Hello Bitcoin

A friendly introduction to Bitcoin

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

Let’s talk about money.

20
FEDERAL RESERVE NOTE
20
THE UNITED STATES OF AMERICA
C 159
ID228[redacted]60B
D4
UNITED STATES FEDERAL RESERVE SYSTEM
THIS NOTE IS LEGAL TENDER
FOR ALL DEBTS, PUBLIC AND PRIVATE
Anna Escobedo Cabral
Treasurer of the United States.
C3
ID228[redacted]60B
Henry M. Paulson Jr.
Secretary of the Treasury.
SERIES 2006
20
20
JACKSON
TWENTY DOLLARS

Money has evolved, since forever.

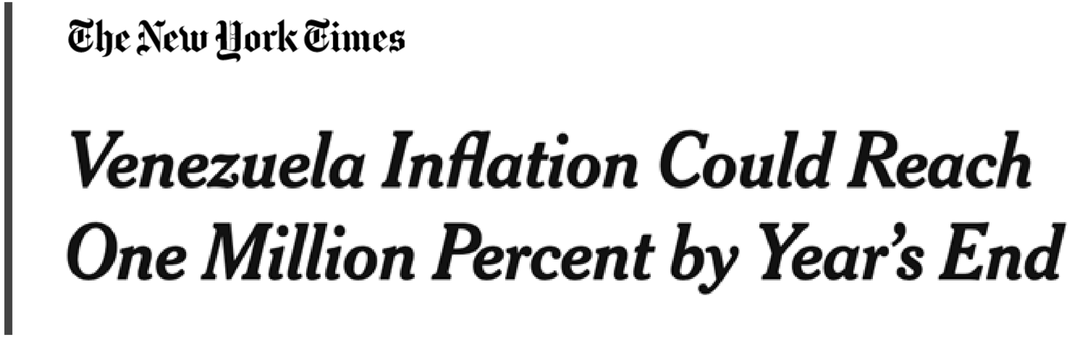
FINE
GOLD
999.9
NET WT
1000 g
NET WT
1000 g

What makes good money? Bad money?

How does where you live change your view?

Imagine...

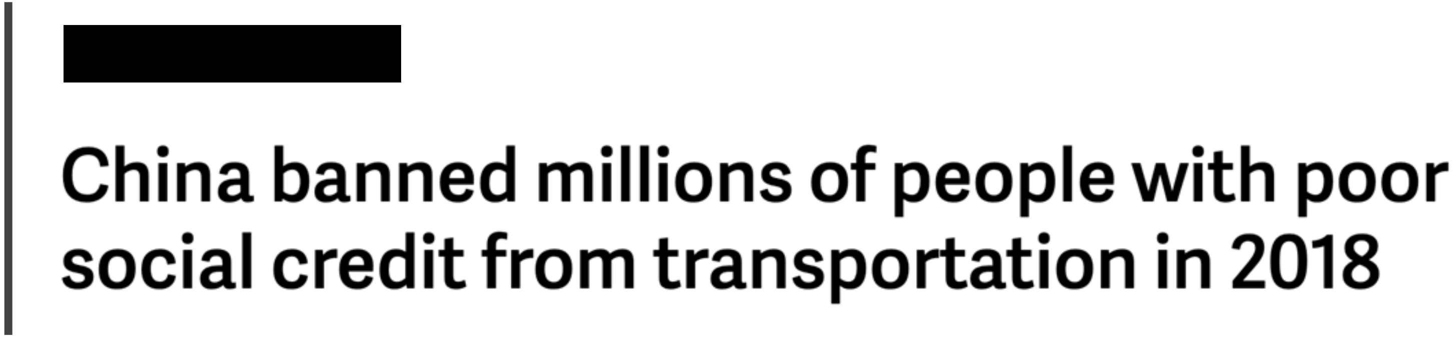
Needing protection against runaway inflation



The New York Times

Venezuela Inflation Could Reach One Million Percent by Year's End

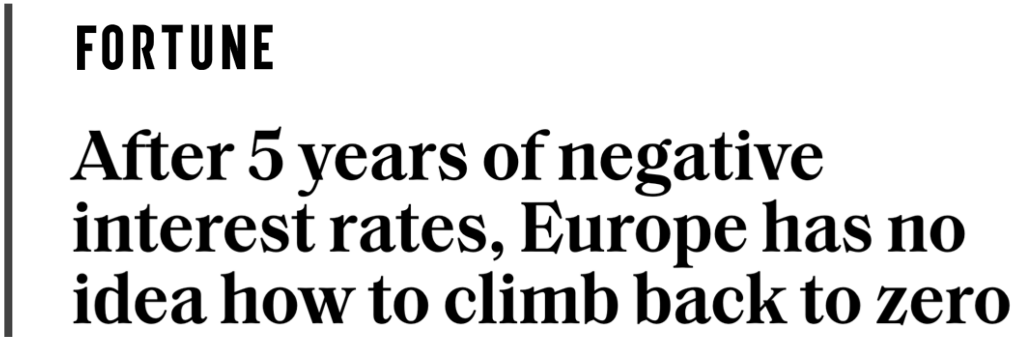
Having a check against government overreach



[redacted]

China banned millions of people with poor social credit from transportation in 2018

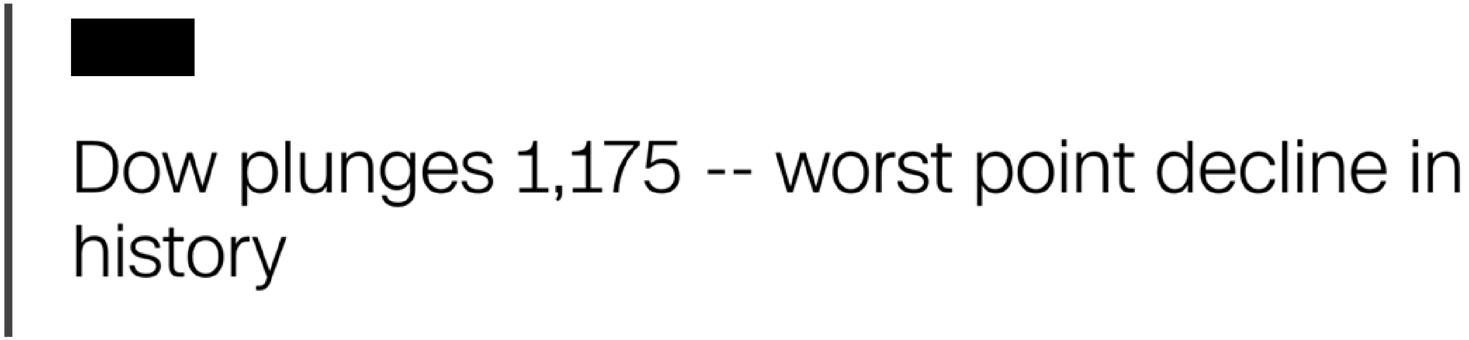
Not having good options to save without risk (1/2)



