



1st principle cybernetics



1st principles of cybernetics

In case of ignorance: ineffectiveness, error, degeneration

- **Ashby's Law** of requisite variety (→ information asymmetries)
- 1st law of thermodynamics: **conservation of energy** (complementary: $E=mc^2$)
- decisions based on **individual** (usually asymmetric) **evaluations/incentives**

} **POSIWID***

* »The **P**urpose **O**f a **S**ystem **I**s, **W**hat **I**t **D**oes« Stafford Beer

→ »The natural state of the free market is deflation« Jeff Booth



Part 1: Monetary Cybernetics



Monetary Cybernetics

Money vs. currency

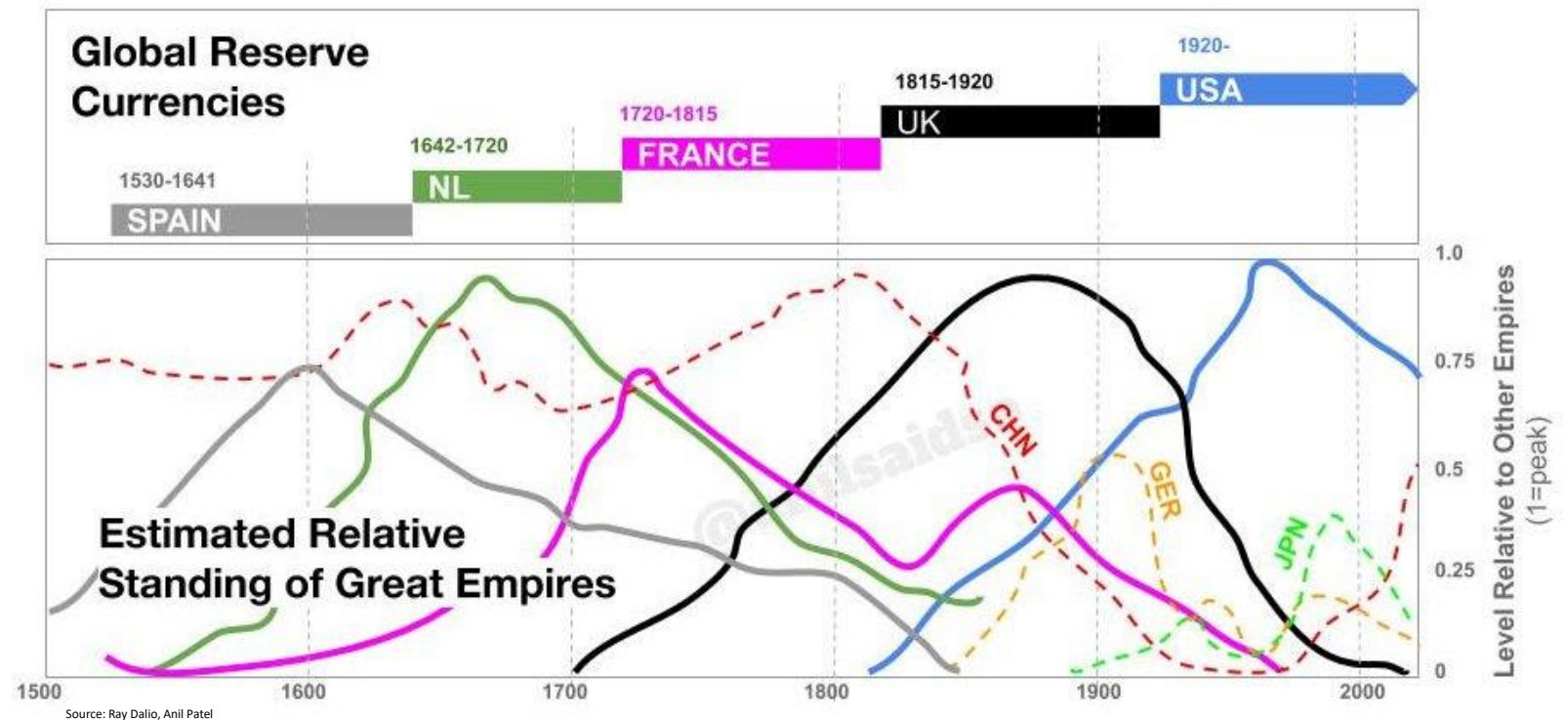
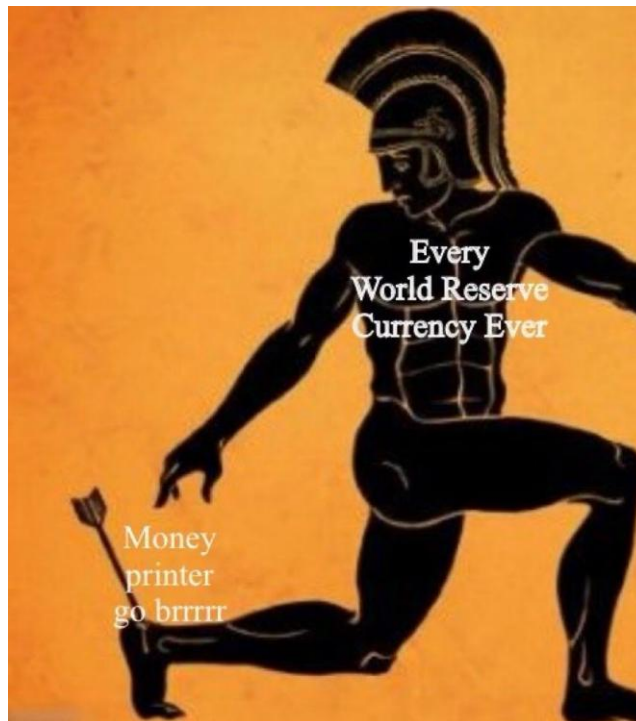


