Digital Gold Institute

# Bitcoin and Blockchain Technology

## Bitcoin as Digital Gold

v2021.3.29

Comments, corrections, and questions: https://drive.google.com/file/d/1FpudunEQrBY8WLTSLzwThOoFxMKGTCho

# Understanding Lags Well Behind The Hype

*"Understanding of the technology however lags well behind the hype, amongst practitioners, policy makers and industry commentators alike. 'Blockchain' technology seems to promise major change for capital markets and other financial services – some say it may ultimately prove to be as important an innovation as the internet itself – but few can say exactly how or why."*

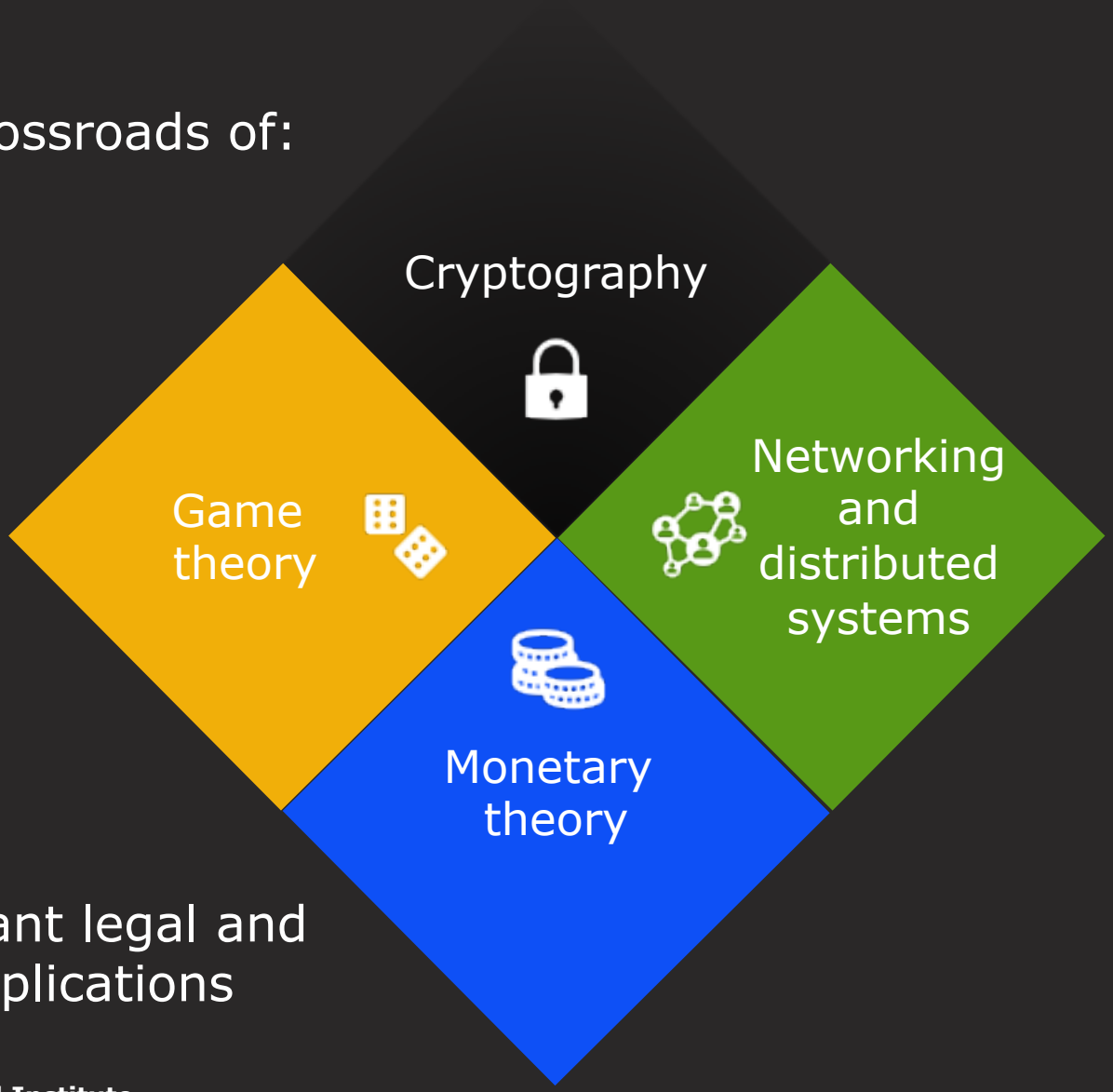
***Michael Mainelli, Alistair Milne*** *(2016)*

*The Impact and Potential of Blockchain on the Securities Transaction Lifecycle*

http://ssrn.com/abstract=2777404

# Bitcoin is Hard to Understand

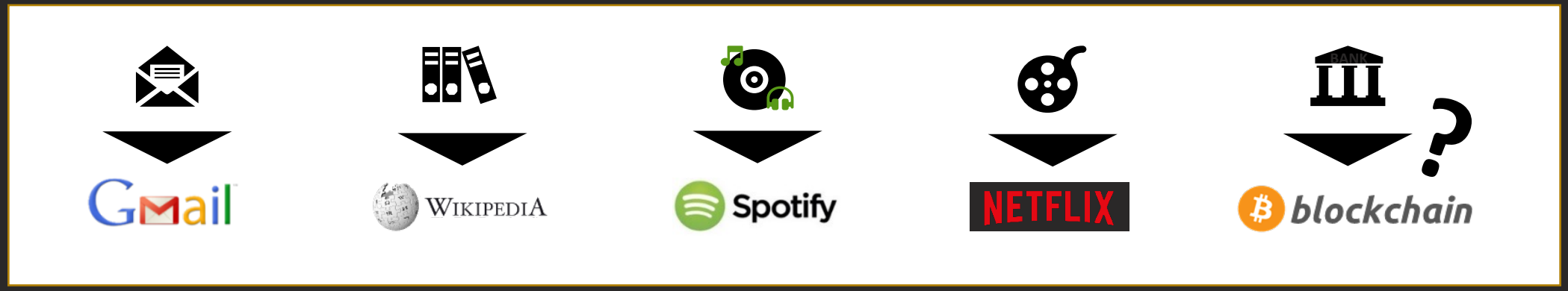
At the crossroads of:




*Mainly not a technology, a <u>cultural paradigm shift</u> instead*

With relevant legal and political implications

# The Information Economy




- Data is transferred with zero marginal cost
- Why pay a fee to move the few bytes representing wealth?
- Why only 9-5, Monday-Friday, two days settlement?
- Who (and when) will gift humanity with a global instantaneous free p2p payment network?

# Reliable Internet eCash Will Be Developed

*"The one thing that's missing, but that'll soon be developed, is a reliable eCash, a method whereby on the internet you can transfer funds from A to B,* ***without A knowing B or B knowing A****, the way I can take a 20 Dollar bill and hand it over to you"*

Milton Friedman, 1999

https://www.youtube.com/watch?v=ZoaXLzFhWIw

# Table of Contents

# Cash vs Electronic Money

## Cash

- Physical instance only: banknotes and coins
- Universal access: users are not identified or authorized
- Bearer asset: it cannot be recovered if lost
- Privacy preserving
- Usually issued by a central bank

## Electronic Money

- Purely digital
- Identified eligible users: *Know-Your-Customers* (KYC)
- If credentials are lost, money can usually be recovered
- Traced for *Anti Money Laundering* (AML) and *Contrast to Terrorism Financing* (CTF)
- Issued by both central and non-central banks

# Cashless Society

- Ban cash in favor of electronic money
- Recently and frequently proposed to contrast the crime that uses cash
- Pervasive controls would be dangerous when used by illiberal governments: cash defends privacy
- Cash stands in the way of the State Leviathan protecting citizens from
  - fiscal aggression
  - confiscation of wealth via negative interest rates

# Central Bank Money

- Only selected financial institutions have access to electronic central bank money in the form of central bank accounts
- Everybody else has access only to non-electronic central bank money in the tangible form of cash
- A bank account balance is not central bank money: just the promise of a private company that the account owner will be able to redeem the balance for central bank money
- Not even true, if everybody wants to redeem their amounts at the same time (*bank run*)

# Central Bank Digital Currency? 1/3

*"[… it would be] appealing […] it would mean people have direct access to the ultimate risk-free asset [...] it could exacerbate liquidity risk by lowering the frictions involved in running to central bank money [...] it could fundamentally and perhaps abruptly re-shape banking"*

Mark Carney, Governor of the Bank of England, June 2016

http://www.bankofengland.co.uk/publications/Documents/speeches/2016/speech914.pdf

# Central Bank Digital Currency? 2/3

*"Allowing the public to hold claims on the central bank might make their liquid assets safer, because a central bank cannot become insolvent. This is a feature which will become relevant especially in times of crisis – when there will be a strong incentive for money holders to switch bank deposits into the official digital currency simply at the push of a button. But what might be a boon for savers in search of safety might be a bane for banks, as this makes a bank run potentially even easier"*

Jens Weidmann, President of Bundesbank, June 2017

https://www.ft.com/content/414072b7-0de5-3864-9493-14438eab30ae

# eCash: Goals, Security, and Guarantees

- Reduce the cost of managing physical cash
- Allow fast effective electronic transactions
- Central bank issuer
- Private issuer (backed by reserve asset)
- Entrance/exit gateway (electronic money ←→ digital cash) monitored with KYC and AML processes
- Electronic trails for investigators
- Issuer/admin able to confiscate eCash if needed/required

# eCash: A Proof of Concept

- Bitcoin core codebase
- Mining, i.e. transaction finalization, reserved to vetted nodes (e.g. block signing from Elements)
- Thousands transactions per second
- Apps: wallets (iOS, Android, Desktop), blockexplorer, issuer dashboard

# eCash: Regulators' Feedback

Transactions must be attributed to known customers → electronic money, not eCash

Allowed applications must be certified, i.e. closed network → client-server approach, not peer-to-peer

# Facebook and Libra/Diem

# Central Bank Digital Currency? 3/3

*"It doesn't only matter how central bank money is created, but also to whom it is issued.*

*From today's perspective, there are no clear benefits from allowing the general public to hold digital central bank reserves, in particular in economies where demand for cash remains robust, such as in the euro area. This assessment includes considerations related to the potential impact of central bank digital currencies on financial structures in general, and the stability of bank deposits in particular."*

Benoît Cœuré, ECB Executive Board, May 2018

https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp180514_4.en.html

# Facebook's Libra is a threat to national sovereignty

*"Financial innovation must respect the monetary sovereignty of states, which cannot be shared with private interests."*

Bruno Le Maire, France's economy and finance minister, October 2019

https://on.ft.com/30zuKxH

# Central bankers believe digital cash could be a useful addition to their toolbox

*"CBDC would ensure that, as our economies go digital, the general public would retain access to the safest form of money, a claim on a central bank which can never go bust. A CBDC would be a kind of digital banknote and, as such, could satisfy more use cases than paper while the issuer, being a central bank, could support liquidity, settlement finality and trust in the value of the currency."*

Benoît Cœuré, Head of BIS Innovation Hub, October 2020
https://www.bis.org/speeches/sp201021a.htm

# Digital Euro

*"In identifying the appropriate threshold, one would need to strike the right balance between unlocking the benefits of a digital euro as a means of payment and mitigating risks of disintermediation or even bank runs. As a yardstick, a threshold of €3,000 would be more than the amount of cash most citizens hold today and would be above the average monthly wage in most euro area countries."*

Fabio Panetta, ECB Executive Board, February 2021
https://www.ecb.europa.eu/press/key/date/2021/html/ecb.sp210210~a1665d3188.en.html

# The Likely Scapegoats

# Table of Contents


- Decentralized digital currency
- Not supported by any government or organization
- No need for trusted third party
- Not backed by any asset or reserve *(but Proof-of-Work)*
- Instantaneous peer-to-peer transactions
- Cryptographic security
- Synergic economic incentives
- Efficient low-cost banking for everybody everywhere

https://bitcoin.org/en/faq
http://www.coindesk.com/information/

4410c8d14ff9f87ceeed1d65cb58e7c7b2422b2d7529afc675208ce2ce09ed7d

| | | |
|---|---|---|
| 1PfceCKGraSPEvx6nfjw5ZCLLy8Ct23Qd5<br>1JCe8z4jJVNXSjohjM4i9Hh813dLCNx2Sy<br>1KKiEAkpnQR2FH5kpkGP6442ZDkd6ZdrRS<br>15NQthxeLSwMtEaXJFM7YUCf59LzmFjkeH<br>15K8LDNMqvcVyPk9oubtQ6yYtdGdpENPXq<br>1LKgn2jGzb18e4xR9EMtFtRoAtYdt3ayUP<br>19TRvmJ8QBETFDSYb9xvK6MueHtWjXfeDX<br>17u2yhkqA9sWNXr1cuU3DrUukTriApMWmW<br>1Q5YT4TU6skrLs2LdqDmRNpvFaQYT4iAis<br>18b3BfortqFEPHx8vRHVz3LJU7gBECuP51<br>1LbsYwDAgELE5Jt3hdGj7NzbfYAsrzq8yX<br>17gzF6ebz6Sv269jUEjnPfjR474FvphVzy<br>1LLu7rReMdLnWqZuZeim1v1Cav8aPdri25<br>14M5DJyPB9JUYcqMpd4htKvve3vSAUjJ8F<br>1PHFNNfsJ7rQBwRExvTM3D6t1Svx5mNLwv | → | 37XuVSEpWW4trkfmvWzegTHQt7BdktSKUs | 94,504.03465148 BTC |

**@ $10,683 per BTC**
**it moved $1B for a $7 fee**

94,504.03465148 BTC

| Summary | |
|---|---|
| Size | 13611 (bytes) |
| Weight | 54444 |
| Received Time | 2019-09-06 03:13:12 |

| Inputs and Outputs | |
|---|---|
| Total Input | 94,504.1 BTC |
| Total Output | 94,504.03465148 BTC |
| Fees | 0.06534852 BTC |

# The Bitcoin Announcement

From: Satoshi Nakamoto <satoshi <at> vistomail.com>
Subject: Bitcoin P2P e-cash paper
Newsgroups: gmane.comp.encryption.general (The Cryptography Mailing List)
Date: 2008-10-31 18:10:00 GMT

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party. The paper is available at: http://www.bitcoin.org/bitcoin.pdf

The main properties:

- Double-spending is prevented with a peer-to-peer network.
- No mint or other trusted parties.
- Participants can be anonymous.
- New coins are made from Hashcash style proof-of-work.
- The proof-of-work for new coin generation also powers the network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System
Abstract. A purely peer-to-peer version of electronic cash [...]

http://archive.today/2012.12.28-025845/http://article.gmane.org/gmane.comp.encryption.general/12588/

# Satoshi Nakamoto


- Worked on Bitcoin since 2007
- Published the paper in October 2008
- Released the code in January 2009
- Gradually reduced his involvement
- Stopped any interaction in mid-2010
- Unknown identity: pseudonymous person or group?
- He owns about 1M bitcoins, never spent

http://mag.newsweek.com/2014/03/14/bitcoin-satoshi-nakamoto.html

https://www.wired.com/2016/05/craig-wright-privately-proved-hes-bitcoins-creator/

http://www.bbc.com/news/technology-36168863

# Nakamoto's Political Motivations

- "*Yes, [we will not find a solution to political problems in cryptography,] but we can win a major battle in the arms race and gain a new territory of freedom for several years. Governments are good at cutting off the heads of a centrally controlled networks like Napster, but pure P2P networks like Gnutella and Tor seem to be holding their own*."
- "*[Bitcoin is] very attractive to the libertarian viewpoint if we can explain it properly. I'm better with code than with words though*."
- In the Bitcoin's transaction database, the first entry has a note by Nakamoto, using a peculiar newspaper headline: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"

# Nakamoto Timeline

- 2008-08-18 bitcoin.org registered
- 2008-10-31 Bitcoin paper published
  http://article.gmane.org/gmane.comp.encryption.general/12588/
- 2008-11-09 Bitcoin project registered at sourceforge.net
- 2009-01-03 Genesis block at 18:15:05 GMT
  https://blockstream.info/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
- 2009-01-09 Bitcoin v0.1 released and announced on the cryptography mailing list
  http://www.mail-archive.com/cryptography@metzdowd.com/msg10142.html
- 2009-01-12 First transaction (block 170) from Satoshi to Hal Finney
  https://blockstream.info/block/00000000d1145790a8694403d4063f323d499e655c83426834d4ce2f8dd4a2ee

THE TIMES

Max 5C, min -5C | Saturday January 3 2009 timesonline.co.uk No 69523 | £1.50

Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Start collecting tokens today Pullout Inside

Israel prepares to send tanks and troops into Gaza

Israel allowed foreigners to flee the Gaza Strip as it prepared for a ground offensive. At least 430 Palestinians were killed in a week of airstrikes News, page 3

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

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 £37billion 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.

The Bank of England revealed yesterday that, despite intense pressure, the banks curbed lending in the final quarter of last year and plan even tighter restrictions in the coming months. Its findings will alarm the Treasury.

The Bank is expected to take yet more aggressive action this week by cutting the base rate from its current level of 2 per cent. Doing so would reduce the cost of borrowing but have little effect on the availability of loans.

Whitehall sources said that ministers planned to "keep the banks on the hoil" but accepted that they need more help to restore lending levels. Formally, the Treasury plans to focus on state-backed guarantees to encourage private finance, but a number of interventions are on the table, including further injections of taxpayers' cash.

Under one option, a "bad bank" would be created to dispose of bad debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying" the mainstream banking system.

The idea would mirror the initial proposal by Henry Paulson, the US Treasury Secretary, to underpin the American banking system by buying

Continued on page 6, col 1
Leading article, page 2

99p

Pub chain cuts the price of a pint from £1.69 to 1989 levels

Business, page 47

Michael Sheen Frost, Nixon and me
Magazine

Working mums So that's how she does it
Body&Soul

Detox in style The best spas on the planet
Travel

Salmon Rushdie I Won't Marry Again
Pages 22, 23

Giant Killing? Guide to the FA Cup Third Round
Sport

# Source Code License

Bitcoin was released under the MIT license

- open source: cryptographic software's source code must be available to allows public inspection (absence of backdoor and security vulnerabilities)
- free software: the user the right to use, copy, modify, and redistribute the software

Instead, proprietary software is almost always close source and it only grants the right to use


- Decentralized: no central authority, no intermediaries
- Permissionless: no regulator
- Censorship resistant: no frozen funds
- Open-access: no discrimination, no amount limits, 24/7/365
- Free: negligible transaction costs
- Borderless: no geographic limits
- Transnational: no special country
- Cross-jurisdictional: no specific jurisdiction applies
- Secure: non-falsifiable, non-repudiable transactions
- Resilient: nothing has been able to stop it or break it

# Mt Gox Bankruptcy

- As of January 2014 Mt Gox (Magic The Gathering Online eXchange) was world's largest USD/Bitcoin exchange
- In February 2014 it filed for bankruptcy protection from creditors
- About 850,000 bitcoins belonging to customers and the company were missing and likely stolen, an amount valued at more than $450 million at the time
- Fraud or theft?

