CBS COPENHAGEN BUSINESS SCHOOL
HANDELSHØJSKOLEN

Elective Course on Mastering Blockchain: Foundations to Consensus

Chronology of key ideas in Bitcoin and Cryptoeconomics A Simple Cryptocurrency

Raghava Mukkamala

Associate Professor & Director, Centre for Business Data Analytics
Copenhagen Business School, Denmark
Email: rrm.digi@cbs.dk, Centre: https://cbsbda.github.io/

Course Coordinator at SRMIST:

Prof. K. Shantha Kumari

Associate Professor
Data Science and Business Systems Department,
SRM Institute of Science and Technology, India
Shanthak@srmist.edu.in

EQUIS ACCREDITED AACSB ACCREDITED ASSOCIATION AMBA ACCREDITED CEMS PIM

Outline

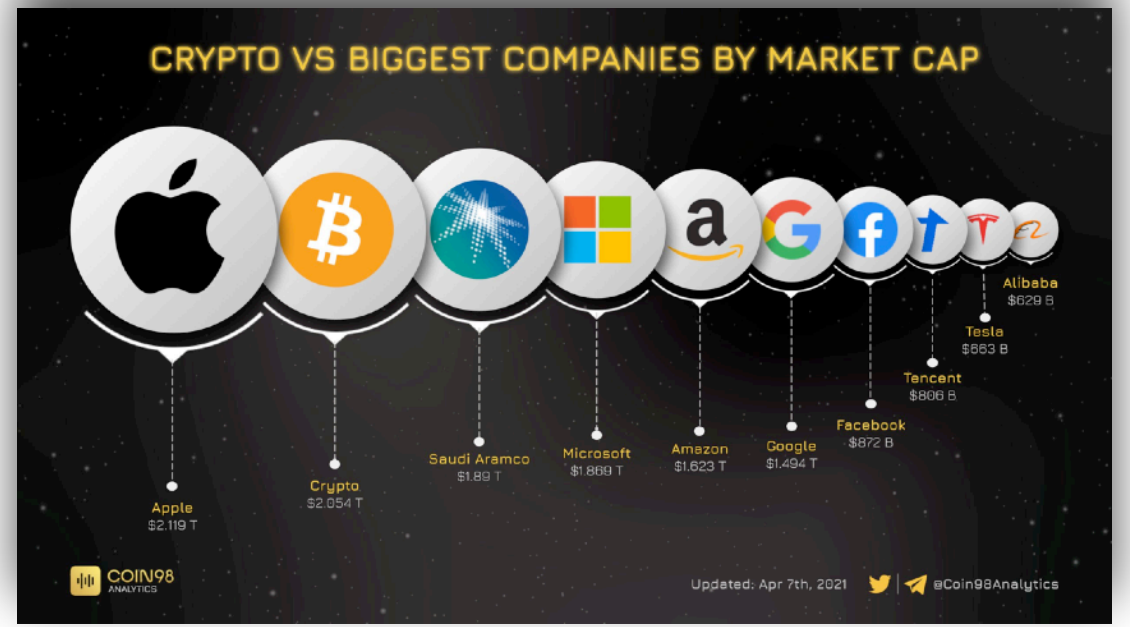
- History of Bitcoin: What contributed to its discovery?
  - Economic and Political Conditions
  - CypherPunk Movement
- Double Spending Problems and Other Digital Currencies
- Simple Mechanics of Digital / Crypto Currencies

Why History of Bitcoin?

- ***How do we know whether Blockchain is just hype or a paradigm shift, or disruptive?***
- First of all, why is it important to answer that question?
    - As of now, the total Crypto market share is around $2.0 trillion USD
- Revolutionary ideas/Disruptive technologies are not born in a day!
- When Satoshi Nakamoto published his/her/their white paper on Bitcoin in 2008, they advocated a new way of thinking about **money** and **its value**.
- Despite the ever-growing cryptocurrency environment, Bitcoin's history is the most colorful and meaningful.
- It is quite important to understand the historical evolution and ideas behind Bitcoin as it is considered some kind of *Paradigm Shift.*

1) Source: Nathan Lenga https://zerocap.com/insights/articles/bitcoin-history-first-cryptocurrency/
2) Bitcoin whitepaper. https://bitcoin.org/bitcoin.pdf

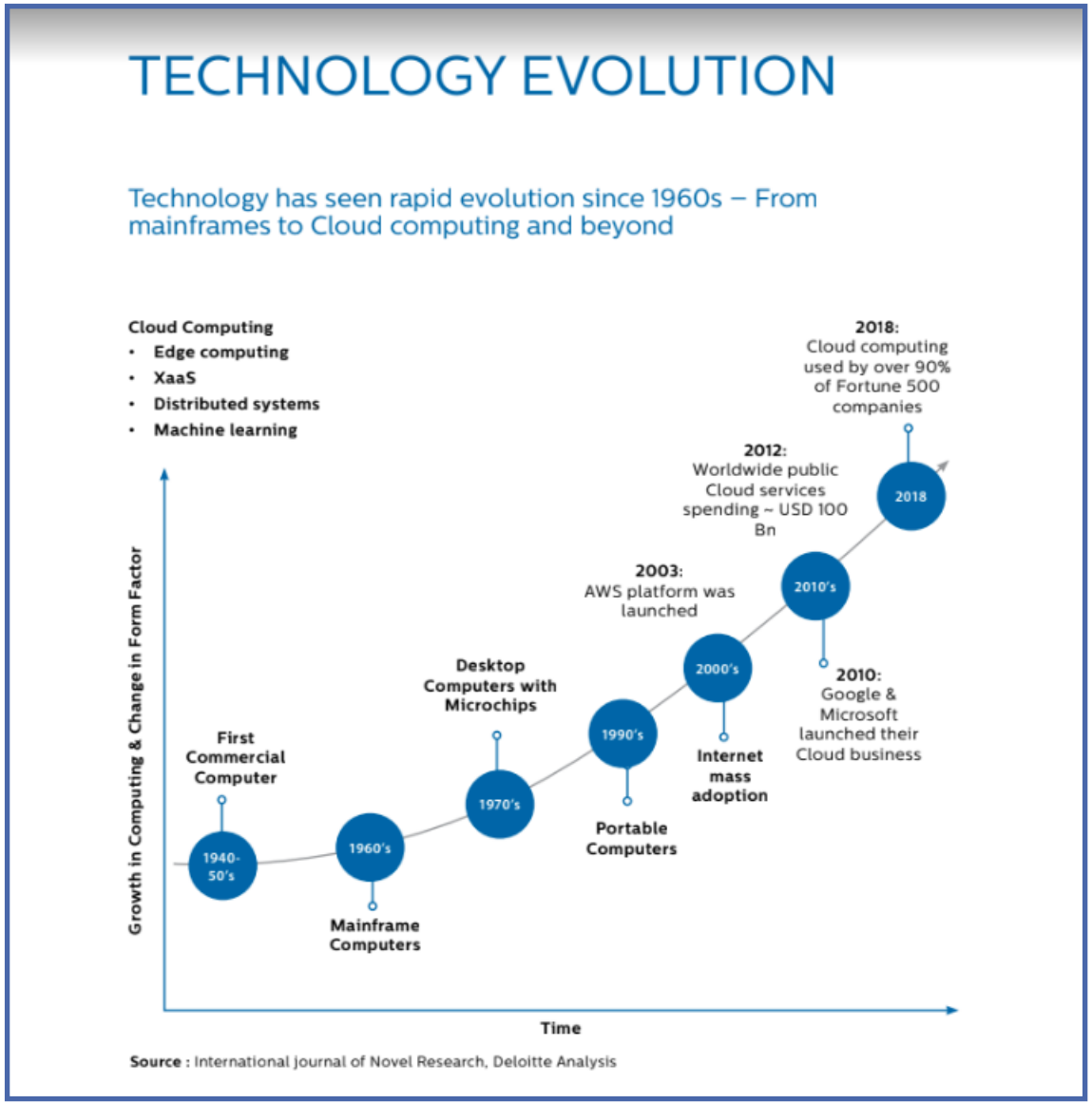
Why is it a Paradigm Shift?



1) https://www.digitalinformationworld.com/2021/04/bitcoin-has-reached-1-trillion-mark.html
2) https://twitter.com/Coin98Analytics/status/1379732985402904581/photo/1

Paradigm Shift vs Disruptive Technology?

- Is it a *Paradigm Shift or Disruptive Technology?*
- Programming Models/ Application types, from Console applications to Cloud technologies, evolved over many years of research
- Bitcoin is a collection of *existing technologies/ideas* + *economic & political conditions* that lead to a new way of thinking -> Distributed and Decentralised applications!



1) Source: Nathan Lenga https://zerocap.com/insights/articles/bitcoin-history-first-cryptocurrency/

KEY TECHNOLOGIES BEHIND BITCOIN

DOI:10.1145/3132259

Article development led by acmqueue
queue.acm.org

The concept of cryptocurrencies is built from forgotten ideas in research literature.