Currency := political money. Not all money is currency, not all currency is *good* money.



Monetary Cybernetics

Fundamental problem of traditional currency systems





Monetary Cybernetics

Fundamental problem in action

The Making of a Debt Spiral

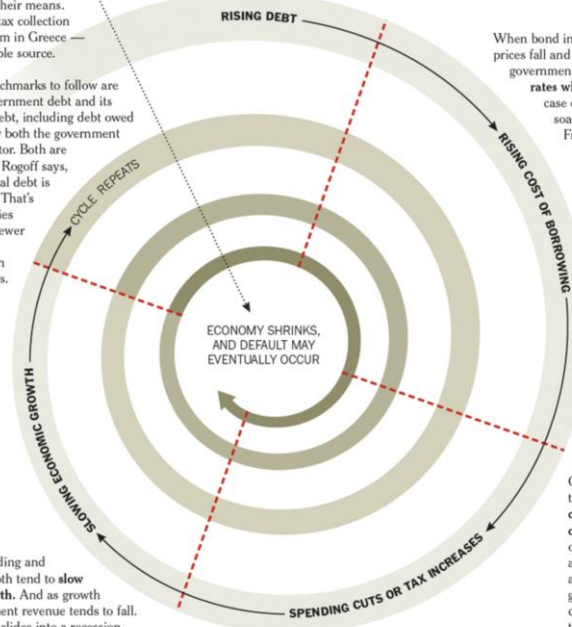
DEBT spirals: the term sounds ominous. As it should — these market vortexes are posing grave dangers to the global economy right now. A national debt crisis is a bank run writ large, says Kenneth Rogoff, an economics professor at Harvard and co-author with Carmen M. Reinhart of "This Time Is Different," a history of financial crises. When a country like Greece goes deep into debt, bond investors start to worry they won't get their money back. What can happen next is a debt spiral, a vicious circle of sinking confidence, rising borrowing costs and, ultimately, rising debt burdens. — DYLAN LOEB
McCLAIN Related Article »

HOW DEBT SPIRALS WORK

Countries **run up debt** for many reasons, not the least of which is that they simply spend beyond their means. But inefficient tax collection — a big problem in Greece — is another trouble source.

