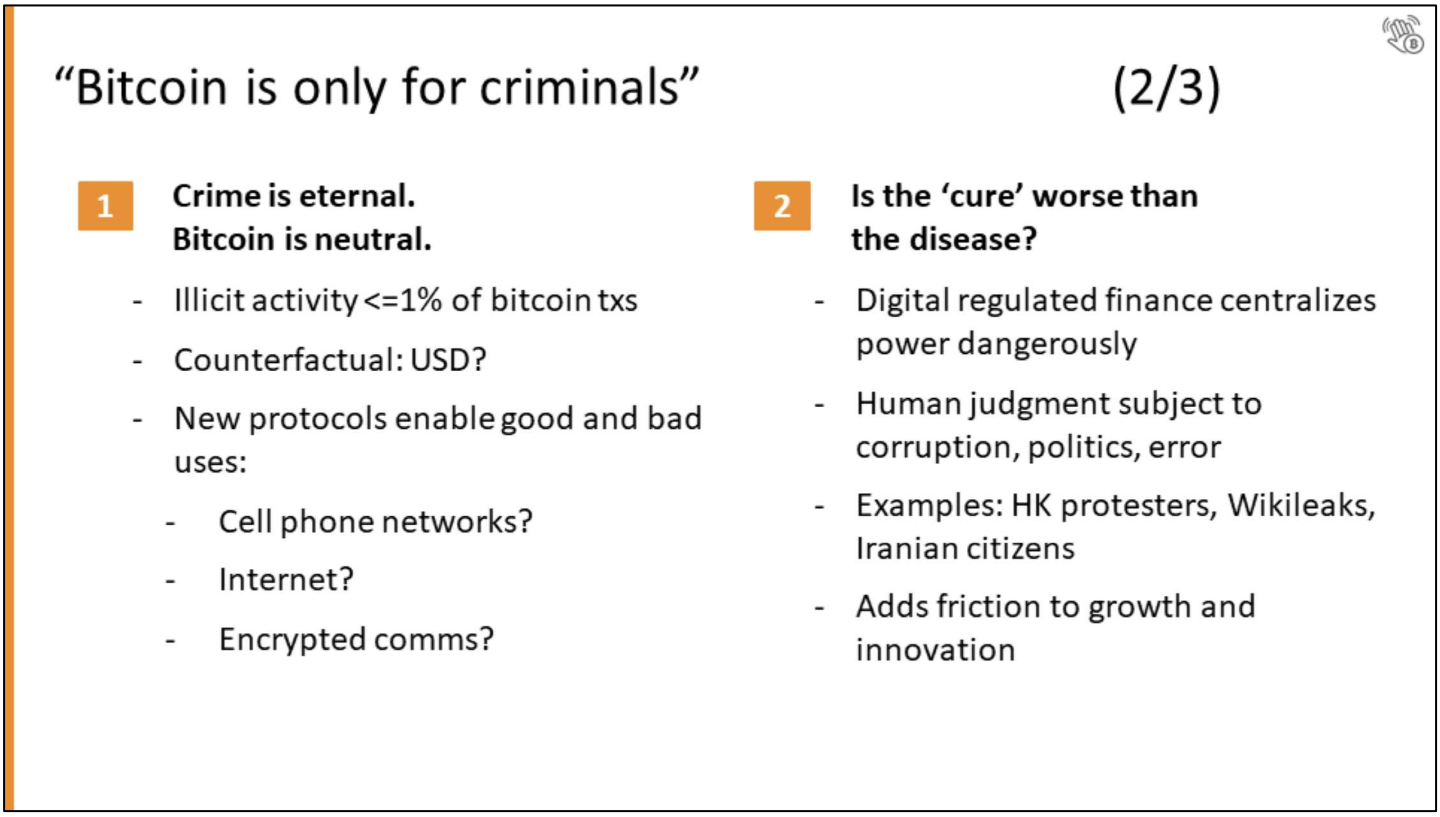
Jamie Dimon
CEO
JP Morgan

“ Bitcoin is rat poison squared.

Warren Buffett
CEO
Berkshire Hathaway

“ Bitcoin is evil.