# Silk Road

- Online dark market, operated as a Tor hidden service
- Online users were able to buy illicit goods using bitcoins, while browsing it anonymously and securely without potential traffic monitoring

- Launched in Feb 2011, shut down in Oct 2013
- Ross William Ulbricht, alleged to be the owner of Silk Road has been sentenced to life in prison
- Other black markets have filled in as successors

# Bitcoin Used by Terrorists

Europol, January 2016:

*"Despite third party reporting suggesting the use of anonymous currencies like Bitcoin by terrorists to finance their activities, this has not been confirmed by law enforcement"*

https://www.europol.europa.eu/sites/default/files/publications/changes_in_modus_operandi_of_is_in_terrorist_attacks.pdf

# Money Laundering and Terrorism Financing (1/2)

UK HM Treasury, **October 2015**:
*"The money laundering risk associated with digital currencies is low, though if the use of digital currencies was to become more prevalent in the UK this risk could rise"*

UK HM Treasury, **October 2017**:
*"There remains little evidence of digital currencies being used as an established tool for money laundering, and the money laundering risk is therefore still assessed to be low. […] While digital currencies could in theory be used to facilitate and finance terrorist activity, the lack of evidence of this occurring and the greater attractiveness of other methods mean that digital currencies continue to be assessed as low risk for terrorist financing"*

Table 1.A: National risk assessment on money laundering

| National risk assessment on money laundering | | | | | | |
|---|---|---|---|---|---|---|
| Thematic area | Total vulnerabilities score | Total likelihood score | Structural risk | Structural risk level | Risk with mitigation grading | Overall risk level |
| Banks | 34 | 6 | 211 | High | 158 | High |
| Accountancy service providers | 14 | 9 | 120 | High | 90 | High |
| Legal service providers | 17 | 7 | 112 | High | 84 | High |
| Money service businesses | 18 | 7 | 119 | High | 71 | Medium |
| Trust or company service providers | 11 | 6 | 64 | Medium | 64 | Medium |
| Estate agents | 11 | 7 | 77 | Medium | 58 | Medium |
| High value dealers | 10 | 6 | 56 | Low | 42 | Low |
| Retail betting (unregulated gambling) | 10 | 5 | 48 | Low | 36 | Low |
| Casinos (regulated gambling) | 10 | 3 | 32 | Low | 24 | Low |
| Cash | 21 | 7 | 147 | High | 88 | High |
| New payment methods (e-money) | 10 | 6 | 60 | Medium | 45 | Medium |
| Digital currencies | 5 | 3 | 15 | Low | 11 | Low |

https://www.gov.uk/government/publications/uk-national-risk-assessment-of-money-laundering-and-terrorist-financing
https://www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2017

# Money Laundering and Terrorism Financing (2/2)

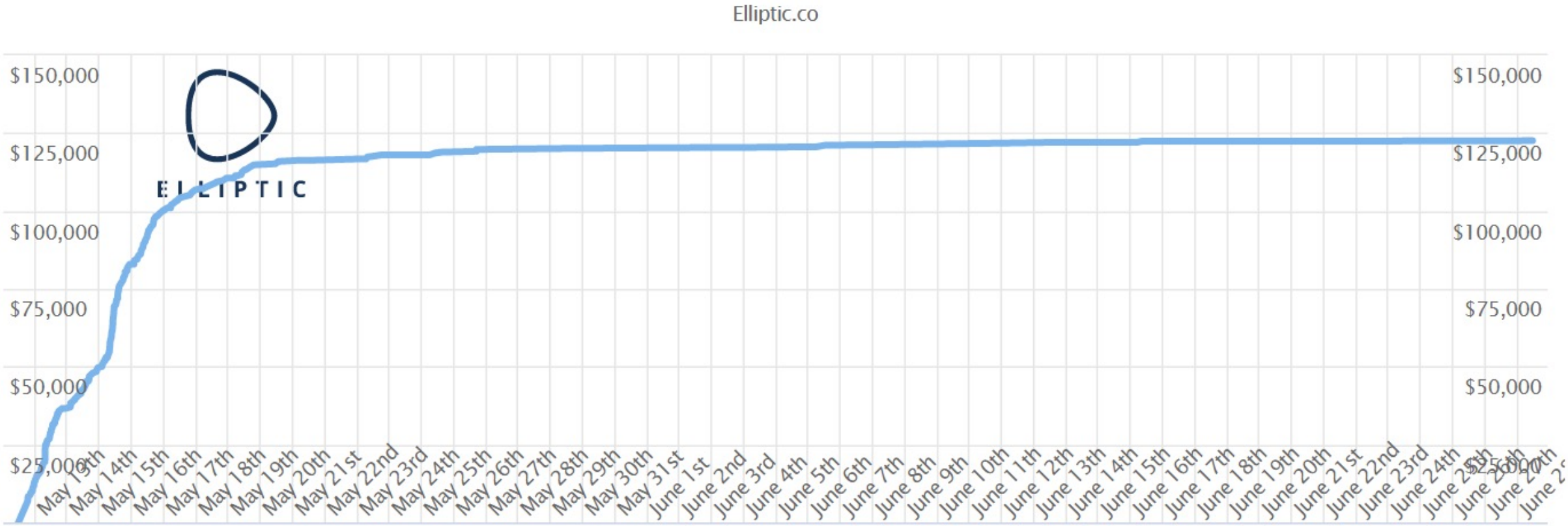
- The risk of money laundering through has increased
- The cryptoasset ecosystem **has developed, matured and expanded** considerably in the last 3 years
- Although cryptoassetys use by terrorists **is not widespread**
- The government's understanding of cryptoassets has developed considerably since 2017, improving understanding of the risks and respective mitigations. The inclusion of **cryptoasset exchange providers and custodian wallet** providers into the Money Laundering Regulations (MLRs) since January 2020 will **help to mitigate vulnerabilities in time**.

| Cryptoasset risk scores | | |
|---|---|---|
| | 2017 Risk Score | 2020 Risk Score |
| Money laundering | Low | Medium |
| Terrorist financing | Low | Medium |

# Ransomware

- A malware propagated via infected email attachments and botnets
- When activated, it encrypts files stored on local and mounted network drives
- Then it displays a message which offers to decrypt the data if a bitcoin payment is made

# Balance of WannaCry Ransomware (2017)



# Bitcoin Resilience

Is there anything else in financial world:

- Just 12 years old
- Without government or corporation backing
- Fraud/theft at its main reference exchange (Mt Gox)
- With such a bad reputation (Silk Road, Money Laundering, Terrorism, Ransomware)

That could be still alive and kicking?

# Table of Contents

# Bitcoin: A Protocol and a Currency

- **B**itcoin: protocol, software, and community
- **b**itcoin**s**: units of the currency

*bitcoins are sent using the Bitcoin protocol*

**bitcoins are the native digital asset intrinsic to the Bitcoin protocol**

# Bitcoin: The Protocol

- Public ledger of transactions
- Shared (i.e., distributed) with peer-to-peer technology
- Massively duplicated across computer network nodes
- Allowing ownership transfer of a native digital scriptural asset
- Its native “digital token” can be exchanged, but not duplicated
- Keeps records of every transaction forever

# Bitcoins: The Currency

- Only exist as public ledger documented transactions
- Are associated to public address(es) like

bc1qnehtvnd4fedkwjq6axfgsrxgllwne3k58rhdh0

It is mine; you are **REALLY** encouraged to tip

- the bitcoin distributed public ledger certifies for everybody how many bitcoins are associated to any address

https://blockstream.info/address/bc1qnehtvnd4fedkwjq6axfgsrxgllwne3k58rhdh0

formerly https://blockstream.info/address/1FEz167JCVgBvhJBahpzmrsTNewhiwgWVG

# Pseudonymity, Anonymity

Bitcoin is pseudonymous, not anonymous:

- The bitcoin address does not provide direct information about the actual bitcoin owner
- All transactions are transparent to everybody's inspection
- Perfect persistent public account history: the public ledger is forever

https://blockstream.info

http://blockexplorer.com/

# Asymmetric Cryptography: Public/Private Key Pair

Two mathematically linked keys perform opposite digital signature functions:

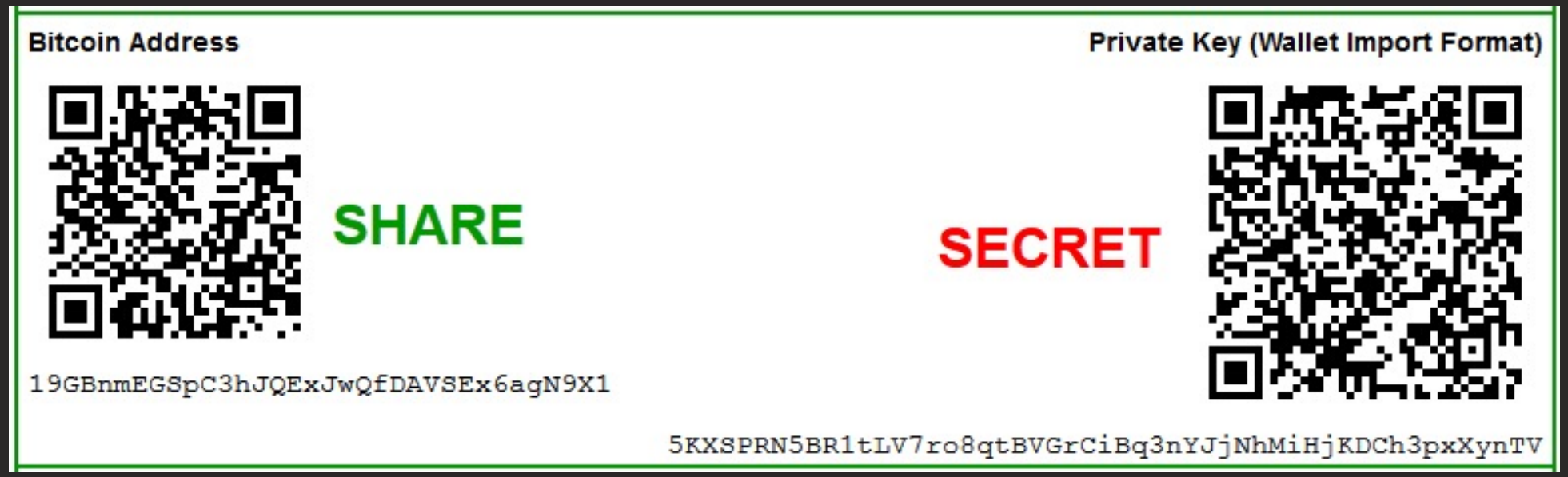
- The private (secret) key is used to generate digital signatures
- The public key is used by anyone to verify those signatures

- The public key derives from the private key, but the private key cannot be derived from the public one

- The bitcoin address is derived from the public key, but the public key cannot be derived from the address

# Asymmetric Cryptography: Public/Private Key Pair

- private key → public key → bitcoin address(es)
- the private key allows spending the bitcoin associated to the corresponding address(es)




https://www.bitaddress.org

# A Bitcoin Transaction: From Alice's Address to Bob's Address

- Transaction message: bitcoin amount to transfer + Bob's address (+ Alice's public key)
- Alice's private key digitally signs the transaction message
- The transaction message is broadcasted to the network
- With Alice's public key any network node can verify that:
  - The bitcoin amount is at Alice's address disposal
  - The digital signature is valid, i.e., the transaction message has not been tampered or modified (*integrity*)
  - The transaction has been signed by the private key associated to Alice's address (*authentication* and *non-repudiation*)
- The public ledger is updated with the new transaction
- Everybody knows Bob's address has received those bitcoins

# Transactions Cannot Be Altered, They Could Be Censored

- Transactions cannot be altered
- Bitcoins cannot be redirected
- Transactions could only be censored, preventing their registration on the public ledger, as if they never happened; anyway, this is hard to achieve

# Bitcoin Safe Custody

- Bitcoins are effectively owned by whoever can spend them
- i.e. whoever can access the private key needed to spend them
- Securing private keys is crucial for safe storage
- Software (and hardware) wallets can be used to manage keys and addresses:
  - Desktop client: Bitcoin Core, Electrum
  - Mobile client: Samurai Wallet (Android), Green (iOS / Android), BreadWallet (iOS), Bitcoin Wallet (Android), Copay (iOS / Android)
  - Hardware wallet: Trezor, Ledger
  - Cold storage: never exposed to Internet, stored away

# Table of Contents

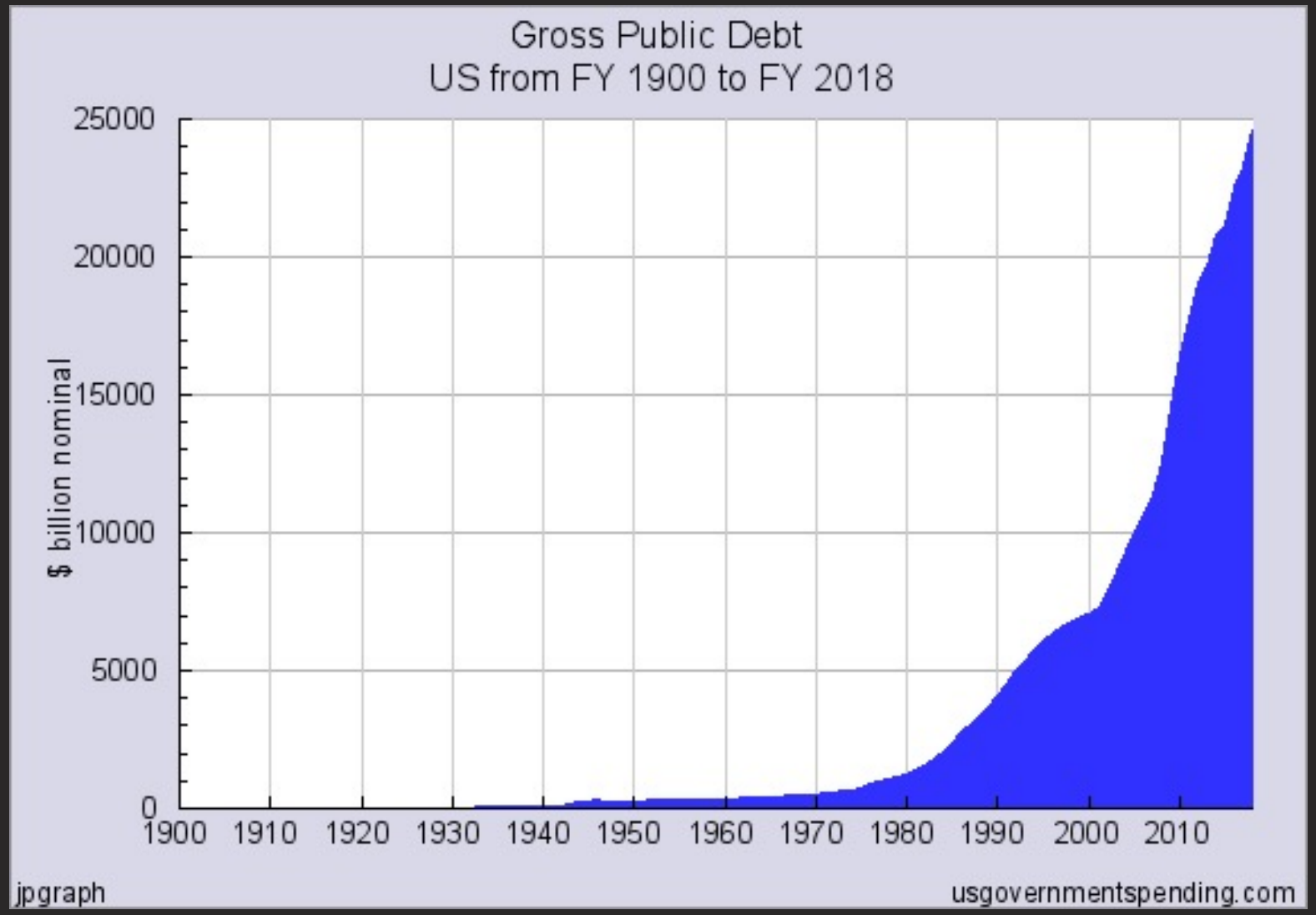
# Money As A Social Relation Instrument

- Human beings are born into a gift economy
- Enlarged relationship circle requires exchange economy
- Barter economy: coincidence of wants
- Trade economy: money as medium of exchange
- Global information economy: supranational digital money

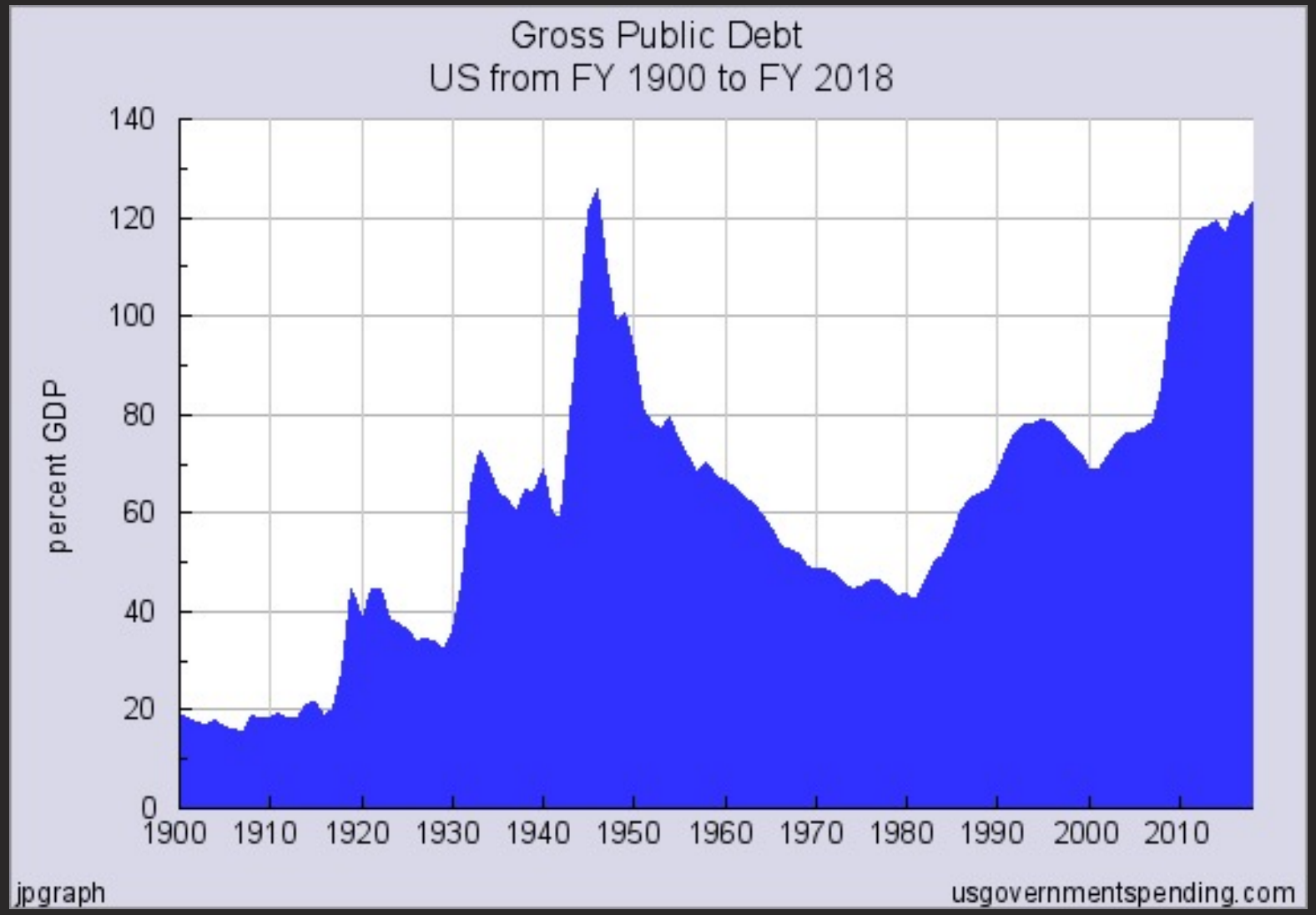
# Trade Economy:
# From Gold Standard to Fiat Money

- Gold: the commodity money standard
  - scarce
  - pleasant color, i.e. resistant to corrosion and oxidation
  - high malleability
  - relative easiness of its purity assessment
- Gold purity certification
- Representative money
- Fractional receipt money
- Fiat money and legal tender

# Gross US Public Debt



# Gross US Public Debt as GDP Percentage



# Properties of Money

1. Medium of exchange
2. Store of value
3. Unit of account

# Properties of Money:
# 1. Medium of Exchange

- Swappable and fungible
- Portable
- Divisible
- Easily recognizable and resistant to counterfeiting

# Money Comparison

| | Medium of Exchange | | |
|---|---|---|---|
| *Live cattle* |  | | |
| *Diamonds* |  | | |
| *Gold* |  | | |
| *Fiat coins and notes* |  | | |
| | | | |

- swappable
- fungible
- portable
- divisible
- recognizable
- resistant to counterfeiting

# Properties of Money:
# 2. Store of Value

- Reliably saved, stored, and retrieved
- Retain usefulness and storage properties over time
- Non-perishable and with low preservation cost

# Money Comparison

| | Medium of Exchange | Store of ~~Stable~~ Value | |
|---|---|---|---|
| *Live cattle* |  |  | |
| *Diamonds* |  |  | |
| *Gold* |  |  | |
| *Fiat coins and notes* |  |  | |
| | | | |

- swappable
- fungible
- portable
- divisible
- recognizable
- resistant to counterfeiting

- reliably saved, stored, and retrieved
- retain usefulness over time
- Maintain its storage properties
- non-perishable or with low preservation cost

# Properties of Money:
# 2. Store of ~~Stable~~ Value

Properties of money overlap to a certain degree, anyway

- The *stability* of the value of money **across time** does not pertain eminently to the *storage* property

- Instead, it pertains to the *unit of account* property

# Properties of Money:
# 3. Unit of Account

- Money is used as numeraire, i.e. relative worth unit of measure
- Money is the unit of account against which the value of every other good is measured
- The price system measures the value of goods relative to the value of money

*To best perform its role as unit of account, good money should have stable value (i.e. purchasing power) allowing for a reliable analysis of the price dynamic and homogeneous comparisons*

- Money supply must be controlled in some way

# Money Comparison

| | Medium of Exchange | Store of ~~Stable~~ Value | Unit of Account |
|---|---|---|---|
| *Live cattle* |  |  |  |
| *Diamonds* |  |  |  |
| *Gold* |  |  |  |
| *Fiat coins and notes* |  |  |  |
| | | | |

- swappable
- fungible
- portable
- divisible
- recognizable
- resistant to counterfeiting

- reliably saved, stored, and retrieved
- retain usefulness over time
- Maintain its storage properties
- non-perishable or with low preservation cost

- relative worth unit of measure
- stable value for stable price comparison
- supply must be controlled in some way

# Stable Prices: the *Holy Grail* of Monetary Research

- Gold standard, bimetallism, symmetallism
- Fixed value of bullion (Aneurin Williams 1892)
- Compensated dollar (1911-20 Irving Fisher)
- Commodity Reserve Currency (1932 J. Goudriaan, 1937-44 B. Graham, 1942 F. Graham, 1951 M. Friedman)
- ANCAP basket (1982 Robert Hall)
- Futures contracts (1984 Miles, 1989-95 Sumner)
- Quasi-futures contract (1994 Kevin Dowd)
- Price index option (2000 Kevin Dowd)
- Ideal Money (John Nash, 2002-2015)

# John Nash: Ideal Money

*Although money itself is merely an artifact of practical usefulness in human societies and/or civilizations, there are some traditional or popular views associating money with sin or immorality or unethical or unjust behavior. And such views can have the effect that an* ***ideal of good money*** *does not seem such a good cause* ***as an ideal of a good public water supply****.*

*[…]*

*If viewed scientifically and rationally (which is psychologically difficult!),* ***money should have the function of a standard of measurement and thus that it should become comparable to the watt or the hour or a degree of temperature***
*[…]*

*"Ideal Money" […] would be* ***intrinsically free of "inflationary decadence"*** *similarly to how money would be free from that on a true "gold standard", but the proposed basis for that [is not necessarily] the proposal of a linkage to gold.*

http://personal.psu.edu/gjb6/nash/money.pdf
https://www.youtube.com/watch?v=Je22xKQekCk
https://www.youtube.com/watch?v=ZO7aDojl6f0
https://www.mediatheque.lindau-nobel.org/videos/31344/ideal-money-and-the-motivation-of-savings-and-thrift-2011/laureate-nash-jr