Two useful benchmarks to follow are a country's government debt and its total external debt, including debt owed to foreigners by both the government and private sector. Both are significant, Mr. Rogoff says, but high external debt is a bigger worry. That's because countries typically have fewer options when negotiating with foreign creditors.

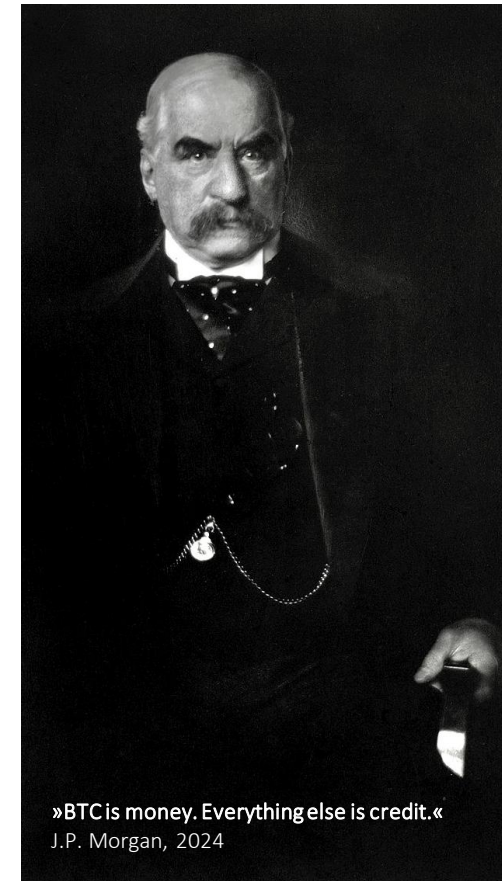
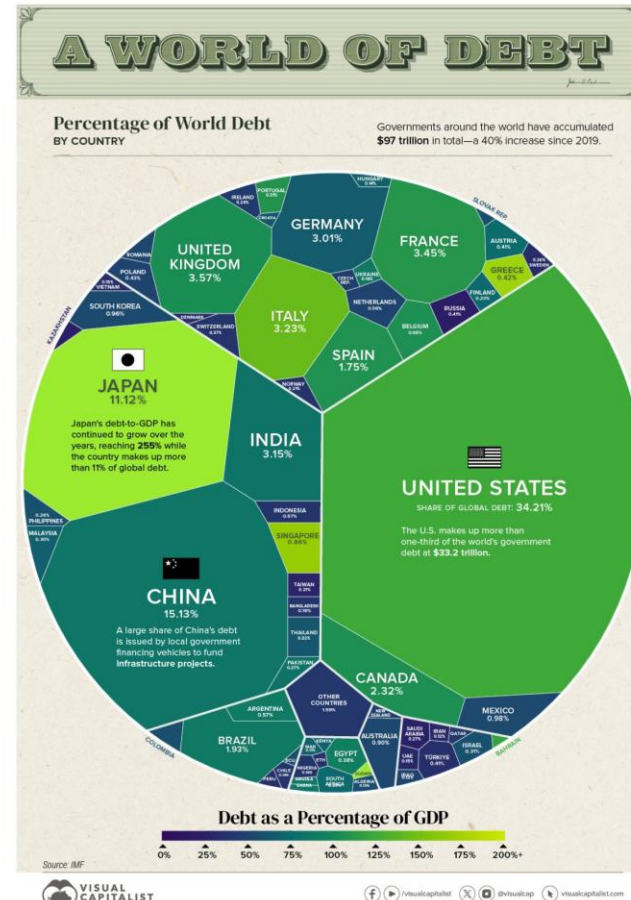
Reducing spending and raising taxes both tend to **slow economic growth**. And as growth slows, government revenue tends to fall. If the economy slides into a recession, revenue may fall steeply, starting the cycle of government shortfalls all over again.



When bond investors lose confidence, bond prices fall and yields rise. As a result, the government must **pay higher interest rates** when it borrows money. In the case of Greece, bond yields have soared to 15.5 percent as of Friday from 5 percent in early December 2009.