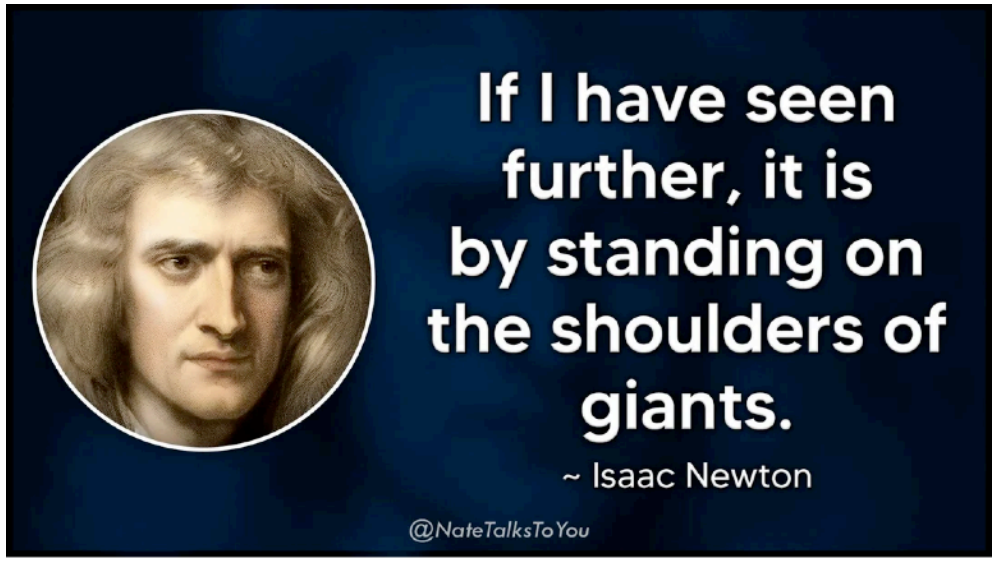
BY ARVIND NARAYANAN AND JEREMY CLARK

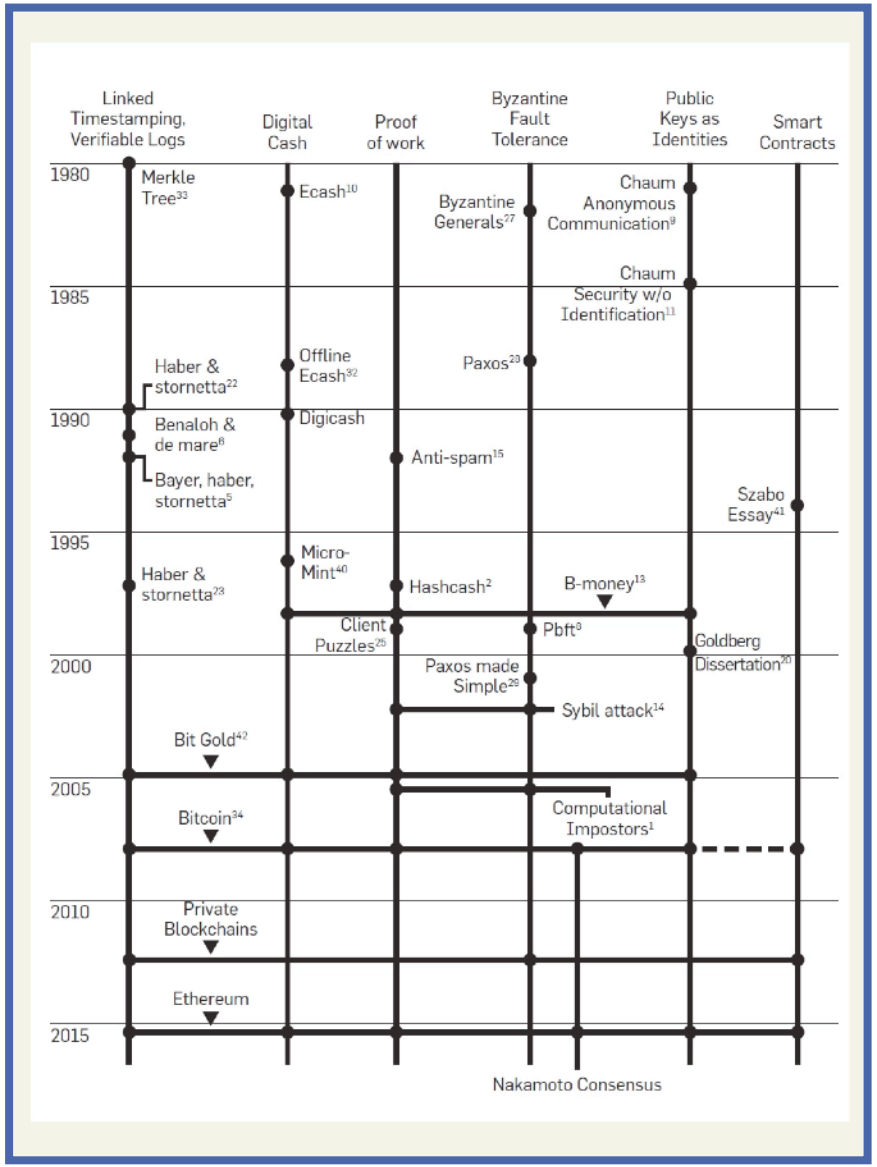
Bitcoin's Academic Pedigree

CBS

Chronology of Key Ideas behind Bitcoin

- Cryptocurrencies are built from forgotten ideas from the research literature
- All of the technical components of Bitcoin originated in the academic literature from the 1980s and 1990s
- Not to diminish Nakamoto's achievement but to prove that he *stood on the shoulders of giants!*

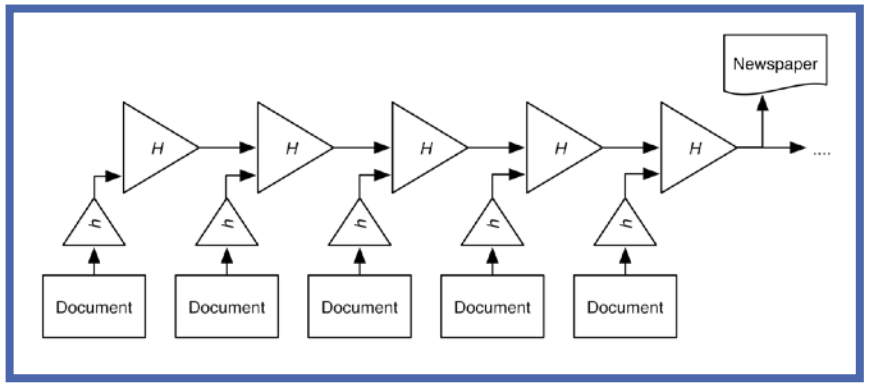




1) Source: Narayanan, A., & Clark, J. (2017). Bitcoin's academic pedigree. Communications of the ACM, 60(12), 36-45.
2) https://www.reddit.com/r/QuotesPorn/comments/15jwlmd/if_i_have_seen_further_it_is_by_standing_on_the/?rdt=46471

Linked Timestamping $\Longrightarrow$ Ledger

- Bitcoin's ledger is borrowed, with minimal modifications, from a series of papers[2&3] by Stuart Haber and Scott Stornetta from 1990 and 1997
- Their work addressed the problem of document timestamping aka "digital notary" service.
- For patents, business contracts, and other documents, one may want to establish that the document was created at a certain point in time, and no later.



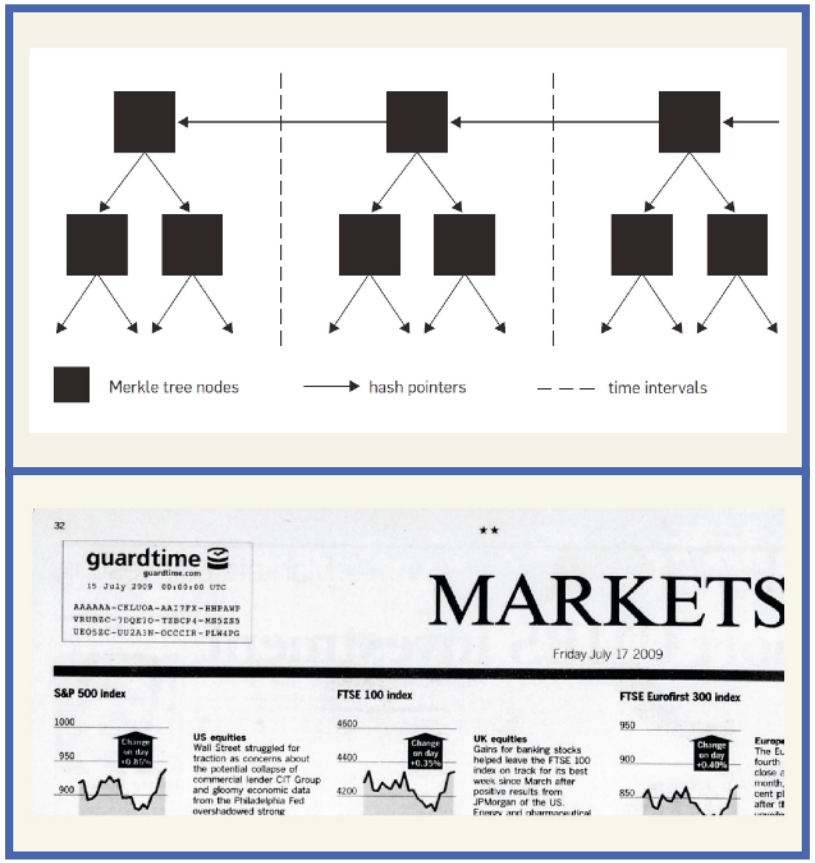
By RistoLaanoja - Own work, Public Domain, https://commons.wikimedia.org/w/index.php?curid=8754152

https://en.wikipedia.org/w/index.php?curid=39214978

2) Haber, S. and Stornetta, W.S. How to timestamp a digital document. J. Cryptology 3, 2 (1991), 99–111; https://link.springer.com/ chapter/10.1007/3-540-38424-3_32.
3) Haber, S. and Stornetta, W.S. Secure names for bit- strings. In Proceedings of the 4th ACM Conference on Computer and Communications Security, 1997, 28–35; http://dl.acm.org/citation.cfm?id=266430.