# Take Money out of the Hands of Government

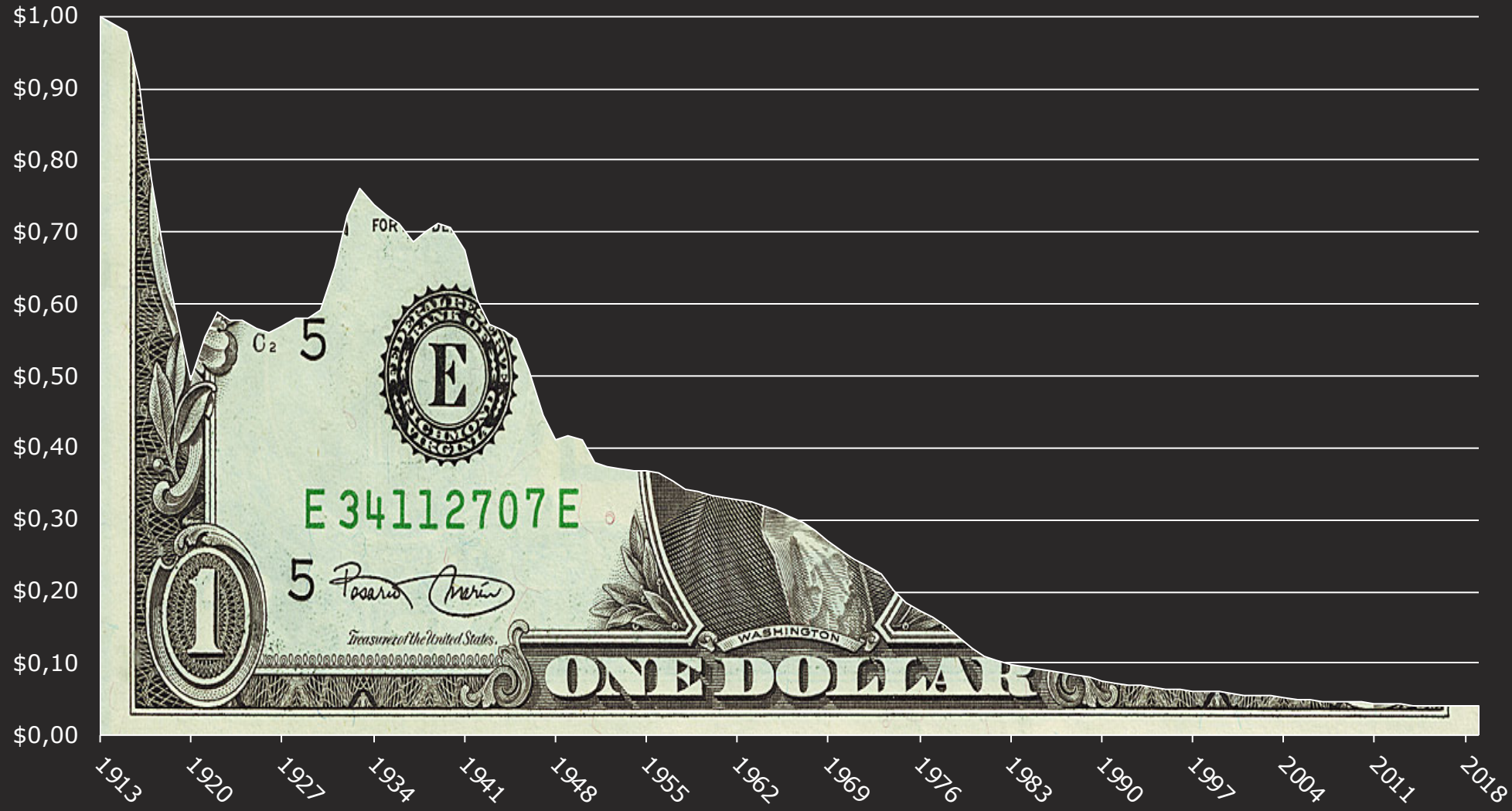
*"I don't believe we shall ever have a good money again before we take the thing out of the hands of government, that is, we can't take them violently out of the hands of government, all we can do is by some sly roundabout way introduce something that they can't stop"*

F. A. Hayek

https://youtu.be/EYhEDxFwFRU?t=19m23s

# Hyperinflation

# USD has lost 96% of its Purchasing Power since Federal Reserve establishment in 1913



# Inflation as Hidden Tax

Over 20 years, the planned inflation rate of 2% per year is

- the confiscation of 33% of the purchasing power of all savings
- the reduction of 33% of the value of all debts

No surprise that the most debt addicted economic agent, the State, does not like ideal inflation-free money

# John Nash: 'Keynesians'

*So let us define "Keynesian" to be descriptive of a "school of thought" that originated at the time of the devaluations of the pound and the dollar in the early 30's of the 20th century. Then, more specifically,* ***a "Keynesian" would favor the existence of a "manipulative" state establishment of central bank and treasury which would continuously seek to achieve "economic welfare" objectives with comparatively little regard for the long term reputation of the national currency*** *and the associated effects of that on the reputation of financial enterprises domestic to the state. And indeed a very famous saying of Keynes was "...in the long run we will all be dead ...".*

# Friedrich August Hayek "*Denationalisation of Money*"

- history of coinage is an almost uninterrupted story of debasements; history is largely a history of inflation engineered by governments for their gain
- why government monopoly of the provision of money is regarded as indispensable? It deprived public of the opportunity to discover and use a better reliable money

*"Blessed will be the day when it will no longer be from the benevolence of the government that we expect good money but from the regard of the banks for their own interest"*

A Free-Market Monetary System, Gold and Monetary Conference, New Orleans, Nov. 1977, https://mises.org/daily/3204

Denationalisation of Money, The Institute of Economic Affairs, http://www.mises.org/books/denationalisation.pdf

# Permissionless Innovation: Gentle and Effective

Permissionless innovation:

- no centralized security mechanism
- no barrier to enter
- no editorial control

- Email has not been designed by a consortium of postal agencies
- Internet has not been developed by a consortium of telecommunication companies
- Will a new money and its decentralized transactional network be designed by a consortium of banks?

# Table of Contents

# Private Monies

- A medium of exchange or payment
  - issued by a non-governmental body
  - without legal privileges
- A private money does not have to be universally acceptable; it is enough that it is accepted in an economic community
- Public demand for private currencies:
  - hold them in the expectation that they will not diminish in purchasing power as state money has
  - wish to be part of a movement against increasing state control of economic and personal behavior
  - conduct illegal activity
  - just want better money

# Austrian School of Economics Meets The Cypherpunk Movement

*"Privacy in an open society also requires cryptography […] We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence. […] We must defend our own privacy if we expect to have any. […] We are defending our privacy with cryptography, […] with digital signatures, and with electronic money"*

Eric Hughes, A Cypherpunk's Manifesto

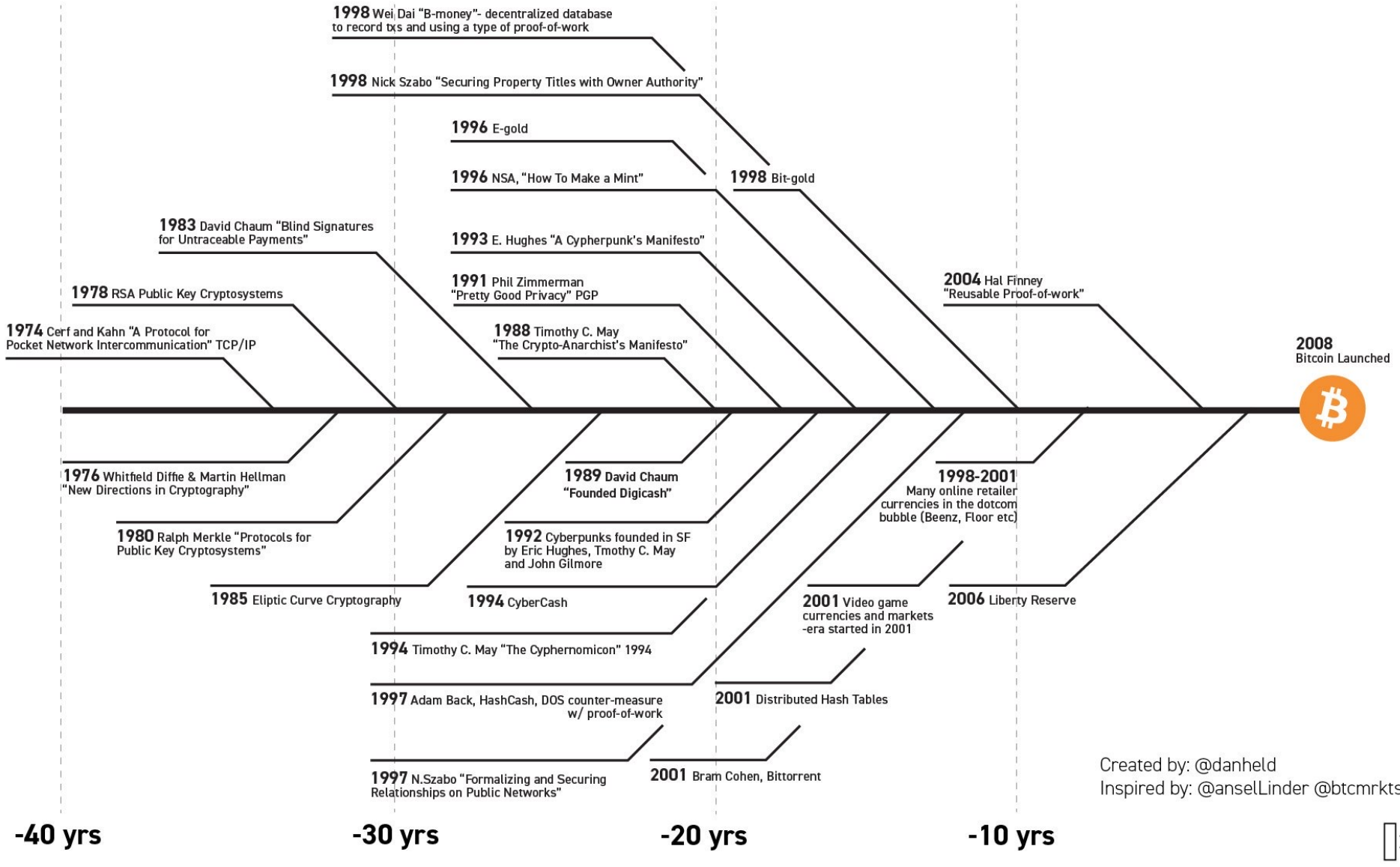
https://www.activism.net/cypherpunk/manifesto.html

Cryptography is the slingshot that David, the little man, can use to kill Goliath, the dystopian Big Brother

# Bitcoin Precursors

- eCash, David Chaum, 1982 (blind signature)
- Hashcash, Adam Back, 1997 (Proof-of-Work)
- B-money, Wei Dau, 1998 (distributed database)
- Bit gold, Nick Szabo, 1998 (distributed database, sequential money creation)
- Anonymous Electronic Cash, Tomas Sander and Amnon Ta-Shma, 1999 (anonymity)
- Reusable Proof-of-Work, Hal Finney, 2004

# Bitcoin prehistory - It's the result of 40 years of research, development and demand



# Liberty Dollar: 1998-2009

- Private mint that issued gold and silver coins; also issued notes redeemable in precious metals
- Periodically revalued against USD: the value of the latter fell over time against precious metals
- Specifically designed to function in parallel with and in competition to USD
- Never marketed or represented as official US currency
- Highly successful: second most popular currency in the US
- Its use declared a federal crime by the US government
- Its founders convicted for counterfeiting, fraud and conspiracy against the United States

# E-gold: 1996-2007

- Digital payment system with gold as unit of account
- User accounts backed by gold reserves
- By 2005, e-gold was second only to PayPal in the online payments industry: 1.2M accounts and $1.5B transactions
- Indicted in April 2007 by US law enforcement services
- Charges: unlicensed money-transmitting entity and a means of moving the proceeds of illegal activities
- Never proven and even the judge expressed major doubts
- 'Offshore' payment system rather than a money transmitter or bank as defined under then-existing regulations, not least because gold was not legally 'money'

# The Centralization Dilemma

- To remove the weakness of a central point of failure, distributed technologies seemed promising (e.g., BitTorrent)
- In digital cash schemes, a digital token, being just a file that can be duplicated, can be spent twice
- A centralized trusted party has always been required to prevent ***double spending***

# Table of Contents

# Double Spending Problem

- To securely transfer value using digital means has been possible for decades
- In digital cash schemes, a single digital token, being just a file that can be duplicated, can be spent twice
- How can we forbid Alice from spending the same bitcoins a second time to Carol's address? Which transaction should be valid: the one to Bob's address or Carol's address?
- A centralized trusted party has always been required to prevent ***double spending***

# Bitcoin Network: A Distributed Back-office

- All computer network nodes validate and clear all transactions
- Those nodes also providing the additional computational power required for transaction settlement are called **miners**

- Without a central trusted party, how do nodes reach *distributed consensus* on the transaction history?

- Consensus in a distributed asynchronous network with faulty (or malicious) nodes is a very hard problem: Computer Science even provides impossibility results

# *Gedankenexperiment* (Thought Experiment)

- Room full of people (*nodes*) that can only talk one-to-one (*asynchronous network*)
- Try to reach (*distributed*) consensus about the smaller possible bit of information: a logical variable TRUE/FALSE
- Assume at least one person is severely hear-impaired (*faulty*) or deceptively untrustworthy (*malicious*)

*(Distributed) consensus in asynchronous network is impossible*

# The Byzantine Generals' Problem

- Generals must decide unanimously whether to attack
- They can communicate using messengers, but cannot have a summit

- There are traitors amongst them

- Success (i.e. fault tolerance) is achieved if the loyal generals agree on their strategy, whatever it might be

# Bitcoin's Public Ledger: A Chain of Blocks

- Transactions are bundled in blocks (one block about every 10 minutes) and sequentially chained
- **The cryptographic link between blocks requires computing power to be created**
- A block is valid only if it includes valid transactions

# Mining

- Miners compete to finalize (settle) a new block of transactions
- The winner providing the *proof-of-work* of having finalized a new block is rewarded with **the issuance of new bitcoins** in a special *coinbase* transaction included in that same block
- Miners solve the double spending problem:
  - a double spending transaction would invalidate the block
  - an invalid block would be rejected from the network
  - the bitcoin reward would be removed from transaction history
  - the winning miner would have wasted his work
- **Miners have an economic incentive to be honest**

# Hash Function

- A function that maps input data of arbitrary size to an output set of hash values, i.e. output data of a fixed size
- Bitcoin uses the (Secure Hash Algorithm) SHA256 that generates a fixed size 256-bit (32-byte) output
- Small differences in the input data produce large differences in the result

```
SHA256("Hello, world!") =
315f5bdb76d078c43b8ac0064e4a0164612b1fce77c869345bfc94c75894edd3

SHA256("Hello, world.") =
f8c3bf62a9aa3e6fc1619c250e48abe7519373d3edf41be62eb5dc45199af2ef
```

- *Non-invertible*: input data cannot be recovered from the output

# Hash Puzzle: Hash Value Below Target

- Find a suffix for “Hello, world!” that results in four leading zeros

SHA256(“Hello, world!”) =
**315f**5bdb76d078c43b8ac0064e4a0164612b1fce77c869345bfc94c75894edd3

SHA256(“Hello, world!0”) =
**1312**af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64

SHA256(“Hello, world!1”) =
**e9af**c424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8

……

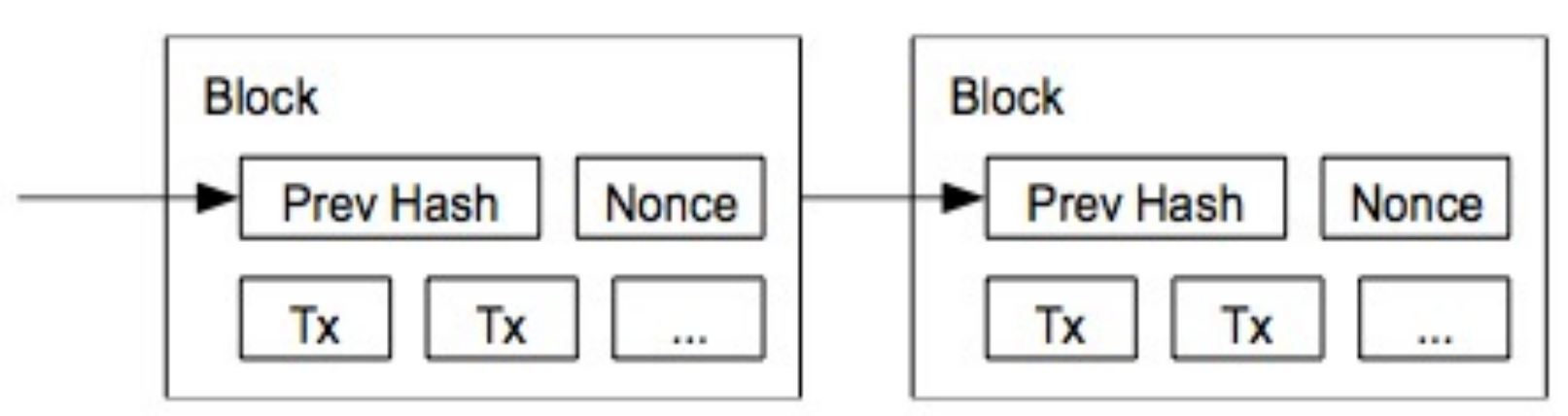
SHA256(“Hello, world!4249”) =
**c004**190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6

SHA256(“Hello, world!4250”) =
**0000**c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9

- Hash function being non-invertible, brute-force is the only approach
- The lower the target threshold, the higher the problem difficulty

# Proof-of-Work

- For a given block of transactions, find a *nonce* such that:
  SHA256(previous block hash, transactions, nonce) <= target




- The nonce provides the *proof of* [SHA256 hash] *work* having been performed
- The longer chain (more precisely, the one with more work) is the consensus chain

# A Tamper-Resistant Ledger

- No ledger can really be *immutable*
- A hash chain of block is *tamper-evident*: changing something in a block change its hash value, requiring alteration of the following block (that includes that hash value), in a cascading effect all way to the last block
- To finalize a block, work is required
- Because of the *proof-of-work*, the chain becomes *tamper-resistant*: the chances of a block being altered decrease exponentially with the number of blocks chained after it
- The chain of blocks is a history of transactions resilient to network attackers because it cannot be altered without huge resources

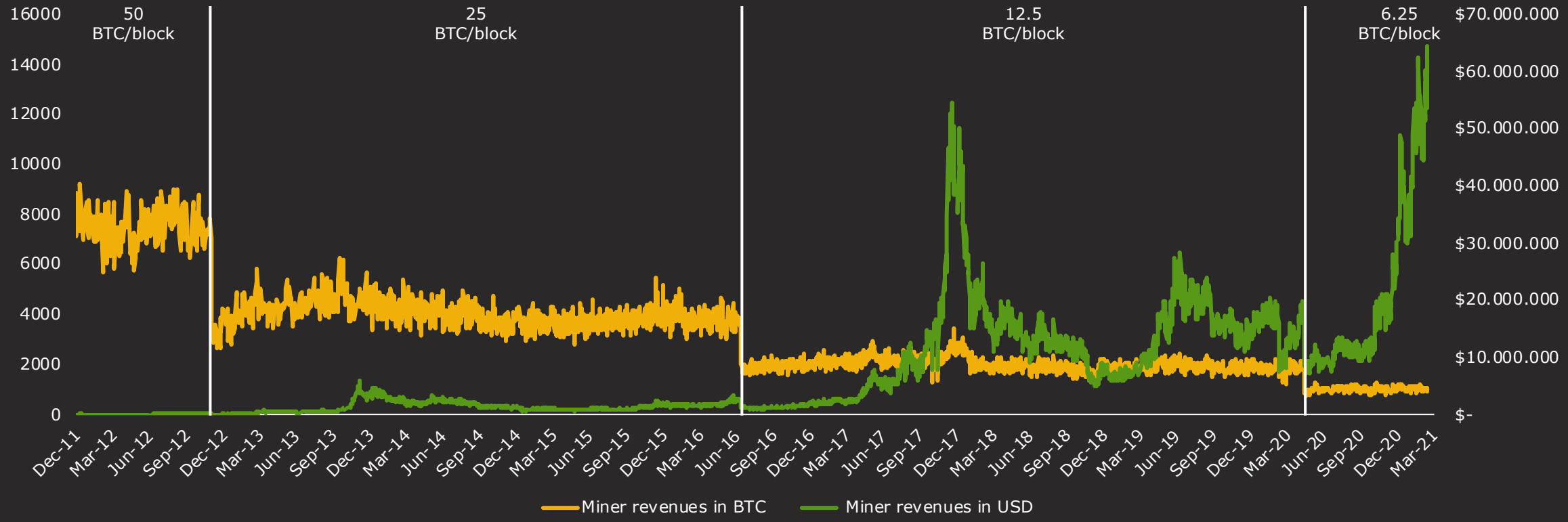
# Nakamoto Distributed Consensus

Practical Byzantine Fault Tolerant (PBFT) *distributed consensus* is achieved using *(game theory) economic incentives* for the mining nodes to be honest

- Double spending is solved without a central trusted party
- Bitcoin can resist attacks of malicious agents, if they do not control network majority
- Miners are compensated for their proof-of-work using seigniorage revenues, i.e. issuance of new bitcoins
- Seigniorage revenues subsidize the network
- Seigniorage revenues covers the cost of distributed consensus

# Seigniorage Revenues Cover Consensus Cost

- Seigniorage revenues subsidize the network, making transactions cheap
- 144 block/day, 365 day/year, 6.25 BTC/block = 328,500 BTC/year
- About $5 billions in 2020, $16.5 billions with BTC/USD=$50,000