FORTUNE

After 5 years of negative interest rates, Europe has no idea how to climb back to zero

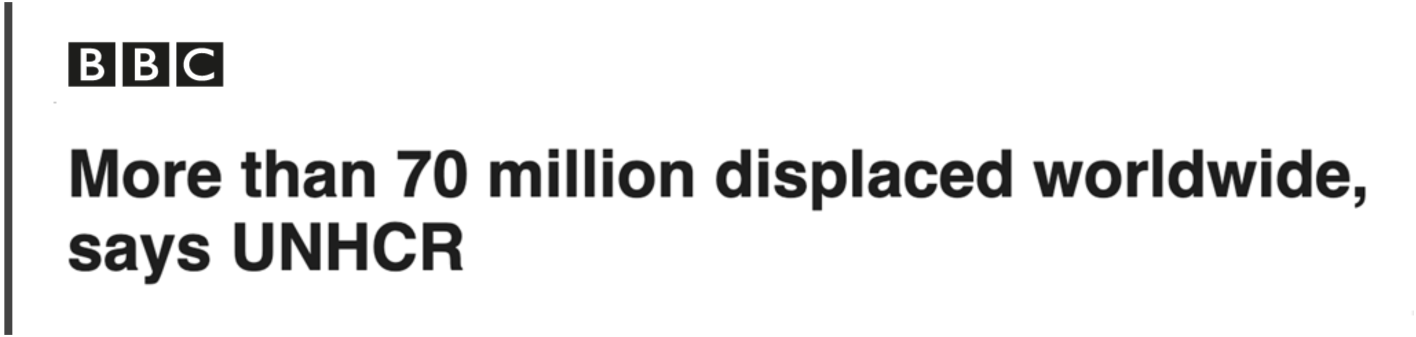
Not having good options to save without risk (2/2)



[redacted]

Dow plunges 1,175 -- worst point decline in history

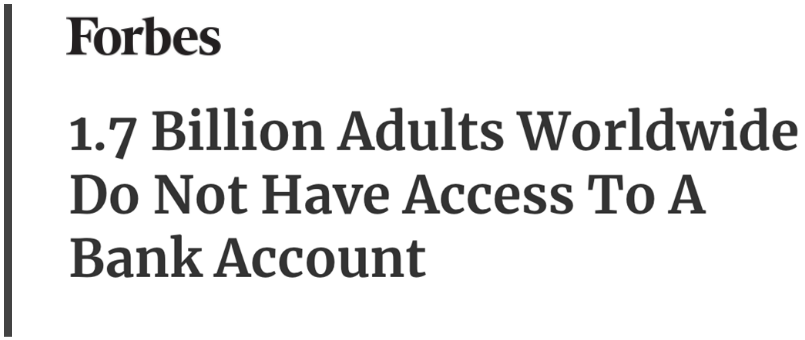
Trying to escape with any savings you have



BBC

More than 70 million displaced worldwide, says UNHCR

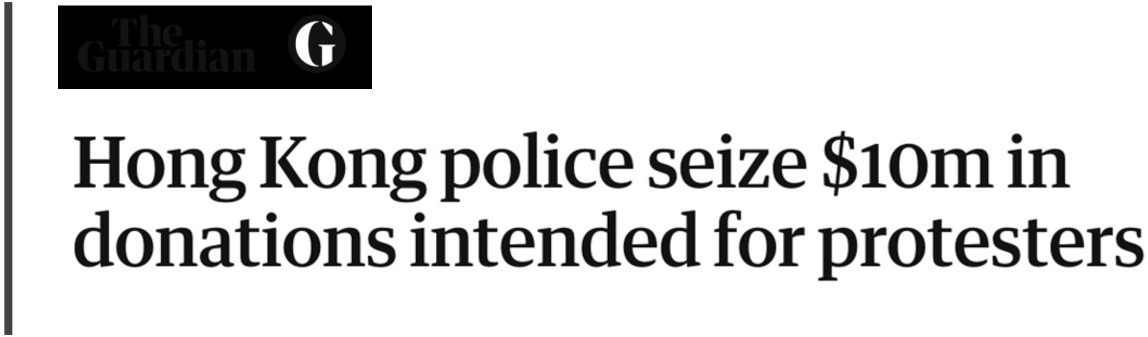
Reaching those lacking access to banking



Forbes

1.7 Billion Adults Worldwide Do Not Have Access To A Bank Account

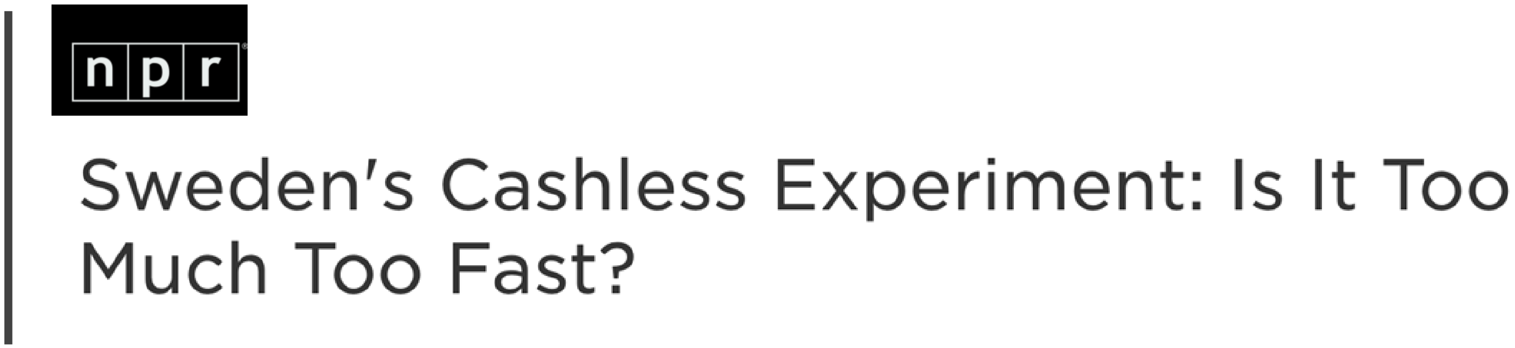
Allowing funds to flow without judgment



The Guardian

Hong Kong police seize $10m in donations intended for protesters

Being powerless to avoid a financial data trail



Sweden's Cashless Experiment: Is It Too Much Too Fast?

