

11:30 AM Part 1: What is Bitcoin?

11:50 AM Break (10 min)

12:00 PM Part 2: Technical talk – Under the hood

12:20 PM Q&A (10 min)

What is Bitcoin?

by Alex Levchuk

Hi! My name is Alex

1. About me and my involvement in bitcoin
2. Why did I decide to organize this talk?
3. Why am I passionate about bitcoin?

What is bitcoin?

It's digital gold

How is bitcoin similar to gold?

- De-centralized
 - No leader
 - No 3rd parties
- Has same or better monetary qualities
 - Divisible
 - Limited supply

... but is it physical?

- Gold's important qualities are monetary, not physical

- Do not matter

- Color, shine, weight, sound

- What matters:

- Hard to produce
 - Can be verified
 - Can be melted, divided
 - Can change hands
 - Censorship resistance


Physical qualities

Monetary qualities

Environmental impact of Gold

- Environmental impact of gold far exceeds bitcoins
- There is no stop to how far gold mining can go if the price of gold rises



#Bitcoin  secures digital property rights for 7.6 billion people using a \$50 smart phone, and for half the energy required to dig rocks out of the ground.

Cambridge Bitcoin Electricity Consumption Index



Cambridge
Centre
for Alternative
Finance

Bitcoin



70.36

TWh per year

Gold mining



131













TWh per year

Bitfarms to start trading on the Nasdaq, June 21st.

With the ticker **\$BITF**, they will become the largest publicly traded **#Bitcoin** **₿** miner in North America using greater than 99% hydroelectric renewable electricity. 



What are your qualifications? (page 1)

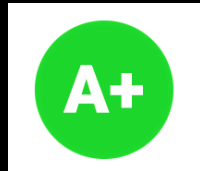
	Bitcoin	Gold	Government Issued Money
Durable			
Portable			
Fungible			
Verifiable			

What are your qualifications? (page 2)

	Bitcoin	Gold	Government Issued Money
Divisible	A+	C	B
Scarce	A+	A	F
Established History	D	A+	C
Censorship Resistant	A	C	D

Verifiable

- Don't Trust, Verify
- You can verify everything in bitcoin



Verifiable

- Gold – yes! “Sound Money” but hard to verify
 - For example, a tungsten weighted gold bar
 - counterfeit gold this is hard to verify because you’ll need to do things like
 - flatten the gold bars into a thin strip and run a spectrometer^[1]



Scarcity

- Something is scarce when it's in demand yet the supply is limited
 - Not the case for most goods
 - When demand rises → prices rise → make more

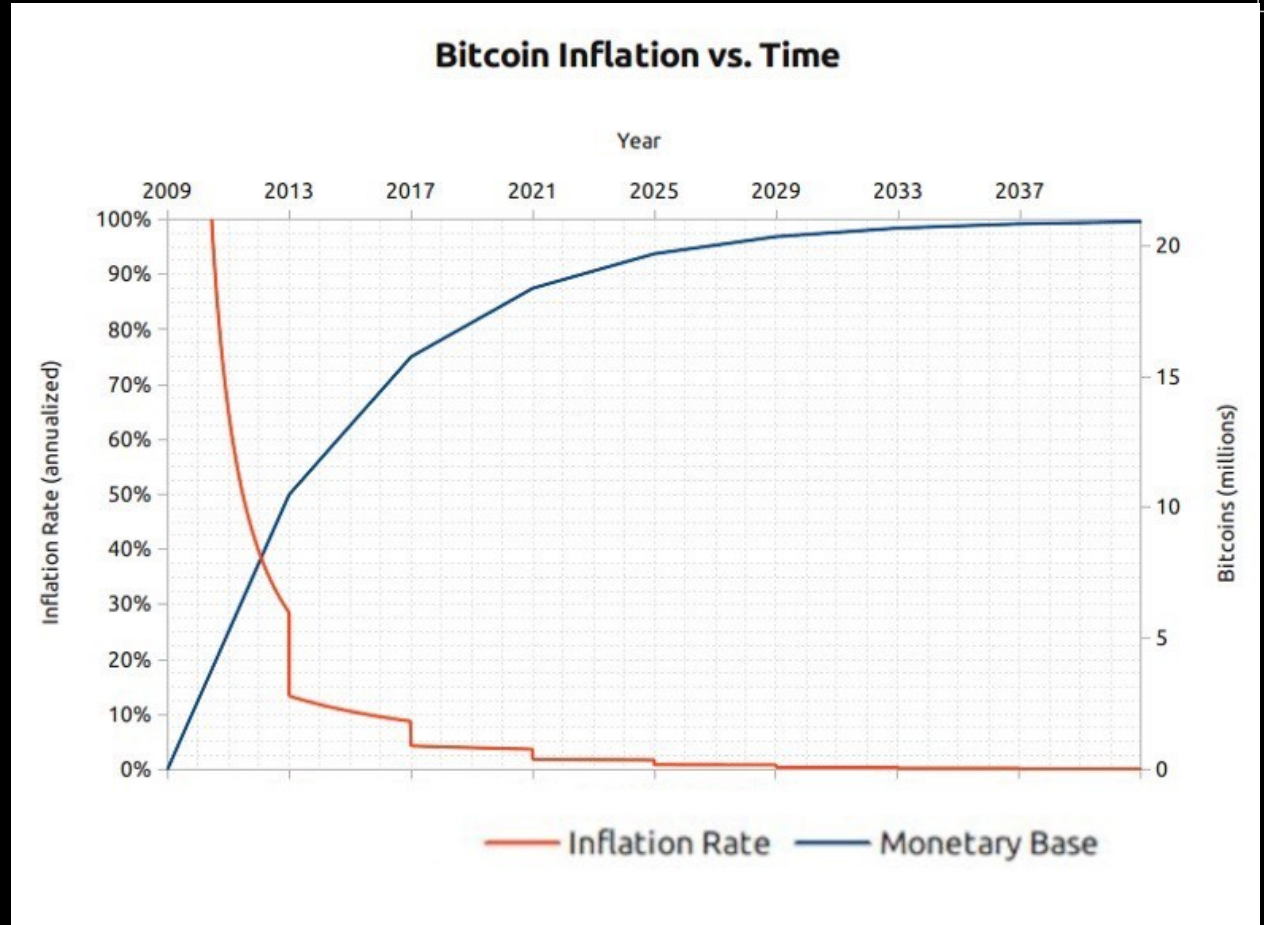
Bitcoin is more scarce than Gold

- Gold was the king of scarcity until bitcoin came into existence in 2009 (A)
 - Gold's supply grows very slowly - doubles every 50 years
 - Gold has demand globally: valued at \$11 trillion
- Bitcoin has a harder limit on Supply (A+)
 - There can never be more than 21 million of bitcoin
 - Bitcoin has demand global demand: valued at \$0.7 trillion



Bitcoin is more scarce than Gold

- Bitcoin supply (A+)
 - There will never be more than 21M
 - 89.37% is already in people's hands
 - **Bitcoin inflation cut in ½ every 4 years**
 - Current inflation rate is 1.7%



Lack of Scarcity

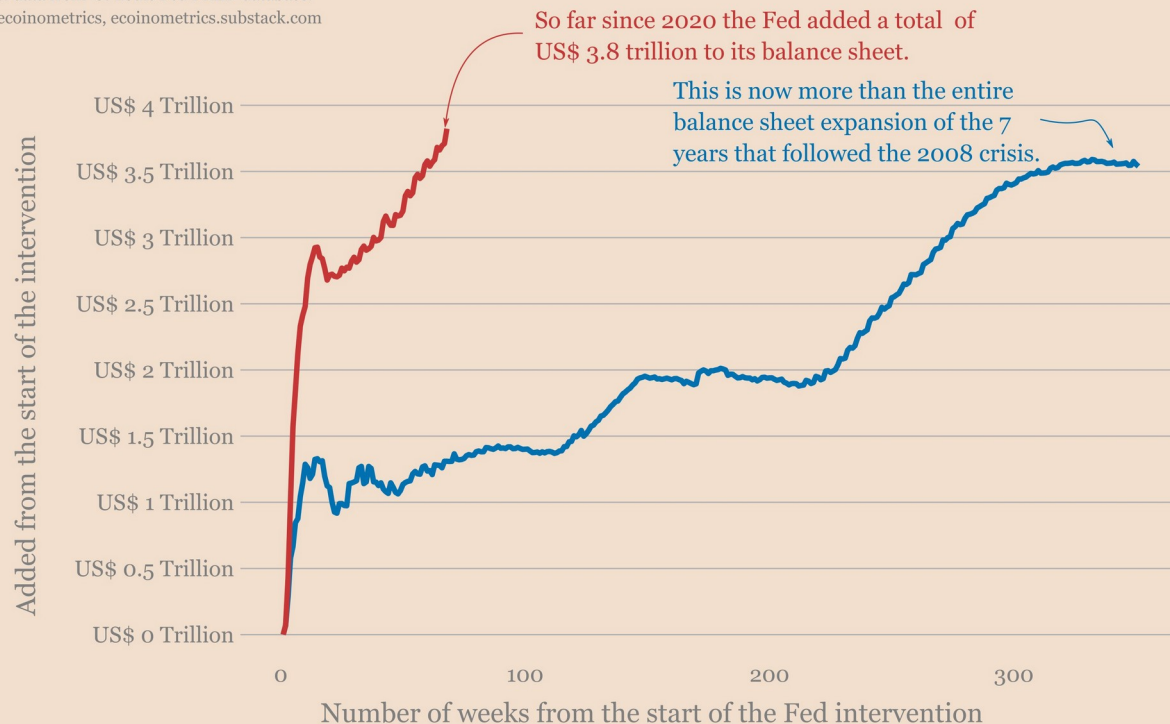
- Government issued money (F)
 - Unpredictable Fed monetary expansion

The U.S. Fed Playbook - Balance Sheet 2008 vs 2020

June 18, 2021

Source: data from St Louis Fed FRED database.