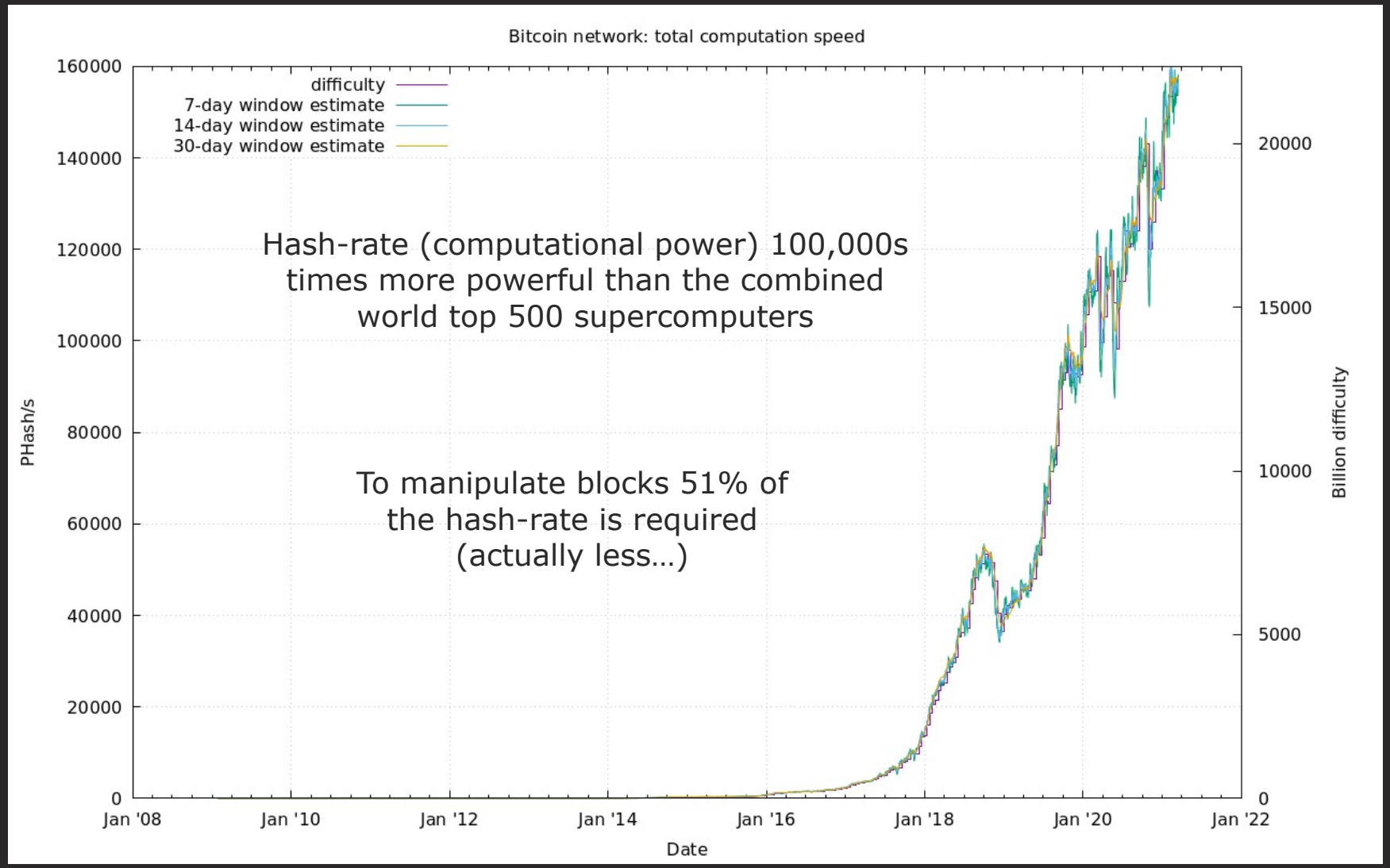
# Mining Hardware

- Computing power is measured in hash/s, hash being the basic operation needed for validation
- Efficiency is defined as lower power consumption for higher hash rate
- CPUs (Computer Processing Unit) were used in 2009
- GPUs (Graphical Processing Unit) performed better since 2010

Specific purpose energy-efficient hardware, designed and manufactured for SHA256 hash computations:

- FPGAs (Field Programmable Gate Array) surpassed GPU in 2011
- ASICs (Application Specific Integrated Circuit) were introduced in 2013 for Bitcoin and are now the standard

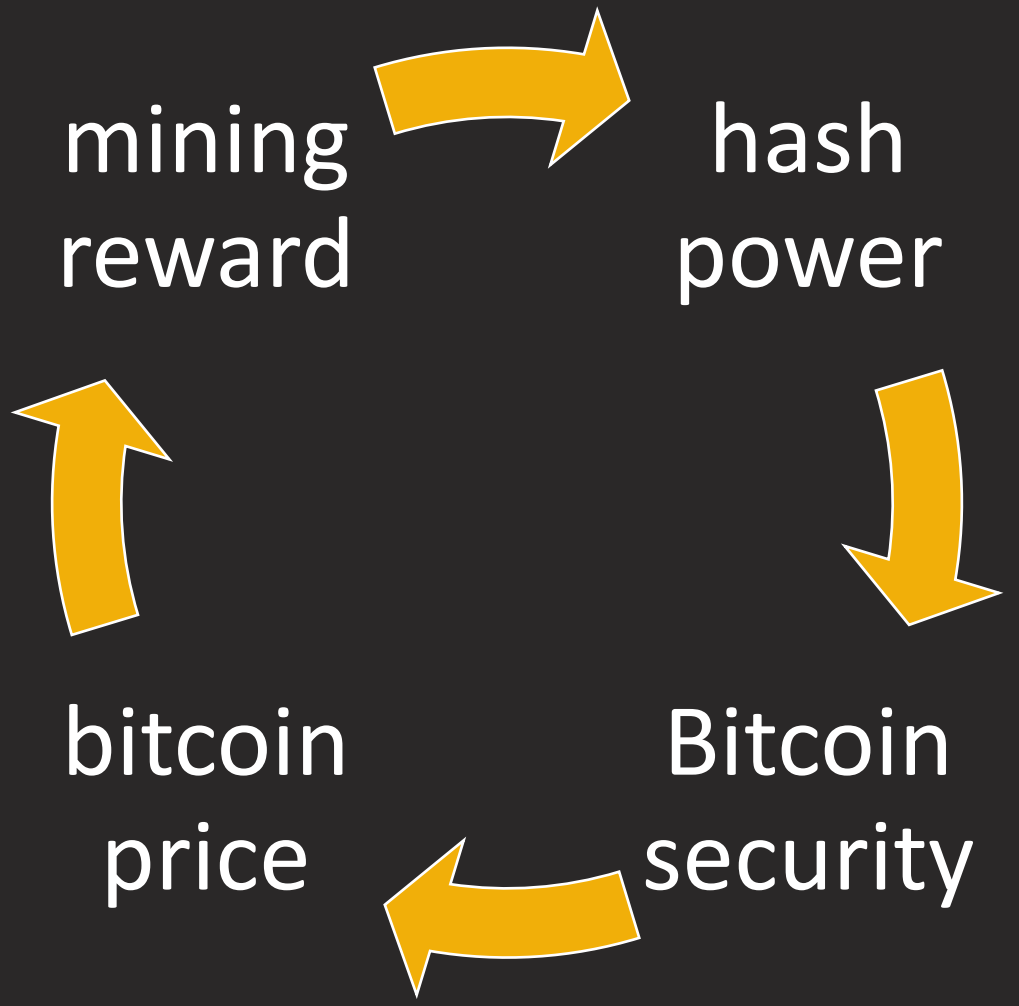
# Total Network Hash Rate






http://bitcoin.sipa.be/speed-lin-ever.png

# Virtuous Cycle



# Proof-of-Work

- Miners devote economic resources to acquire bitcoins: they are the first to recognize the bitcoin market value!
- Resources consumed as *proof-of-work* make bitcoin valuable
- Bitcoin is hard money backed by thermodynamics (proof-of-work)

- Miners are rational economic agents: they locate their business where energy is cheap (renewable energy)

# Environmental Sustainability

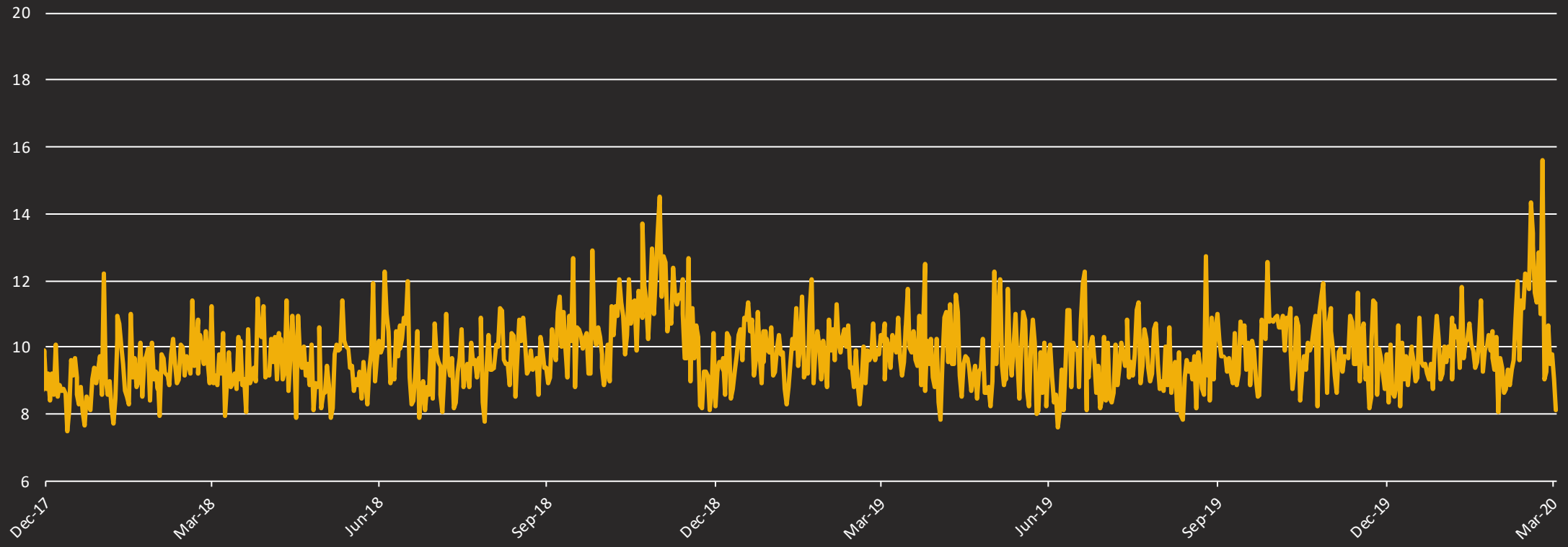
- Energy consumption does not grow linearly, because of efficiency improvement (see CPU→GPU→FPGA→ASIC)
- Bitcoin energy consumption: 8 TWh
  - comparable to Ireland or Denmark
  - 1/8th of US data-centers
  - 0.21% of US overall consumption
- Banknote system: 11 TWh
- Gold extraction: 132 TWh
- 2016 China hydroelectric untapped capacity (dissipated): 95 TWh

- What if PoW will absorb all renewable energy excess capacity available in the future?

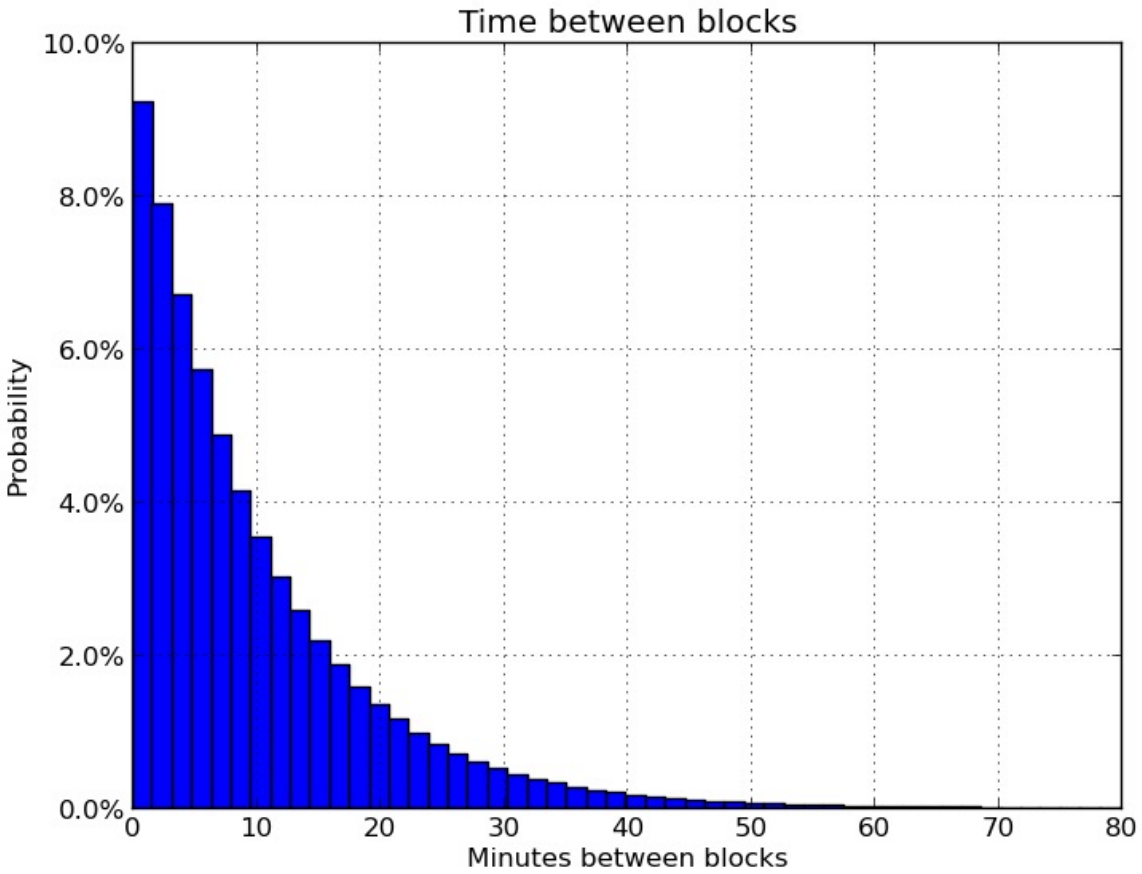
# Table of Contents

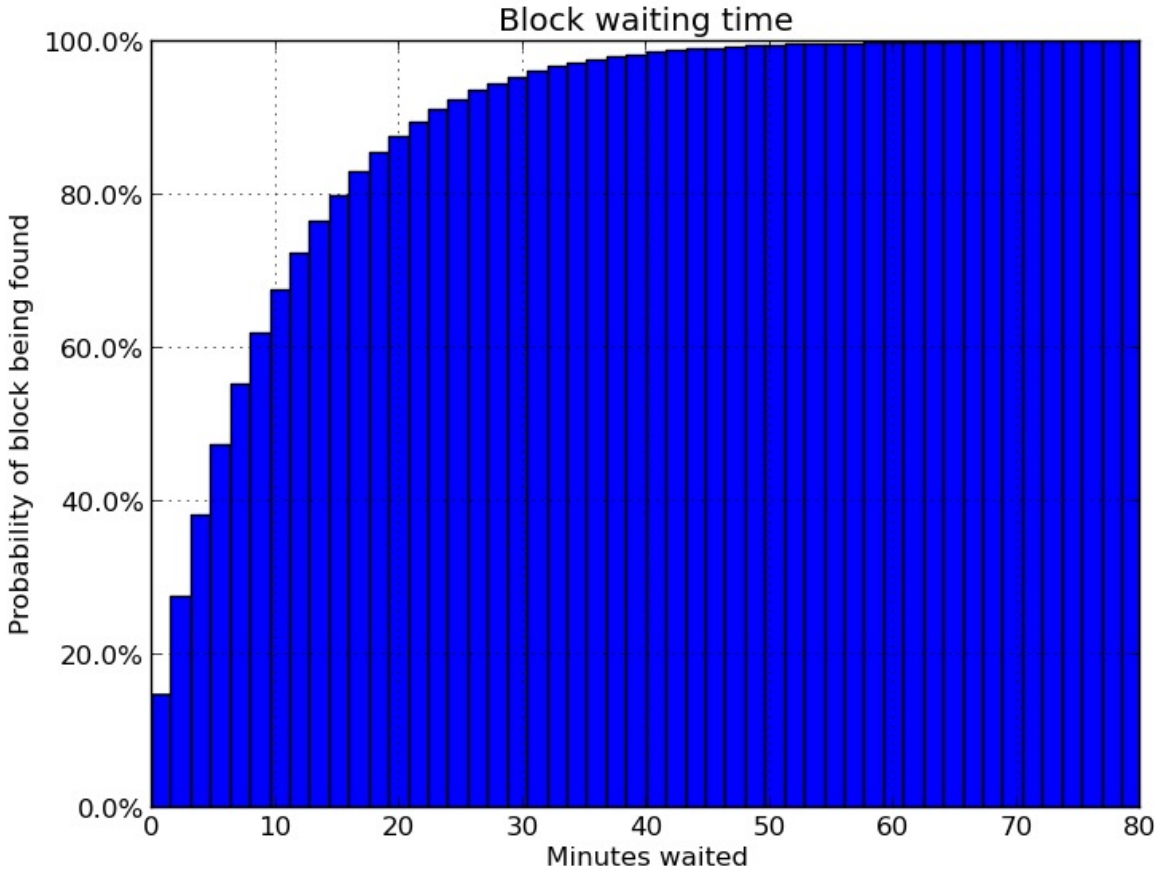
# Validation Process: Block Generation

*Proof-of-work* difficulty is dynamically adapted every 2016 blocks (about 2 weeks) to the overall available computing power, to target one block every 10 minutes



# Block Generation and Confirmation Times





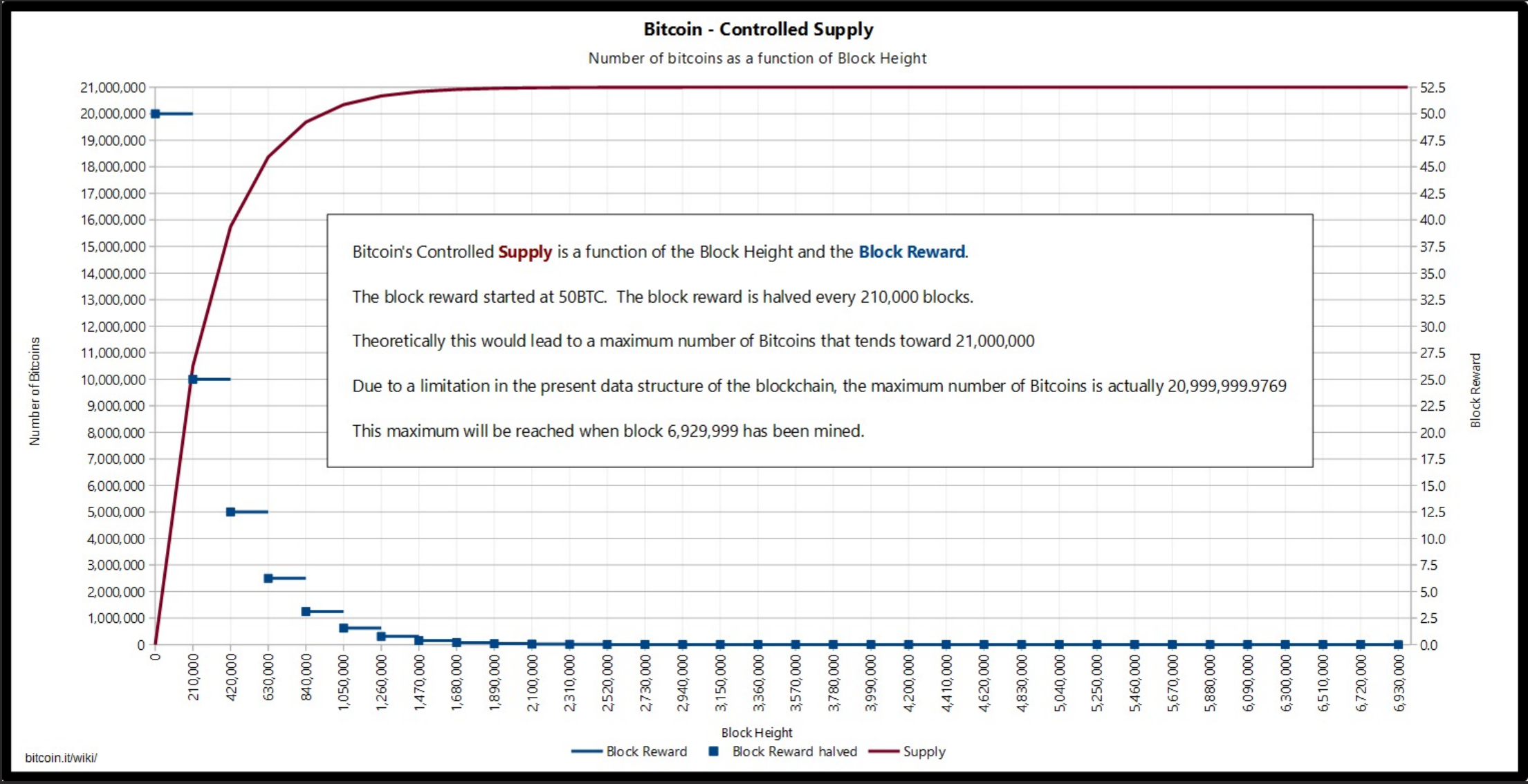

https://en.bitcoin.it/wiki/Confirmation

# Bitcoin Monetary Rule

- 2009: 50BTC per block, every 10 minutes
  - halving every 4Y
  - 6.25BTC since May 2020

- This is the only way new bitcoins are released
- It is called mining because of its similarity with the progressive scarcity of gold extraction
- Supply is free of discretionary intervention