Governments can try to get their fiscal houses in order by **cutting spending, raising taxes or closing tax loopholes**, among other measures. During a crisis, a government may have to adopt such measures in order to get financial aid and restore confidence. But sometimes these are too little, too late. And they are invariably unpopular within the country.

Source: Guilbert Gates for The New York Times

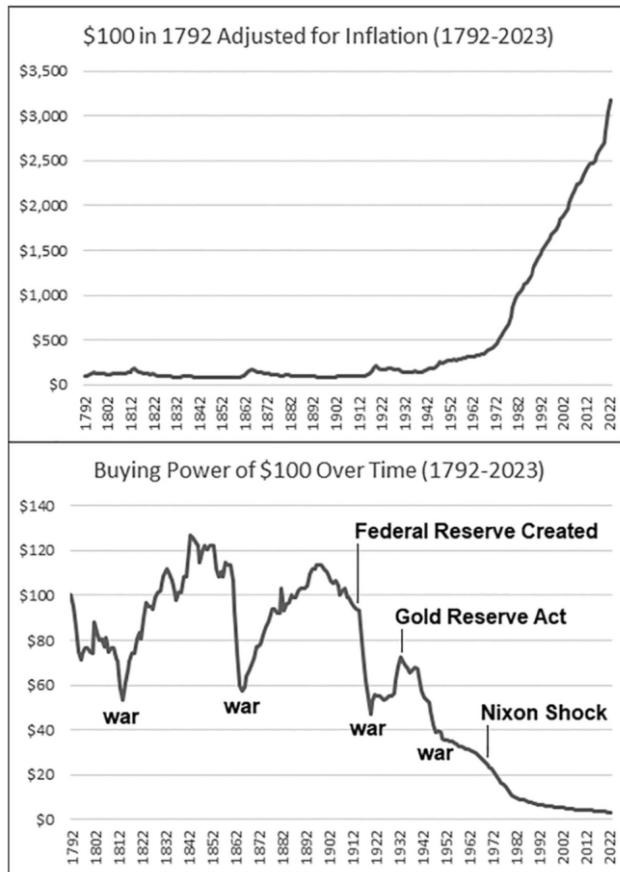


»BTC is money. Everything else is credit.«
J.P. Morgan, 2024



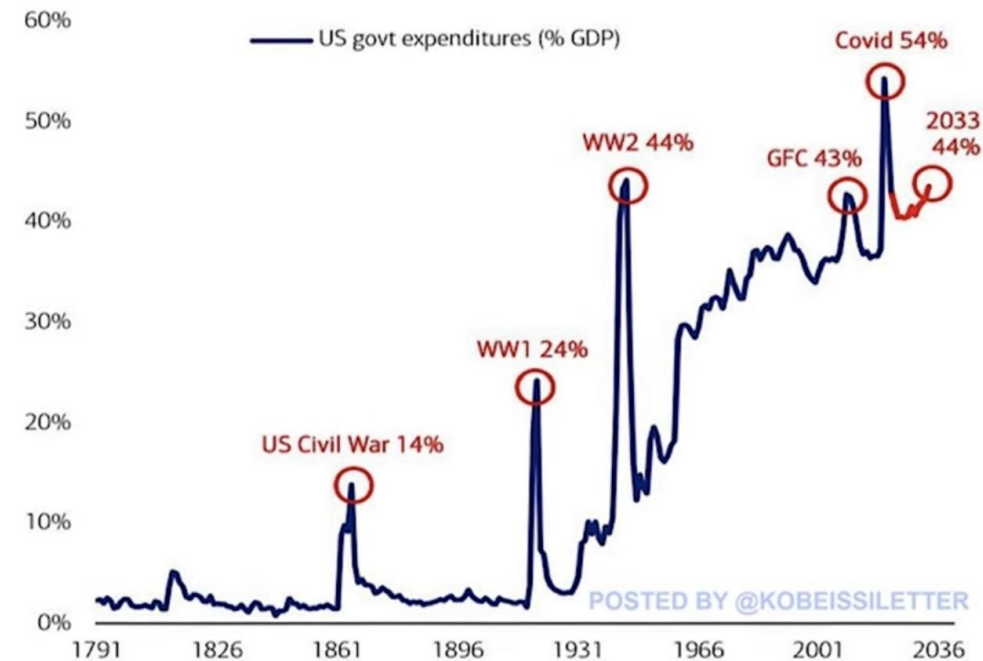
Monetary Cybernetics

»When money is easy to make, society begins to break.«



Source: Lyn Alden, Broken Money Chartbook

Exhibit 3: US government spending is equal to 44% of the economy
US government expenditures % GDP since 1791