Paul Krugman
Economist
NYT, Nobel Prize



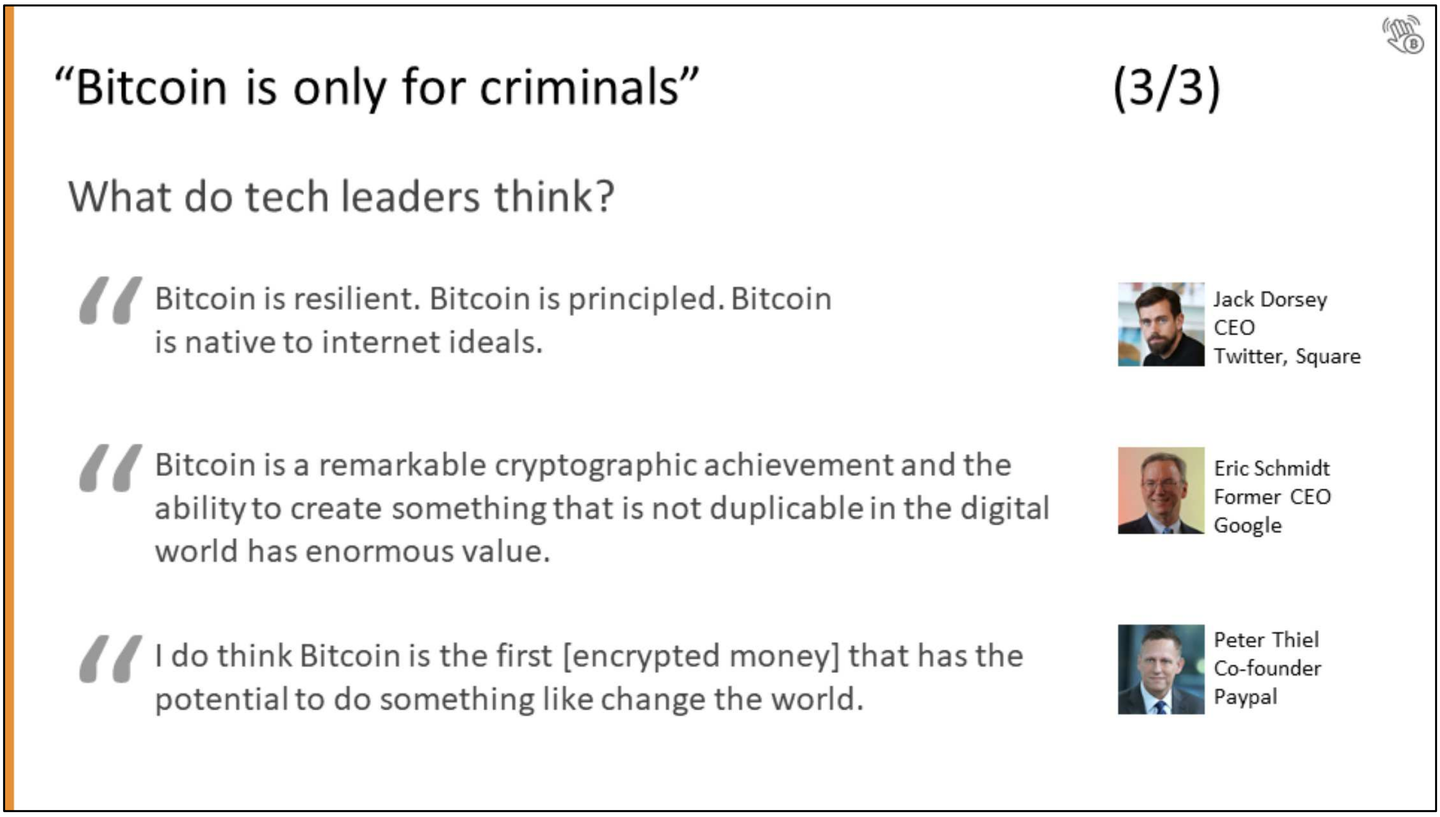
“Bitcoin is only for criminals” (2/3)

1 **Crime is eternal.**
Bitcoin is neutral.

- Illicit activity <=1% of bitcoin txs
- Counterfactual: USD?
- New protocols enable good and bad uses:
  - Cell phone networks?
  - Internet?
  - Encrypted comms?

2 **Is the ‘cure’ worse than the disease?**

- Digital regulated finance centralizes power dangerously
- Human judgment subject to corruption, politics, error
- Examples: HK protesters, Wikileaks, Iranian citizens
- Adds friction to growth and innovation



“Bitcoin is only for criminals” (3/3)

What do tech leaders think?