Merkle Trees

- In each block's Merkle tree[4], the leaf nodes are transactions, and each internal node essentially consists of two pointers. This data structure has two important properties.
- First, the hash of the latest block acts as a digest. A change to any of the transactions (leaf nodes) will necessitate changes propagating all the way to the block's root and the roots of all following blocks.
- Second, someone can efficiently prove to you that a particular transaction is included in the ledger.
- Can verify membership in O(log n) time/space



1) Narayanan, A., & Clark, J. (2017). Bitcoin's academic pedigree. Communications of the ACM, 60(12), 36-45.

5) Bayer, D., Haber, S. and Stornetta, W.S. Improving the efficiency and reliability of digital time-stamping. In Proceedings of Sequences (1991);

4) Merkle, R.C. Protocols for public key cryptosystems. In Proceedings of the IEEE Symposium on Security and Privacy, 1980; http://www.merkle.com/papers/ Protocols.pdf.

Many Other Technologies

- Byzantine Fault Tolerance - Distributed Consensus Algorithms
- Cryptography, Hash Functions, Digital Signatures
- Proof-of-Work as a mitigation strategy against spam, Sybil attacks, and denial of service etc.
- Several other key ideas from Digital currencies

History of Bitcoin: What contributed to its discovery?

Image by MichaelWuensch from Pixabay

CBS

Why History of Bitcoin is relevant and interesting?

The design of Bitcoin includes:

- game theory semantics
- economics theories
- computer science,
- cryptography,
- politics,
- philosophy,
- monetary history,
- human rights, privacy,
- investor psychology,
- and much more.

1) Source: Nathan Lenga https://zerocap.com/insights/articles/bitcoin-history-first-cryptocurrency/

Why History of Bitcoin?

- To understand why Bitcoin has succeeded,
  - First, we need to understand what are economic and political conditions that contributed to its development.
  - Second, some of the important movements toward freedom and privacy in the digital space, especially the Cypherpunks movement
  - Third, what are the other attempts tried to create digital currencies, and how have they failed but influenced the design of Bitcoin (most importantly, how Bitcoin solved double-spending problems)

1) Source: Nathan Lenga https://zerocap.com/insights/articles/bitcoin-history-first-cryptocurrency/

Economic and political Conditions

Image by MichaelWuensch from Pixabay

CBS

The Gold Standard

- Bitcoin was influenced by the gold standard when creating Bitcoin, often referred to as digital gold.
- The gold standard was a system of fixed exchange rates with currencies that was created in the late 1800s and finally abandoned in 1971.
- Countries used the gold standard for pegging the value of their currency to gold.
- Nations could exchange their currencies for gold or other currencies that were denominated by a value in gold, e.g., Dollar.
- As more & more countries subscribed to the gold standard, it became a domestic method for regulating the quantity of the money supply

https://en.wikipedia.org/wiki/Indian_2000-rupee_note

1) Source: Nathan Lenga https://zerocap.com/insights/articles/bitcoin-history-first-cryptocurrency/

The Gold Standard

- Due to the inability of governments to print money, this standard facilitated long-term price stability.
- Therefore, the average inflation rate between 1880 and 1914 was 0.1%. (as against 4.1% between 1946-2003)
- Because exchange rates were fixed, the gold standard caused price levels worldwide to move together.
- Of course, it has other problems, but at least the inflation rates are quite manageable as tight control over how much can govt can print

1) Source: Nathan Lenga https://zerocap.com/insights/articles/bitcoin-history-first-cryptocurrency/

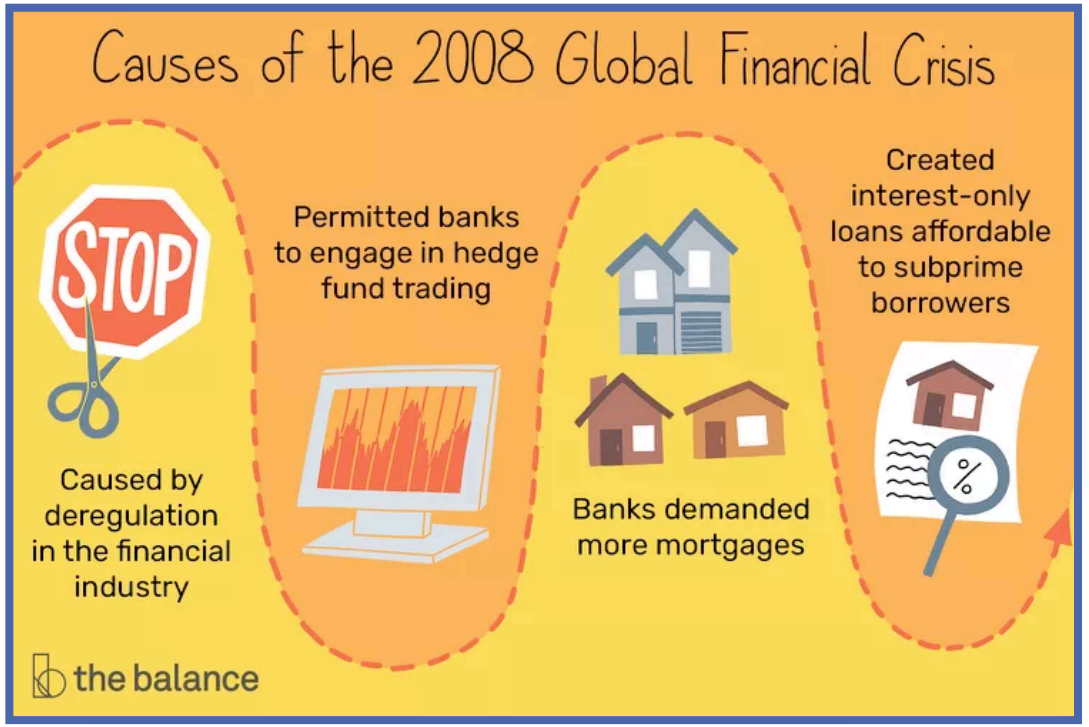
The Gold Standard and Bitcoin

- Bitcoin took two main aspects of the gold standard into consideration in its design.
- Firstly, both Bitcoin and gold are stateless, i.e. currency owned by *no country*, instead to be utilised *internationally*.
- Secondly, Bitcoin, like gold, is limited in supply. Gold is scarce, and Bitcoin's supply is capped at 21 million.
- Restricted supply of Bitcoin led to positive price pressure on the tokens as demand increased at a higher rate to the rise in supply from mining – maintaining its cap of 21 million.

1) Source: Nathan Lenga https://zerocap.com/insights/articles/bitcoin-history-first-cryptocurrency/

2008 Global Financial Crisis

- Bitcoin was created during the 2008 Global Financial Crisis (GFC).
- The recession was caused by a lack of transparency between banks and their customers, whereby unscrupulous (legal but unethical) banking practices transferred the risk to investors and borrowers.
- Banks invested their customers' deposits using derivatives, which led to the GFC.
- Derivatives were created using subprime residential mortgages enabling individuals with low credit ratings to borrow to purchase a house



https://www.thebalancemoney.com/what-caused-2008-global-financial-crisis-3306176

1) Source: Nathan Lenga https://zerocap.com/insights/articles/bitcoin-history-first-cryptocurrency/

2008 Global Financial Crisis

- Banks' derivatives and investments tied to the subprime residential mortgages lost all of their value
- The financial and social implications of this event were catastrophic.
- US unemployment rate reached as high as 9.6%
- Retirement funds fell by more than 20%
- America's GDP loss was $12.8 trillion USD throughout the subsequent years.

Key Takeaways

- A change in bank investing regulations allowed banks to invest customers' money in derivatives.
- Derivatives were created from subprime residential mortgages, and demand for homes skyrocketed.
- When the Federal Reserve raised interest rates, subprime mortgage borrowers could no longer afford their mortgages.
- The supply of houses outran demand, borrowers defaulted on their mortgages, and the derivatives and all other investments tied to them lost value.
- The financial crisis was caused by unscrupulous investment banking and insurance practices that passed all the risks to investors.

https://www.thebalancemoney.com/what-caused-2008-global-financial-crisis-3306176

1) Source: Nathan Lenga https://zerocap.com/insights/articles/bitcoin-history-first-cryptocurrency/

Global Financial Crisis

- People lost their jobs, homes, and mortgage properties
- Banks got trillions of dollars as bailouts from the government, resulting in bank top executives getting hefty bonus packages
- People who lost their jobs/homes and became defaulters got nothing in return from govt/banks
- Nakamoto witnessed what happens when you delegate trust to centralized authorities like banks, governments.
- During this period, he/she/they wanted to create a system where trust was not required.