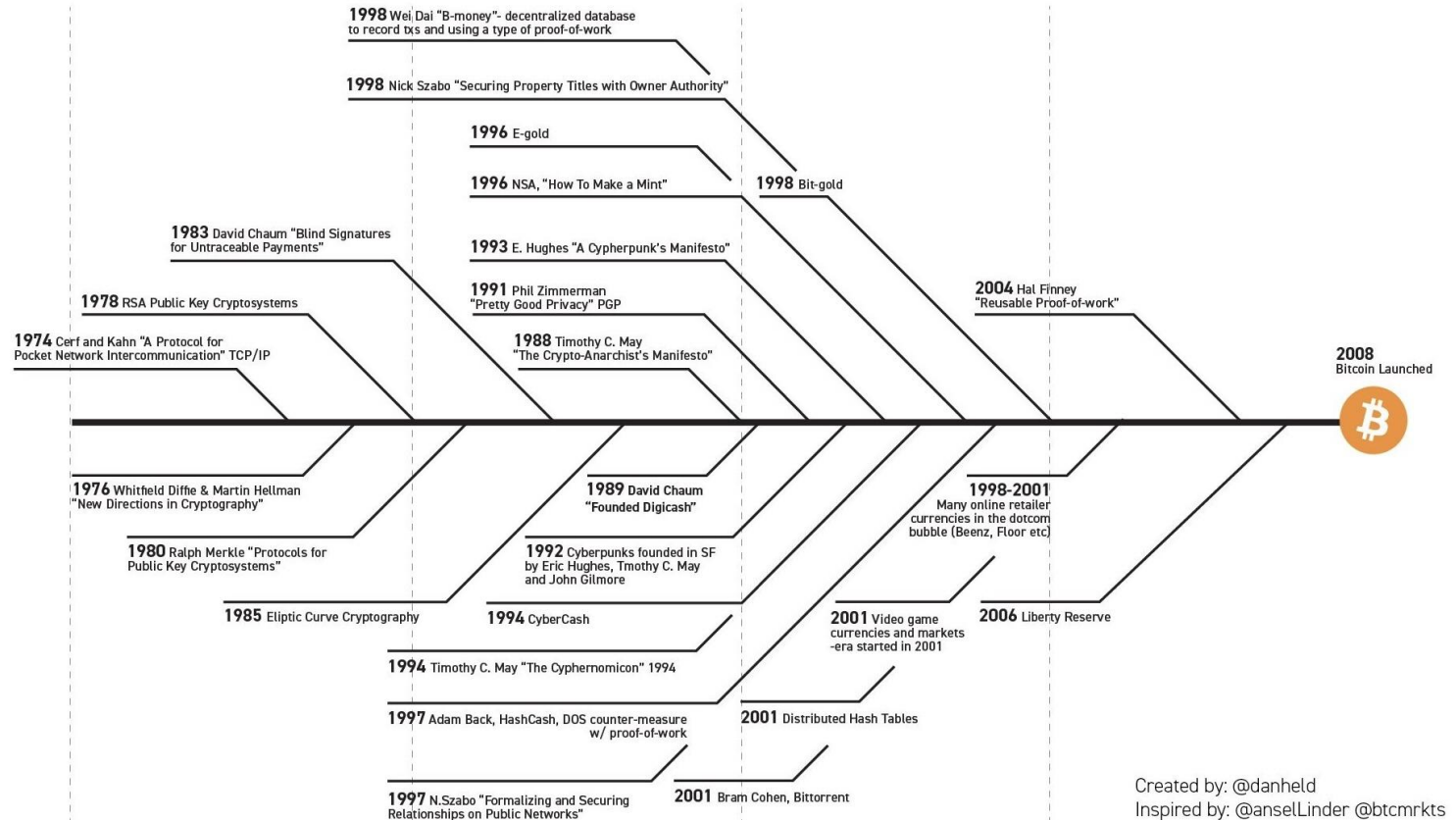


Source: BofA Global Investment Strategy, Bloomberg



Bitcoin's prehistory:

More than 40 years of Research & Development



Created by: @danheld
Inspired by: @anselLinder @btcmrks



Monetary Cybernetics

Best environmental effects despite FUD and disinformation campaigns



Natural-ecological effects:

- efficient management of electricity grids
- mitigation of natural gas flaring / venting
- improving the economics of nuclear power
- accelerating adoption of green energy
 - ocean thermal energy conversion (OTEC)
 - untapped heat recovery
 - geothermal and hydroelectric energy, etc.

■ ...

Humanitarian-ecological effects:

- secure asset protection in war/escape scenarios
- effective financial protection in unstable, hostile systems
- effective financial antidiscrimination and financial freedom
- secure remittances without high fees
- fraud protection (tamper-proof timechain)
- uncensorable communication (e.g. NOSTR)
- banking services for the unbanked
- economic advancement for peripheral, disadvantaged regions