> Bitcoin is resilient. Bitcoin is principled. Bitcoin is native to internet ideals.

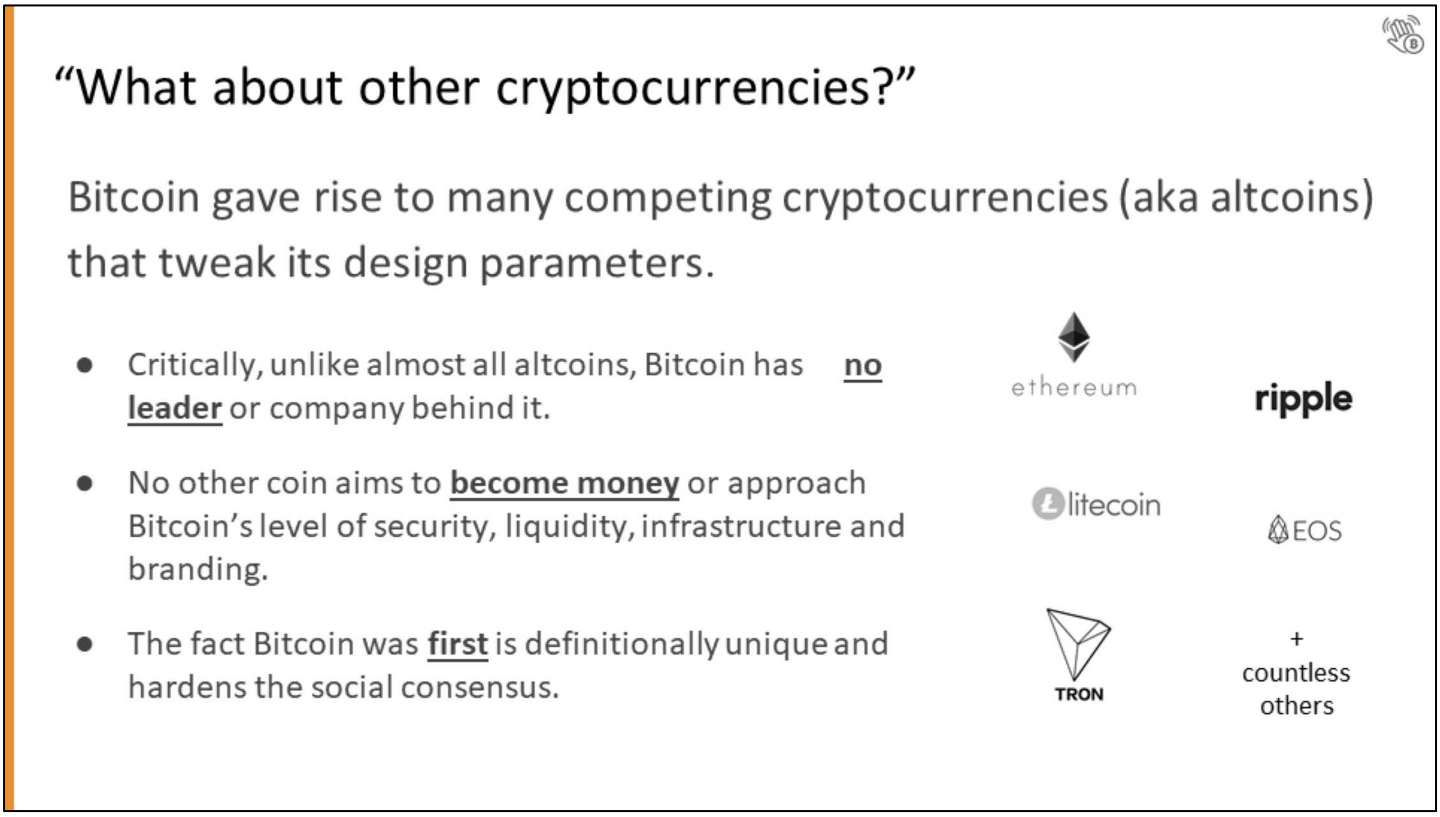
Jack Dorsey
CEO
Twitter, Square

> Bitcoin is a remarkable cryptographic achievement and the ability to create something that is not duplicable in the digital world has enormous value.