1) Source: Nathan Lenga https://zerocap.com/insights/articles/bitcoin-history-first-cryptocurrency/

Global Financial Crisis

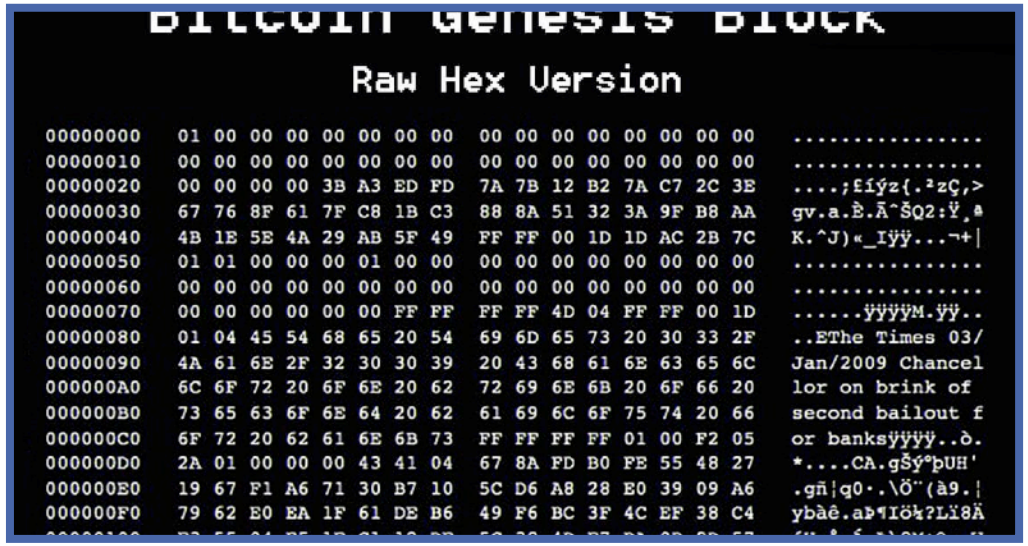
https://newlaborforum.cuny.edu/2021/10/27/occupy-wall-street-a-decade-later/

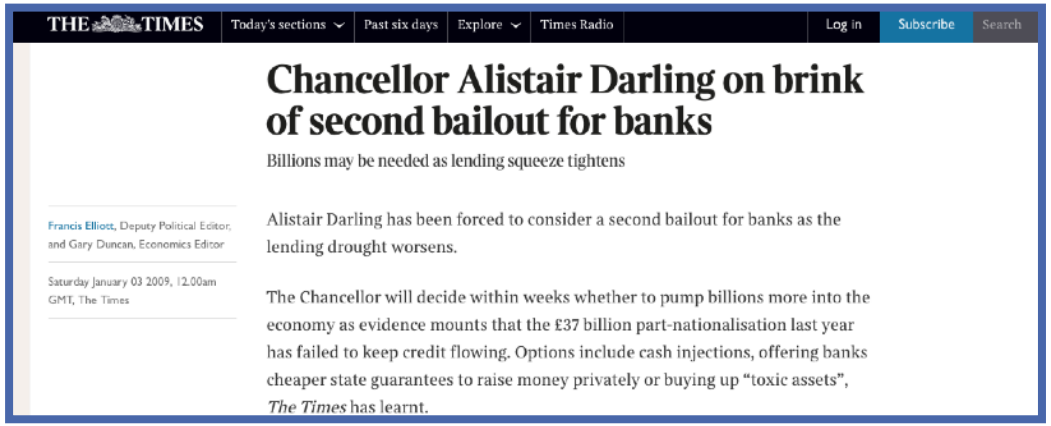
What lessons did Bitcoin take from GFC?

- Avoid trust with centralised authorities such as banks/govt.
- By giving all users access to information, the Bitcoin network intentionally avoided establishing a hierarchy.
- Nakamoto encoded a unique string into Bitcoin's Genesis block.

"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks".

- Bitcoin depicts Nakamoto's motivation to erect an alternative model to the fractional banking system that puts the general public at risk.




THE TIMES | Today's sections | Past six days | Explore | Times Radio | Log in | Subscribe | Search

Chancellor Alistair Darling on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott, Deputy Political Editor, and Gary Duncan, Economics Editor

Saturday January 03 2009, 12.00am GMT, The Times

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37 billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offering banks cheaper state guarantees to raise money privately or buying up "toxic assets", *The Times* has learnt.

1) Source: Nathan Lenga https://zerocap.com/insights/articles/bitcoin-history-first-cryptocurrency/

CypherPunk Movement

https://bitcoinmagazine.com/culture/crypto-art-of-resistance-remember-remember-the-legacy-of-the-cypherpunks

CBS

The Cypherpunks

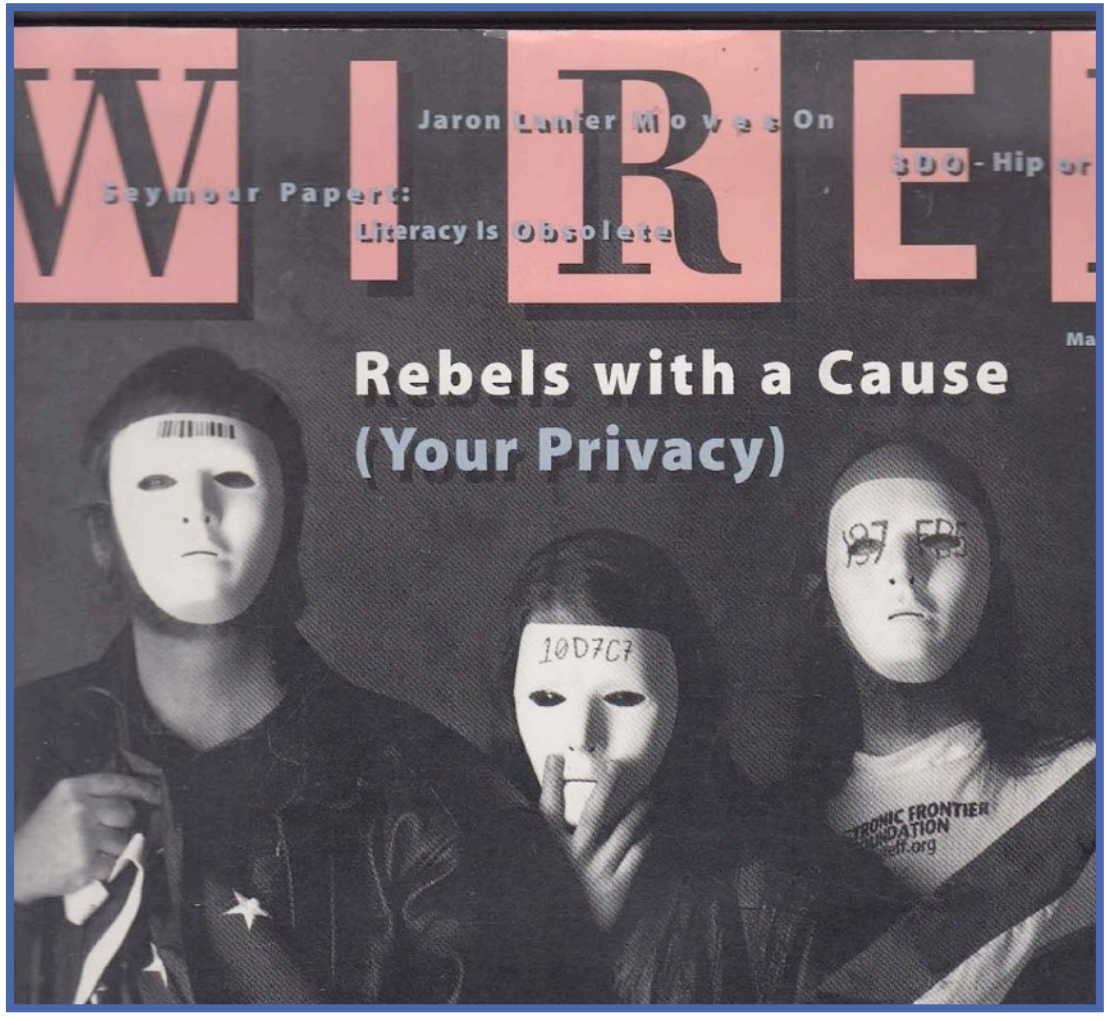
- The cypherpunks were a group with liberal and rebellious ideas from 1990s
- They all shared a core conviction: Internet would soon become an important battleground for human freedom
- Back in the early 90s, cyberspace was still the domain of hobbyists and hackers.
- But the cypherpunks believed that it was only a matter of time before the Internet would become central to society.
- Once governments understood the Internet's importance, they would move to co-opt, monitor, and censor it.

> *Cypherpunks write code. We know that someone has to write software to defend privacy, and we're going to write it.*
>
> *— Eric Hughes*
> *The Cypherpunk's Manifesto, 1993*

Source: Haseeb Qureshi; https://nakamoto.com/the-cypherpunks/

Rebels with a Cause

- Long before Facebook, long before the Great Firewall of China, long before the Snowden revelations, the cypherpunks saw it coming.
- They foretold/predicted a regime of online censorship and surveillance that would eclipse the open Internet.
- And according to the cypherpunks, there was only one tool that could ensure the Internet's freedom: **Cryptography**



Source: Haseeb Qureshi; https://nakamoto.com/the-cypherpunks/

Cryptography

- Cryptography is the mathematics of codes and codebreaking.
- Before the 1970s, cryptography was a relatively arcane field practiced only by the military and spy agencies.
- At the time, strong encryption (anything more than 40 bits of security) was considered to be a military munition and, therefore illegal to export from the US.
- But the cypherpunks believed cryptography was critical to a sovereign Internet.