- protection against state mismanagement (promoting democracy)

■ ...



Monetary Cybernetics

Bitcoin: optimal properties, e.g.

»No man knows what to do against the really new.« Ashby

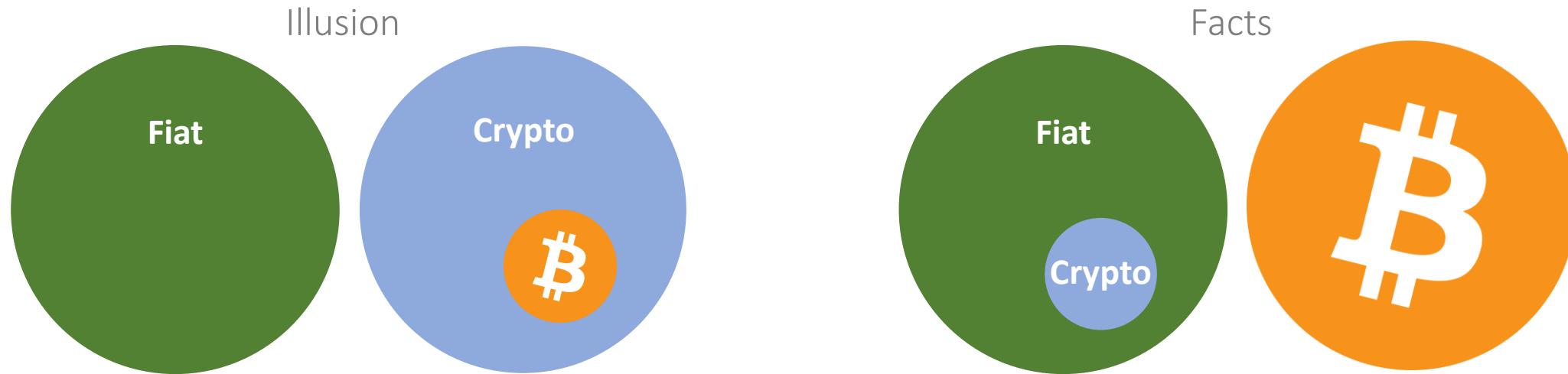
- not easily comprehensible (which enabled an undisturbed development
»under the radar« when the network was still vulnerable)
- thermodynamic-natural-law-foundation (proof of work)
- robust instrumentalisation of human flaws (no need to create unstable system dynamics through virtue signalling)
- highest possible frequency with fastest global final settlement (usually < 1 h)
- comparatively minimal costs with minimal energy requirements
- qualitative dominant asset/money properties
- efficient scalability (base layer → layer n)
- de facto unchangeable absolute scarcity
- no counterparty risk (if handled correctly)
- antifragility
- unkonfiscateability
- global censorship resistance
- unfalsifiable, audit-proof (triple-entry-accounting)
- perfect (pseudonymous) transparency
- perfect combination of individually imperfect components