Eric Schmidt
Former CEO
Google

> I do think Bitcoin is the first [encrypted money] that has the potential to do something like change the world.

Peter Thiel
Co-founder
Paypal



“What about other cryptocurrencies?”

Bitcoin gave rise to many competing cryptocurrencies (aka altcoins) that tweak its design parameters.

- Critically, unlike almost all altcoins, Bitcoin has **no leader** or company behind it.
- No other coin aims to **become money** or approach Bitcoin’s level of security, liquidity, infrastructure and branding.
- The fact Bitcoin was **first** is definitionally unique and hardens the social consensus.

ethereum

ripple

litecoin

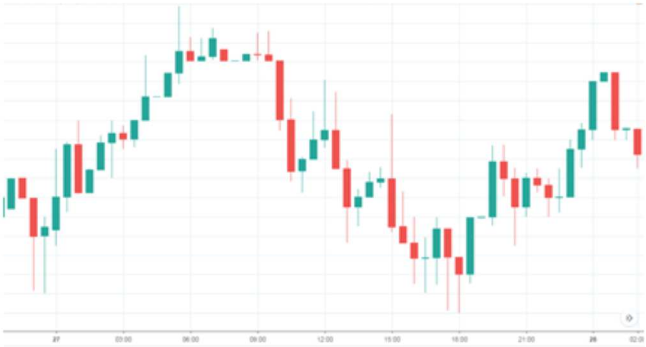
EOS

TRON

+ countless others

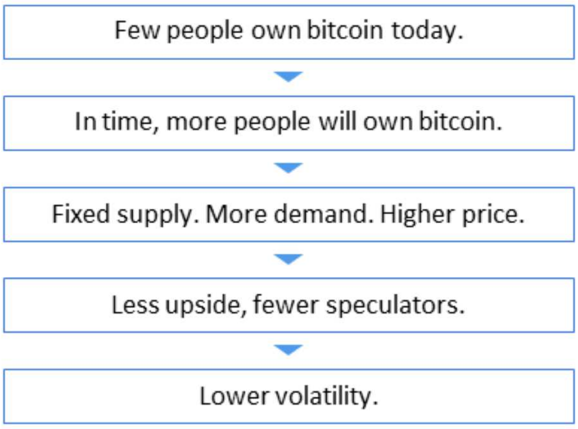
"Bitcoin is too volatile"

BTC is definitely volatile!