By: @ecoinometrics, ecoinometrics.substack.com



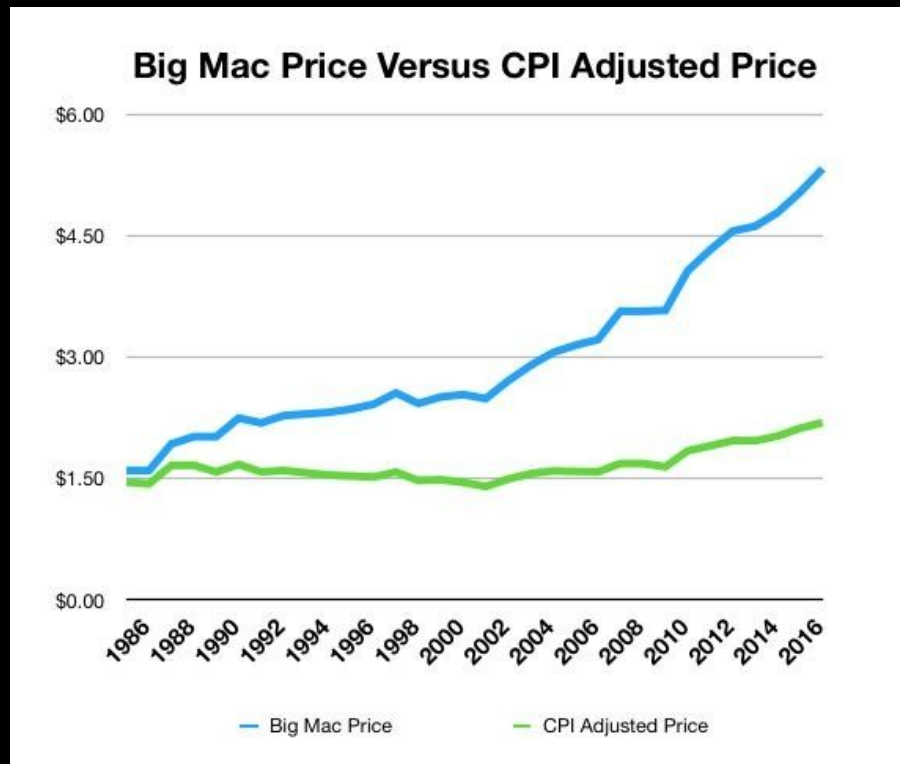
Lack of Scarcity



McDonald's 1973

Lack of Scarcity

- Money printing is rampant in all government issued money
 - Dating back to Roman Empire
 - US fiat dollar
 - Fiat means “by decree” (not backed)
 - Since 1933 (88 years old)
 - Cantillion effect

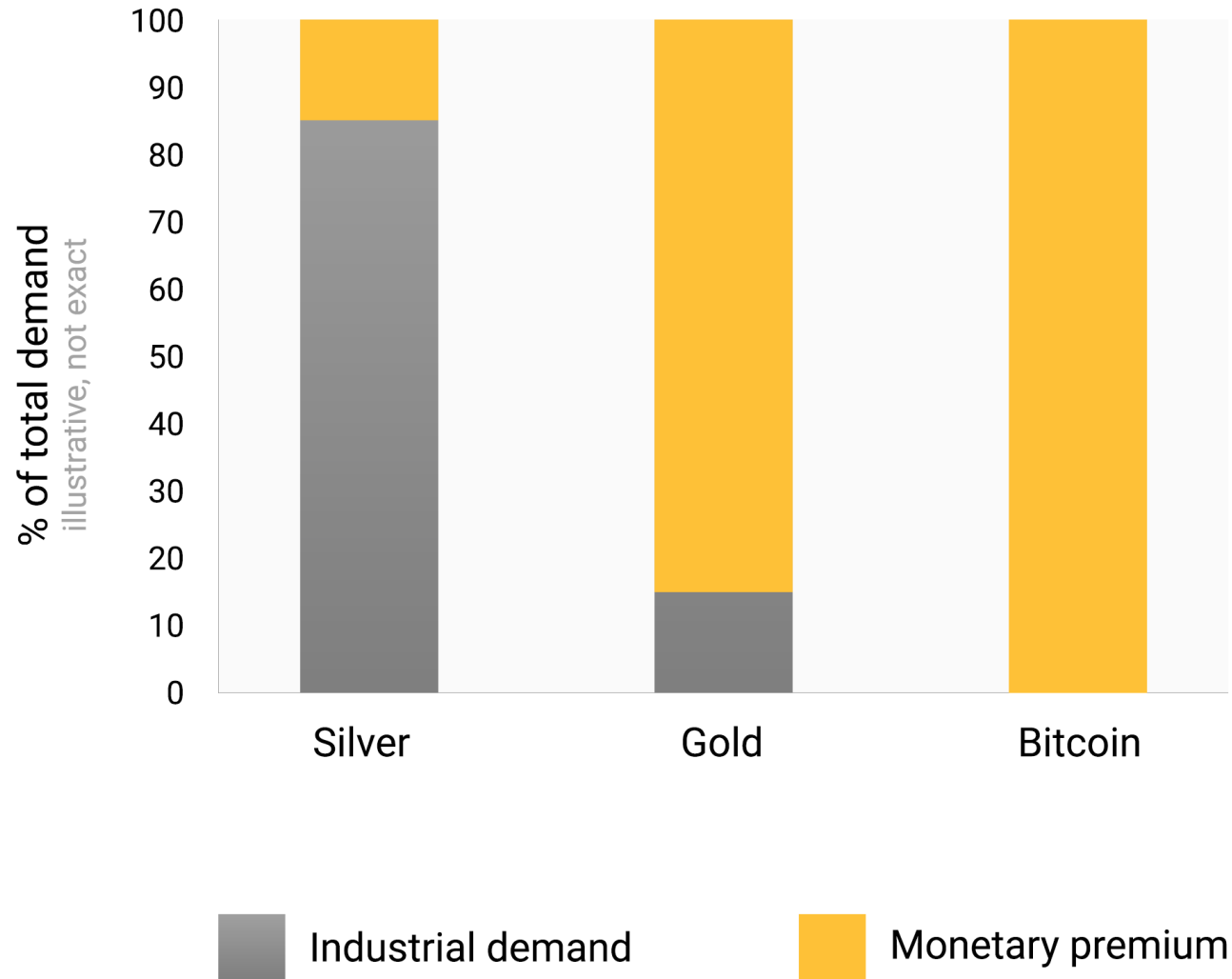


Free market

- Free market
 - Seeks to satisfy needs and wants of consumer
 - Moves towards efficiency thru price discovery
 - Law of Supply and Demand
- Government interventions
 - Money printing → bail outs → reallocation of resources
 - Moves away from efficiency:
 - Creates surplus
 - Creates shortages
 - Moves away from stability



Monetary premium for different monetary goods



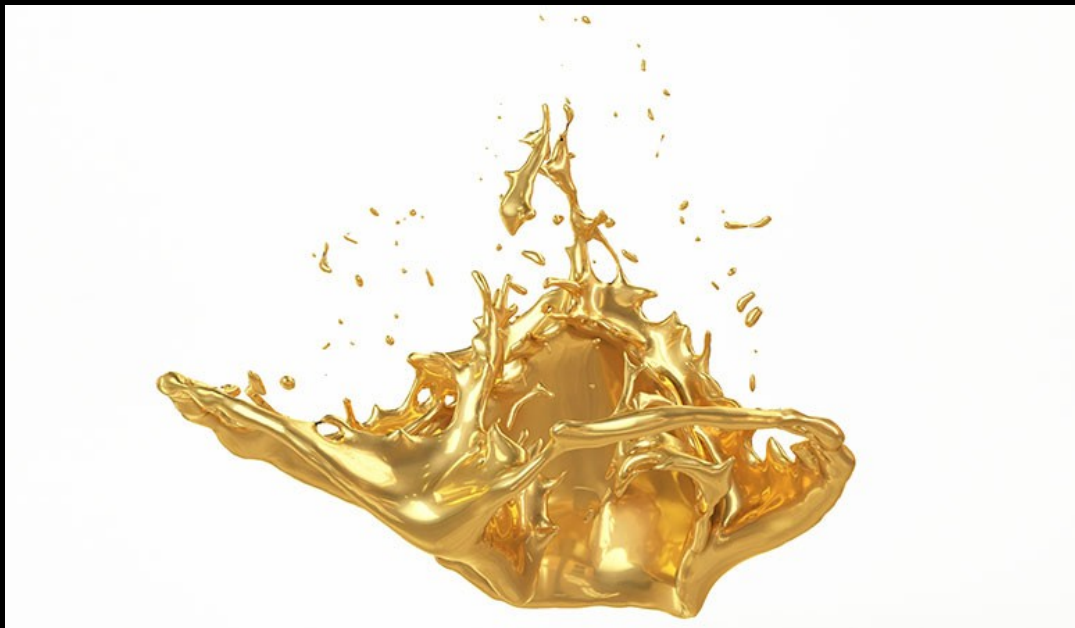
Fungible

- Every ounce of gold is equal
- Every fragment of bitcoin is equal
 - Yet, usually it possible to see where it came from (B)
- Gov. Money (B)

A

B

B



Divisible

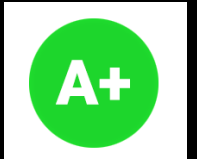
≡ SATS	1	are 0.00037888 \$
≡ SATS	1	are 0.00000001 BTC
\$USD ▼	1	are 2,639 SATS

- 1 bitcoin = 100,000,000 sats
- 1 sat is the smallest unit
- Better visibility than gold and dollar because 1 sat is a fraction of a modern penny



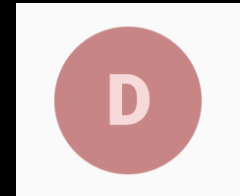
Portable

- Imagine transporting millions of dollars of gold
 - You'll need to hire security, use a plane or ship, etc.
- bitcoin you can send over any communication device. It's like gold with a teleportation ability



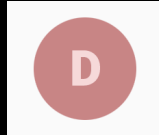
Censorship resistant

- Gold was ceased from people in the US in 1933
 - Because it was not portable
 - Impossible to carry across border
- Bitcoin can be carried in the brain
- If laws change, rich people will escape
- A bitcoin transaction is impossible to stop