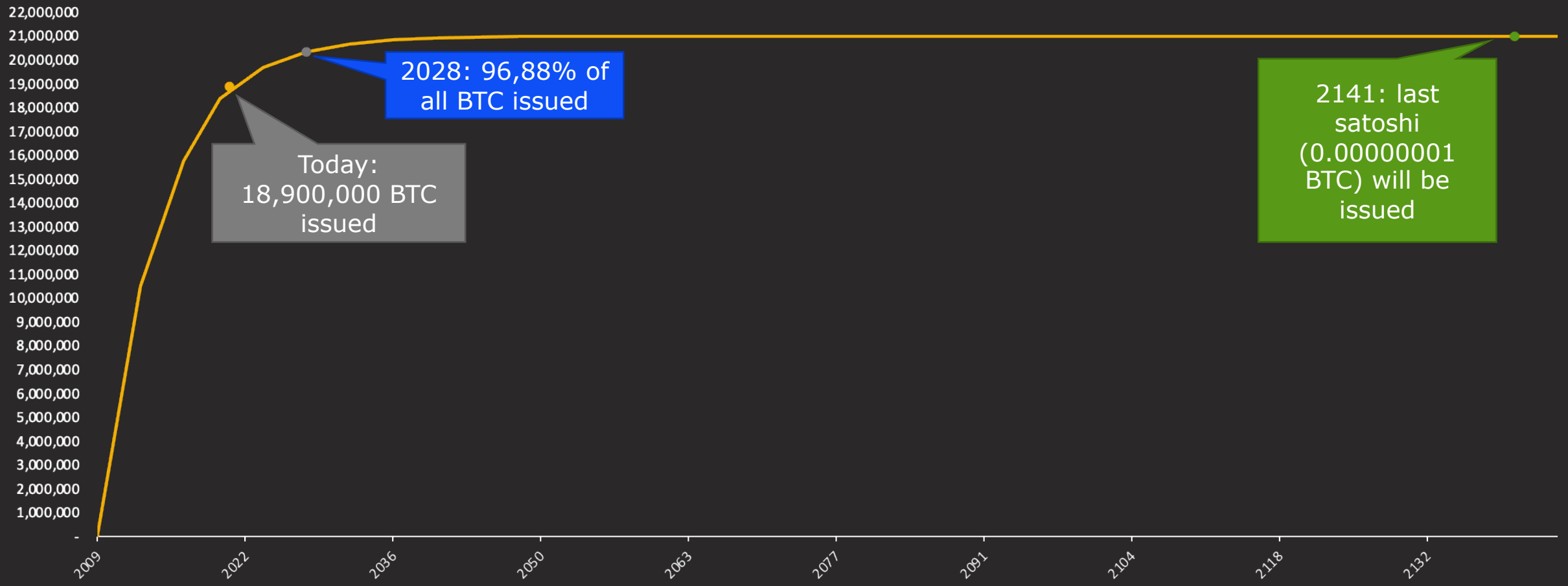
# Bitcoin Controlled Supply






https://en.bitcoin.it/wiki/Controlled_supply

# Bitcoin *Inelastic* Supply: Deterministic Decreasing Rate



# What after 2141?

- We will be all dead ;-)

- Gradually switch over to a fee-based system: “the incentive can transition entirely to transaction fees” (Satoshi)
- As block space is limited, market is already requiring a growing satoshi/byte fee for transactions to be included into a block. After all, it is only natural that transacting on the most secure network in the world will command high fees

- Switch to a different paradigm? We have about 120 years to evaluate alternative solutions

# What Makes Bitcoin Special?

- Digital and scriptural: it only exists as validated transaction
- Asset, not liability
- Bearer instrument
- It can be transferred but not duplicated (i.e. it can be spent, but not double-spent)
- Scarce in the digital realm, as nothing else before
- It mimics gold monetary policy of decreasing incremental extraction

# What Makes Bitcoin Special?

***Bitcoin is digital gold***

*with a secure uncensorable embedded*

***settlement network***

- More a crypto-commodity then a crypto-currency
- This is the groundbreaking achievement by Satoshi Nakamoto, not blockchain "technology"

# Bitcoin Relevance

If one considers the role of physical gold in the history of civilization, money, and finance

***the digital equivalent of gold could be disruptive***

in the current digital civilization and the future of money and finance

Bitcoin can be the new global reserve asset

*It is disconcerting that people are still, continuously, underestimating bitcoin*

# Explain Money to an Alien

| Traditional (*fiat*) money | bitcoin |
| --- | --- |
| ▪ No intrinsic value (social contract) | ▪ No intrinsic value (digital gold) |
| ▪ Currency security based on paper/ink | ▪ Currency security based on math/cryptography |
| ▪ Discretionary governance | ▪ Algorithmic governance |
| ▪ Wicksellian interest-rate approach | ▪ Deterministic supply |
| ▪ Coerced upon everybody with legal tender | ▪ Available as free non-binding choice |

# Different Opinions

## Alan Greenspan

*"It's a bubble. It has to have intrinsic value: you have to really stretch your imagination to infer what the intrinsic value of Bitcoin is. I haven't been able to do it. Maybe somebody else can. I do not understand where the backing of Bitcoin is coming from"*

## Lloyd Blankfein

*"The list of things that are conventional today that I use every day that I thought would never make it is a very long list. If bitcoin works, I say to myself… 'Hmmm, maybe that was a natural progression from hard money to fiat money to consensus money.' So who's to say…"*

https://www.youtube.com/watch?v=YIMWLOSRZ_A

# The Schelling Point of Consensus Money

- In game theory Schelling point is: “focal point[s] for each person’s expectation of what the other expects him to expect to be expected to do”
- e.g. two people unable to communicate are urged to select a square among a series of similar squares and rewarded only if they select the same one


- They will look for a choice that might seem more natural, special, or relevant: **the red one**

**Bitcoin is the Schelling point of consensus money!**

# Bitcoin Transactions Are Not Taking Off

- There is evidence that bitcoin is not really used for transactions
- Max number of transactions per second
  - VISA peak capacity: about *60,000 tx/sec*
  - Bitcoin peak capacity: about *7 tx/sec*
- Bitcoin could scale with second layer solutions, e.g. Lightning Network and Sidechain (Liquid), up to million of tx/sec

- Anyway, Bitcoin is already good enough to be a real-time gross settlement system:
  - ECB TARGET2 in 2016 and 2017: less than 90 million tx/year
  - Bitcoin capacity: over 200 million tx/year

# Two Pizzas for 10,000 Bitcoins... really!!

**laszlo**
Full Member

Activity: 199

**Pizza for bitcoins?**
May 18, 2010, 12:35:20 AM #1

I'll pay 10,000 bitcoins for a couple of pizzas.. like maybe 2 large ones so I have some left over for the next day. I like having left over pizza to nibble on later. You can make the pizza yourself and bring it to my house or order it for me from a delivery place, but what I'm aiming for is getting food delivered in exchange for bitcoins where I don't have to order or prepare it myself, kind of like ordering a 'breakfast platter' at a hotel or something, they just bring you something to eat and you're happy!

I like things like onions, peppers, sausage, mushrooms, tomatoes, pepperoni, etc.. just standard stuff no weird fish topping or anything like that. I also like regular cheese pizzas which may be cheaper to prepare or otherwise acquire.

If you're interested please let me know and we can work out a deal.

Thanks,
Laszlo

**laszlo**
Full Member

Activity: 199

**Re: Pizza for bitcoins?**
May 22, 2010, 07:17:26 PM

I just want to report that I successfully traded 10,000 bitcoins for pizza.

Pictures: http://heliacal.net/~solar/bitcoin/pizza/

Thanks jercos!

BC: 157fRrqAKrDyGHr1Bx3yDxeMv8Rh45aUet

https://bitcointalk.org/index.php?topic=137.msg1195#msg1

# The Ultimate Fate of Bitcoin: To Serve as a Reserve Currency

Hal Finney (1956–2014) was a noted cryptographic activist. He was the second PGP Corporation developer hired after Phil Zimmermann. He created the first reusable proof-of-work. He was an early bitcoin user and received the first bitcoin transaction from bitcoin's creator Satoshi Nakamoto.

**Hal**
VIP
Sr. Member

Activity: 314

**Re: Bitcoin Bank**
December 30, 2010, 01:38:40 AM

#10

Actually there is a very good reason for Bitcoin-backed banks to exist, issuing their own digital cash currency, redeemable for bitcoins. Bitcoin itself cannot scale to have every single financial transaction in the world be broadcast to everyone and included in the block chain. There needs to be a secondary level of payment systems which is lighter weight and more efficient. Likewise, the time needed for Bitcoin transactions to finalize will be impractical for medium to large value purchases.

Bitcoin backed banks will solve these problems. They can work like banks did before nationalization of currency. Different banks can have different policies, some more aggressive, some more conservative. Some would be fractional reserve while others may be 100% Bitcoin backed. Interest rates may vary. Cash from some banks may trade at a discount to that from others.

George Selgin has worked out the theory of competitive free banking in detail, and he argues that such a system would be stable, inflation resistant and self-regulating.

I believe this will be the ultimate fate of Bitcoin, to be the "high-powered money" that serves as a reserve currency for banks that issue their own digital cash. Most Bitcoin transactions will occur between banks, to settle net transfers. Bitcoin transactions by private individuals will be as rare as... well, as Bitcoin based purchases are today.

Hal Finney

https://bitcointalk.org/index.php?topic=2500.msg34211#msg34211

# Unit of Account: Money as ***Numeraire***

- Money is the unit of account against which the value of every other good is measured

- The price system measures the value of goods relative to the value of money

*Good money should provide stable prices to best perform its role as unit of account*

# Money Comparison

| | Medium of Exchange | Store of ~~Stable~~ Value | Unit of Account |
|---|---|---|---|
| *Live cattle* |  |  |  |
| *Diamonds* |  |  |  |
| *Gold* |  |  |  |
| *Fiat coins and notes* |  |  |  |
| *Bitcoin* |  |  |  |

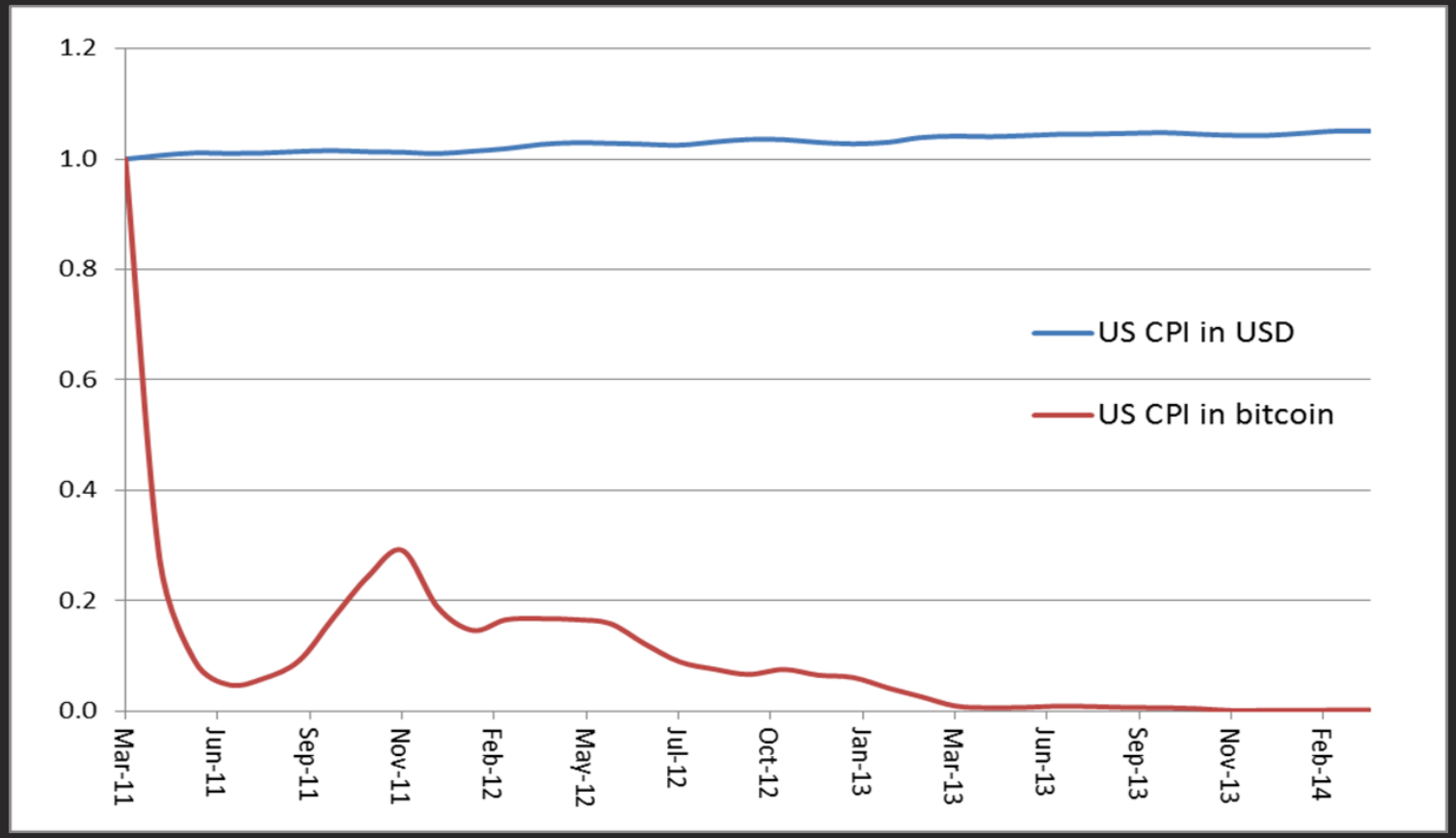
- swappable
- fungible
- portable
- divisible
- recognizable
- resistant to counterfeiting

- reliably saved, stored, and retrieved
- retain usefulness over time
- Maintain its storage properties
- non-perishable or with low preservation cost

- relative worth unit of measure
- stable value for stable price comparison
- supply must be controlled in some way

# Bitcoin is Digital Gold, Not a Good Unit of Account

- no salaries, no mortgages, no stable purchasing power
- successful at getting rid of a central monetary authority, bitcoin has given up the flexibility of an elastic supply of money



# Bitcoin as (Digital) Gold in the History of (Crypto)Money

| gold | bitcoin |
| --- | --- |
| ▪ adopted by every civilization without centrally planning | ▪ its adoption has not been centrally planned |
| ▪ has been the most successful form of money for centuries | ▪ the most successful form of cryptocurrency |
| ▪ has bootstrapped all monetary systems we know of | ▪ is bootstrapping new monetary systems |
| ▪ has been surpassed by other kind of money without becoming obsolete | ▪ might be surpassed by more advanced type of cryptocurrencies without becoming obsolete |

# Bitcoin Is Not Loved… Gold Too!

- 1933 Gold Act "forbidding the hoarding of gold coin, gold bullion, and gold certificates within the continental United States"
- 1966 Greenspan: “This is the shabby secret of the welfare statists' tirades against gold. Deficit spending is simply a scheme for the confiscation of wealth. Gold stands in the way of this insidious process. It stands as a protector of property rights. If one grasps this, one has no difficulty in understanding the statists' antagonism toward the gold standard”
- 1972 Nixon shock: unilateral cancellation of the convertibility of the United States dollar to gold

# IMF Special Drawing Rights

- Special Drawing Rights are international reserve assets, created in 1969 to supplement existing official reserves of member countries
- SDRs address the lack of a non-national currency to be used as reserve asset
- F. Saccomanni: “cryptocurrencies could be an effective monetary policy instruments [...] we should pay more attention to the geniuses working on them, try to understand what of interest they could teach us”

https://it.finance.yahoo.com/notizie/saccomanni-non-bisogna-demonizzare-cripto-valute-172912255.html

http://www.ufficiostampa.rai.it/pdf/2014/2014-10-09/20141009284904 98.pdf

# Geopolitical Implications

- IMF sponsored token: possible, but unrealistic as it would severely undermine US dollar predominance
- To challenge the USD supremacy as reserve asset is hard
- Monetary engineering might be not only the next cypher-punk frontier, but a weapon of geopolitical «wars»
- Even the development on CBDC are pushed by the international competition on payment and reserve asset, namely the push of the Chinese digital renminbi


# Digital Gold for New Monetary Standards

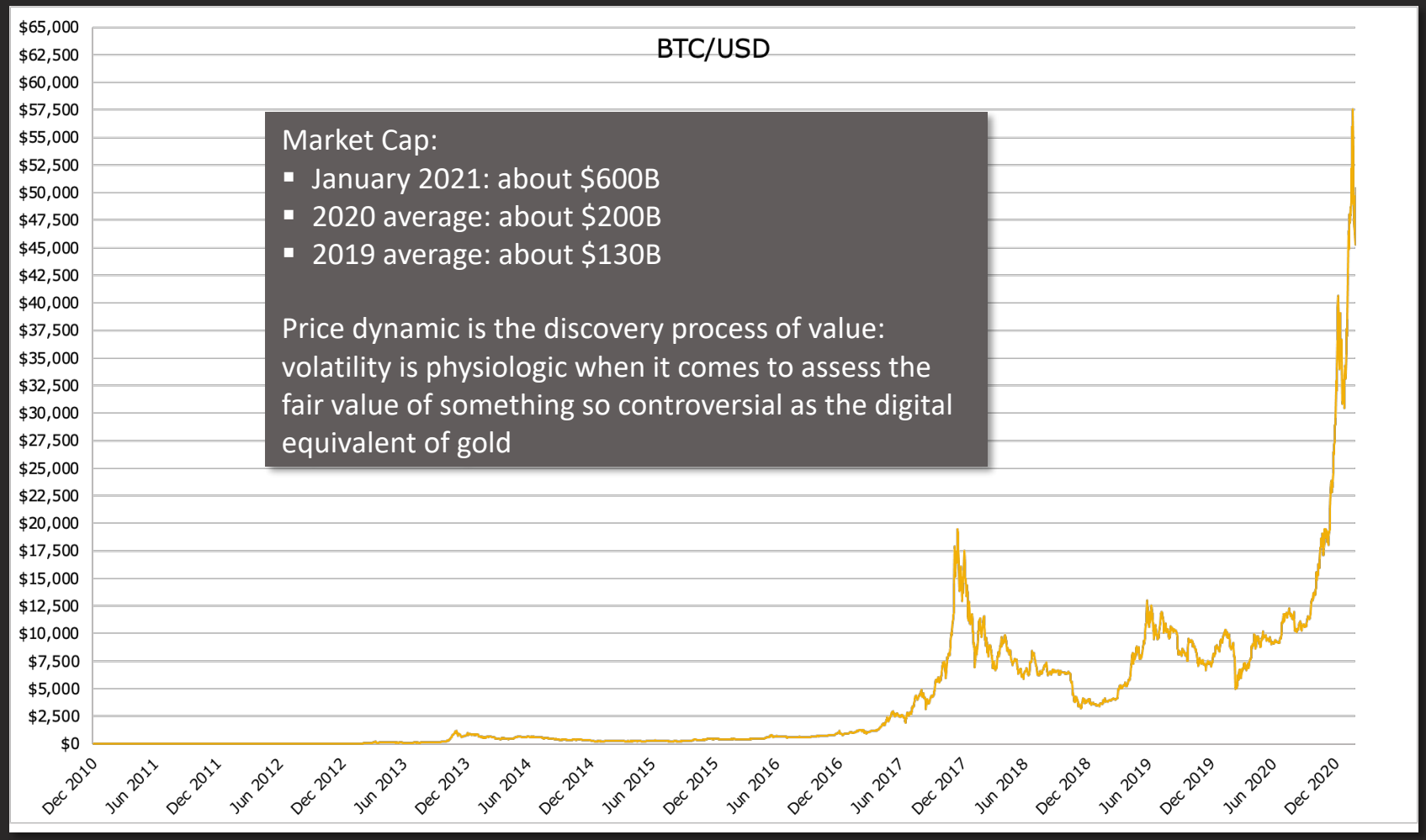
*Bitcoin: oro digitale per nuovi standard monetari*, Ferdinando M. Ametrano

included in *Dal sesterzio al Bitcoin. Vecchie e nuove dimensioni del denaro.* (2020 Rubbettino)

https://www.amazon.it/Dal-sesterzio-bitcoin-Angelo-Miglietta/dp/8849856806

# Table of Contents

# The Driver: Bitcoin Price Performance



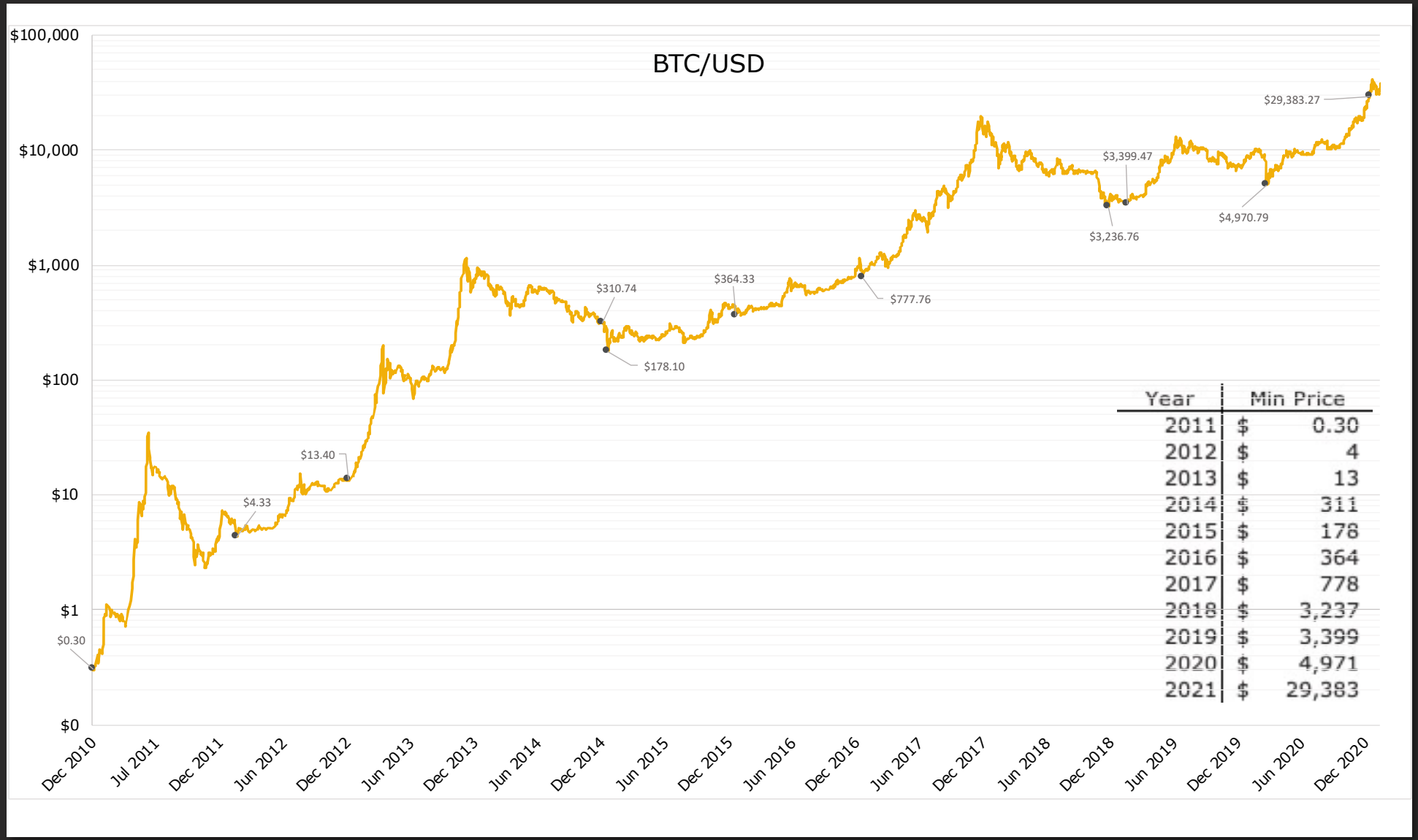

Market Cap:

- January 2021: about $600B
- 2020 average: about $200B
- 2019 average: about $130B

Price dynamic is the discovery process of value: volatility is physiologic when it comes to assess the fair value of something so controversial as the digital equivalent of gold

| Date | Price | Yearly performance |
|---|---|---|
| 31-Dec-11 | $ 5.00 | |
| 31-Dec-12 | $ 13.59 | 172% |
| 31-Dec-13 | $ 754.01 | 5448% |
| 31-Dec-14 | $ 320.19 | -58% |
| 31-Dec-15 | $ 430.57 | 34% |
| 31-Dec-16 | $ 963.74 | 124% |
| 31-Dec-17 | $ 14,156.40 | 1369% |
| 31-Dec-18 | $ 3,742.70 | -74% |
| 31-Dec-19 | $ 7,193.60 | 92% |
| 31-Dec-20 | $ 28,964.02 | 303% |
| 28-Feb-21 | $ 45,251.19 | 56% |

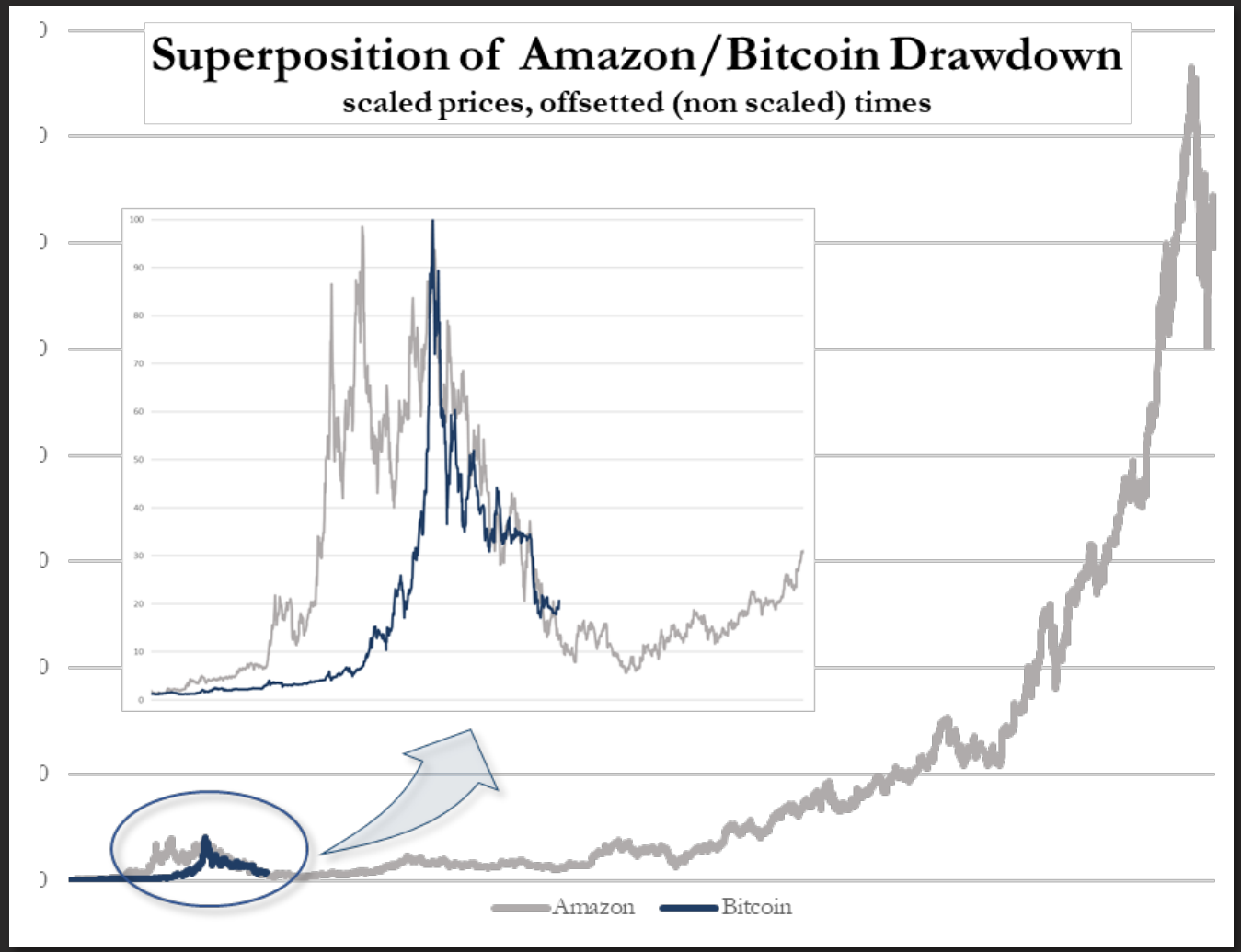
# Bitcoin Performance (Log Scale)




| Year | Min Price |
|---|---|
| 2011 | $ 0.30 |
| 2012 | $ 4 |
| 2013 | $ 13 |
| 2014 | $ 311 |
| 2015 | $ 178 |
| 2016 | $ 364 |
| 2017 | $ 778 |
| 2018 | $ 3,237 |
| 2019 | $ 3,399 |
| 2020 | $ 4,971 |
| 2021 | $ 29,383 |

# Comparison with Amazon

- Bitcoin worst drawdown: 93.07%
- Amazon worst drawdown: 94.40%% (dot-com bubble burst)
- The value of digital gold is as hard to grasp today as the value of e-commerce in the 90s



# Volatility Comparison

# High Return: Compensation for High Risks

Bitcoin risks are an order of magnitude greater than other asset classes

| *Jul 2010 - Nov 2018* | | BITCOIN | GOLD | WTI | GRAIN | IND. METALS | EUR | GBP | CHF | JPY |
|---|---|---|---|---|---|---|---|---|---|---|
| Return | Daily Mean Return | 0,50% | 0,00% | -0,01% | -0,04% | -0,02% | -0,01% | -0,01% | 0,00% | -0,02% |
| | Daily Min Return | -60,09% | -9,39% | -10,79% | -6,06% | -6,71% | -2,30% | -7,37% | -9,06% | -3,51% |
| | Daily Max Return | 51,70% | 5,07% | 11,62% | 6,39% | 5,54% | 2,95% | 2,58% | 13,45% | 3,38% |
| | Mean Return (annualized) | 250,95% | -0,95% | -3,40% | -8,90% | -5,06% | -2,46% | -2,54% | -0,29% | -3,90% |
| Risk | Volatility (daily) | 6,48% | 0,98% | 2,02% | 1,34% | 1,15% | 0,53% | 0,52% | 0,67% | 0,57% |
| | Volatility (annualized) | 102,89% | 15,62% | 32,00% | 21,24% | 18,19% | 8,45% | 8,30% | 10,61% | 8,99% |
| | Skewness | -0,264 | -0,693 | 0,072 | 0,053 | -0,062 | 0,046 | -1,431 | 2,864 | -0,142 |
| | Excess Kurtosis | 15,154 | 7,136 | 3,332 | 2,375 | 2,398 | 1,793 | 21,171 | 95,506 | 3,510 |
| | VaR 99% | 18,83% | 2,87% | 5,61% | 3,69% | 2,94% | 1,45% | 1,23% | 1,47% | 1,63% |
| | Expected Shortfall at 99% | 28,60% | 3,97% | 6,83% | 4,77% | 3,89% | 1,69% | 1,93% | 2,19% | 2,13% |
| | Worst Drawdown | 93,07% | 44,58% | 76,99% | 65,23% | 57,82% | 30,19% | 29,69% | 29,21% | 39,66% |
| Risk/Ret | Sharpe Ratio | 2,416 | -0,211 | -0,180 | -0,529 | -0,407 | -0,568 | -0,588 | -0,248 | -0,695 |
| | Correlation with Bitcoin | 100% | 0,02% | 1,42% | 3,41% | 3,41% | 2,94% | 0,72% | 3,47% | -1,42% |

# High Return: Compensation for High Risks

Bitcoin has volatility and worst draw-down like the VIX index; anyway, VIX is anticorrelated with equities, Bitcoin is decorrelated

| *Jul 2010 - Nov 2018* | | BITCOIN | MSCI BRIC | EURO STOXX50 | NASDAQ | S&P500 | VIX | Euro Bonds | US Bonds | EUR Bonds |
|---|---|---|---|---|---|---|---|---|---|---|
| Return | Daily Mean Return | 0,50% | -0,01% | 0,00% | 0,05% | 0,04% | 0,00% | 0,00% | 0,01% | 0,00% |
| | Daily Min Return | -60,09% | -6,93% | -10,67% | -7,15% | -6,90% | -31,41% | -2,76% | -1,01% | -2,62% |
| | Daily Max Return | 51,70% | 4,75% | 8,43% | 5,16% | 4,63% | 76,82% | 2,55% | 0,83% | 2,43% |
| | Mean Return (annualized) | 250,95% | -2,81% | -0,86% | 13,72% | 10,53% | -0,17% | 1,08% | 2,19% | 0,92% |
| Risk | Volatility (daily) | 6,48% | 1,09% | 1,39% | 1,02% | 0,88% | 7,64% | 0,51% | 0,20% | 0,54% |
| | Volatility (annualized) | 102,89% | 17,38% | 22,09% | 16,15% | 14,05% | 121,22% | 8,10% | 3,16% | 8,64% |
| | Skewness | -0,264 | -0,283 | -0,330 | -0,544 | -0,602 | 1,204 | -0,117 | -0,262 | -0,065 |
| | Excess Kurtosis | 15,154 | 2,582 | 4,917 | 4,041 | 5,528 | 8,133 | 1,555 | 1,345 | 1,414 |
| | VaR 99% | 18,83% | 2,94% | 4,14% | 2,98% | 2,56% | 17,98% | 1,36% | 0,54% | 1,46% |
| | Expected Shortfall at 99% | 28,60% | 3,90% | 5,33% | 3,99% | 3,64% | 22,24% | 1,62% | 0,65% | 1,70% |
| | Worst Drawdown | 93,07% | 51,05% | 42,76% | 18,71% | 19,39% | 80,96% | 16,84% | 4,87% | 17,66% |
| Risk/Ret | Sharpe Ratio | 2,416 | -0,297 | -0,145 | 0,705 | 0,583 | -0,021 | -0,156 | -0,047 | -0,165 |
| | Correlation with Bitcoin | 100% | 1,39% | 5,01% | 4,00% | 5,07% | -5,31% | 2,06% | -1,27% | 2,59% |

# A New Uncorrelated Asset Class

## Bitcoin provides a huge diversification to an investment portfolio

Data set: 2017-01-01 / 2019-12-31

| | BTC | ETH | LTC | XRP | GOLD | IND MET | WTI | GRAIN | EUR | CHF | GBP | JPY | NASDAQ | EUR SX5E | S&P500 | MSCI BRIC | VIX | EUR AGG | PAN EUR | PAN US |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| BTC | 100,00% | | | | | | | | | | | | | | | | | | | |
| ETH | 17,09% | 100,00% | | | | | | | | | | | | | | | | | | |
| LTC | 15,65% | 56,63% | 100,00% | | | | | | | | | | | | | | | | | |
| XRP | 12,02% | 37,21% | 39,55% | 100,00% | | | | | | | | | | | | | | | | |
| GOLD | 5,68% | 5,03% | 0,11% | 0,20% | 100,00% | | | | | | | | | | | | | | | |
| IND MET | -0,15% | 2,05% | -1,11% | 1,34% | 14,06% | 100,00% | | | | | | | | | | | | | | |
| WTI | -0,75% | 1,99% | -2,92% | -0,44% | 3,99% | 20,64% | 100,00% | | | | | | | | | | | | | |
| GRAIN | 5,34% | 1,20% | -2,64% | 1,82% | 2,93% | 6,13% | 10,94% | 100,00% | | | | | | | | | | | | |
| EUR | 3,39% | 9,31% | 4,16% | 1,31% | 48,27% | 19,98% | 2,37% | 6,38% | 100,00% | | | | | | | | | | | |
| CHF | 4,25% | 8,58% | 1,10% | -2,17% | 56,04% | 9,29% | -0,71% | 4,32% | 73,19% | 100,00% | | | | | | | | | | |
| GBP | 3,51% | 3,85% | 0,50% | -2,59% | 27,11% | 9,32% | 4,37% | 4,45% | 55,11% | 40,57% | 100,00% | | | | | | | | | |
| JPY | 4,61% | 8,90% | 2,57% | 0,98% | 63,67% | -8,62% | -8,25% | -1,80% | 39,66% | 57,71% | 20,73% | 100,00% | | | | | | | | |
| NASDAQ | 2,88% | 1,84% | 2,36% | 1,23% | -12,20% | 19,32% | 21,89% | 4,60% | -0,56% | -14,89% | 5,54% | -28,62% | 100,00% | | | | | | | |
| EUR SX5E | 1,07% | 2,44% | 8,19% | 1,42% | -25,46% | 24,80% | 18,94% | 8,55% | -10,59% | -27,97% | 4,76% | -44,63% | 47,75% | 100,00% | | | | | | |
| S&P500 | 2,31% | 2,11% | 2,24% | 1,54% | -14,22% | 20,77% | 26,54% | 5,44% | 0,89% | -14,73% | 6,34% | -32,01% | 95,05% | 52,89% | 100,00% | | | | | |
| MSCI BRIC | 1,20% | 3,62% | 3,48% | 4,15% | 2,74% | 36,61% | 21,85% | 10,64% | 13,09% | -0,10% | 15,76% | -15,09% | 48,33% | 48,63% | 46,30% | 100,00% | | | | |
| VIX | -5,69% | -4,14% | -1,52% | -2,85% | 10,12% | -15,35% | -20,77% | -10,44% | -0,95% | 14,13% | -5,11% | 27,47% | -76,17% | -47,64% | -79,15% | -40,97% | 100,00% | | | |
| EUR AGG | -0,36% | -4,63% | -3,80% | -1,48% | 29,05% | -12,83% | -2,78% | -5,53% | -9,76% | 4,35% | -10,71% | 27,78% | -4,48% | -4,49% | -6,98% | -6,99% | 1,92% | 100,00% | | |
| PAN EUR | 0,85% | -5,08% | -3,83% | -1,30% | 27,70% | -16,19% | -2,30% | -4,79% | -18,74% | 2,18% | 7,88% | 28,93% | -5,90% | -5,39% | -8,87% | -7,66% | 4,89% | 91,63% | 100,00% | |
| PAN US | 0,55% | 0,36% | 0,48% | 4,24% | 46,06% | -14,36% | -13,04% | -3,50% | 9,89% | 27,91% | 3,65% | 52,39% | -26,55% | -27,34% | -30,30% | -16,68% | 25,71% | 55,09% | 57,03% | 100,00% |
| | Crypto-currency | | | | Commodity | | | | Currency | | | | Equity | | | | Volatility | Bond | | |

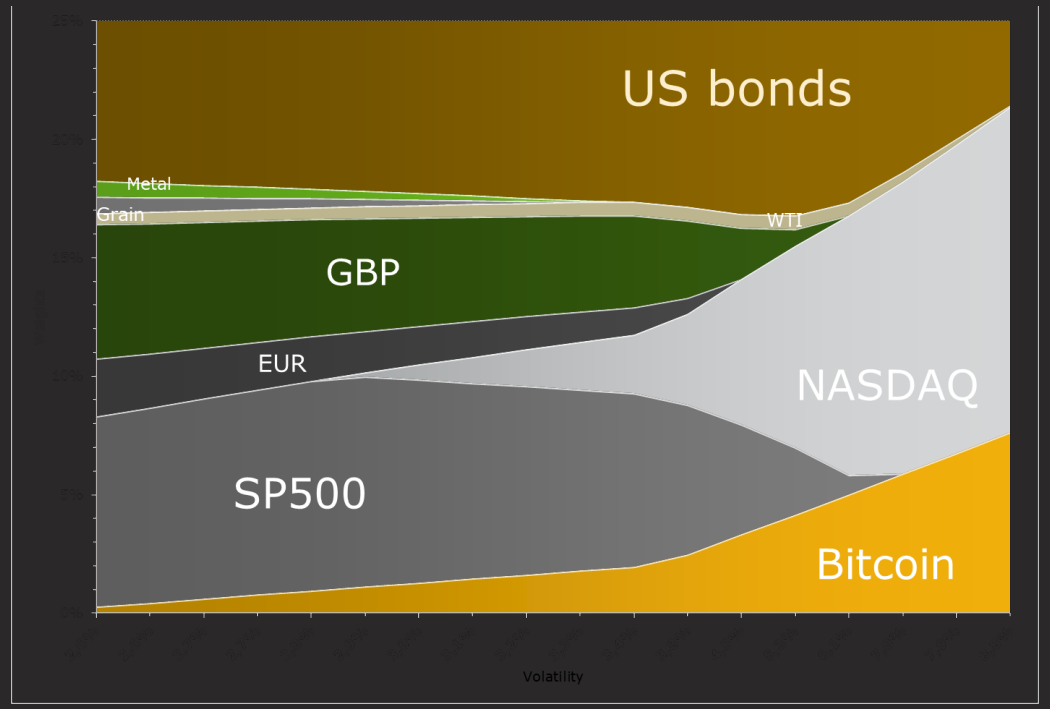
Positive
Negative

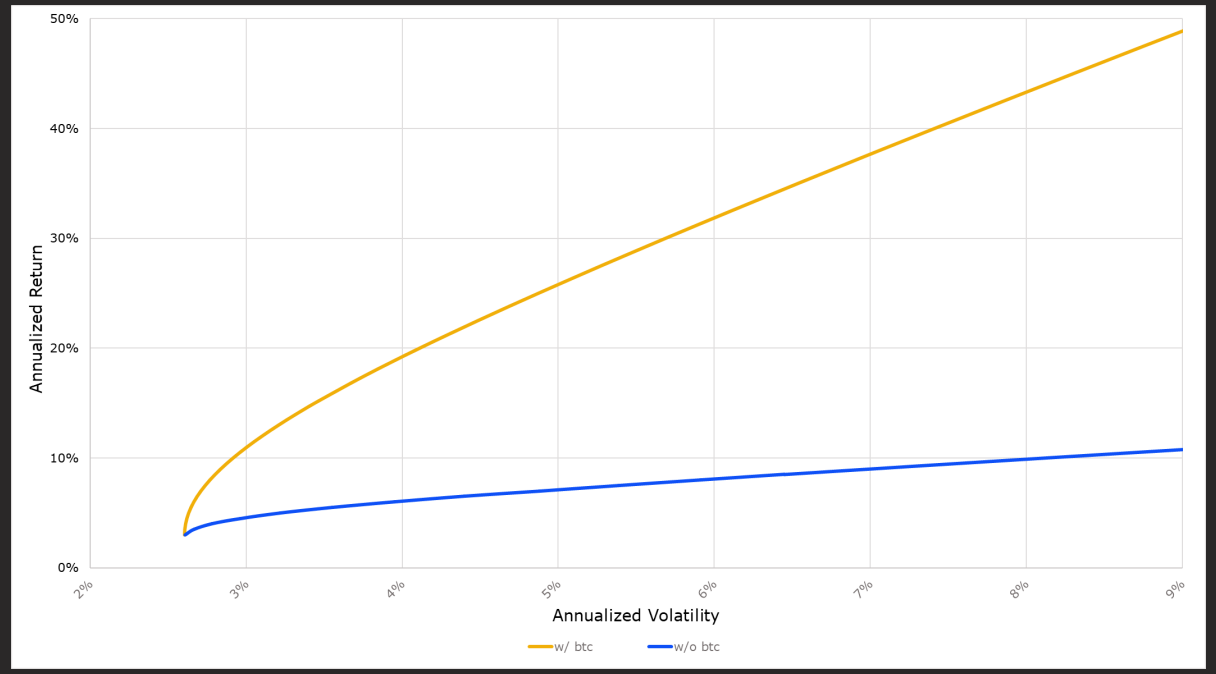
# Bitcoin: CAPM Diversification

Bitcoin increases expected return for a given level of risk, e.g.