Main problem with money today: the abuse of trust.

When money went digital—even more trust required.

Less trust → more privacy.

→ more fairness.

→ more freedom.

Can we make better money?

Goals for today

- Appreciate why Bitcoin is interesting
- Learn the basics about how it works
- Q&A and conversation
- Not an investment pitch

Bitcoin: innovating at the money layer.

What is Bitcoin?

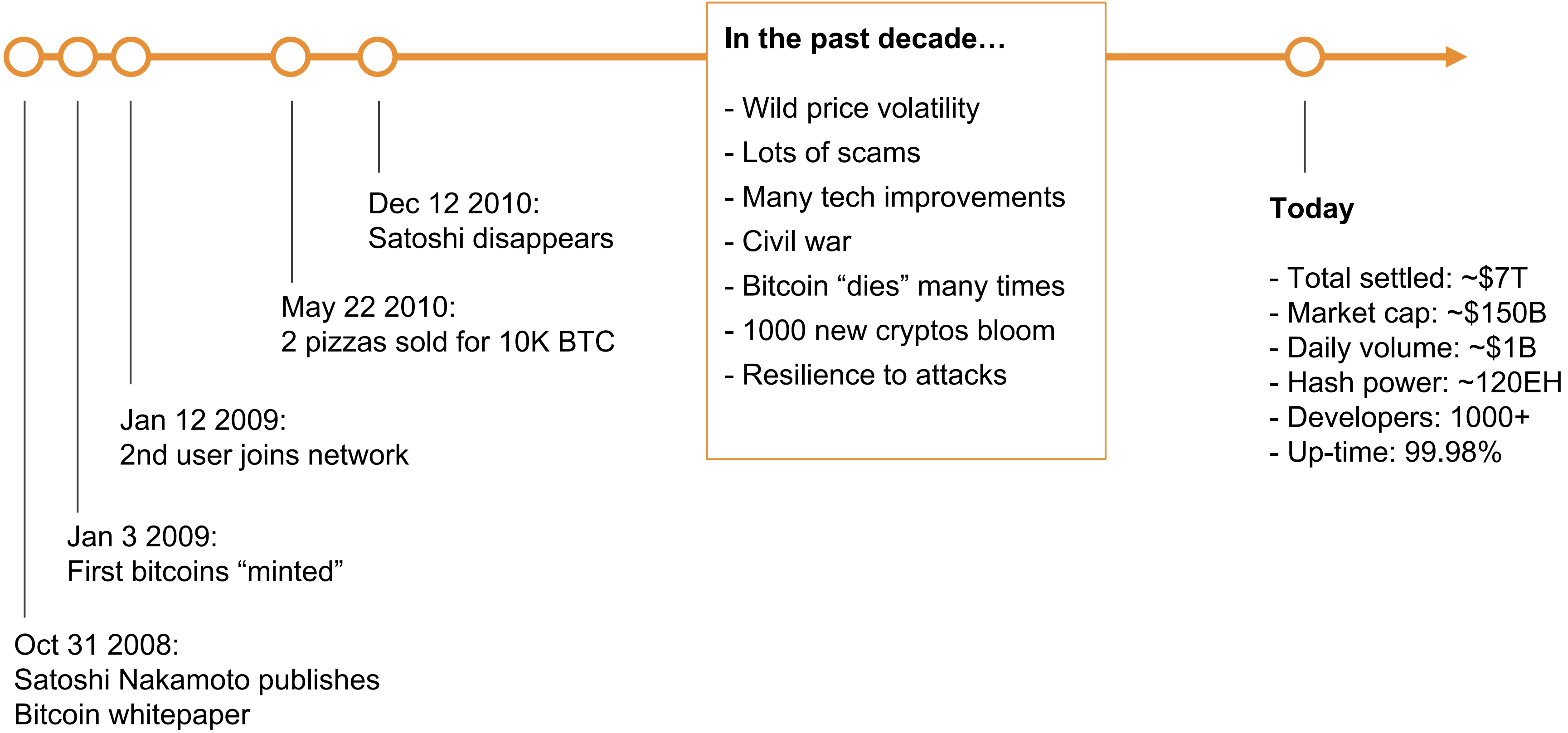
Bitcoin is a new form of p2p digital money that is:

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

The big idea: eliminates the need to trust anyone.

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

- Total settled: ~$7T
- Market cap: ~$150B
- Daily volume: ~$1B
- 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.

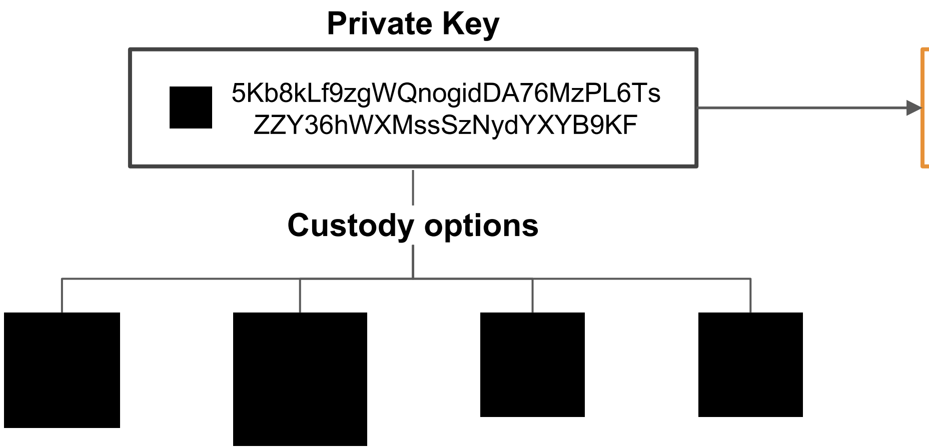
Satoshi’s coins have never moved (~$6B)

Many impostors: beware!