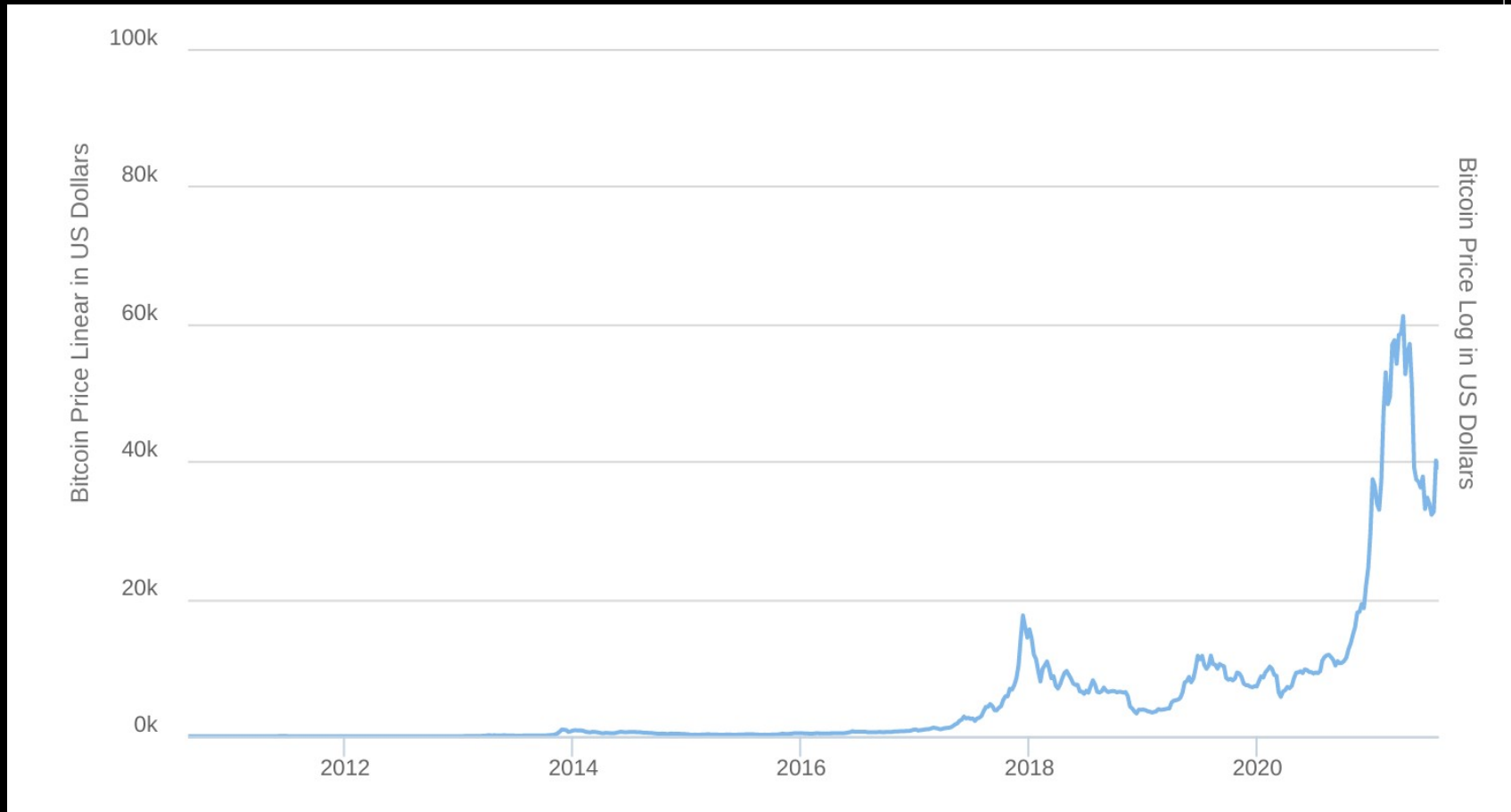


Durable and Established history

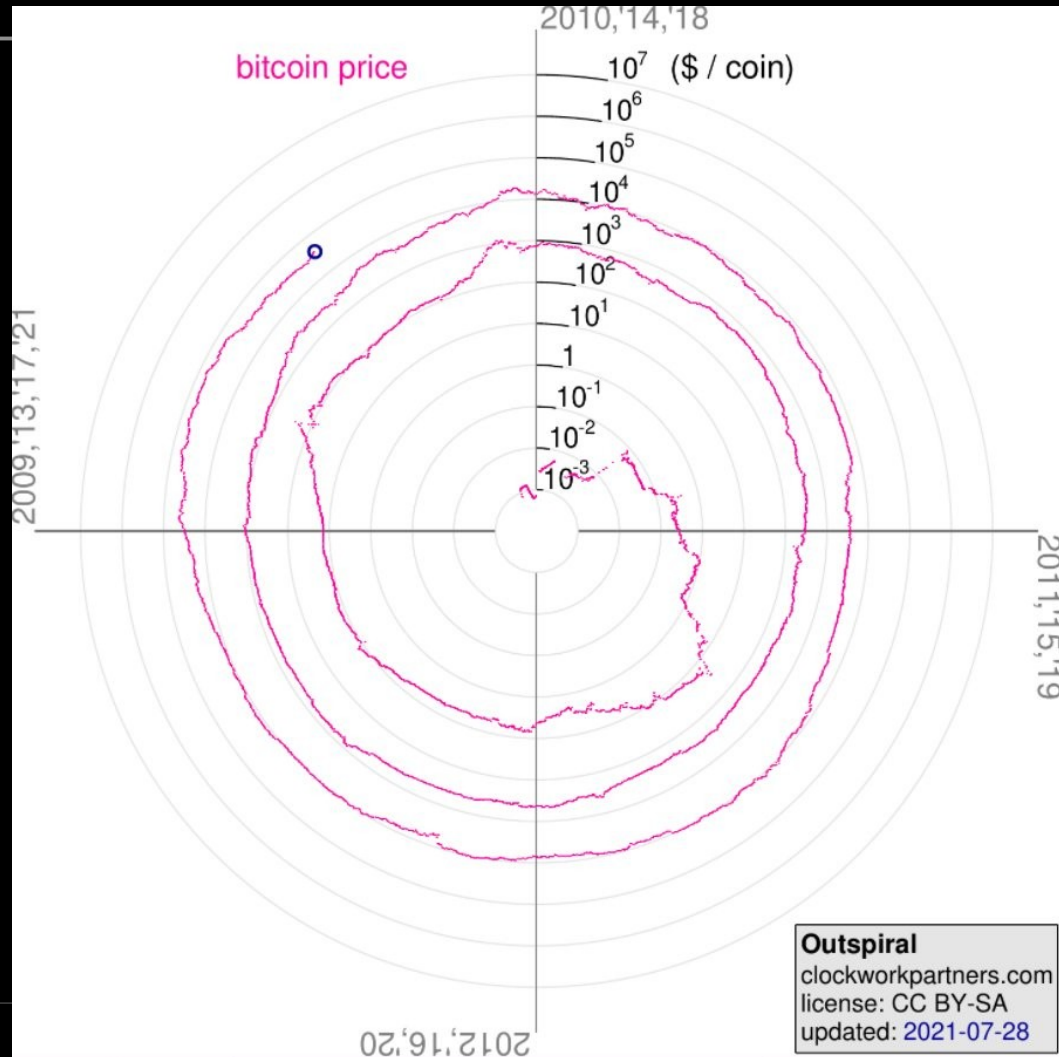
- Gold for Egyptian pharaohs still here
- Government money ~100 years
- Bitcoin 12 years
- Lindy effect



History of bitcoin price



History of bitcoin price

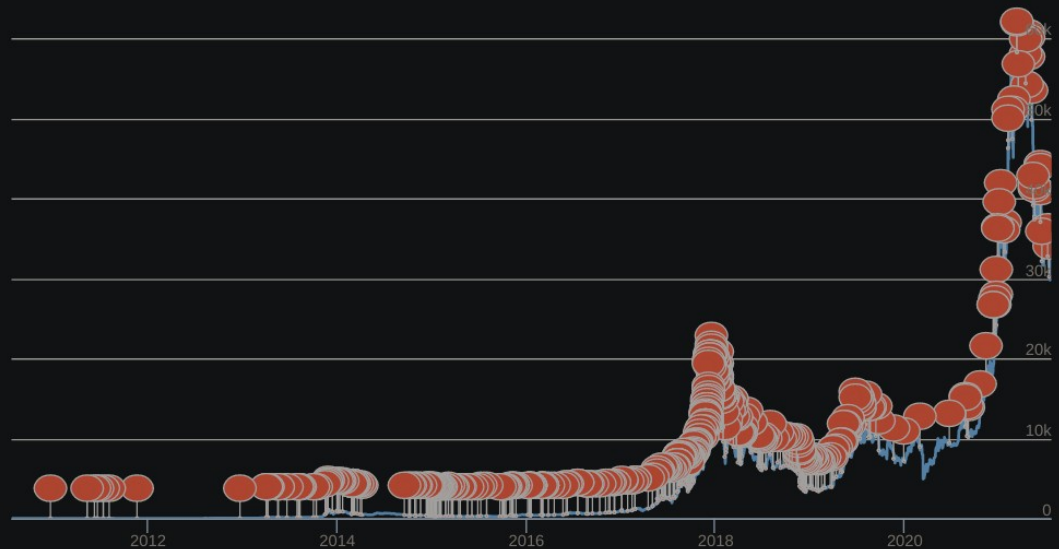


FUD around bitcoin

- FUD (Fear, Uncertainty, Doubt)
- Very misinformed writers fill the TV, or YouTube, News, and even things you get on Google searches
- Bitcoin was declared dead 425 time in 12 years of it's existence while the price and world wide adoption continued to rise