	 GOLD	 BITCOIN	 FIAT CURRENCY	Source: David Lee @Medium
 DURABLE	+	+	—	While all are physically durable, fiat currency over history has not maintained purchasing power durability
 DIVISIBLE	—	+	+	Physical gold is only divisible to small pieces; bitcoin is divisible to eight decimals
 FUNGIBLE	+	+	—	Gold and bitcoin are fungible, but fiat currency is not fungible with other fiat (US Dollar is not fungible with Canadian dollar)
 PORTABLE	—	+	+	Gold has a high value to weight ratio, but compared to the others is still heavy and cumbersome to transport
 VERIFIABLE	—	+	—	Both gold and fiat currency have been counterfeited; gold can be verified but only through cumbersome assay
 SCARCE	+	+	—	Gold is scarce, bitcoin is scarce and finite; the only constraint on fiat currency is willingness of government or central bank
 TRACK RECORD	+	—	—	Gold has the longest track record as money and maintaining purchasing power; bitcoin's history is the shortest; fiat currency has a poor track record ¹



Monetary Cybernetics

Illusion vs. facts: relationship between Fiat, Bitcoin and altcoins (»crypto«)



- Fiat-currencies: the *state* can print as much money as it wants (→ inflation).
- Altcoins (»crypto«): *anyone* can print as much money as they want (→ greater fools and/or fraud).
- Bitcoin: *nobody* can print money (→ guaranteed absolute scarcity, ethically immaculate).



Monetary Cybernetics

Status 2024: NGU and game theory in action

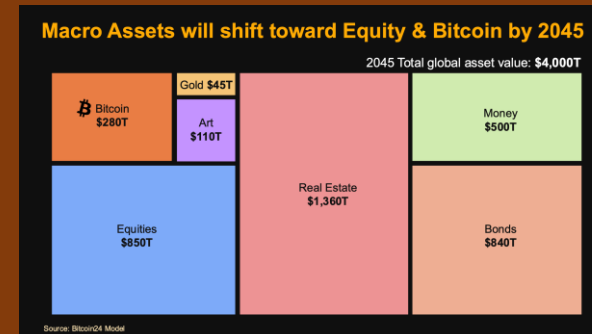
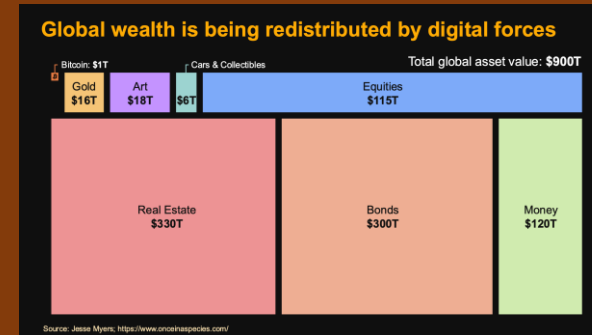
»Bitcoin will be adopted like gunpowder: if you don't own it, you'll be it's victim.«

- start of institutional adoption (most successful ETF of all time)
- new FASB rule (fair value accounting)
- Bitcoin as US election campaign topic
- national strategic reserve asset discussions
- geopolitical prisoners dilemma:

		Don't Buy	Buy
Nation B	Don't Buy	1 Central banking is unaffected.	2 A buys early and gets rich. B is a late adopter and poor.
	Buy	3 B buys early and gets rich. A is a late adopter and poor.	4 A & B become early adopters but give up monopoly on money.