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

5Kb8kLf9zgWQnogidDA76MzPL6Ts
ZZY36hWXMssSzNydYXYB9KF

Custody options

Risk vs UX tradeoffs

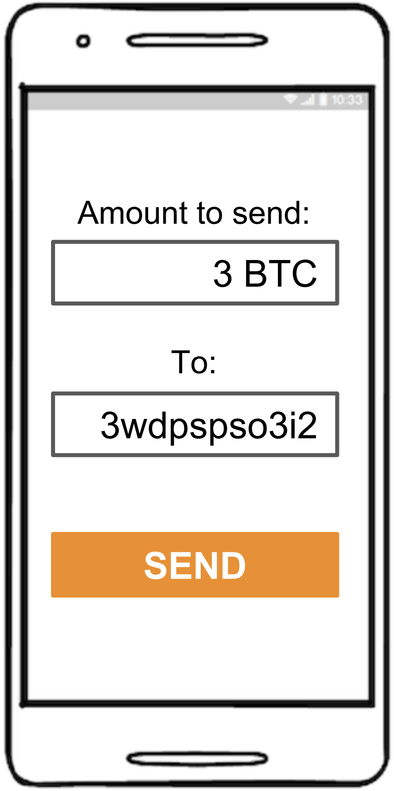
Bitcoin Public Ledger

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.

What happens when you send bitcoin?



Amount to send:

3 BTC

To:

3wdpspso3i2

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

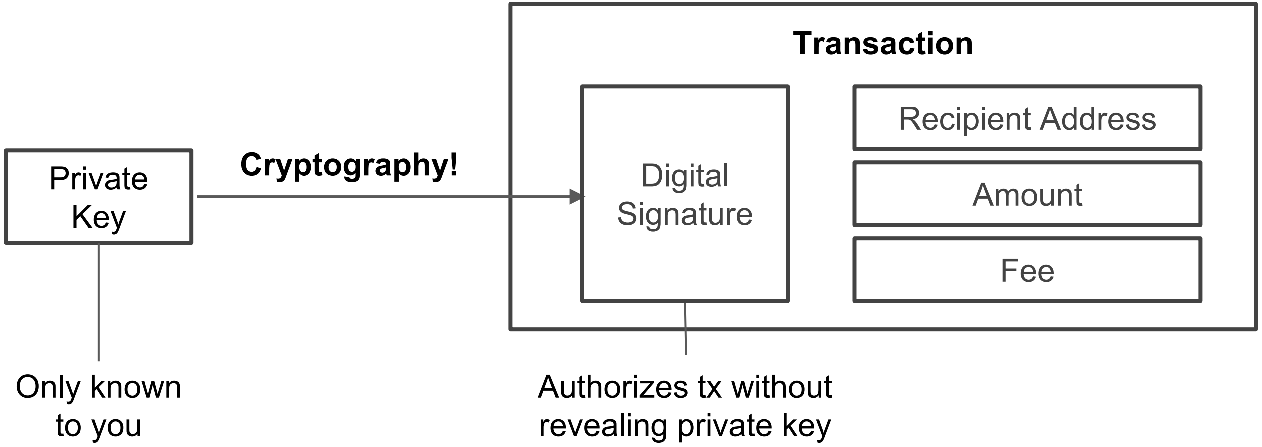
To:

3wdpspso3i2

SEND

2 **Generate a transaction.**

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



Transaction

Private Key

Cryptography!

Digital Signature

Recipient Address

Amount

Fee

Only known to you

Authorizes tx without revealing private key

What happens when you send bitcoin?

Amount to send: 3 BTC

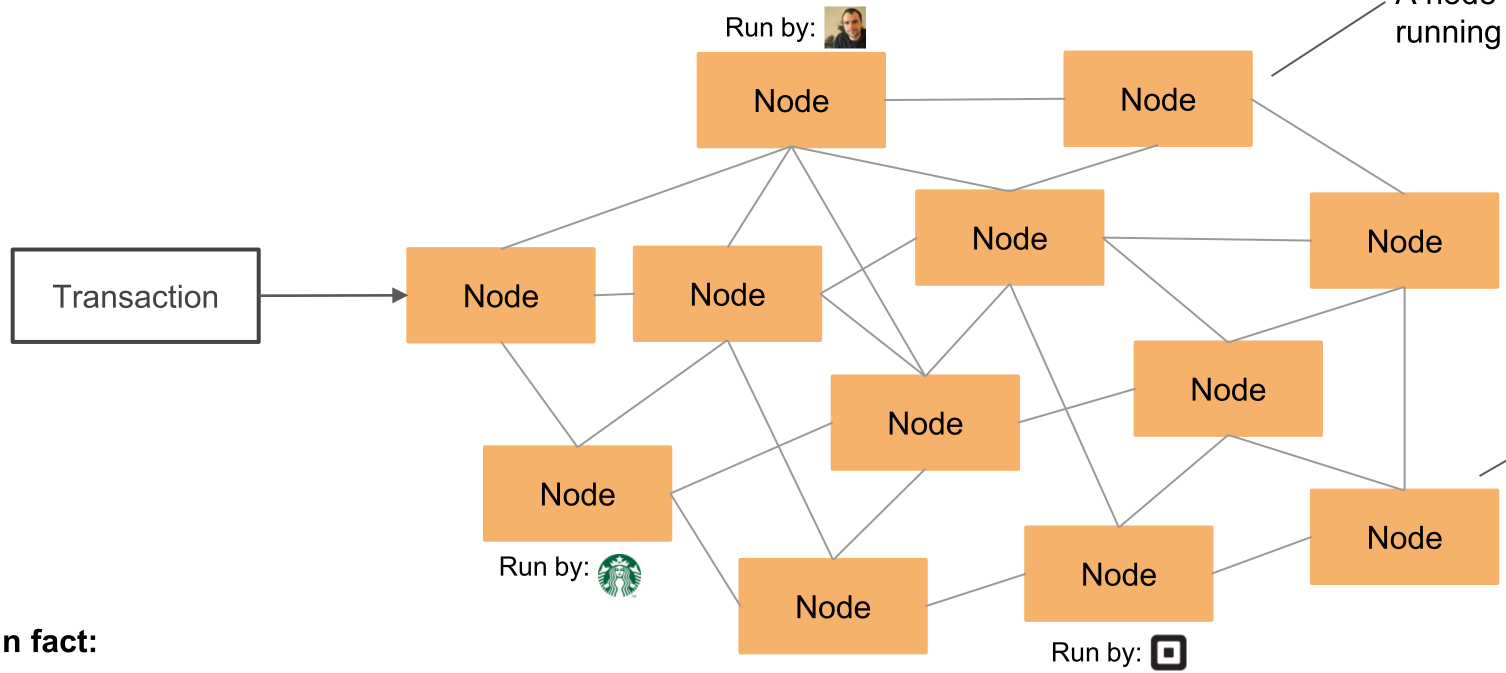
To: 3wdpspso3i2

3 **Broadcast the transaction.**

The transaction is sent to the p2p bitcoin network.