ⓘ Trading BTC is high risk

Volatility will decrease over time



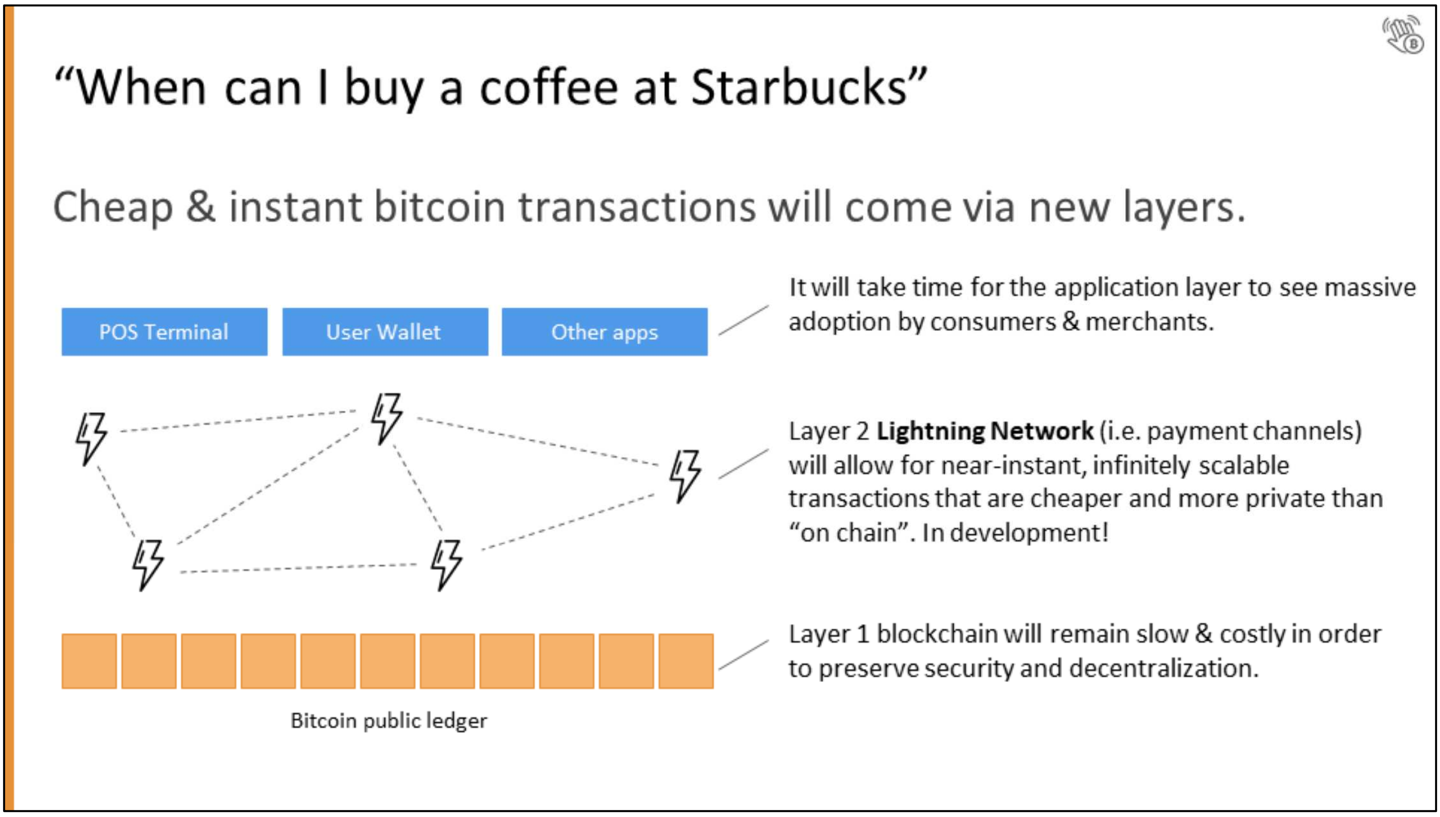
Few people own bitcoin today.

In time, more people will own bitcoin.

Fixed supply. More demand. Higher price.

Less upside, fewer speculators.

Lower volatility.



“When can I buy a coffee at Starbucks”

Cheap & instant bitcoin transactions will come via new layers.