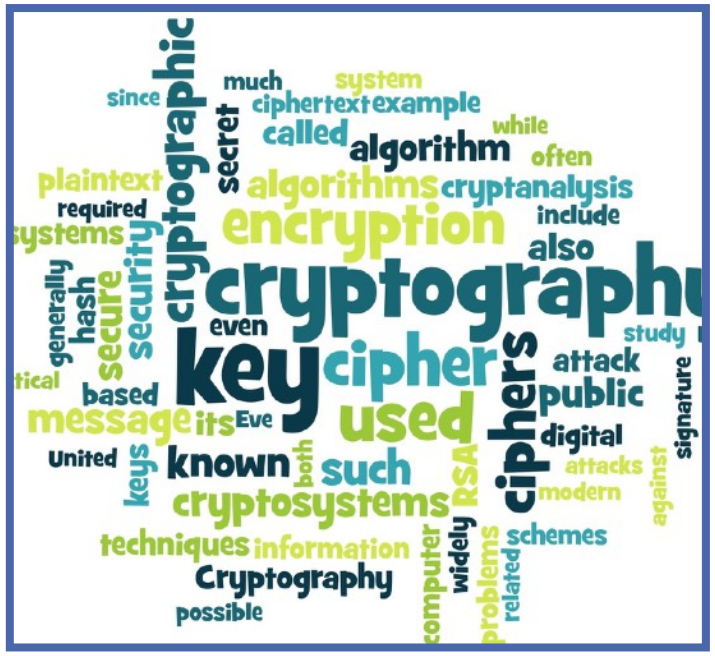


Image by tumbledore from Pixabay

The Imitation Game

Source: Haseeb Qureshi; https://nakamoto.com/the-cypherpunks/

The Cypherpunks and Cryptography

- They believed that encryption was the best way to wrest power away from governments back toward individuals.
- But the cypherpunks knew that encryption alone would not be enough to liberate cyberspace.
- *To build a truly free digital commons, you needed a completely sovereign economy.*
- In other words, you needed a **digitally native form of money** which is beyond the control of Govt and banks

https://bitcoinmagazine.com/culture/crypto-art-of-resistance-remember-remember-the-legacy-of-the-cypherpunks

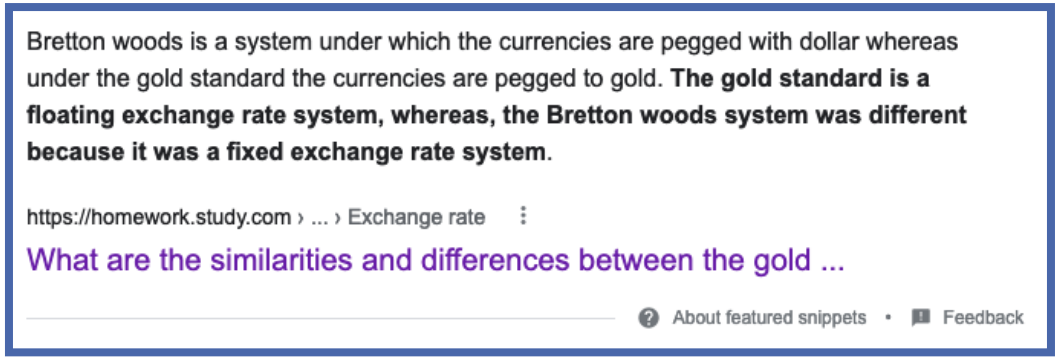
Source: Haseeb Qureshi; https://nakamoto.com/the-cypherpunks/

Cypherpunk Economics

- It's important to understand the cypherpunk take on economic philosophy.
- The cypherpunks were deeply suspicious of central banks and their control over monetary policy after the end of Bretton Woods
- Many years later, their suspicions were arguably justified after the financial crisis of 2008, when central banks created massive amounts of money to bail out failing banks.
- To dig a little bit deeper, we need to understand how govts earn or make money

> *"Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world."*
>
> *A Cypherpunk's Manifesto*

https://bitcoinmagazine.com/culture/crypto-art-of-resistance-remember-remember-the-legacy-of-the-cypherpunks



Source: Haseeb Qureshi; https://nakamoto.com/the-cypherpunks/

How do Governments earn money?

- The first is taxation (income tax, GST, etc.), where a government directly transfers money from citizens into its account through taxes.
- The second way is by printing money, traditionally known as *seigniorage*, which also transfers money to the government but is a little more subtle to analyze.
- When a government prints money, the government obviously acquires currency,
- However, citizens find that the value of their currency holdings has depreciated since there is now more money in the market chasing the same set of real assets/goods —> which increases the price of goods and leads to inflation.

Source: Haseeb Qureshi; https://nakamoto.com/the-cypherpunks/

What is inflation?

Johnny Harris: https://www.youtube.com/watch?v=zIbNJCSCEjk

Cypherpunk Economics

- Taxation and seigniorage are roughly economically equivalent for govt.
- But taxation generally requires the assent of citizens, whereas printing money can be done unilaterally.
- The cypherpunks thus saw money printing as a form of theft by the governments from its citizens.
- Tying a digital economy to a singular fiat currency would subjugate it to the whims of a single country's central bank.

https://bitcoinmagazine.com/culture/crypto-art-of-resistance-remember-remember-the-legacy-of-the-cypherpunks

Source: Haseeb Qureshi; https://nakamoto.com/the-cypherpunks/

Cypherpunk Economics

- Internet itself was already borderless and international, and an Internet-native currency puts everyone, regardless of nationality, on the same level.
- A central party capable of surveilling such a system should not exist. Otherwise, that central party would be tempted to censor the system or manipulate the currency.
- The cypherpunks believed that the soundest economic system was one that no one could manipulate.
- Thus, cyberspace could not be truly free unless it had its own form of money. This they could agree on.
- But creating digital money had a technical problem that no one had yet been able to crack: the ***double spending*** problem.

https://bitcoinmagazine.com/culture/crypto-art-of-resistance-remember-remember-the-legacy-of-the-cypherpunks

CBS CENTRE FOR BUSINESS DATA ANALYTICS

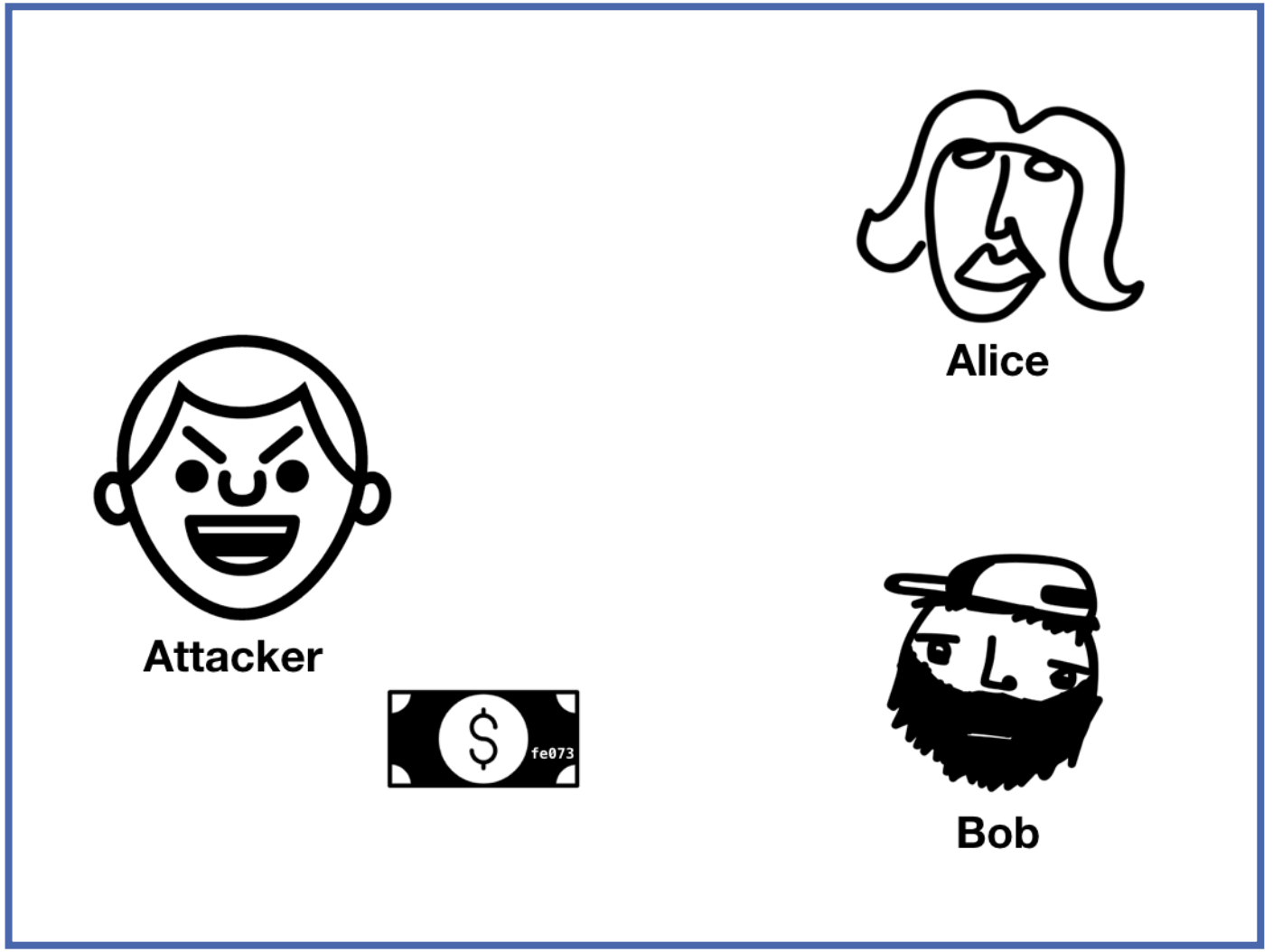
Source: Haseeb Qureshi; https://nakamoto.com/the-cypherpunks/