What happens next does not require trust…

P2P nodes propagate new transactions



A node is a computer running 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.

BUT—how does the system maintain integrity?

Need good solutions to many important questions:

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

Mining is the solution to these problems

First, a few definitions

Blocks

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

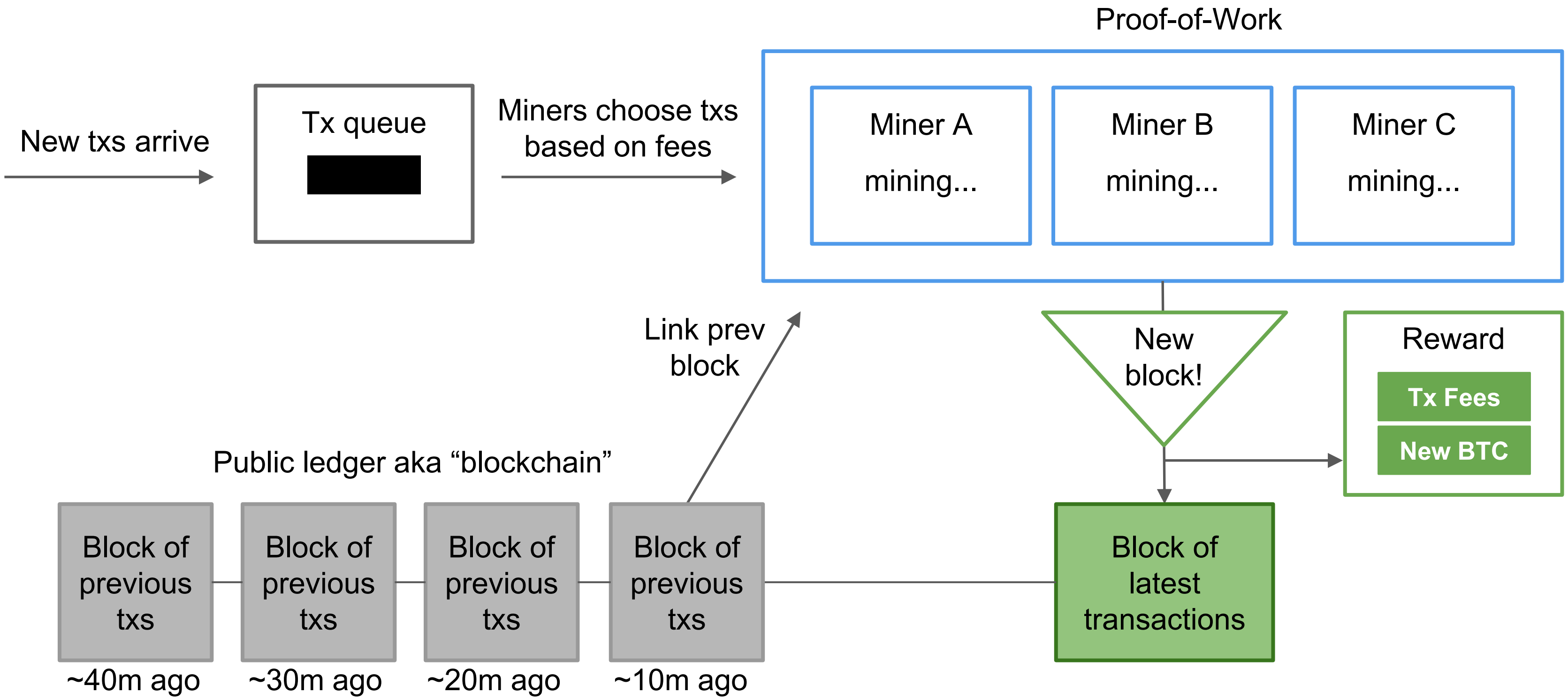
Miners

Miners are special Bitcoin nodes that create blocks.