POS Terminal

User Wallet

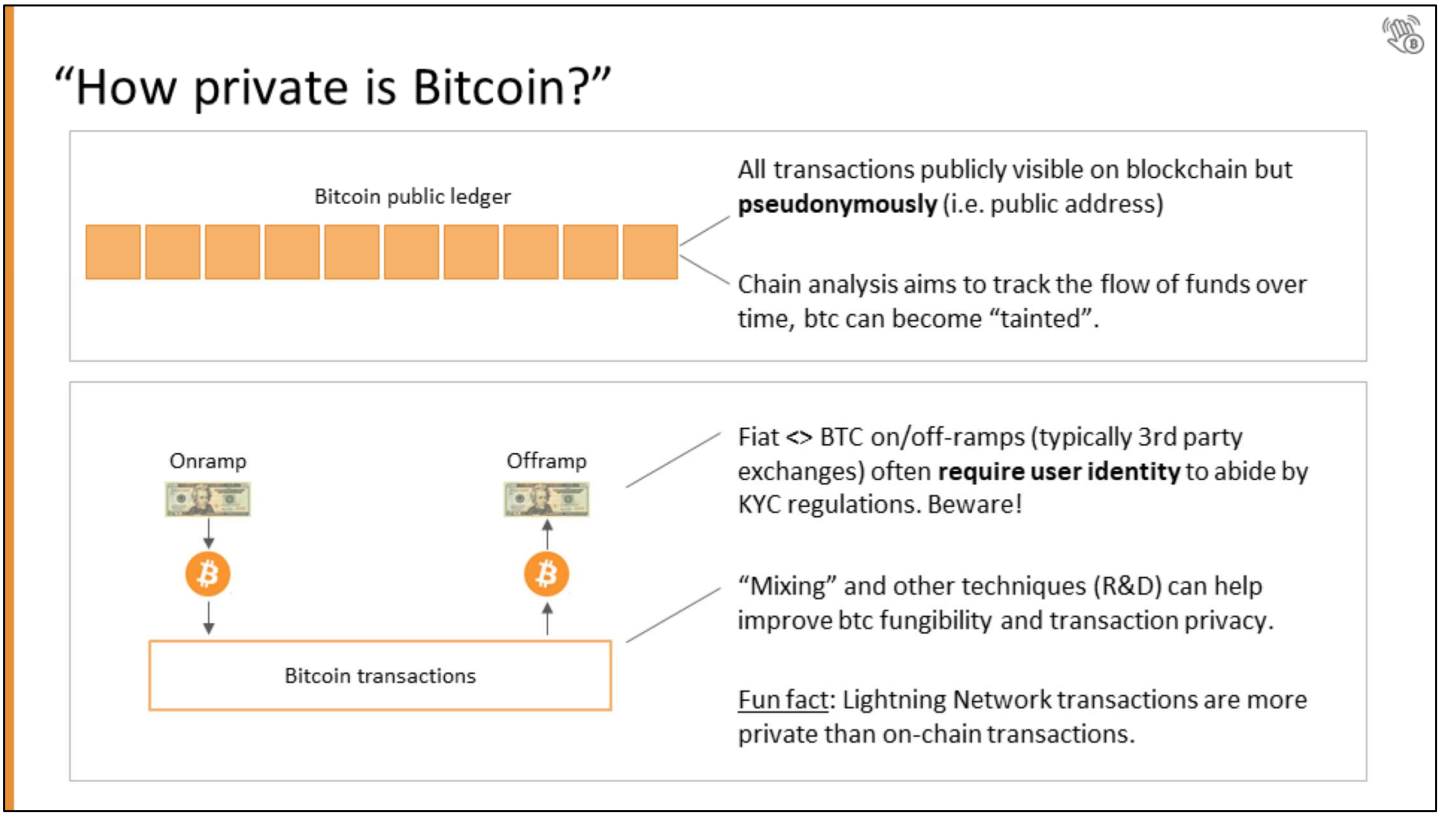
Other apps

It will take time for the application layer to see massive adoption by consumers & merchants.

Layer 2 **Lightning Network** (i.e. payment channels) will allow for near-instant, infinitely scalable transactions that are cheaper and more private than “on chain”. In development!

Layer 1 blockchain will remain slow & costly in order to preserve security and decentralization.

Bitcoin public ledger



“How private is Bitcoin?”

Bitcoin public ledger

All transactions publicly visible on blockchain but **pseudonymously** (i.e. public address)

Chain analysis aims to track the flow of funds over time, btc can become “tainted”.

Onramp

Offramp

Bitcoin transactions

Fiat <> BTC on/off-ramps (typically 3rd party exchanges) often **require user identity** to abide by KYC regulations. Beware!

“Mixing” and other techniques (R&D) can help improve btc fungibility and transaction privacy.

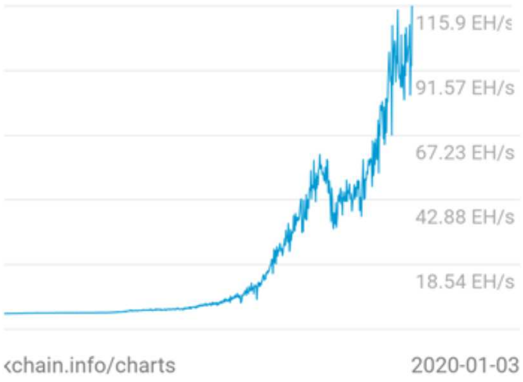
Fun fact: Lightning Network transactions are more private than on-chain transactions.

“Why not do something *useful* with PoW”

PoW mining has a singular useful purpose: securing Bitcoin.

Any "useful" work done *outside* of that purpose **does not** contribute to security (e.g. comes at the expense of security).

Bitcoin Network Hashrate



‹chain.info/charts

“How do I buy bitcoin?” (1/2)

Step 1: Buy BTC with fiat currency on a reputable site.

coinbase

Established in 2012, good UX for new users, strong security record.

$ Cash App

Mobile app from Square. Nice/easy for buying small amounts.

RIVER FINANCIAL

New Bitcoin-only startup, supports recurring buys (DCA).