- at 4% volatility, return increases more than 140bps
- at 10% return, volatility decreases from 8.60% to 2.90%

For conservative risk levels, optimal CAPM diversification suggests to invest in Bitcoin up to 5% of the portfolio



# Bitcoin Potential Upside

**Asset Under Management worldwide:**
$100T

If 3% will invest in BTC, then its price should be:

**~ $150,000/BTC**

**Gold capitalization:**
$10T

if BTC reaches a similar level, then its price should be:

**~ $500,000/BTC**

**Metcalfe's law*:**
*"network value is proportional to the square of the number of users"*

Estimated BTC investors: 100m
Forecasted investors: 300m
BTC price might increase x9:

**~ $450,000/BTC**

* https://quantpedia.com/Blog/Details/metcalfes-law-in-bitcoin

# Table of Contents


Press and Information

Court of Justice of the European Union

**PRESS RELEASE No 128/15**

Luxembourg, 22 October 2015

Judgment in Case C-264/14
Skatteverket v David Hedqvist

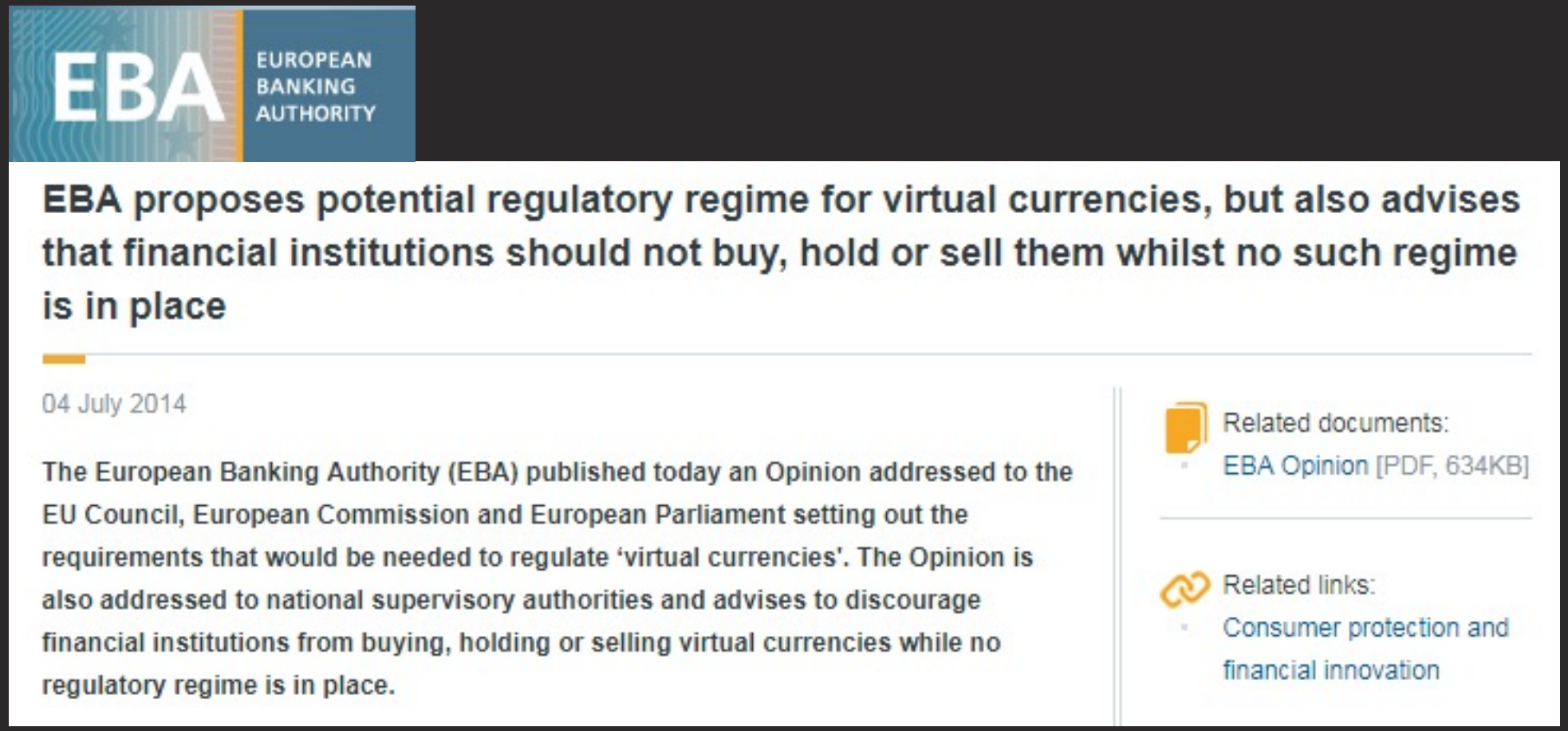
## The exchange of traditional currencies for units of the 'bitcoin' virtual currency is exempt from VAT

The VAT Directive[1] provides that the supply of goods and services for consideration within the territory of a Member State by a taxable person acting as such is to be subject to VAT. However, Member States must exempt, inter alia, transactions relating to 'currency, bank notes and coins used as legal tender'.

In today's judgment, the Court holds that transactions to exchange traditional currencies for units of the 'bitcoin' virtual currency (and vice versa) constitute the supply of services for consideration within the meaning of the directive, since they consist of the exchange of different means of payment and there is a direct link between the service provided by Mr Hedqvist and the consideration received by him, namely the margin created by the difference between, on the one hand, the price at which he purchases currencies and, on the other hand, the price at which he sells them to his clients.

The Court also holds that **those transactions are exempt from VAT under the provision concerning transactions relating to 'currency, bank notes and coins used as legal tender'.** To exclude transactions such as those envisaged by Mr Hedqvist from the scope of that provision would deprive it of part of its effects having regard to the aim of the exemption, which is to alleviate the difficulties connected with determining the taxable amount and the amount of VAT deductible which arise in the context of the taxation of financial transactions.

# European Banking Authority



# Bitcoin Regulated Markets

## Futures

CME Group
A CME/Chicago Board of Trade Company

Chicago Mercantile Exchange:

- Quoted since December 2017
- Regulated by the Commodity Futures Trading Commission (CFTC)
- Cash-settled (delivery of the USD-equivalent at maturity)
- $650M average daily volume

Bakkt

Bakkt (ICE, NYSE):

- Listed on ICE Futures U.S. and cleared by ICE Clear U.S.
- Physically-settled (delivery of Bitcoin at maturity)

## Options

CME Group
A CME/Chicago Board of Trade Company

Chicago Mercantile Exchange:

- Quoted since January 2020
- The value of options is based on the regulated CME CF Bitcoin Reference Rate (BRR) and settles into actively traded Bitcoin futures
- $300M average daily open interest

## ETP

XBTPROVIDER
A CoinShares Company

XBT Provider: listed on Nasdaq Stockholm

WisdomTree®

Wisdom Tree: listed on SIX Swiss Exchange

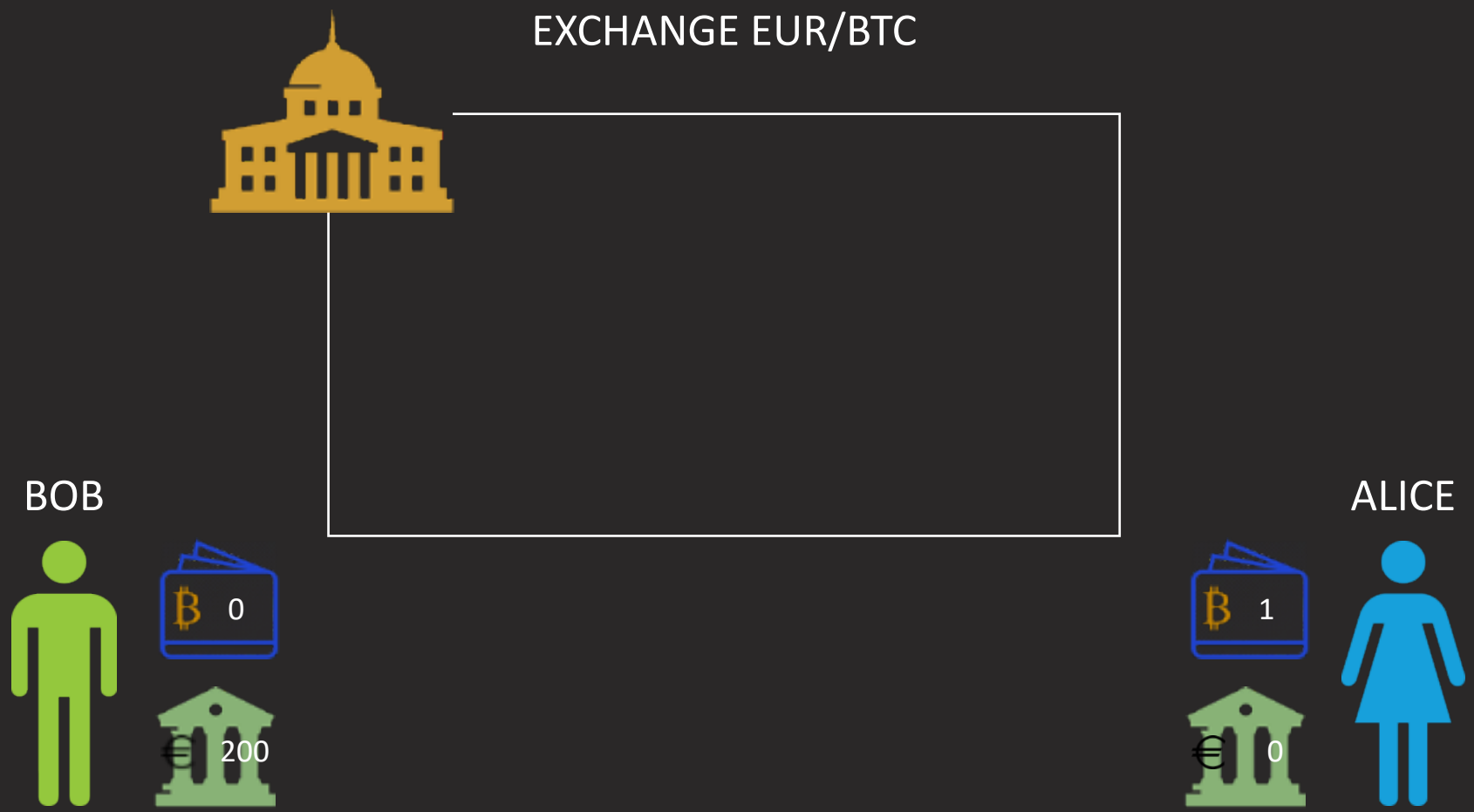
21SHARES

21Shares: listed on SIX Swiss Exchange

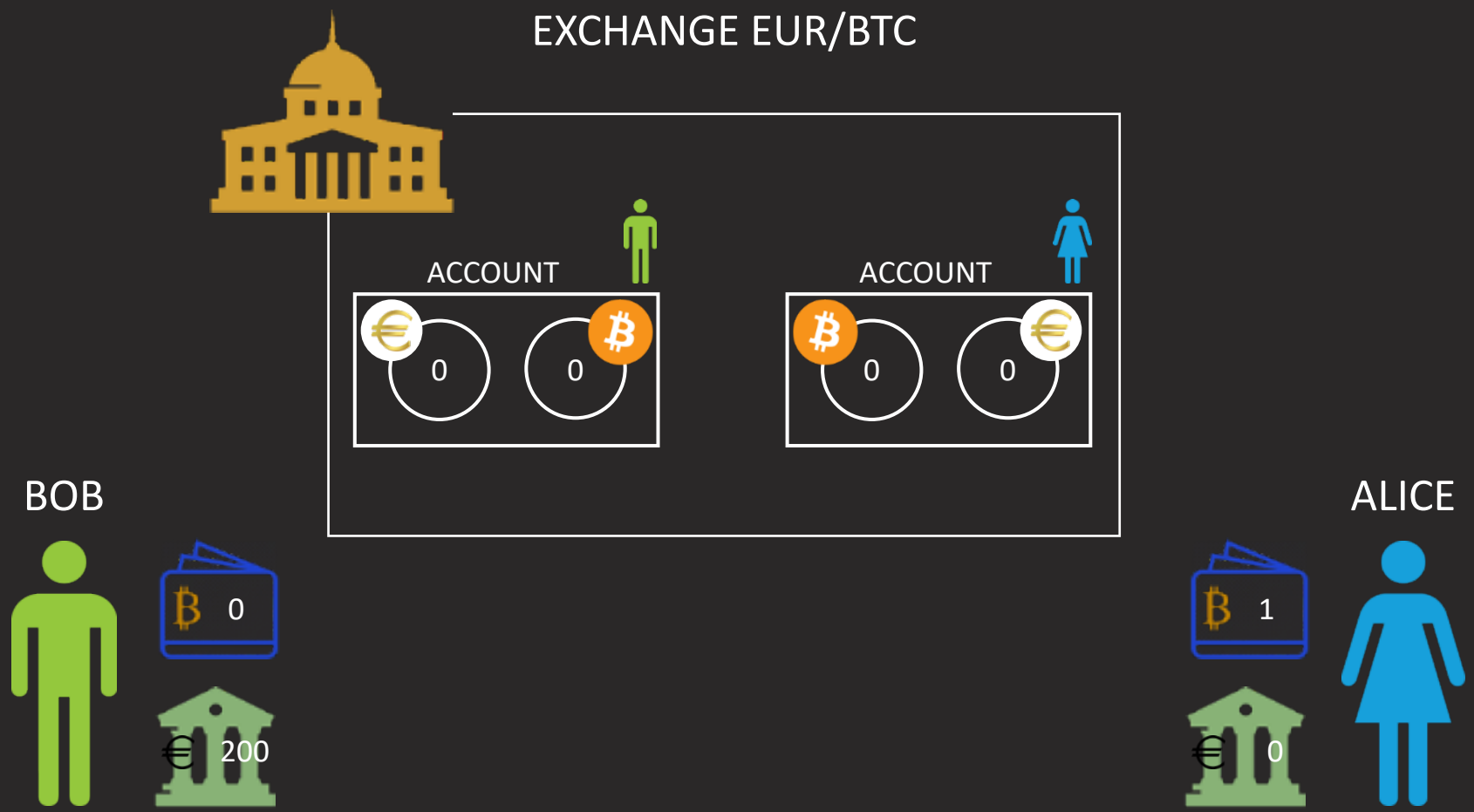
ftp://ftp.cmegroup.com/bitcoinfutures/Bitcoin_Futures_Liquidity_Report.pdf

https://www.cmegroup.com/trading/bitcoin-futures.html?redirect=/bitcoinoptions

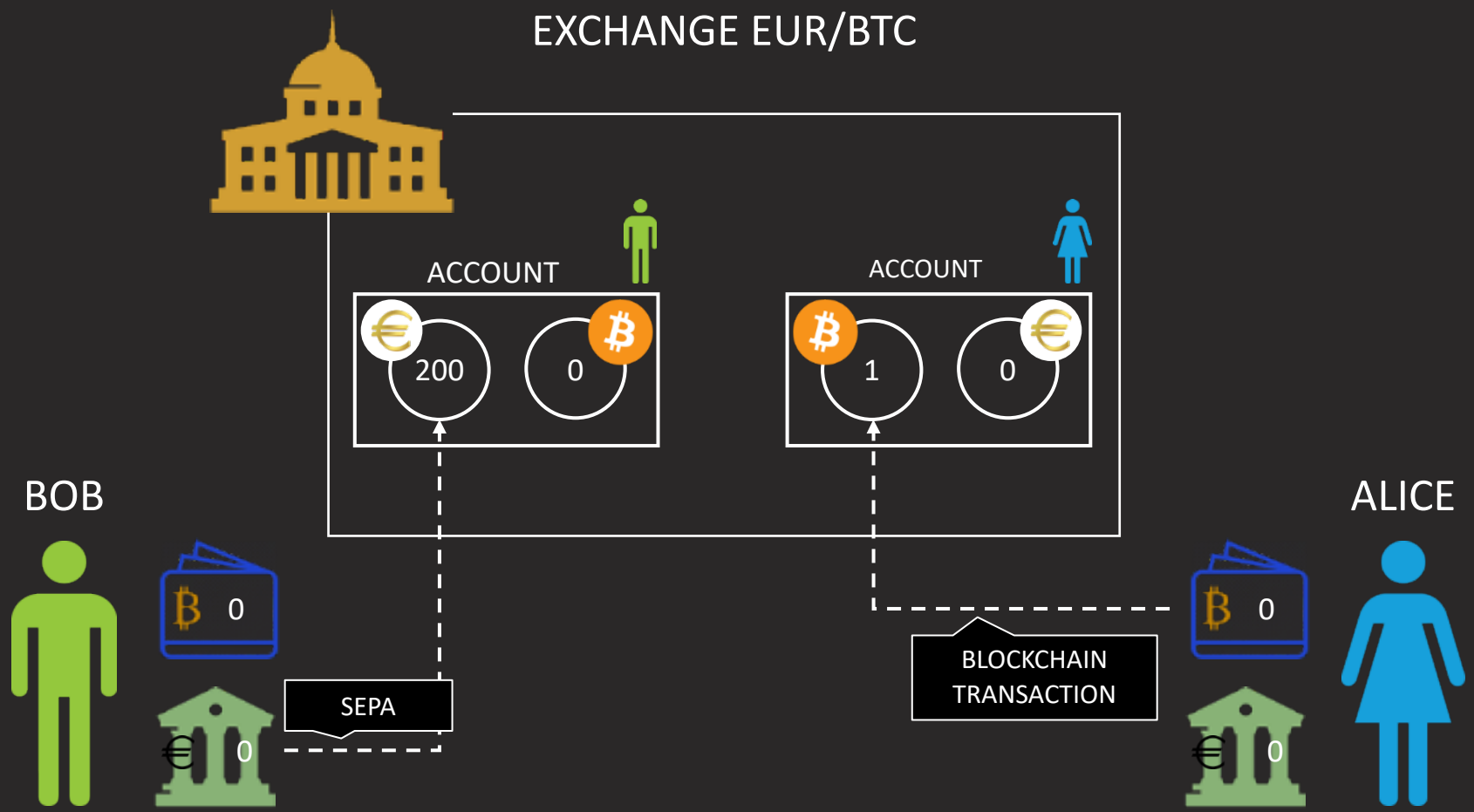
# Buying and Selling BTC: the Exchange



# Exchange Account Creation



# Exchange Account Deposit

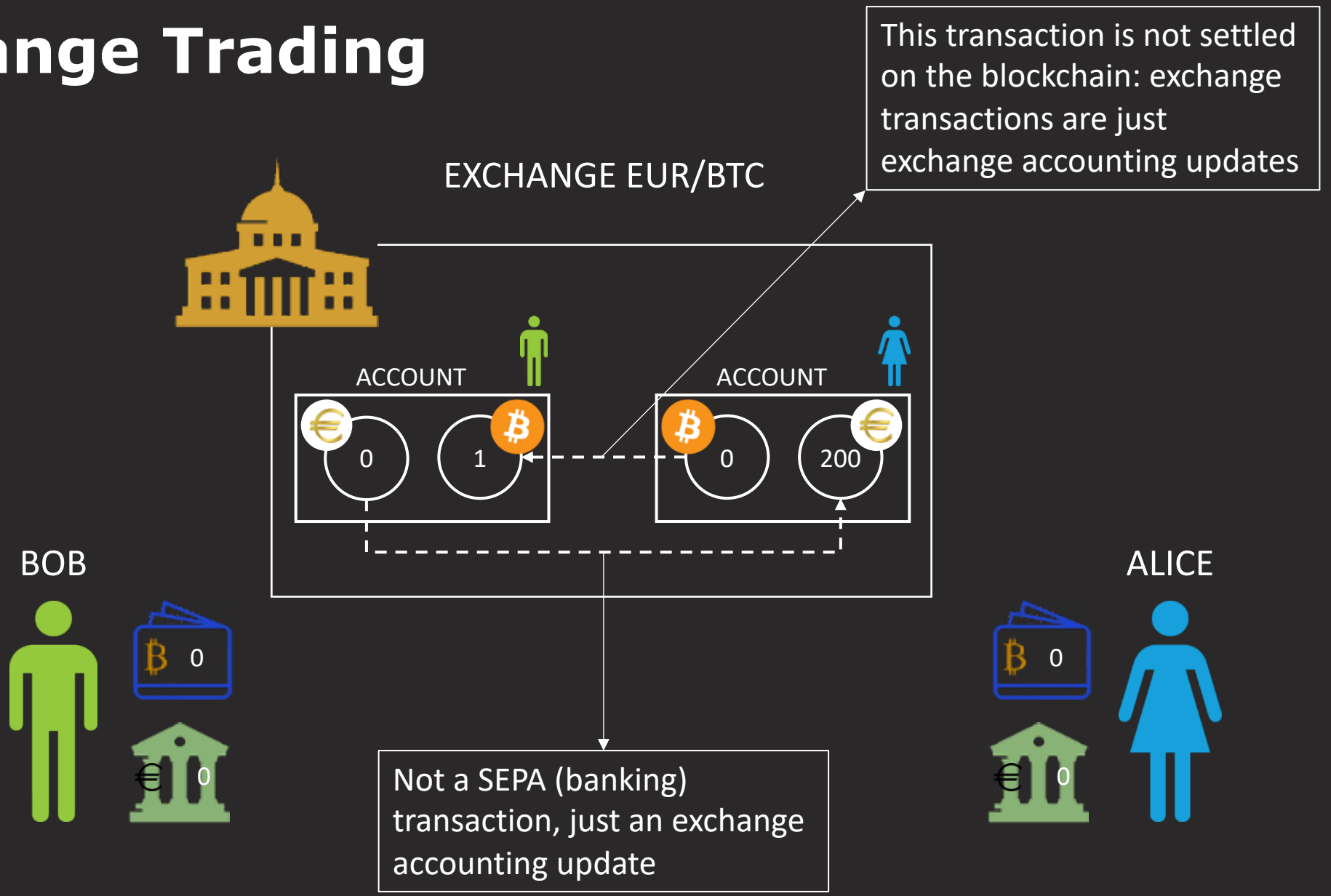


# ***Warning!!***

- At this stage bitcoins are associated to a key-pair effectively controlled by the exchange