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



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

~40m ago

Block of previous txs

~30m ago

Block of previous txs

~20m ago

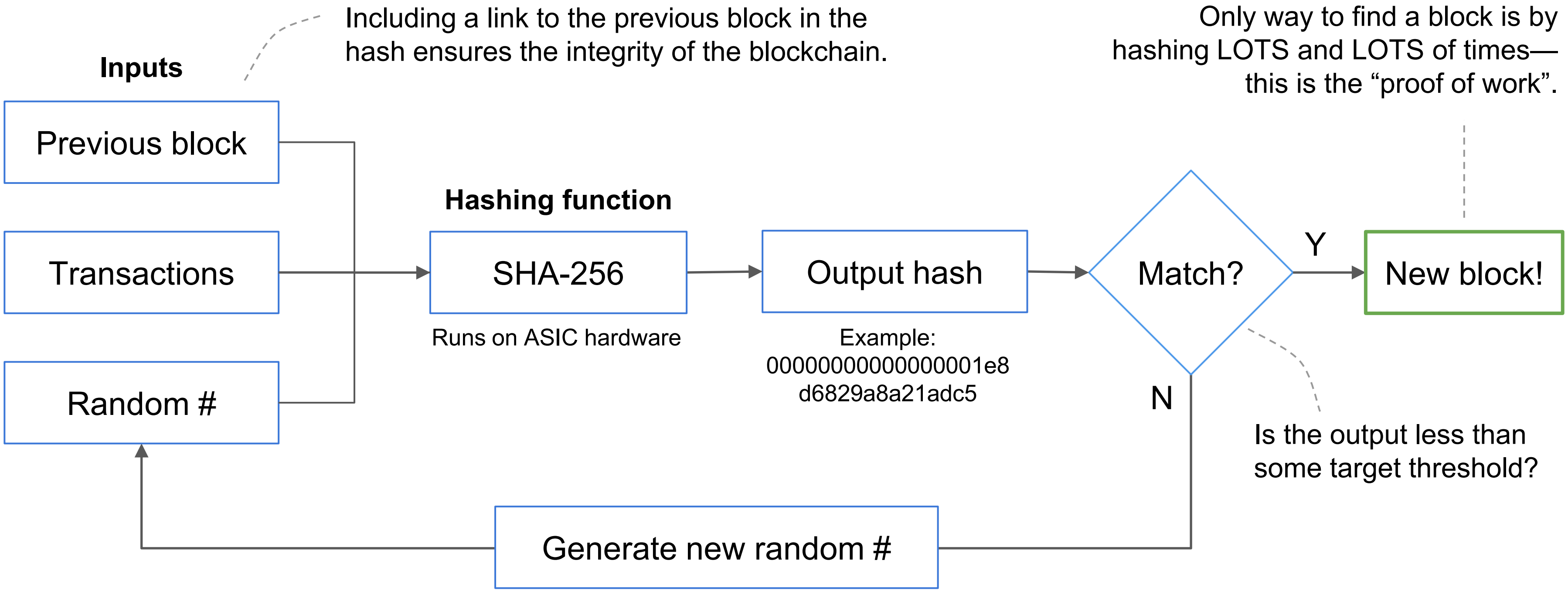
Block of previous txs

~10m ago

Block of latest transactions

The cost of mining a block: illustrated

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



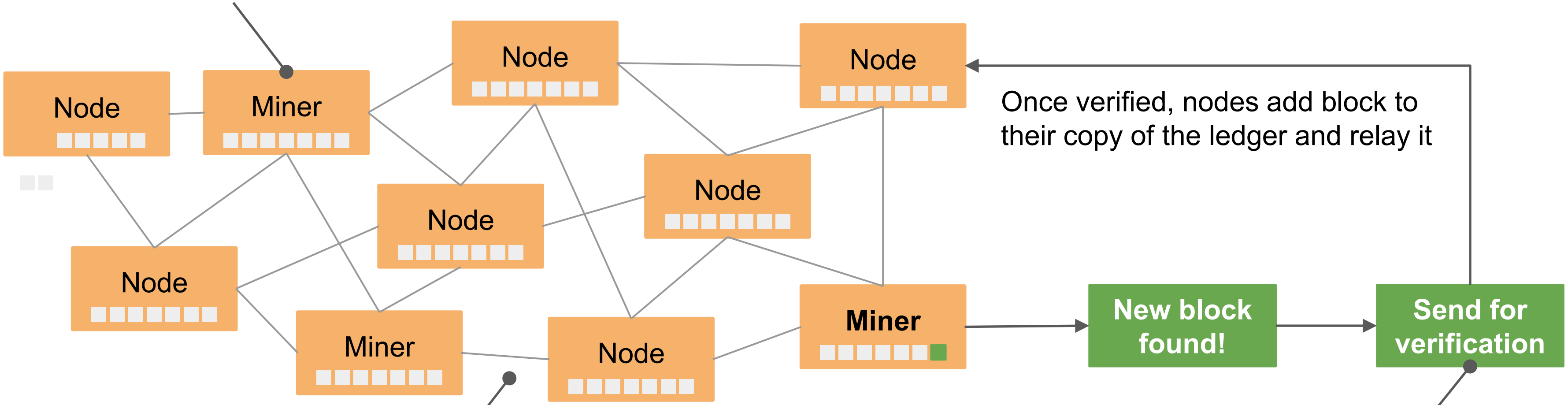
Including a link to the previous block in the hash ensures the integrity of the blockchain.

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?

Nodes verify the validity of newly mined blocks

Game theory suggests that miners begin mining next block immediately



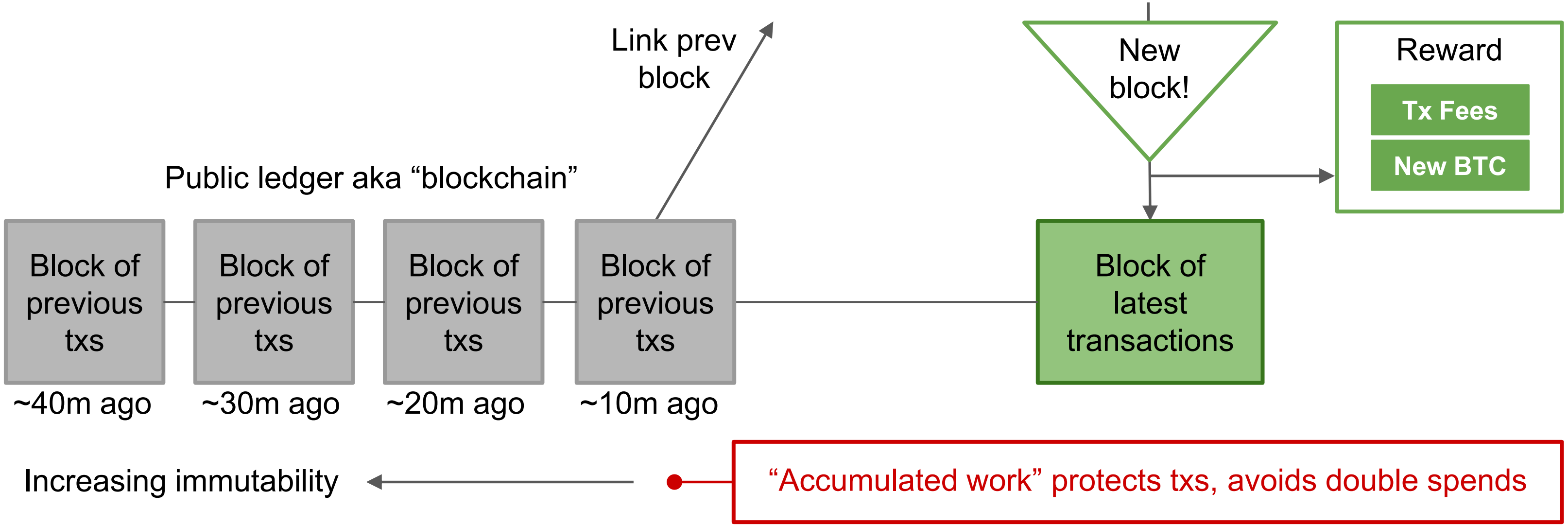
Once verified, nodes add block to their copy of the ledger and relay it

Critical that verification remain a decentralized process to keep miners honest

Blocks are valid if they:

1. Obey protocol rules
2. Meet PoW requirements

Miners settle transactions on the blockchain



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.

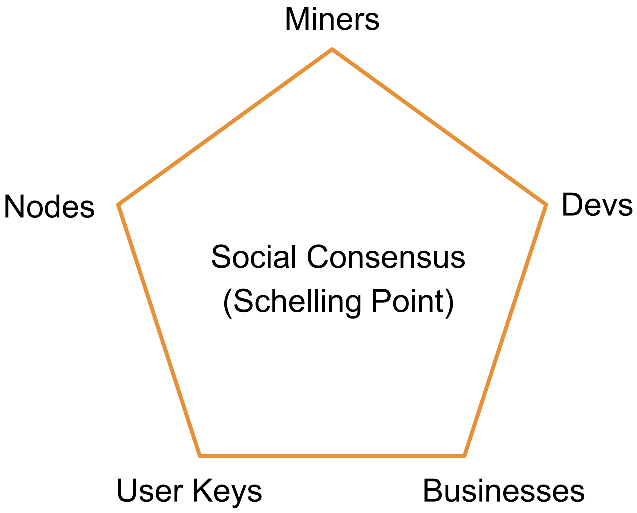
Let’s zoom out again.