“How do I buy bitcoin?” (2/2)

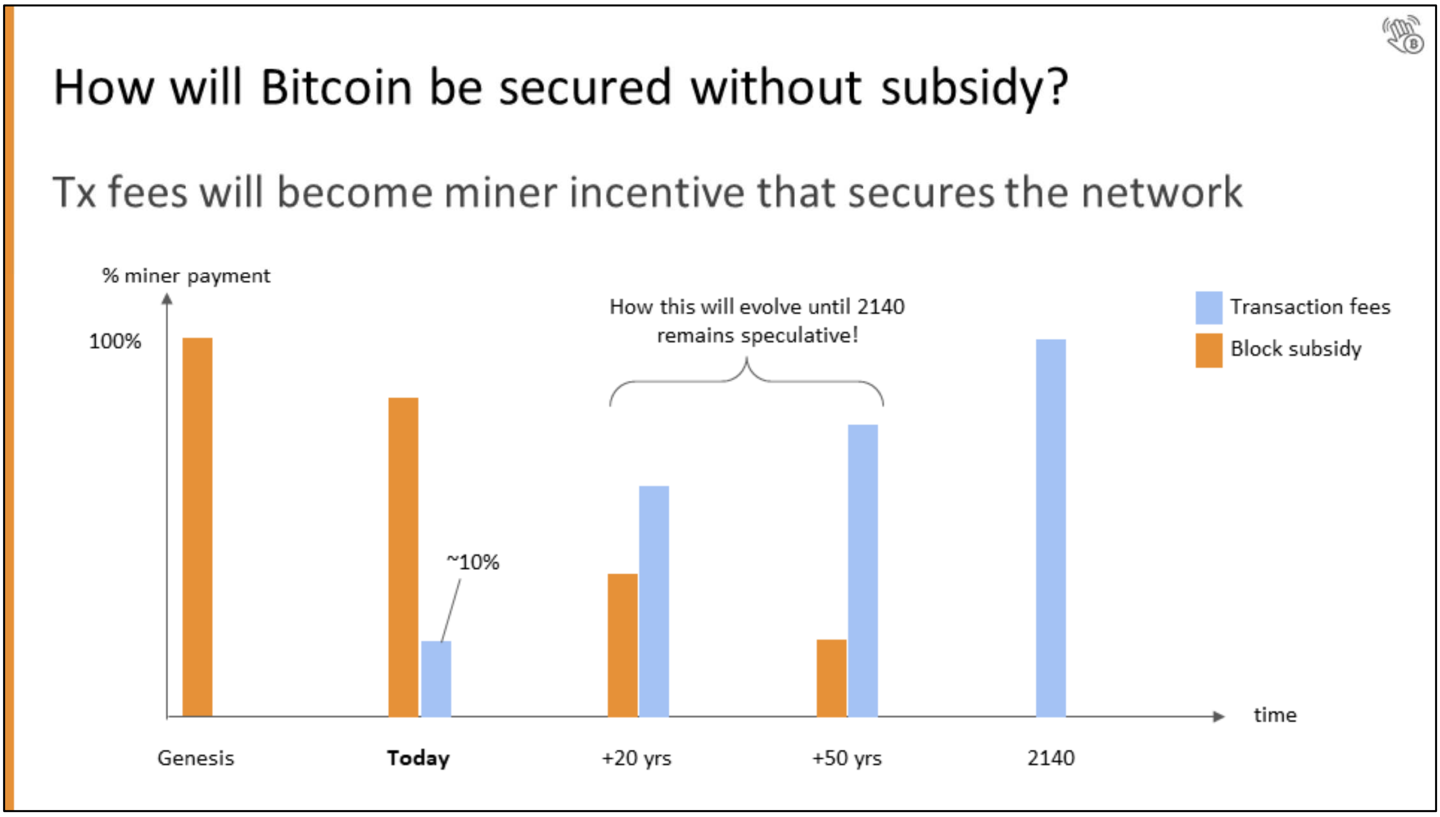
Step 2: Take custody of your private keys.

Trezor Model T — probably best user experience.

Ledger Nano X — very good, slightly clunky user input.

Blockstream Green — free mobile wallet with 2-factor auth.

Casa Keymaster Multisig Wallet — distributed private keys.



How will Bitcoin be secured without subsidy?

Tx fees will become miner incentive that secures the network