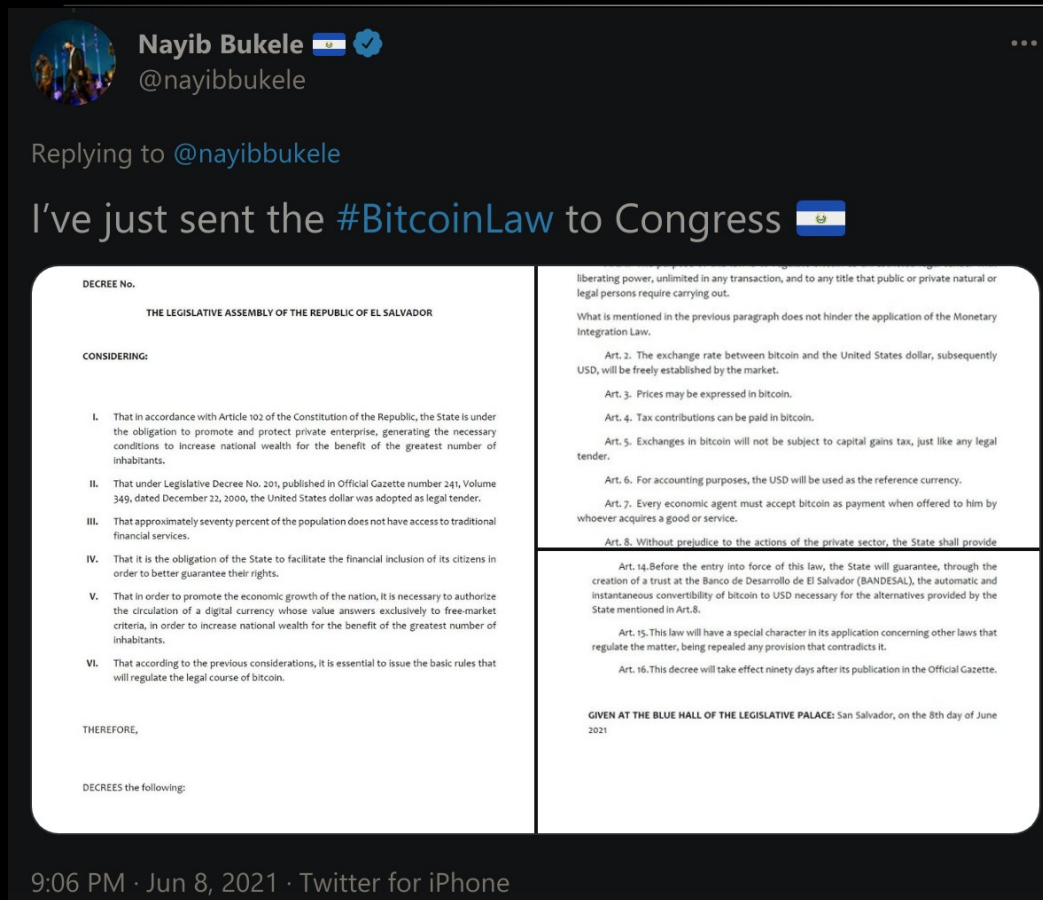
Bitcoin Obituaries

Bitcoin has died 425 times



Adoption

- Individual tinkerers
- Groups
 - Cypherpunks
 - Libertarians
 - US Senators
- Public Companies
 - Microstrategy (\$4.2 B)
 - Tesla (\$1.7 B)
 - Square (\$300 M)
- Countries
 - El Salvador

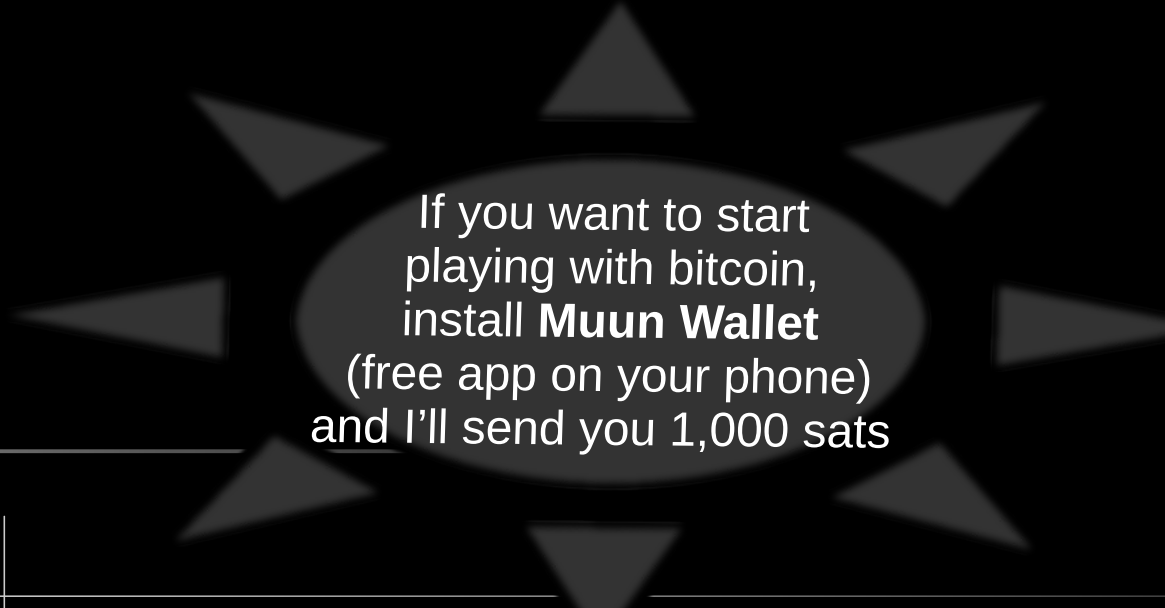


9:06 PM · Jun 8, 2021 · Twitter for iPhone


11:50 AM Break (10 min)

12:00 PM Part 2: Technical talk – Under the hood

12:20 PM Q&A (10 min)



If you want to start
playing with bitcoin,
install **Muun Wallet**
(free app on your phone)
and I'll send you 1,000 sats



Part 2:

Not your , not your

The technical side of

- Internet is the wild west
 - State sponsored attacks are likely
 - Bitcoin is money for enemies
 - Adversarial thinking
- If you're going to own bitcoin, you have to figure out how to keep it safe
 - What if can't learn it?
 - Trust someone that does.
 - “Uncle Jim” method

Not your , not your

- Custodial

- Traditional companies
- Can be confiscated
- Not censorship resistant
- Risk of company going out of business

- Non-Custodial

- No trust on anything
- DIY
- Option to use a trust-less service / company
- The key to your bitcoin is a 24 word secret

Hot-wallet VS Hardware wallet

- Hot-wallet

- Connected to Internet
 - Risk of getting hacked
- Use for small amounts
- Option to use Lightning Network
 - fast micropayments

- Hardware wallet

- Never connected to Internet
- Has steel backups
 - In case of fire
- Security in keeping backups in multiple locations