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



Warning

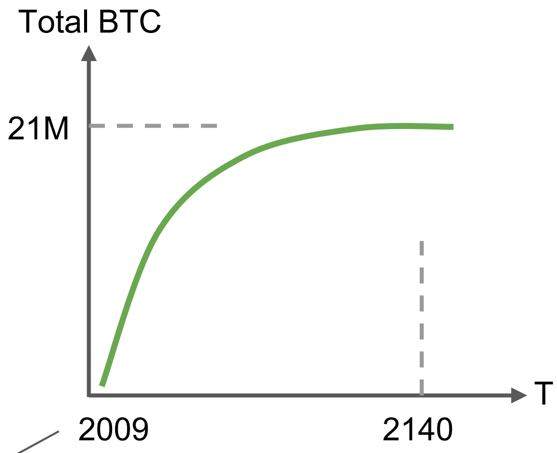
- Bitcoin Cash (BCH) is a non-consensus fork away from Bitcoin (BTC)
- Even though promoted on bitcoin.com — this is not real Bitcoin. Beware!

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

- Current block reward: 12.5 BTC
- 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.

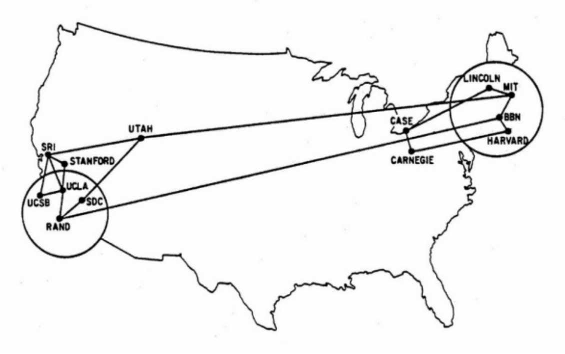
No one can seize (or freeze) your bitcoin wealth.

No one required to guarantee property rights.

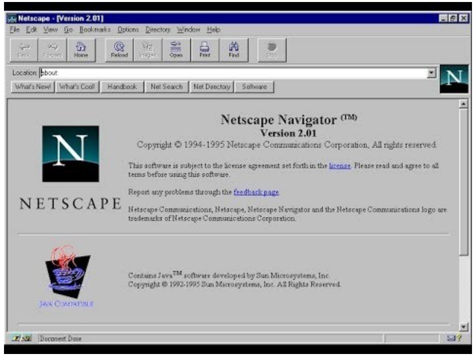
No one can devalue your bitcoin.

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
Back Forward Home Reload Images Open Print Find Stop
Location: about:
What's New! What's Cool! Handbook Net Search Net Directory Software
NETSCAPE
JAVA COMPATIBLE
Document: Done

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

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.

Additional resources to keep learning:

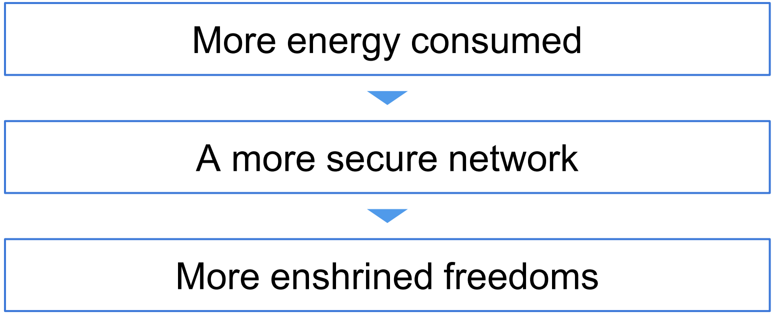
- The Bullish Case for Bitcoin
- The Little Bitcoin Book
- Bitcoin Information & Resources

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.

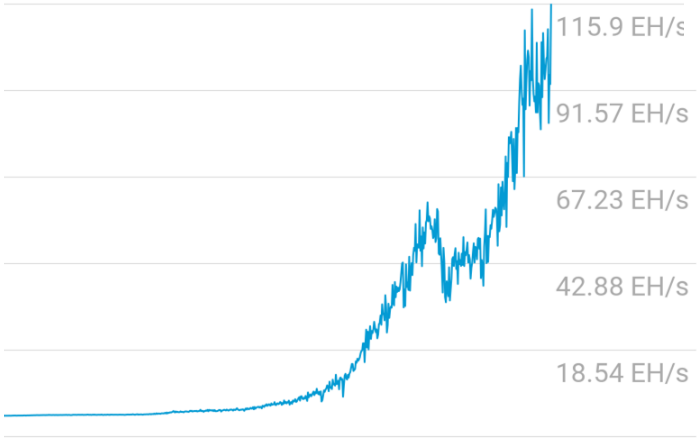


More energy consumed

A more secure network

More enshrined freedoms

Bitcoin Network Hashrate



❗ 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.

> “ Bitcoin is rat poison squared.

> “ Bitcoin is evil.

“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.