Double Spending Problems and other currencies

https://bitcoinmagazine.com/culture/crypto-art-of-resistance-remember-remember-the-legacy-of-the-cypherpunks

The Double Spending Problem

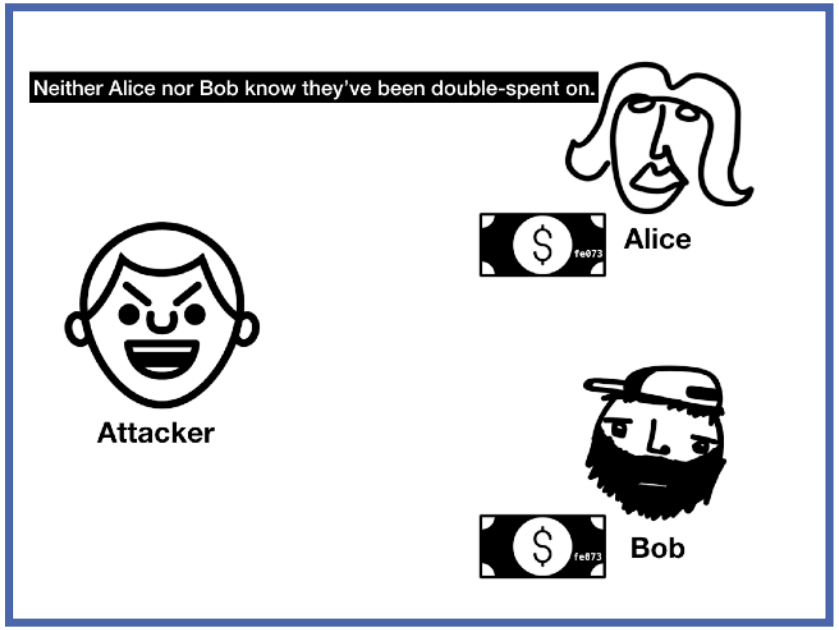
- If a $10 bill is entirely digital, then it's just a bunch of bits
- What's to stop me from copy and pasting those bits so I now have two $10 bills?
- And if I pay two people with copies of that $10 bill, how could they know which one is the "real" one?



Source: Haseeb Qureshi; https://nakamoto.com/the-cypherpunks/

The Double Spending Problem

- The double spend problem can be conceived of as a counterfeiting problem, but the notion of counterfeiting only makes sense for a physical bill
- In the digital world, a bill is just information. The "real bill" is just a sequence of bytes.
- How is this problem solved with digital payment schemes like PayPal?
- Simple: PayPal's servers enforce the "anti-counterfeiting." It has a single unified database that moves around its bytes—as a user; you don't get direct access to it.
- This protects the system from double spending, but at the expense of giving PayPal complete control over the monetary system.



Source: Haseeb Qureshi; https://nakamoto.com/the-cypherpunks/

Chaum's eCash

- David Chaum is considered by many to be the father of the cypherpunk movement.
- A prolific academic researcher, Chaum single-handedly created the field of anonymous communications research
- Invented many cryptographic protocols, including group signatures, mix networks, and ***blind signatures***
- In 1990, David Chaum spearheaded the first serious attempt at building private digital money: DigiCash.
- DigiCash used novel cryptography to ensure user privacy while solving the *double spend* problem.

https://chaum.com/ecash/

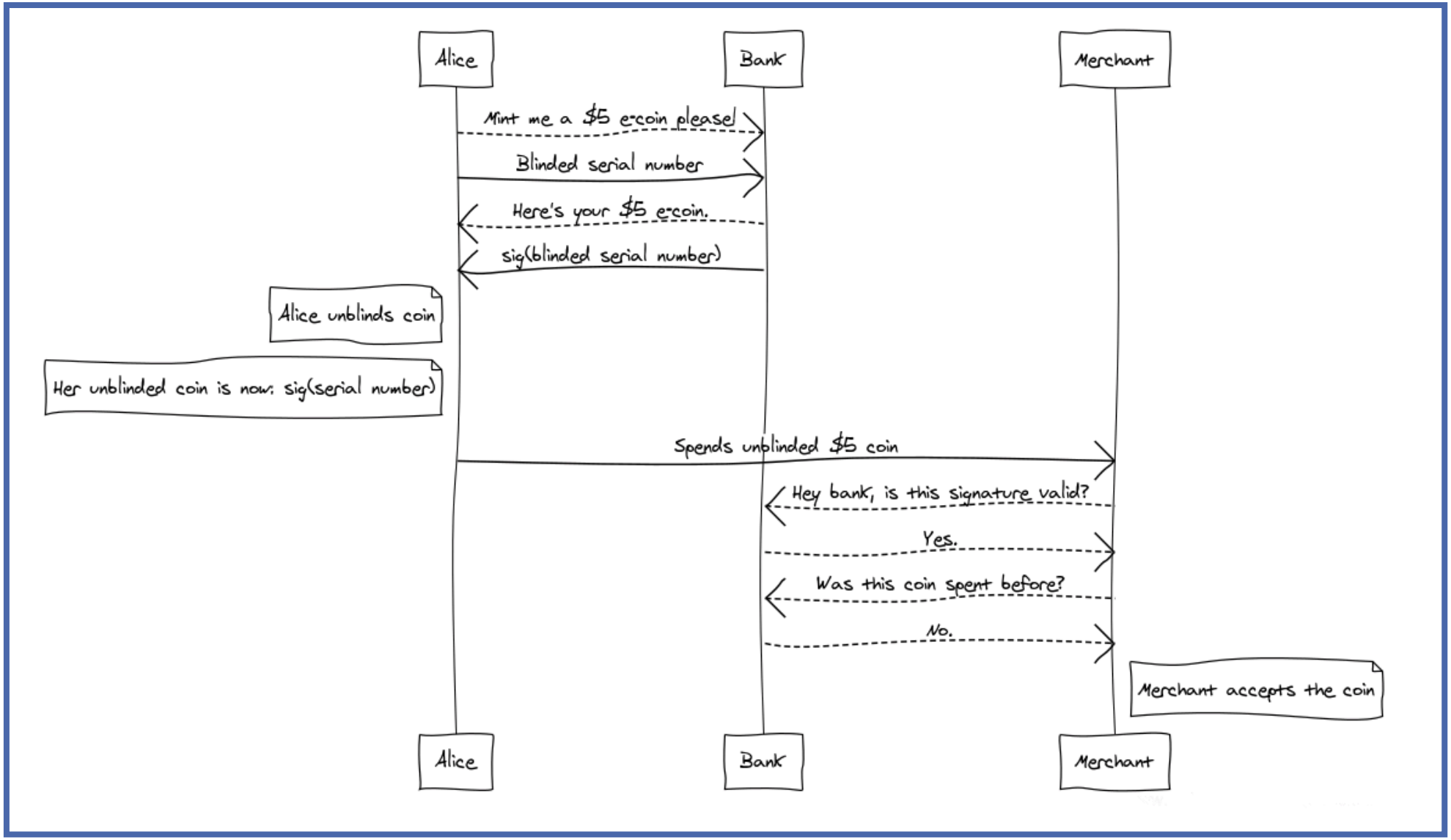
Source: Haseeb Qureshi; https://nakamoto.com/the-cypherpunks/

DigiCash

- First, coins are issued to users by a bank. Each coin has a specific denomination and serial number, which are cryptographically signed by the bank.
- When a merchant receives a coin from a user, the merchant relays the coin to the issuing bank.
- The bank verifies that the signature over the denomination and serial number is valid and whether the coin has been previously spent.
- If these check out, the bank ensures that all spent coins are real and haven't been spent before.

Source: Haseeb Qureshi; https://nakamoto.com/the-cypherpunks/

Chaum's eCash protocol



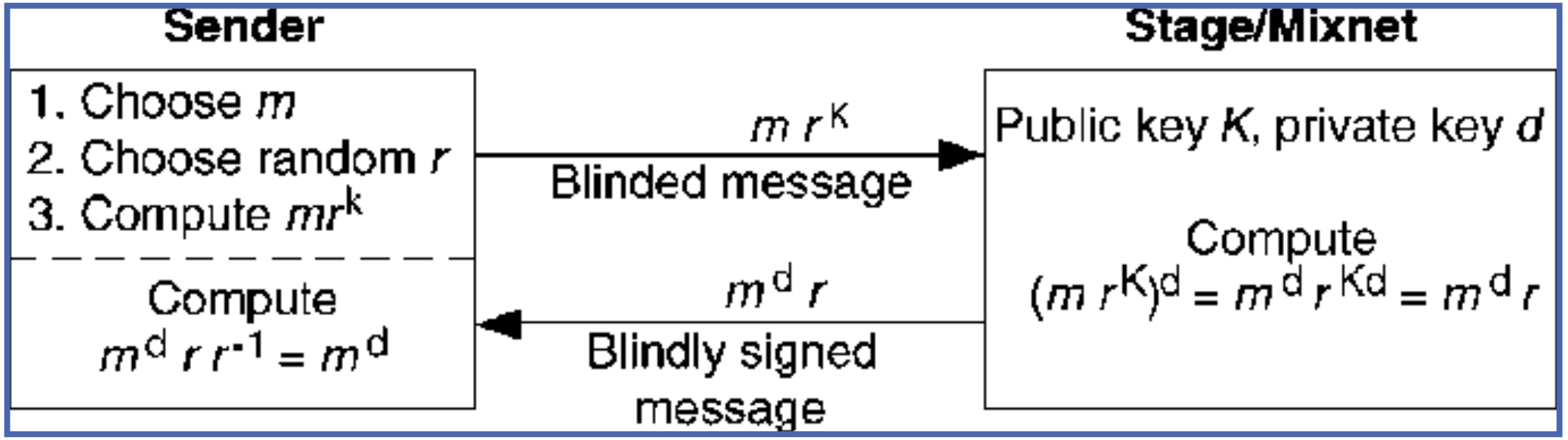
CBS CENTRE FOR BUSINESS DATA ANALYTICS

Source: Haseeb Qureshi; https://nakamoto.com/the-cypherpunks/

eCash - blind signatures

- On the face, this setup solves the double spend problem, but it seems quite centralized given the bank's presence.