Hot-wallet VS Hardware wallet

- Hot-wallet

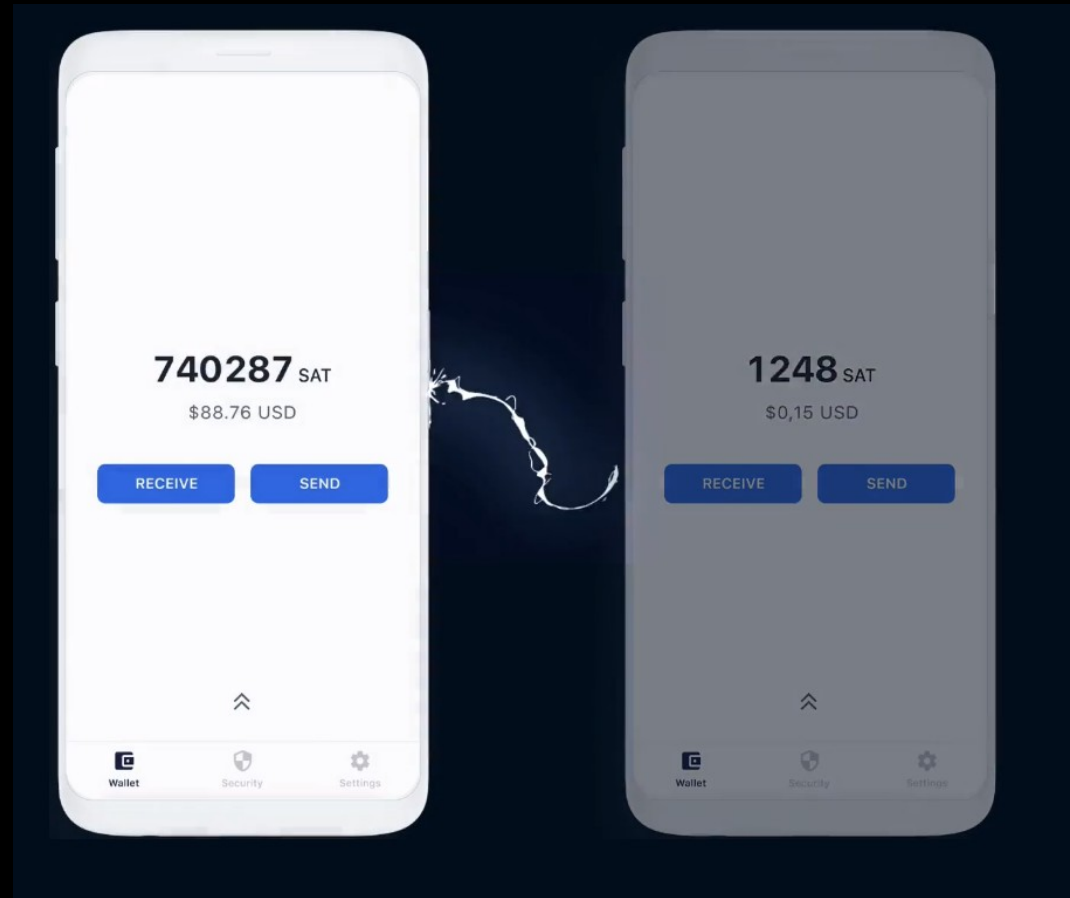
- Muun
- Breez

- Hardware wallet

- ColdCard

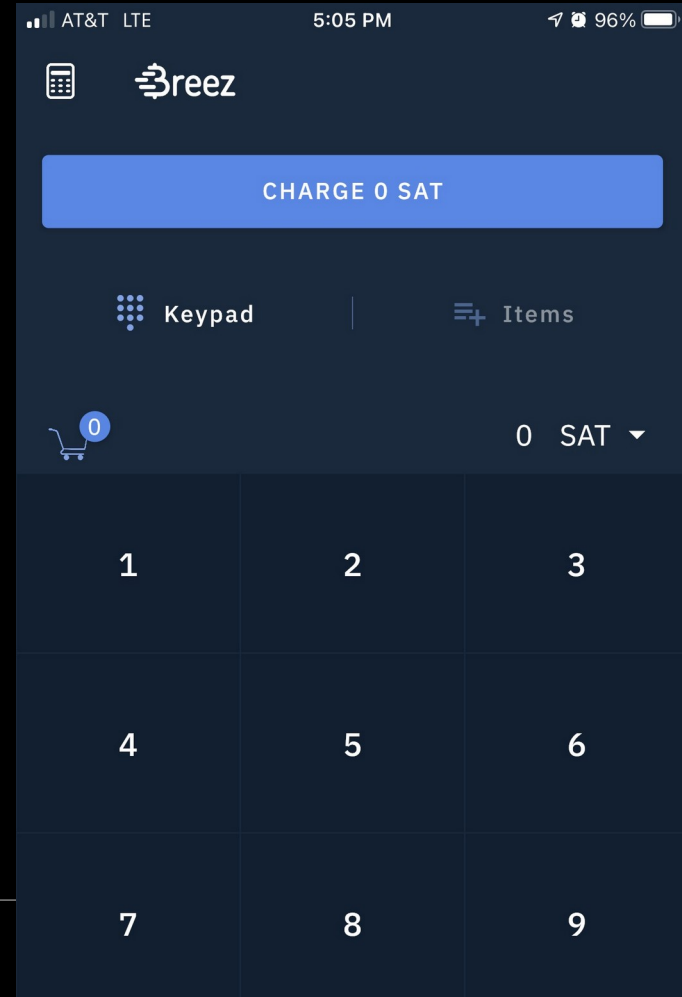
Hot-wallet examples

- Muun Wallet



Hot-wallet examples

- Breez Wallet
 - Includes a Cash Register Point Of Sale system

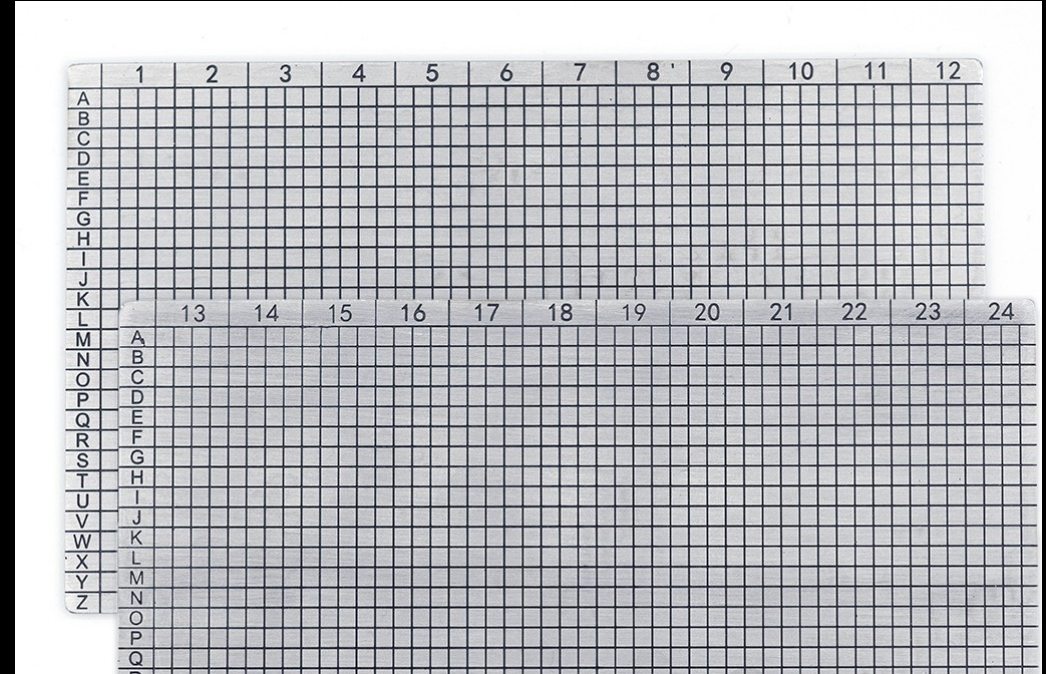


Hardware wallets

- ColdCard



Backups of Hardware wallets

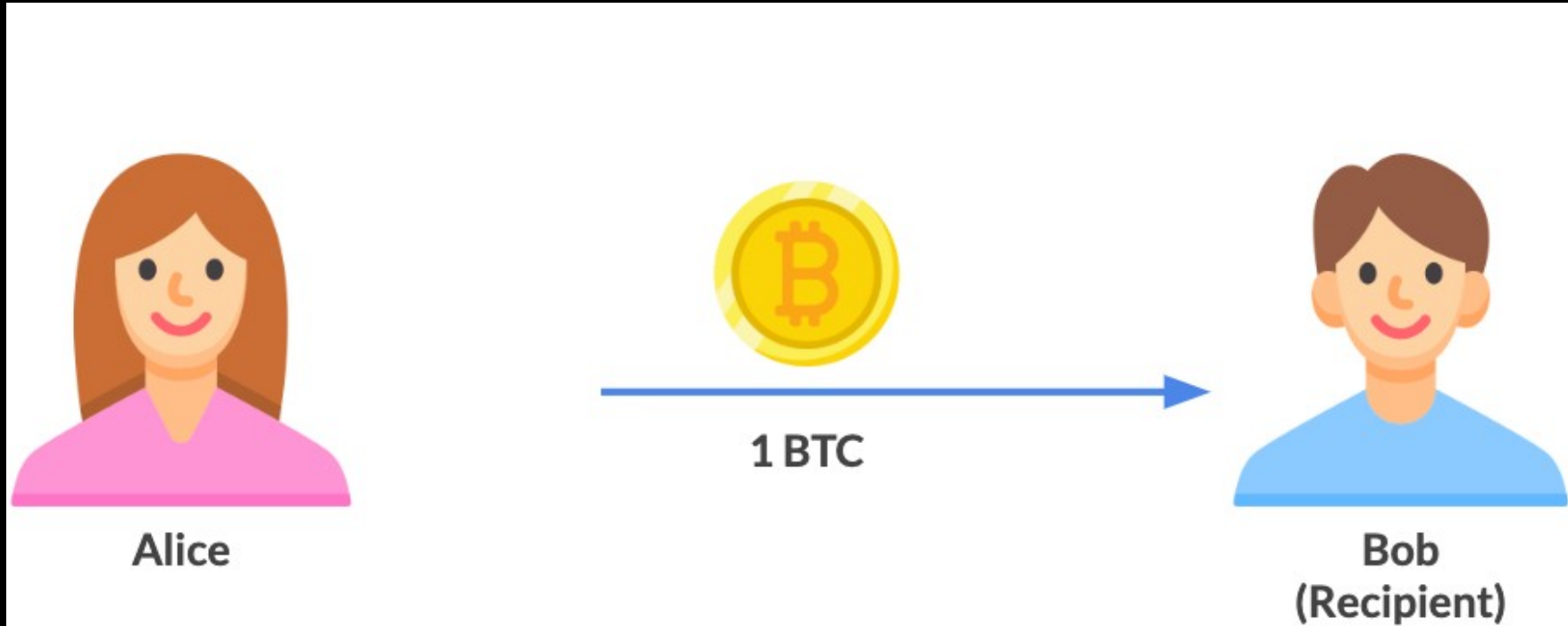


Backups of Hardware wallets

- Two or more steel backups
- In different locations
- If a thief finds one, it's not enough to access funds

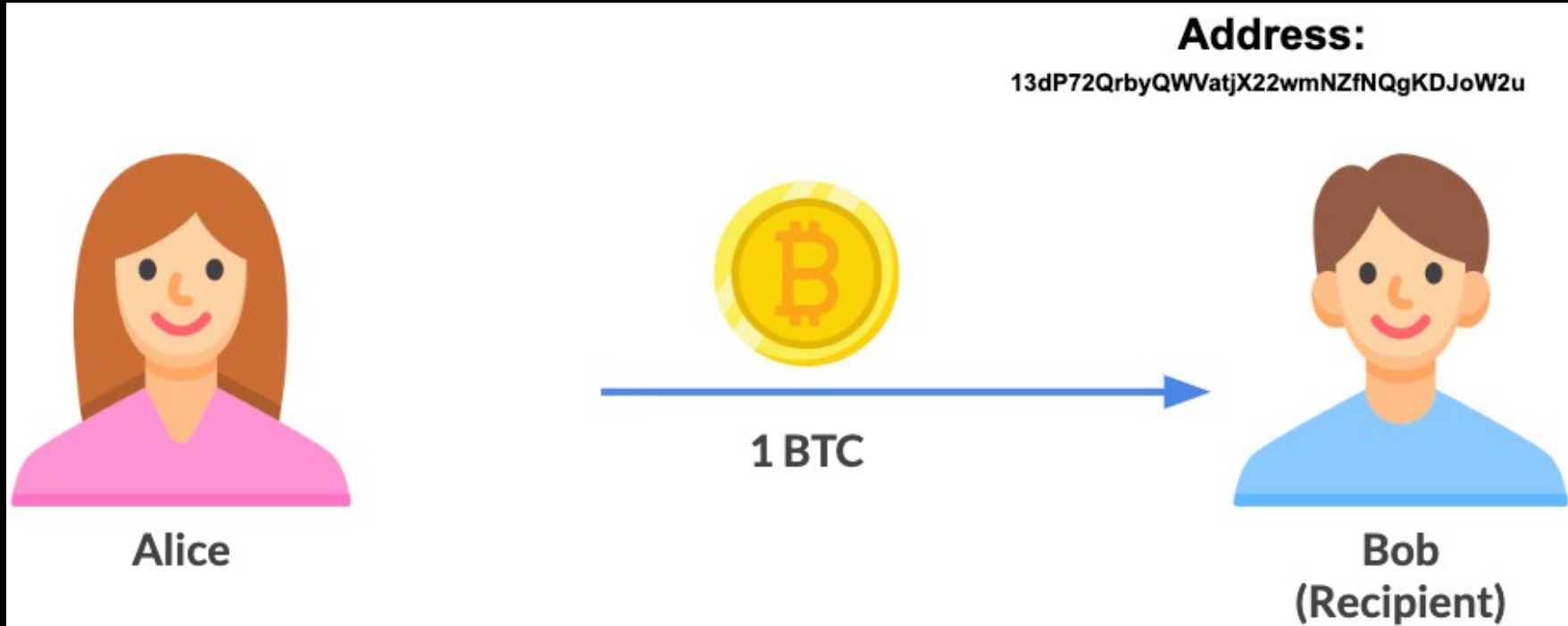


What's under the hood?