- Usually, the Euro amount does not enjoy any kind of deposit insurance

# Exchange Trading

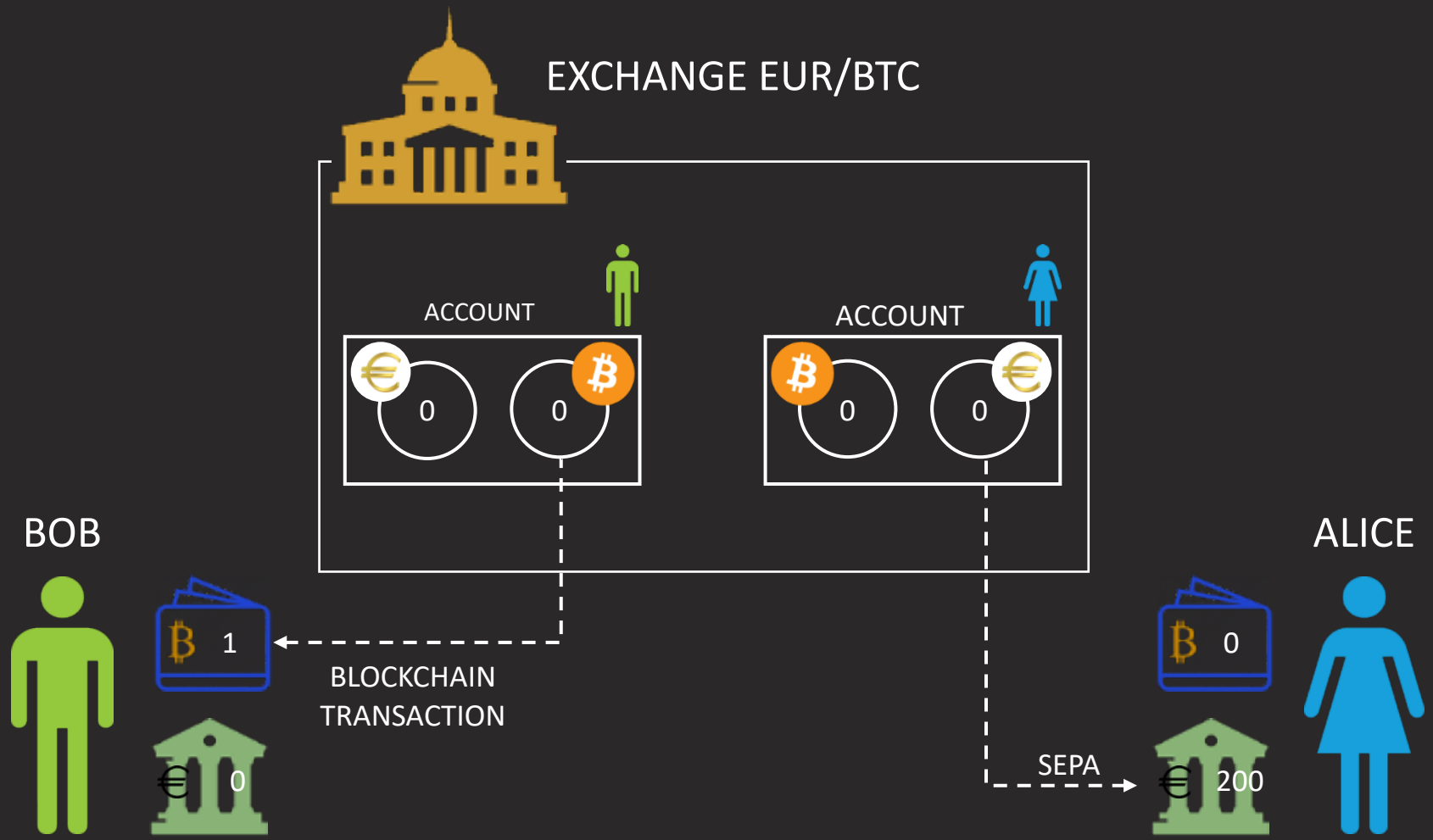


# ***Warning!! Again!***

- At this stage bitcoins are associated to a key-pair effectively controlled by the exchange

- Usually, the Euro amount does not enjoy any kind of deposit insurance

# Exchange Account Withdrawal



# Bitcoin Investing

- Bitcoins are easy to buy on exchanges, but to leave them there has proved to be unsafe (multiple hacks and incidents)
- If one does not own the bitcoins' private key, then those are not his bitcoins: bitcoins are owned by whoever can effectively spend them
- *Not your keys? Not your bitcoins!*
- Bitcoin financial sovereignty; *be your own bank!*

*Unfortunately…*

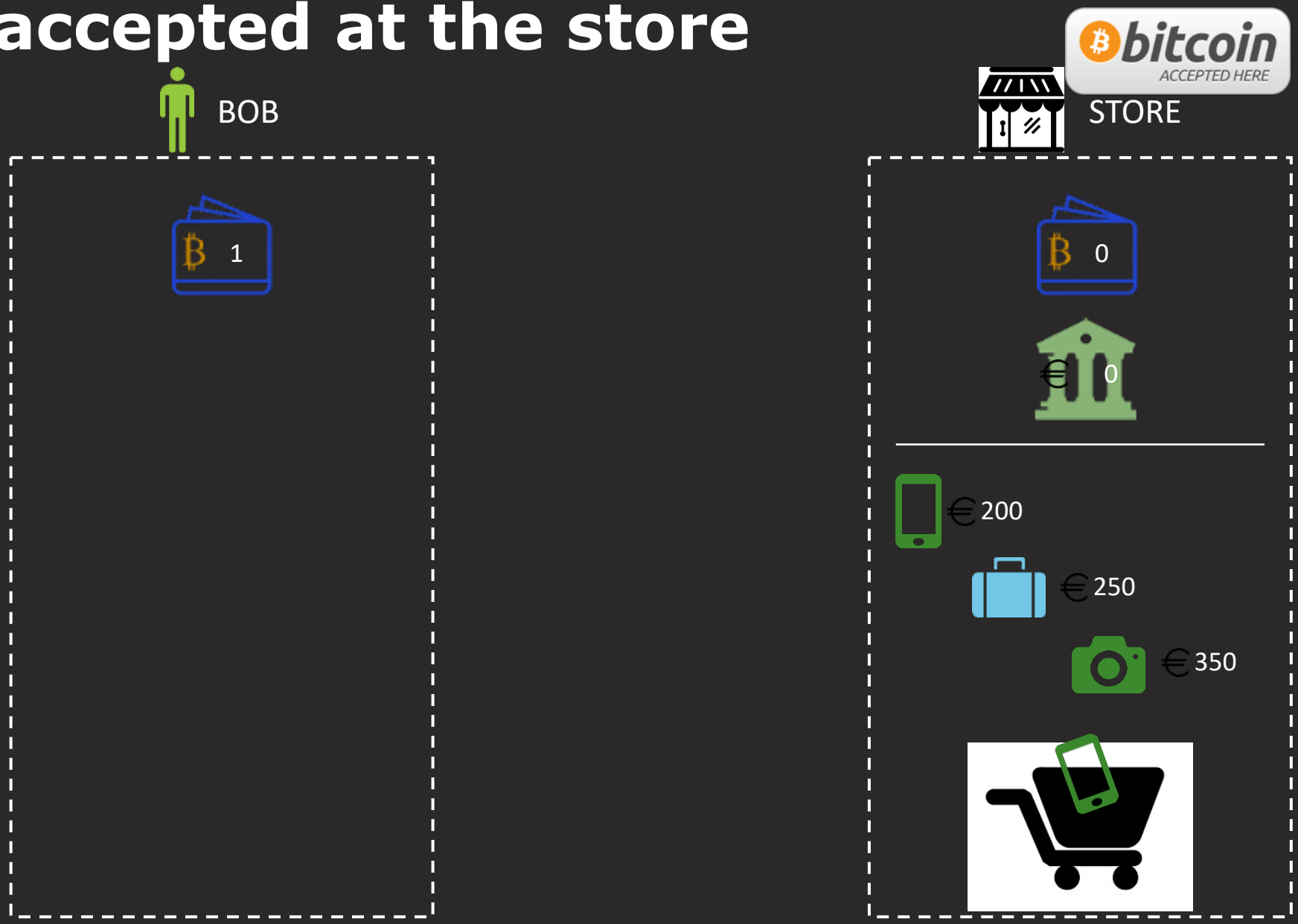
- Bitcoin safe storage is quite technical, for the time being mostly a geeky thing

# Bitcoin for Institutional Investors and HNWI

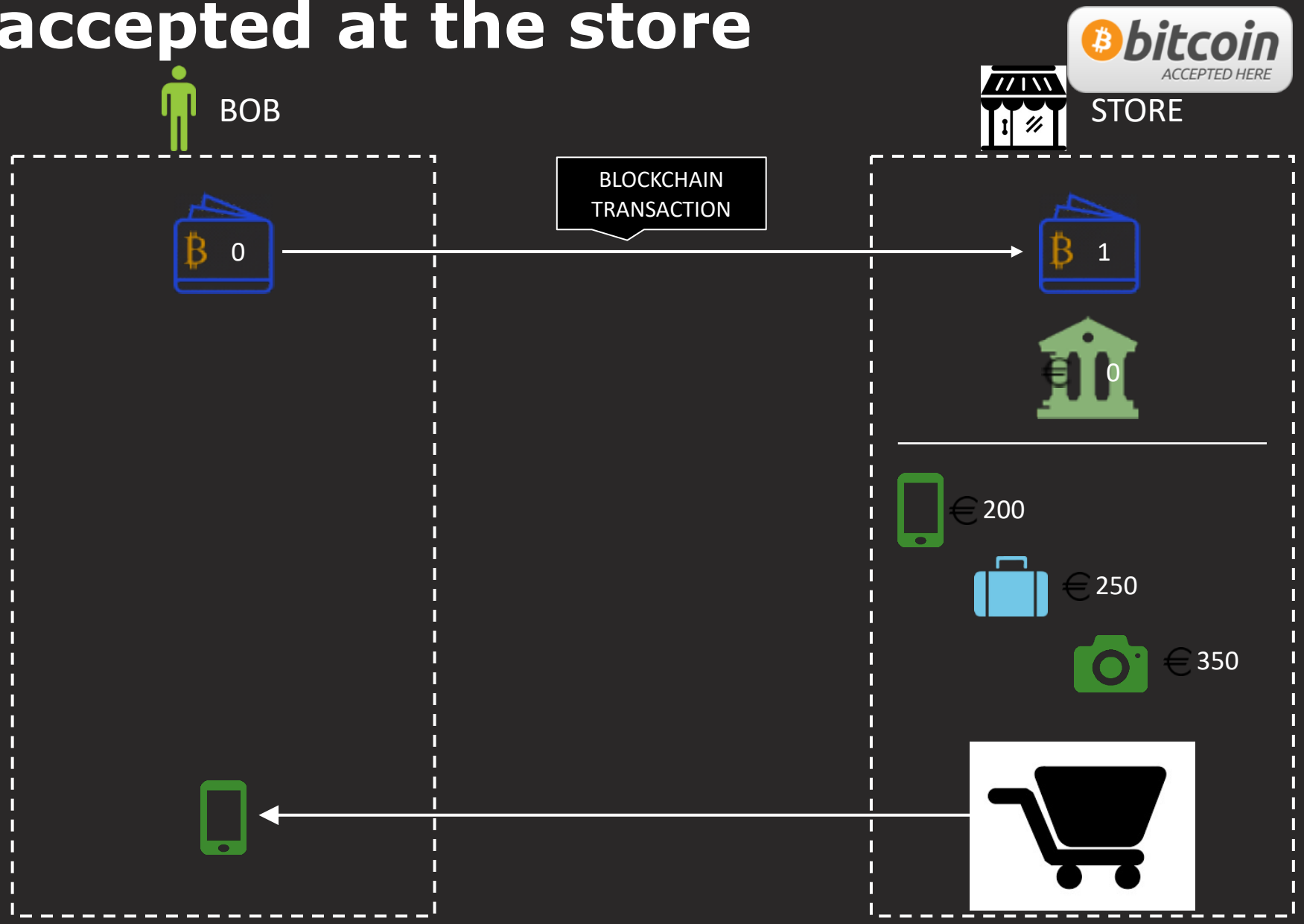
- Institutional investors: safe custody of digital assets is not their business and/or core competence. Compliance usually prescribes their assets to be held by a delegated third-party custodian
- High-net-worth individuals: their threat model (coercion, violence, ramson, etc.) suggests shielded possession

- The need for digital gold intermediaries and vaults is exploding: funds, custodians, etc.
- Professional intermediaries can be better equipped at efficient custodian selection

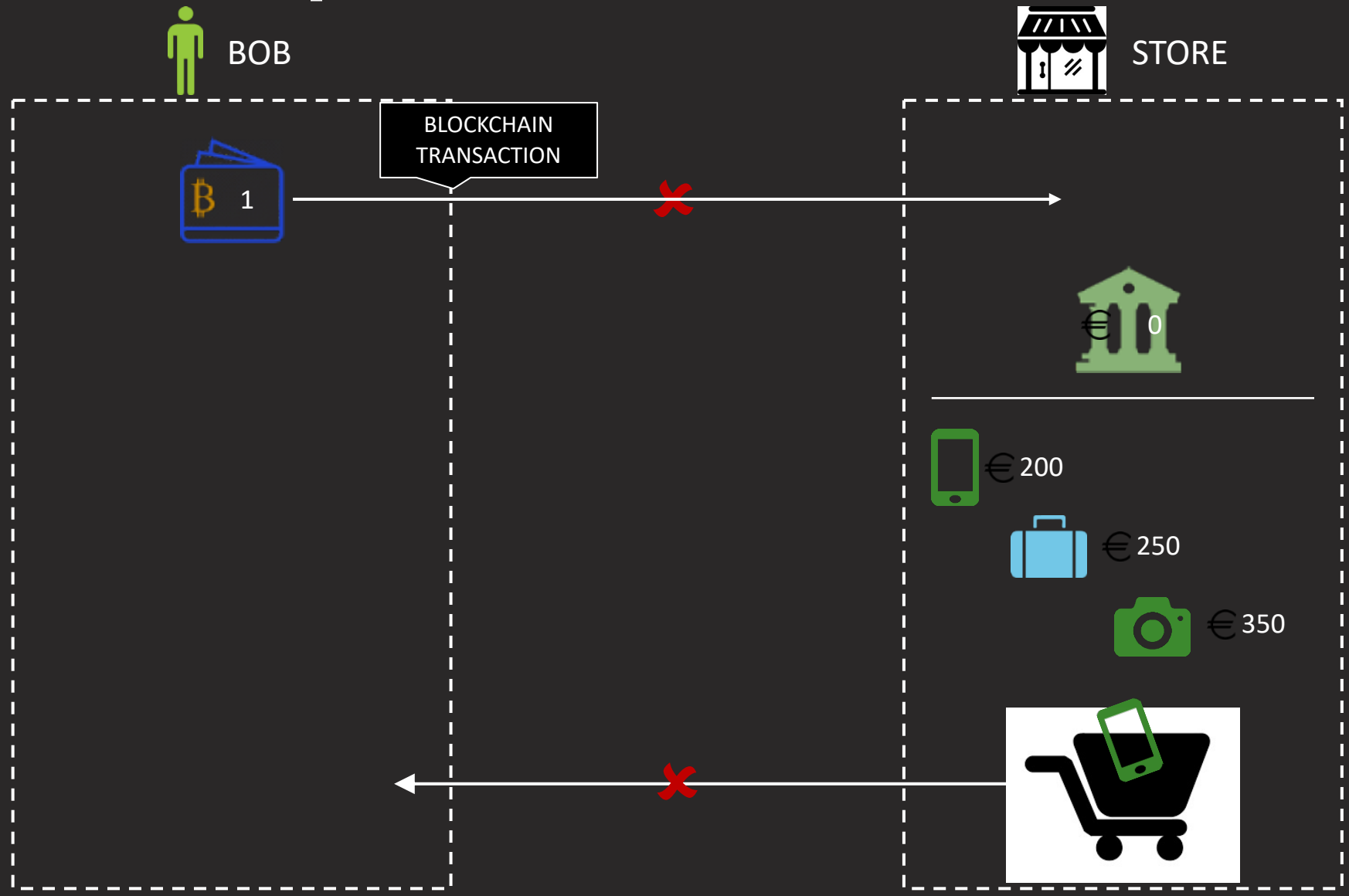
# BTC accepted at the store



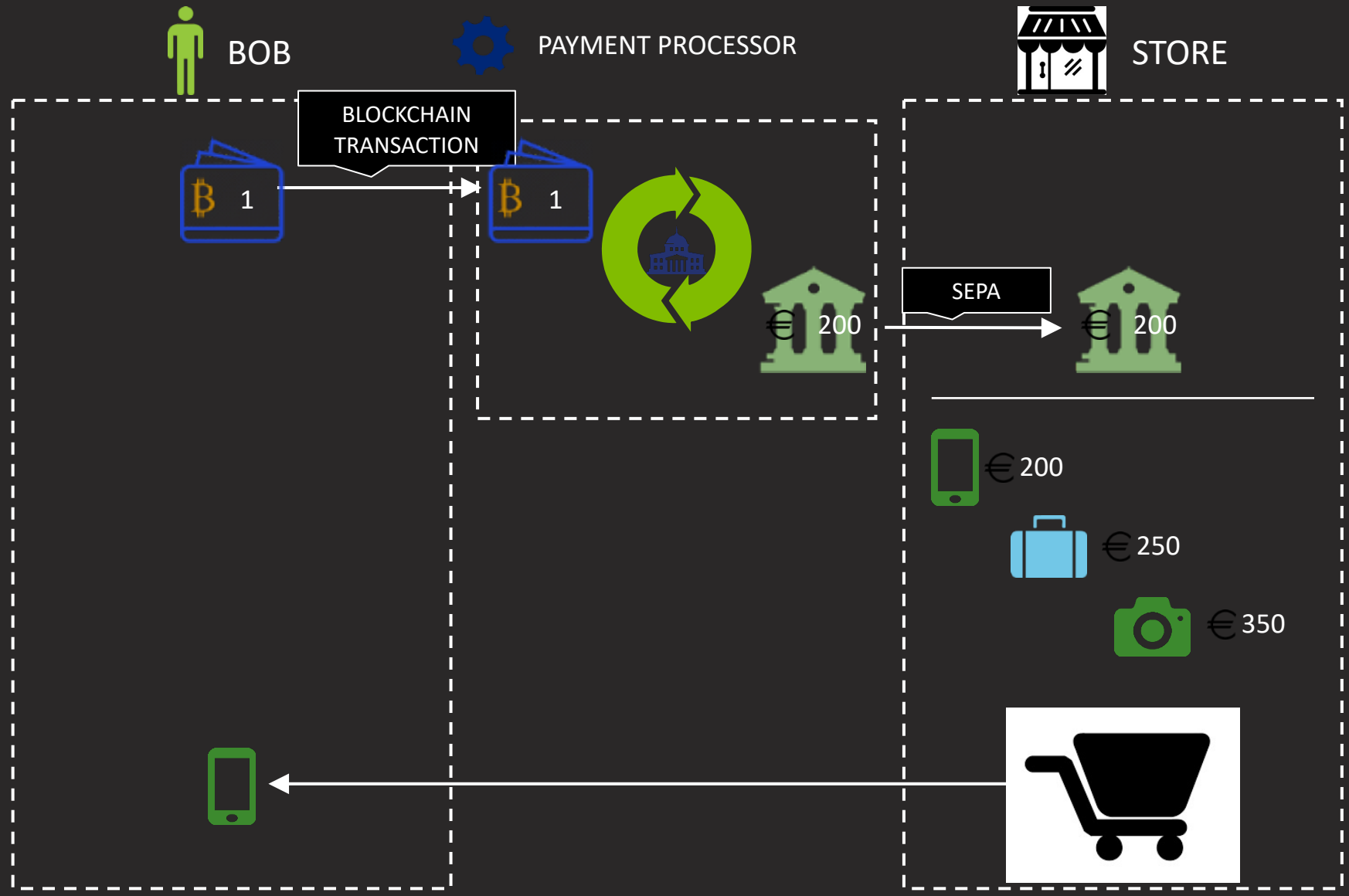
# BTC accepted at the store



# BTC *not* accepted at the store



# Payment Processor



# Blockchain and Finance

- Finance does not really need blockchain
- The blockchain economy of digital gold needs financial services
- Futures, Options, Custodian Services, ETF, etc.

# Disruptive Innovation

Incumbents that did not understand it:


Used innovation to build new business:

The entertainment industry has wasted its resources fighting MP3 and illegal p2p sharing

We now buy music and movies from iTunes, Google Play, and Amazon… NOT from Sony Universal

# Bibliography


- N. Szabo, Shelling Out: The Origins of Money (2002) https://nakamotoinstitute.org/shelling-out/
- S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2008) https://bitcoin.org/bitcoin.pdf
- F. Ametrano, Hayek Money: the Cryptocurrency Price Stability Solution (2014), http://ssrn.com/abstract=2425270
- S. Ammous, The Bitcoin Standard: The Decentralized Alternative to Central Banking (2018)
- F. Ametrano, Bitcoin as Digital Gold (2018), United Nations Department of Economic and Social Affairs; video: https://goo.gl/NkEC9w; slides: https://goo.gl/szzBXh
- F. Ametrano, YouTube playlist: https://goo.gl/qDvKXi

# Bibliografia (ITA)


- Le Iene (Mediaset): video-intervista https://www.mediasetplay.mediaset.it/video/leiene/ferdinando-ametrano_FD00000000028448
- Il Foglio: Tenete il resto della rivoluzione Bitcoin https://www.ilfoglio.it/economia/2018/11/11/news/tenete-il-resto-della-rivoluzione-bitcoin-223164
- IlSole24Ore 2017: Il Far West dell'oro digitale, http://bit.ly/2qjpvzr
- Milano-Bicocca 2017: Tre lezioni dal corso Bitcoin and Blockchain Technology https://www.youtube.com/playlist?list=PLrVvuryXHYTdzvtpzrj4wvYEhCwF6G82b
- Playlist YouTube completa: https://www.youtube.com/playlist?list=PLrVvuryXHYTdKXzpIx7aYAzqAiRpaebWp
- Intervista Bitcoin: oro digitale, finanza e tulipani (2018), https://goo.gl/eyjDJ2

# Takeaways

- Central bank digital currency is not to be expected anytime soon
- Private digital cash backed by reserves is possible
- Bitcoin (and blockchain): not a technology, a cultural paradigm shift instead
- Bitcoin solves the double spending problem (distributed consensus) relying on seigniorage revenues
- Bitcoin is the digital equivalent of gold:
  - as relevant as gold for the history of civilization and the future of money and finance; it is already bootstrapping new monetary systems
  - no correlation with other asset classes: bitcoin investing is rational diversification
- Bitcoin as investment asset has a huge upside potential: time will tell if the experiment of scarcity in the digital realm is economically and game-theoretically sustainable
- Be your own bank, if you can; else resort to reputed professionals for intermediation and custody
- The blockchain economy needs financial services for its digital gold

Digital Gold Institute

www.dgi.io info@dgi.io