- And how does this achieve privacy? Well, there's a little extra cryptographic magic for that *blind signature*.



Source: Haseeb Qureshi; https://nakamoto.com/the-cypherpunks/

Chaum's eCash

- Chaum's eCash was a major leap forward in digital currencies, but in 1998, the company founded on eCash (DigiCash) went bankrupt.
- It lost out in user adoption against credit cards and other systems like PayPal.
- The cypherpunks saw this failure and realized that eCash had another weakness that had previously gone underappreciated.
- **It relied on a single company. If digital cash were to flourish, it must grow beyond dependence on any central party.**

https://chaum.com/ecash/

Source: Haseeb Qureshi; https://nakamoto.com/the-cypherpunks/

Other Attempts: e-gold

- Founded in 1996, e-gold was one of the first dotcom companies to create a digital currency, two years before PayPal.
- e-gold issued a digital currency backed by gold reserves that anyone could hold and transfer. At its height, e-gold processed more than $2B in transfers a year.
- It was immensely popular, but because it had few sign-up restrictions, the currency was widely co-opted by hackers, scammers, and organized cybercriminals

https://en.bitcoinwiki.org/wiki/E-gold

Source: Haseeb Qureshi; https://nakamoto.com/the-cypherpunks/

Other Attempts: e-gold

- The US government took notice. After a lengthy court case, a court ruled e-gold guilty of money laundering and retroactive violations of money transmitter laws.
- The founder was found criminally liable, and in 2008, all e-gold balances were frozen. Over the next five years, the US government would manage redemptions of all e-gold account holders.
- To the cypherpunks, e-gold demonstrated yet another important lesson: ***regulators did not want digital cash to exist***.

https://en.bitcoinwiki.org/wiki/E-gold

Source: Haseeb Qureshi; https://nakamoto.com/the-cypherpunks/

The problem with collateral

- While e-gold was collateralized with gold, DigiCash was collateralized with US dollars.
- But both ultimately fell within the purview of the state. If you wanted to create a currency that was beyond state control, it seemed that every form of collateral came with a centralization chokepoint.
- The cypherpunks explored several schemes for non-collateralized digital currencies.
- Two of the most important schemes were b-money, described by Wei Dai in 1998, and BitGold, described by Nick Szabo in 2005.
- Both schemes were designed by prominent cypherpunks and were strikingly similar to Bitcoin, but they were both missing key ingredients.

Source: Haseeb Qureshi; https://nakamoto.com/the-cypherpunks/

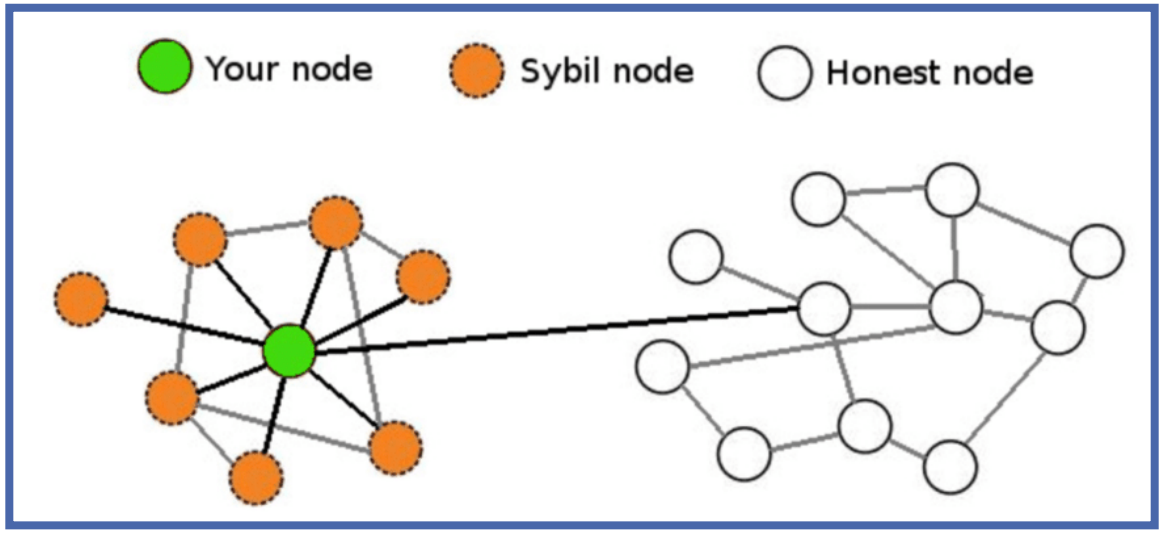
BitGold and b-money

- B-money and BitGold, like Bitcoin, use public key cryptography for identity.
- Both b-money and BitGold use proof-of-work to mint new coins. Bitcoin also uses proof-of-work to update the blockchain and append transactions.
- B-money and BitGold each use trusted timestamping servers for transaction ordering. Bitcoin implements a decentralized timestamping server via the "longest chain rule," as we'll discuss later.
- B-Money and BitGold achieved consensus by counting the ***total nodes*** in the network and letting the nodes vote. Bitcoin achieves consensus by counting the total work performed in the network.

Source: Haseeb Qureshi; https://nakamoto.com/the-cypherpunks/

BitGold and b-money - Sybil Attack

- B-Money and BitGold were ultimately both vulnerable to sybil attacks.
- A sybil attack is when a malicious user cheaply spins up many new "sybils" or identities, such as via a botnet.
- If the system has a simple majority vote rule, a dishonest attacker can easily overwhelm the system and determine the outcome of a vote.
- **Any robust decentralized currency must be resistant to sybil attacks.**



https://coincentral.com/sybil-attack-blockchain/

Source: Haseeb Qureshi; https://nakamoto.com/the-cypherpunks/

B-money, BitGold and Bitcoin

- At the end of the day, b-money and BitGold were only described in blog posts, so they were relatively underspecified.
- But these two designs would ultimately influence the digital currency that would see the light of day—Bitcoin.
- It was ultimately the cypherpunks who laid all the groundwork for the creation of something like Bitcoin.

https://vegaxholdings.medium.com/digital-currencies-ab7e5af697e5

Source: Haseeb Qureshi; https://nakamoto.com/the-cypherpunks/

Bitcoin History

Source: ColdFusion https://www.youtube.com/watch?v=W15A7Lf0_fI

Simple Mechanics of Digital / Crypto Currencies

Image by WorldSpectrum from Pixabay

Many of the slides were taken and adapted from the course on Bitcoin and Cryptocurrency Technologies: http://bitcoinbook.cs.princeton.edu/
with due credit to the original authors and thanking them for their generosity in sharing their slides

CBS

GoofyCoin

Goofy can create new coins

signed by sk_{Goofy}

CreateCoin [uniqueCoinID]

Note that sk_Goofy is private key of Goofy

A coin's owner can spend it.

signed by sk_{Goofy}

Pay to pk_{Alice} : H( )

signed by sk_{Goofy}

CreateCoin [uniqueCoinID]

Note that sk_ is private key

The recipient can pass on the coin again.

signed by sk_{Alice}

Pay to pk_{Bob} : H( )