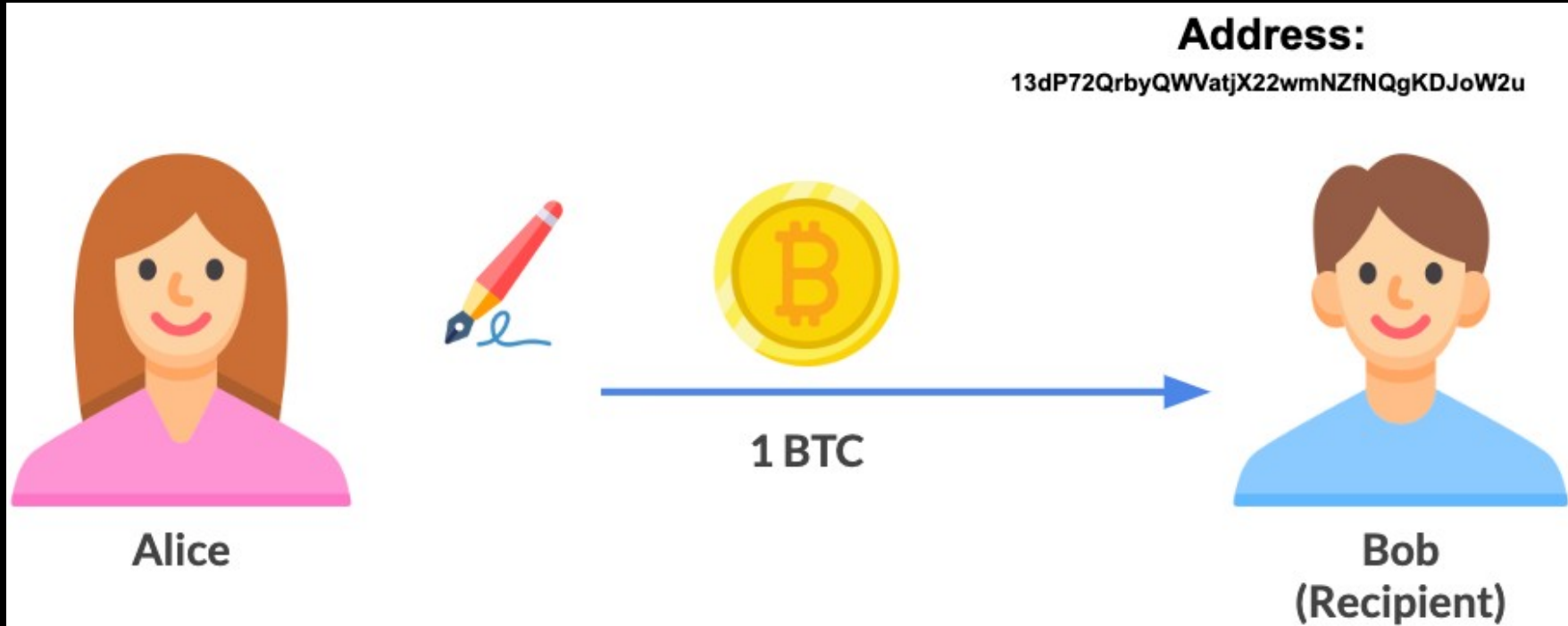
What's under the hood?

Step 1: Bob generates a bitcoin address



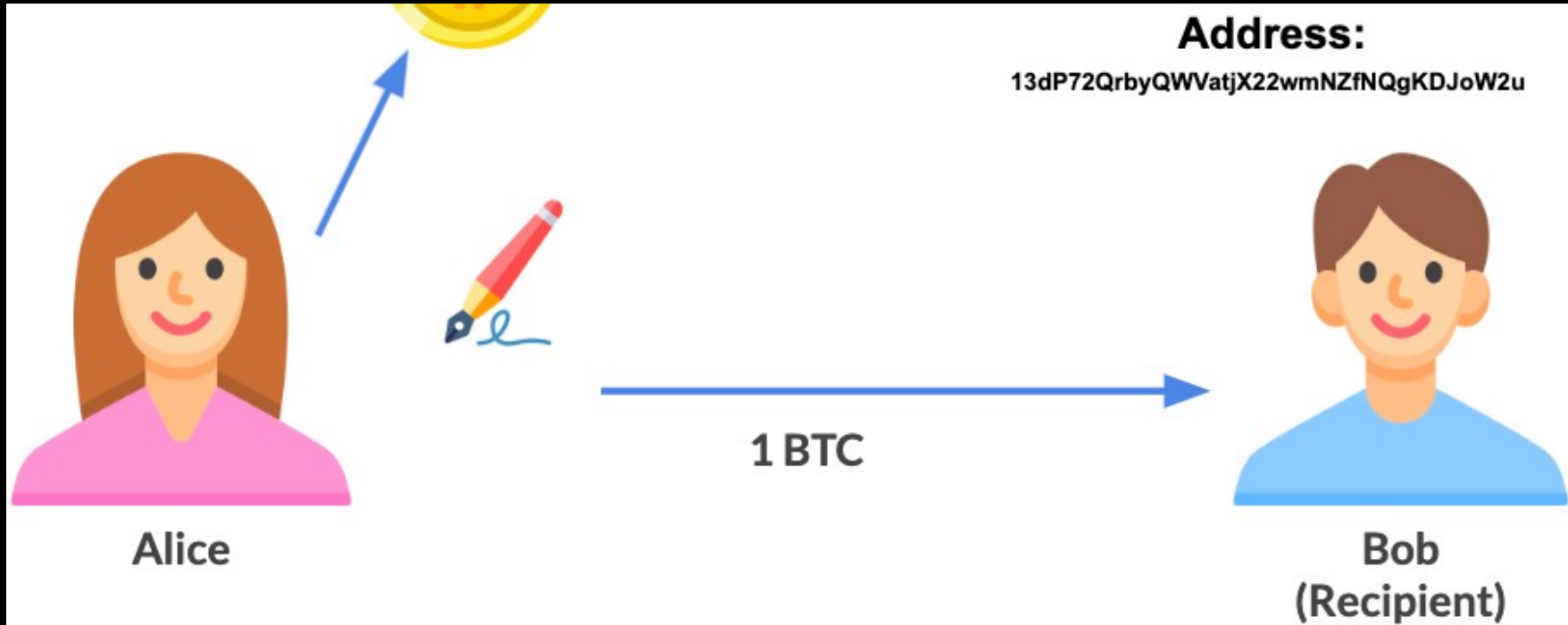
What's under the hood?

Step 2: Alice signs a “check” to the address



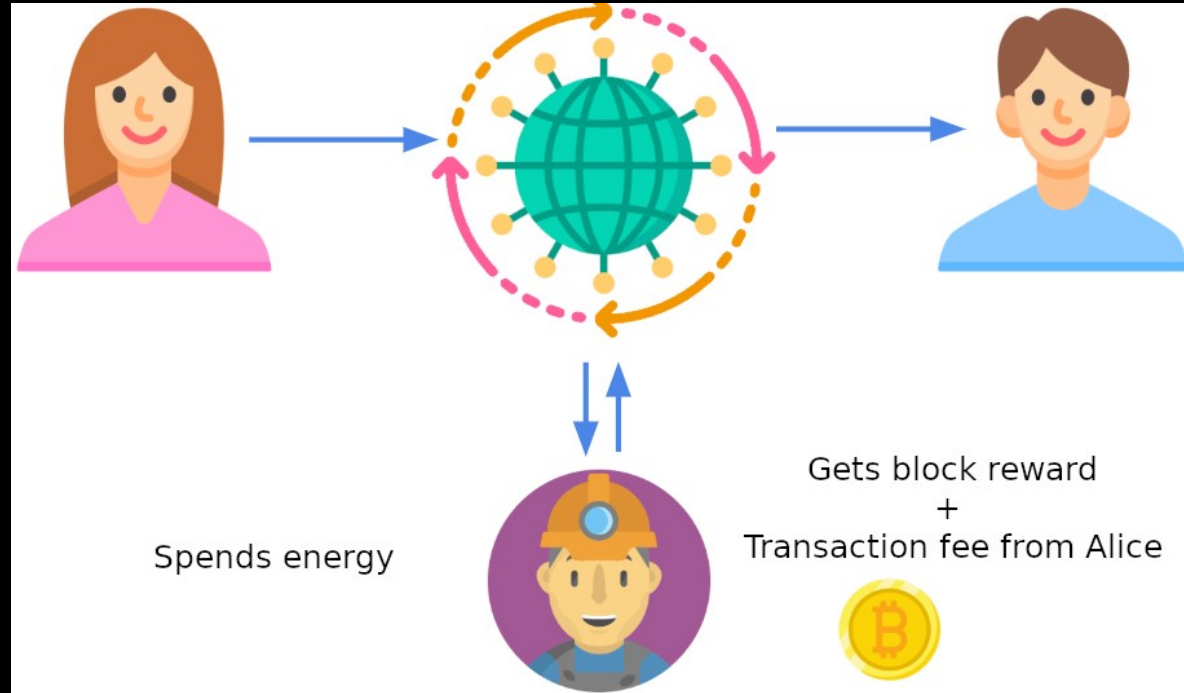
What's under the hood?

Step 3: Alice sends out the “check” to network



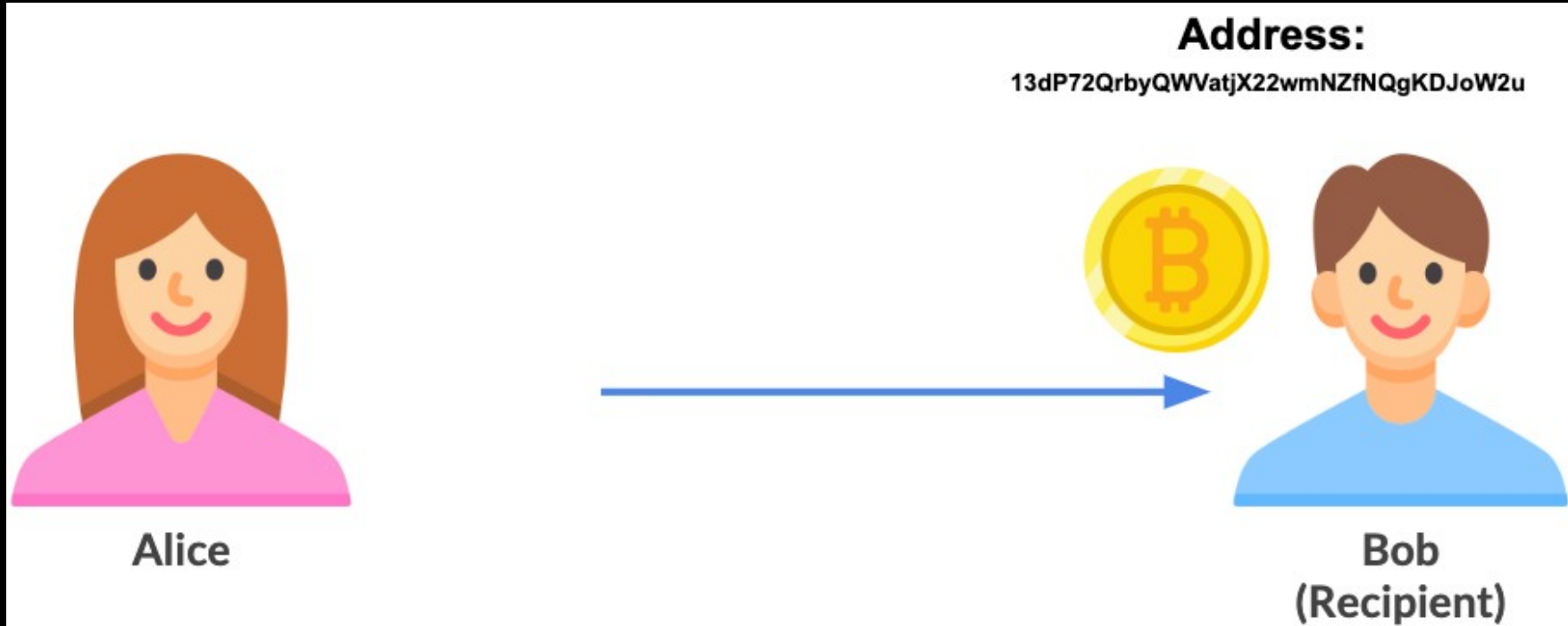
What's under the hood?