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

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

“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

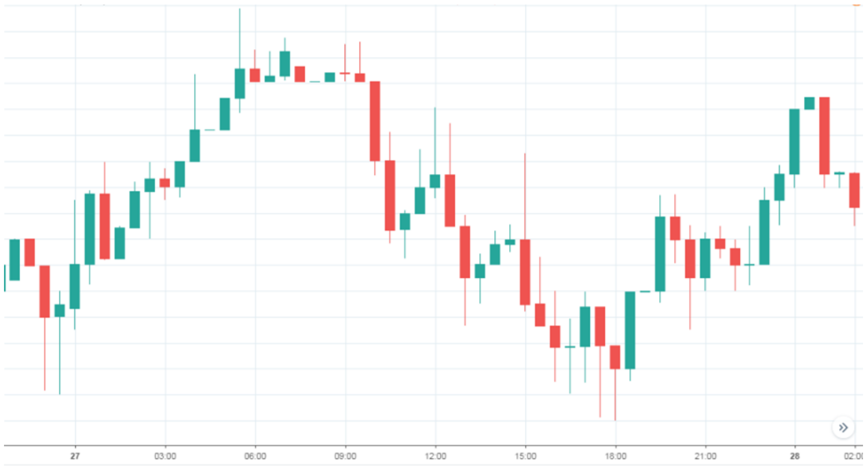
EOS

TRON

+
countless
others

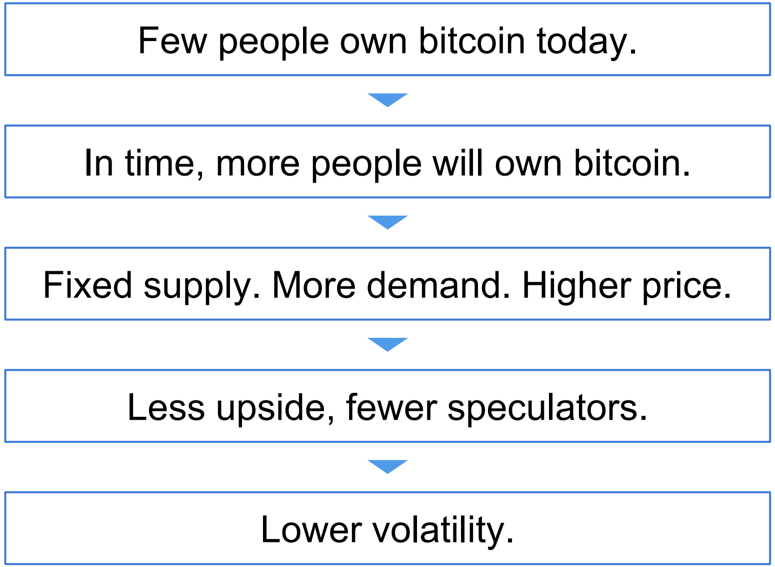
“Bitcoin is too volatile”

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.

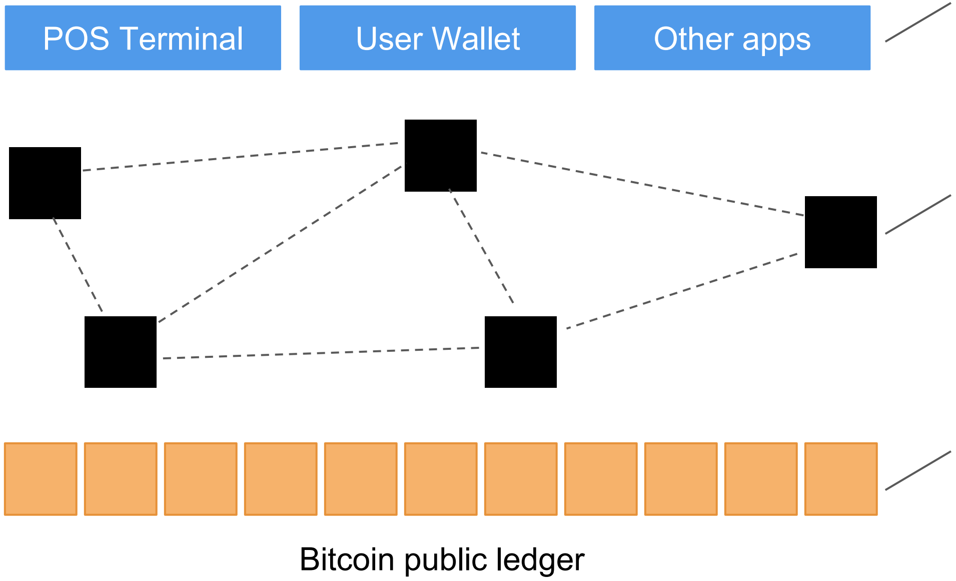
Fixed supply. More demand. Higher price.

Less upside, fewer speculators.

Lower volatility.

“When can I buy a coffee at Starbucks”

Cheap & instant bitcoin transactions will come via new layers.

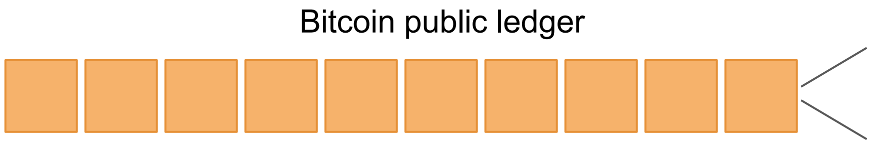


It will take time for the application layer to see massive adoption by consumers & merchants.

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!

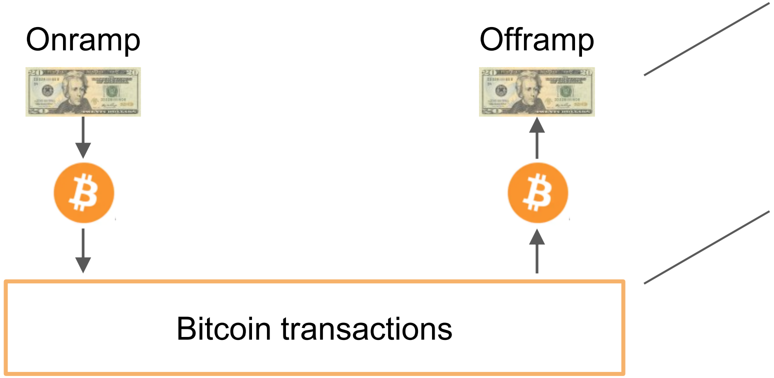
Layer 1 blockchain will remain slow & costly in order to preserve security and decentralization.

“How private is Bitcoin?”



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”.



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.

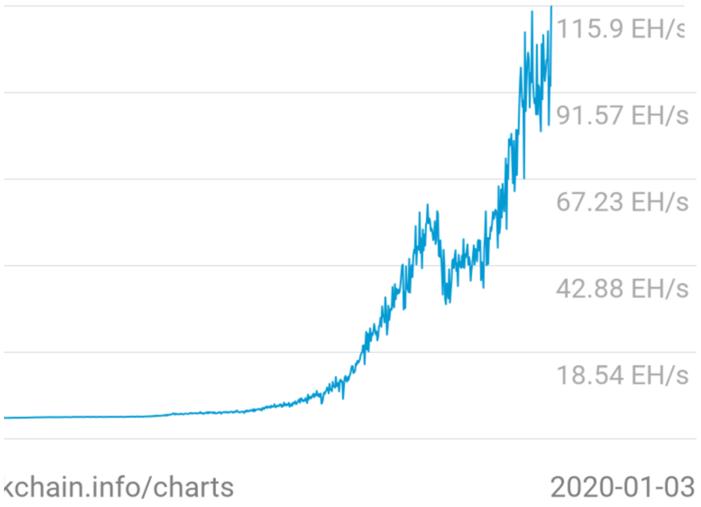
Fun fact: Lightning Network transactions are more private than on-chain transactions.

“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



“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.
xapo	Can verify existence of your bitcoin on the blockchain.
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.