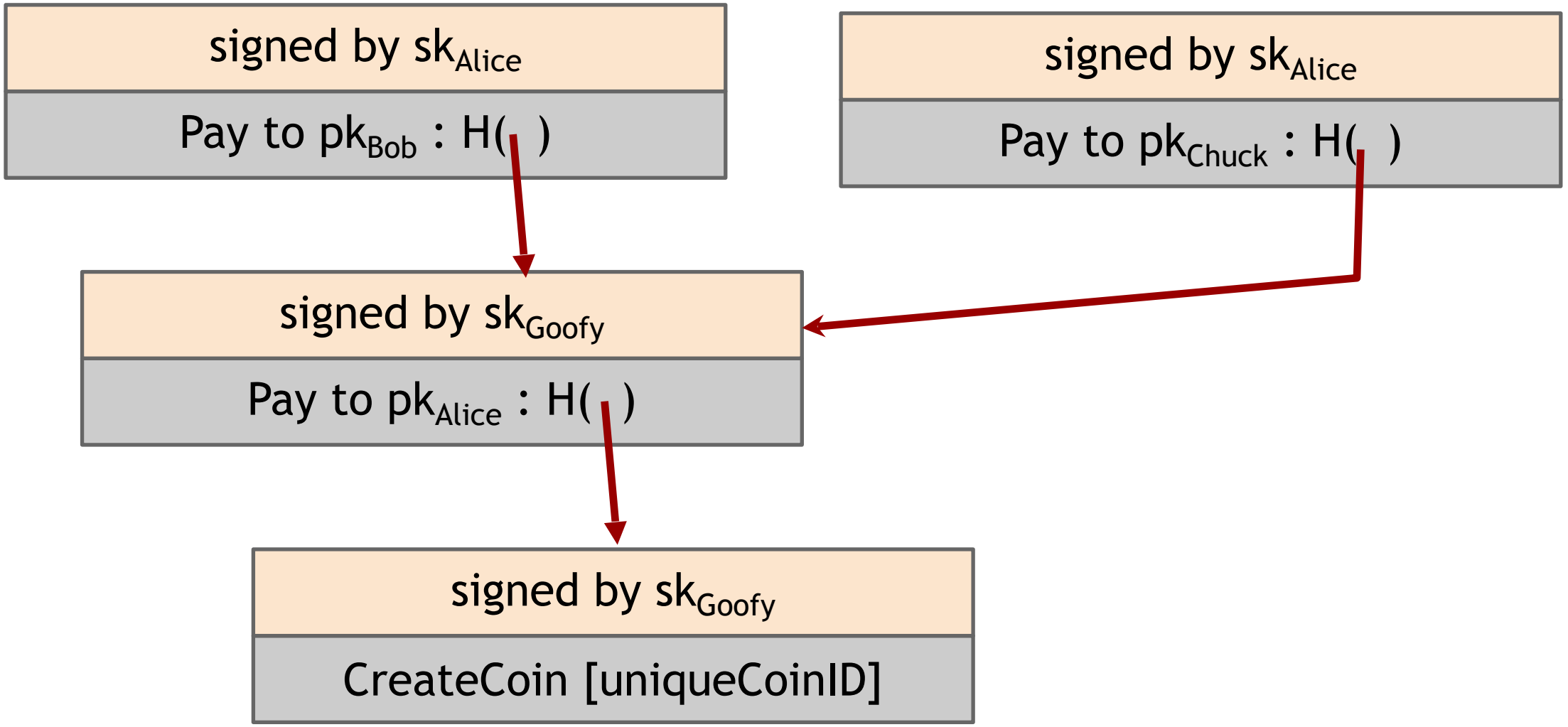
signed by sk_{Goofy}

Pay to pk_{Alice} : H( )

signed by sk_{Goofy}

CreateCoin [uniqueCoinID]

double-spending attack



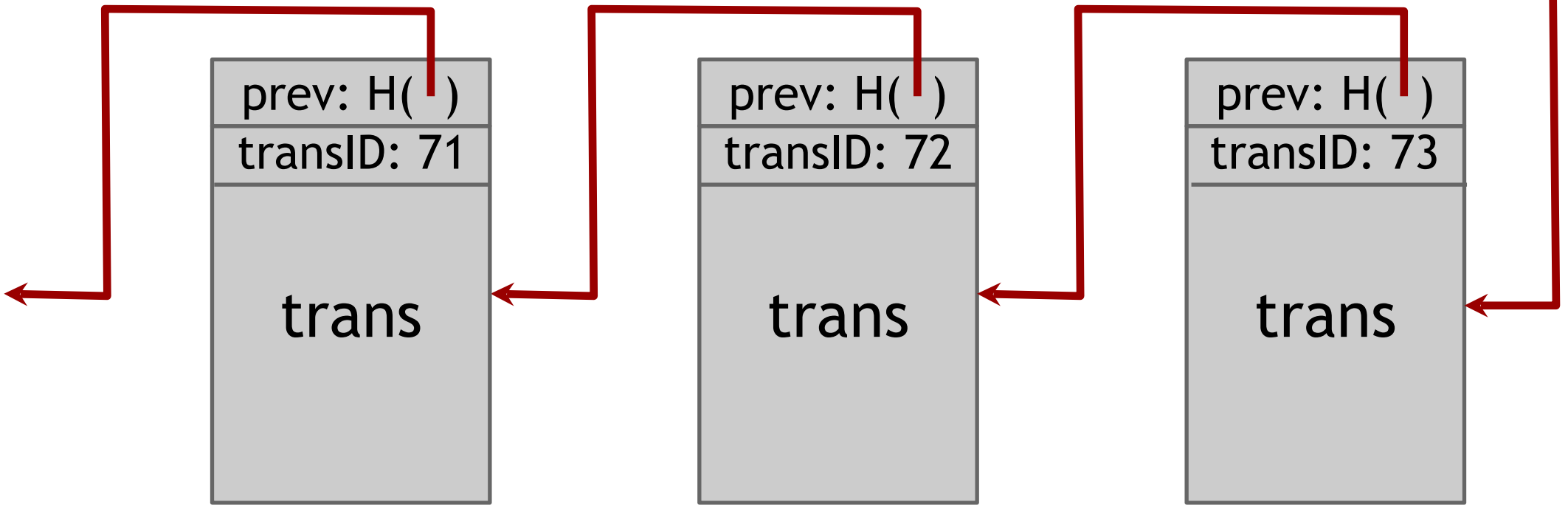
double-spending attack

the main design challenge in digital currency

ScroogeCoin

Scrooge publishes a history of all transactions
(a block chain, signed by Scrooge)

H( )



optimization: put multiple transactions in the same block

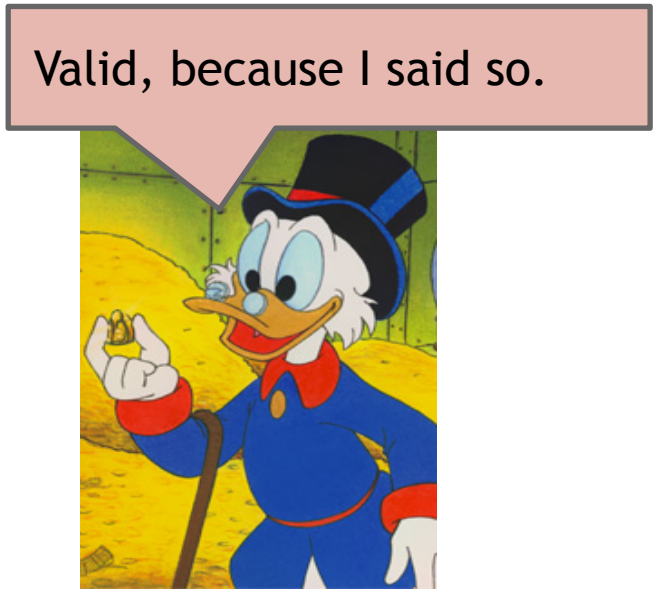
CreateCoins transaction creates new coins

transID: 73	type:CreateCoins	
coins created		
num	*value*	*recipient*
0	3.2	0x...
1	1.4	0x...
2	7.1	0x...

coinID 73(0)

coinID 73(1)

coinID 73(2)



PayCoins transaction consumes (and destroys) some coins, and creates new coins of the same total value

transID: 75 type:PayCoins

consumed coinIDs:
68(1), 42(0), 73(2)

coins created

num	*value*	*recipient*
0	2.5	0x...
1	0.6	0x...
2	6.4	0x...

signatures

Valid if:
-- consumed coins valid,
-- not already consumed,
-- total value out = total value in, and
-- signed by owners of all consumed coins

Immutable coins

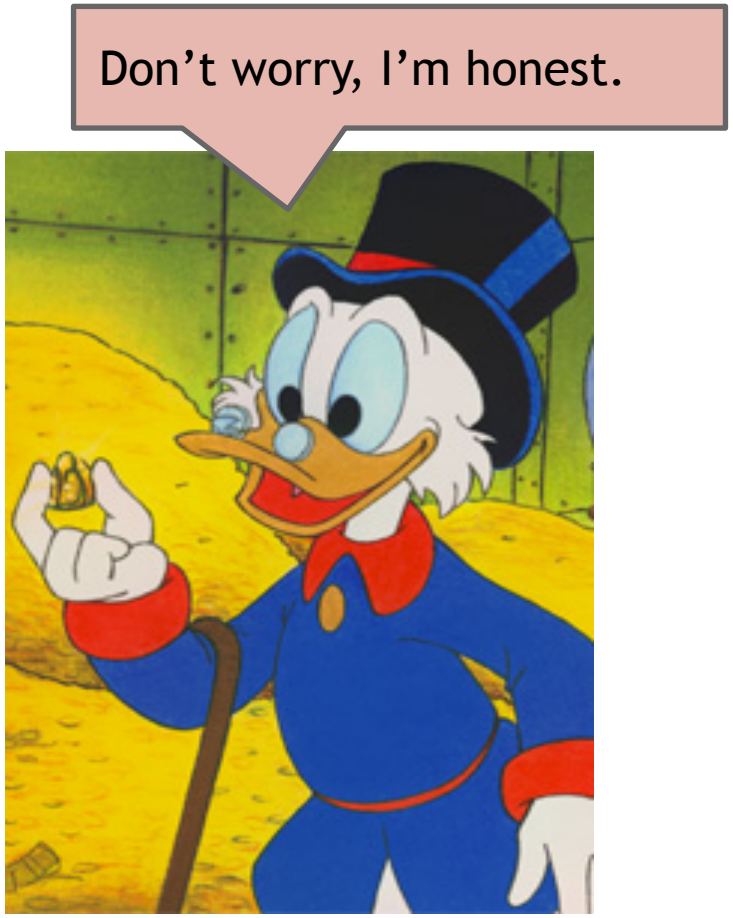
Coins can’t be transferred, subdivided, or combined.

But: you can get the same effect by using transactions

to subdivide: create new trans

consume your coin

pay out two new coins to yourself



Crucial question:

Can we descroogify the currency, and operate without any central, trusted party?

Thank you!

Raghava Mukkamala

rrm.digi@cbs.dk

https://www.cbs.dk/staff/rrmdigi

https://raghavamukkamala.github.io/

https://cbsbda.github.io/