Step 4: miner selects Alice's "check" and confirms it



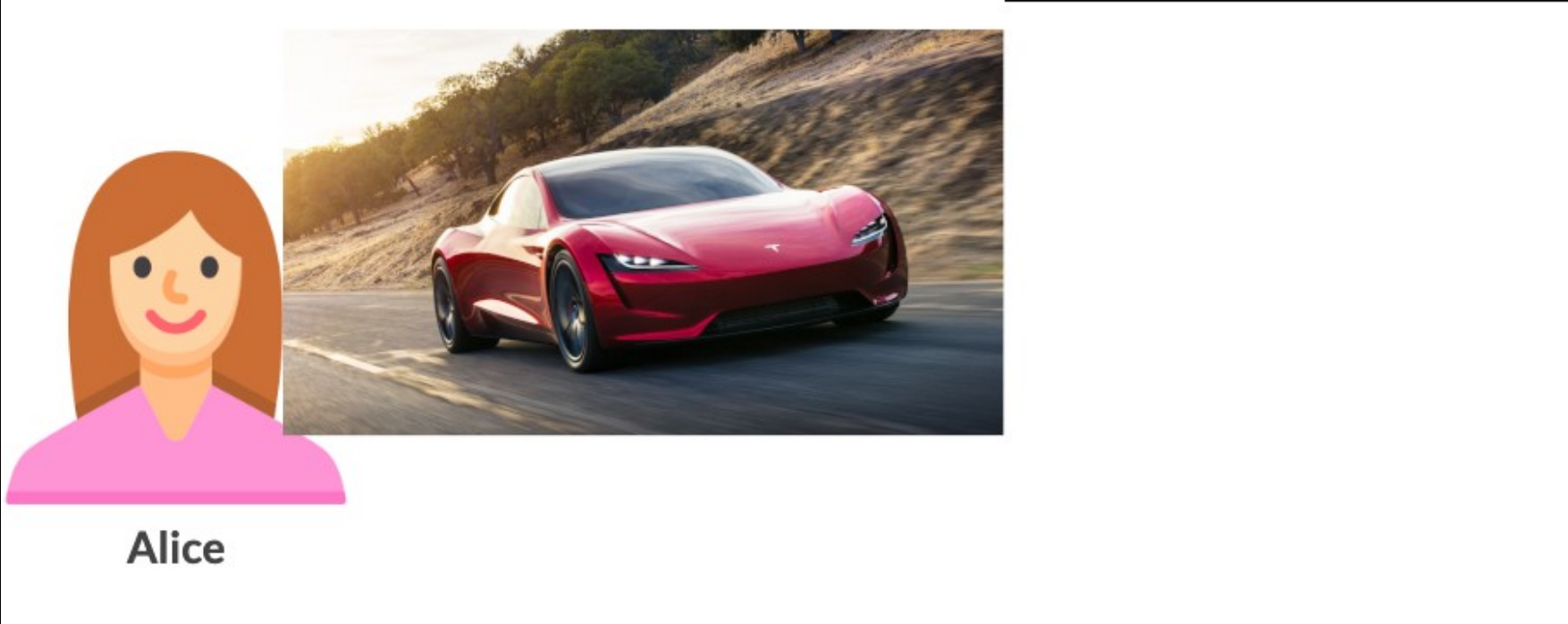
What's under the hood?

Step 5: Bob verifies that he now owns 1 bitcoin

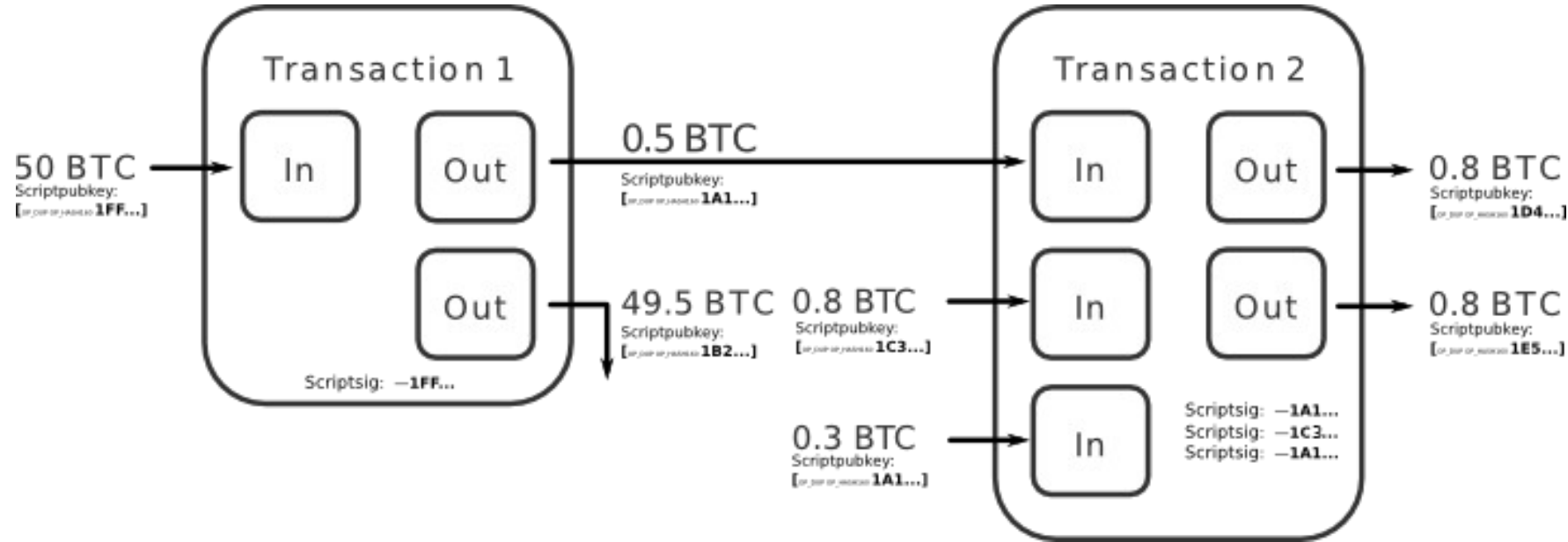


What's under the hood?

Step 6: Bob gives the car to Alice



a transaction is a record of bitcoin changing hands



Keys prove ownership but how does one avoid double spending?

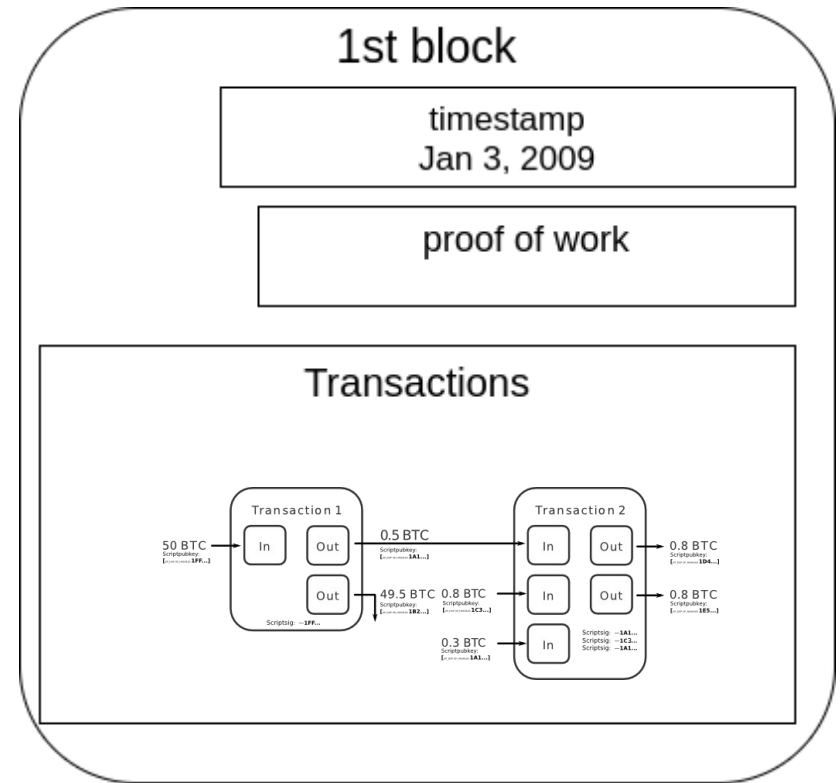


a **block** records some transactions

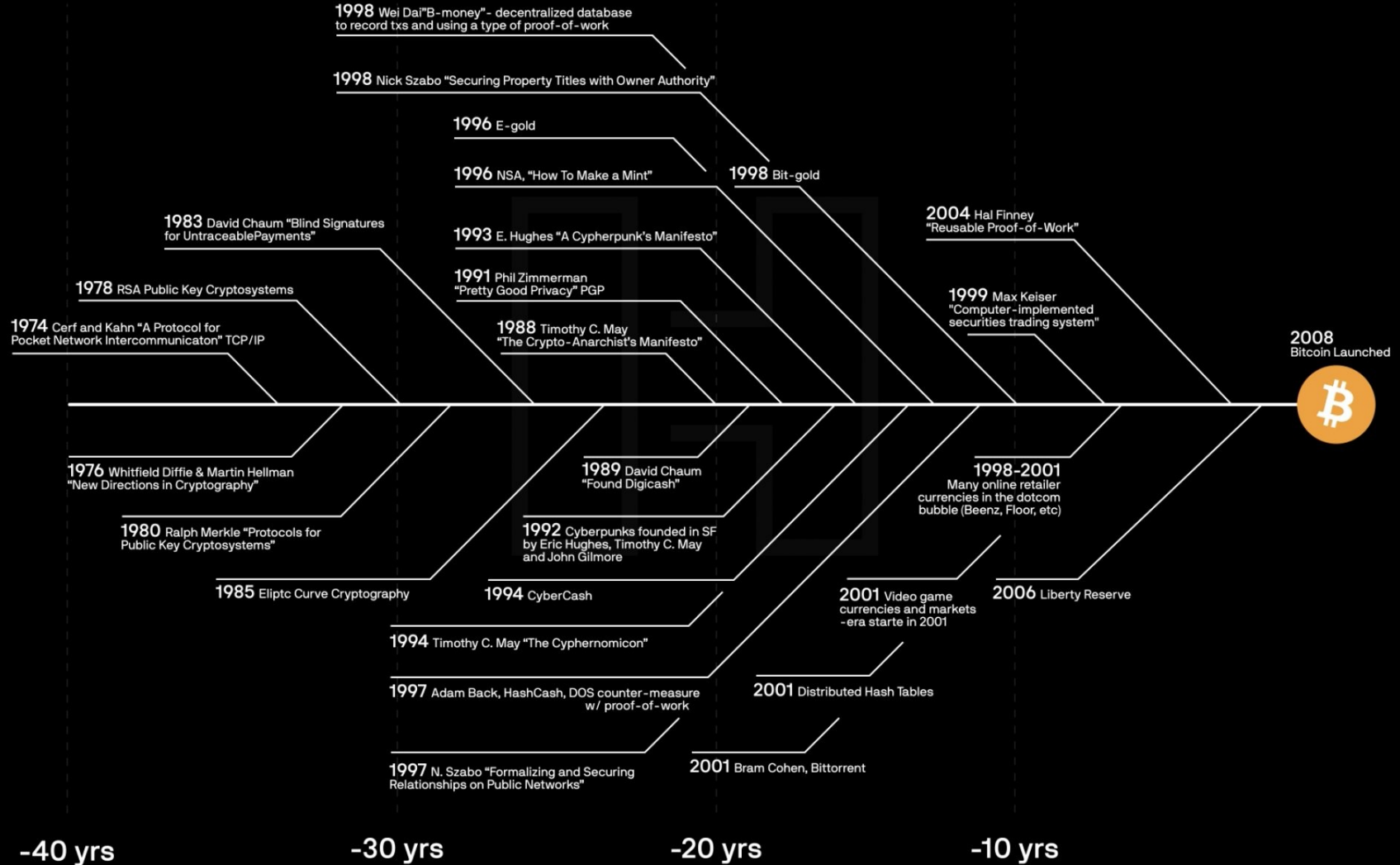
1 block = 2 megabytes = 1,000 to 2,000 transactions

A new block get added every
10 minutes (on average)

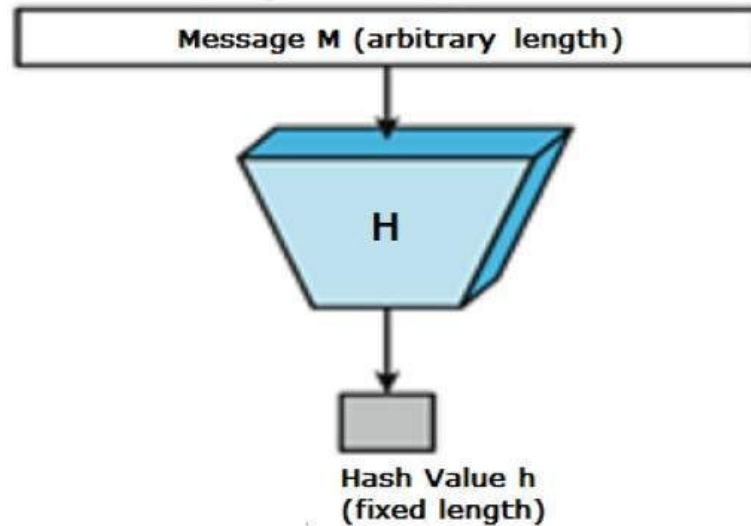
Proof of Work = Physical energy (kWh)



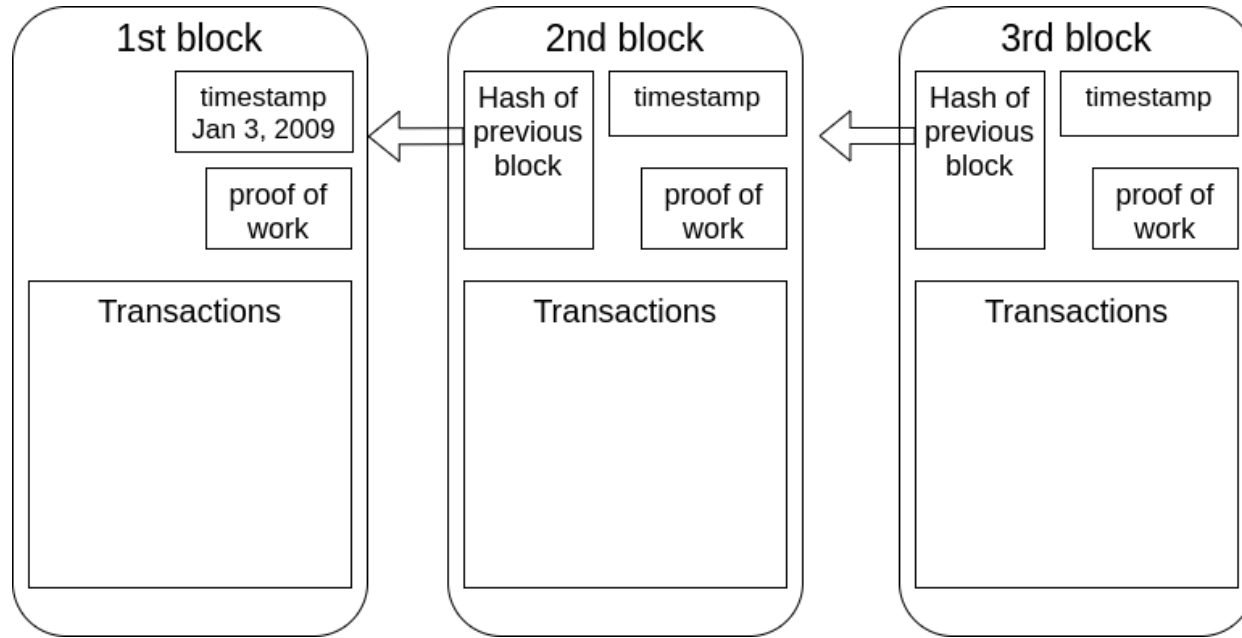
Bitcoin Prehistory – It's the result of 40 years of research, development and demand



a **hash function** is a mathematical way verify a large message without using 3rd parties



the **ledger** records all valid blocks

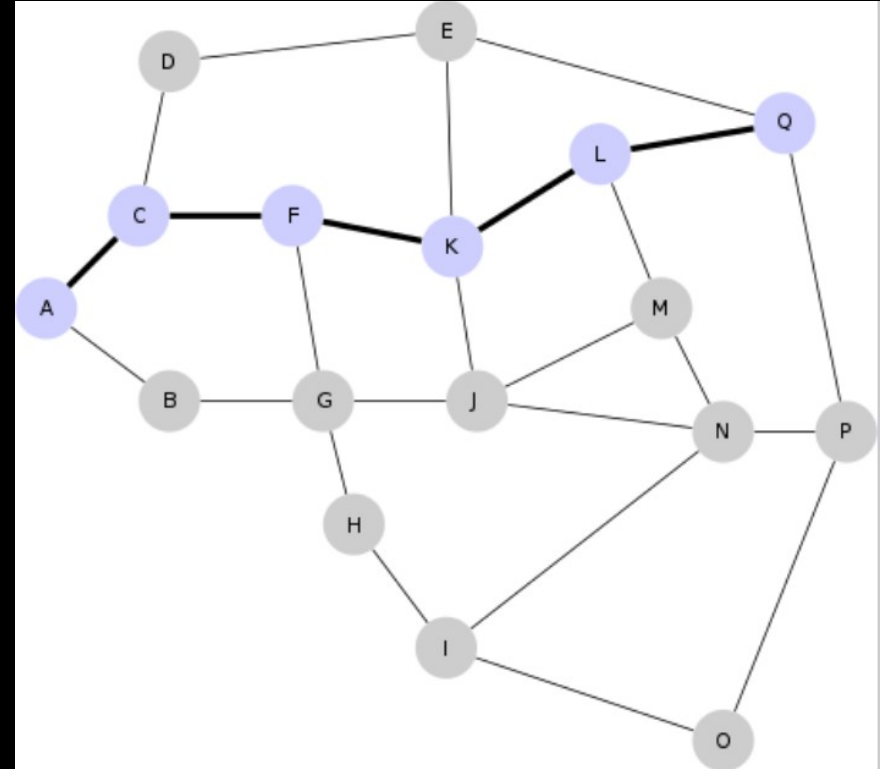


What stops a large state actor from censor transactions?



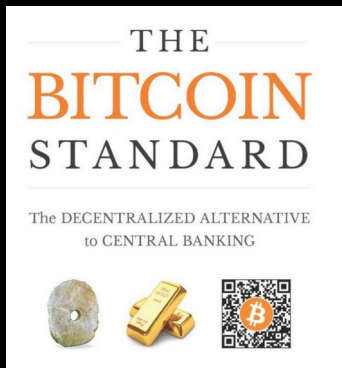
Lightning Network

- Trust-less
- Makes bitcoin payments
 - Fast
 - Cheap
- Has limits payment size
 - Up to ~\$100 works great
- Examples of use:
 - El Salvador remittances



Continue Learning...

Books:



Podcasts:

1. Noded Bitcoin Podcast
2. Stephan Livera Podcast
3. Tales from the Crypt

YouTube:

BTC Sessions



High-quality articles on big topics:

1. Shelling Out: The Origins of Money (2002)
2. Speculative Attack by Pierre Rochard (2014)
3. The Bullish Case for Bitcoin (2018)

Follow people on Twitter:

- | | |
|-------------------|------------------|
| 1. Pierre Rochard | @BitcoinIsSaving |
| 2. Vijay Boyapati | @real_vijay |
| 3. Alex Gladstein | @gladstein |
| 4. Jimmy Song | @jimmysong |

My email: alevchuk@gmail.com