<https://www.nasdaq.com/articles/ukraines-blueprint-to-bitcoin-adoption-2021-09-13>

- increasing demonetization of other asset classes to be expected:





Monetary Cybernetics

Bitcoin's weakness: not easy to understand



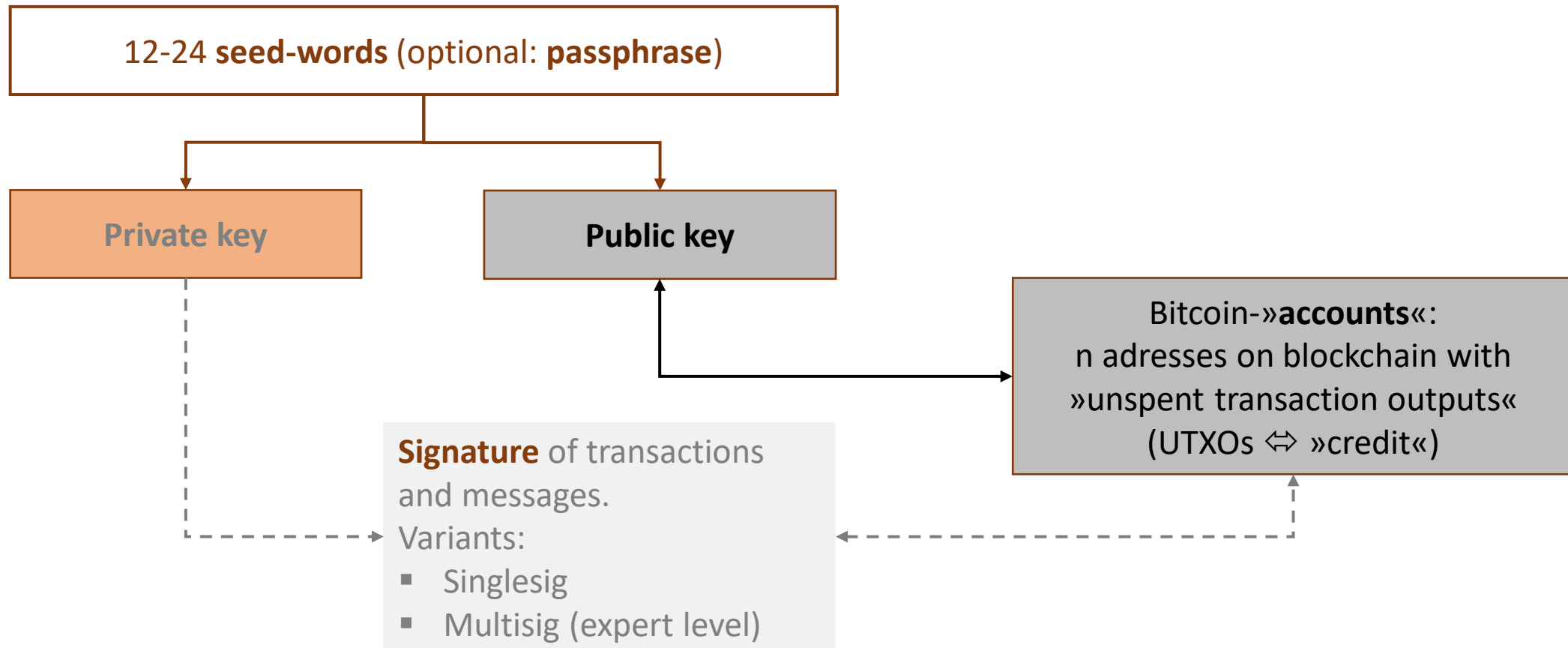
Cedric Youngelman ⚡ 🔵
@CedYoungelman

#Bitcoin ₿ is everything you don't know about money combined with everything you don't about computers combined with everything you don't know about economics combined with everything you don't about game theory combined with everything you don't about thermodynamics.



Bitcoin Starter Package

Base Layer: from secret to transaction





Bitcoin Starter Package

Base layer: 21M Bitcoin from 2024 words (BIP39)

2,099,999,997,690,000 sats from:

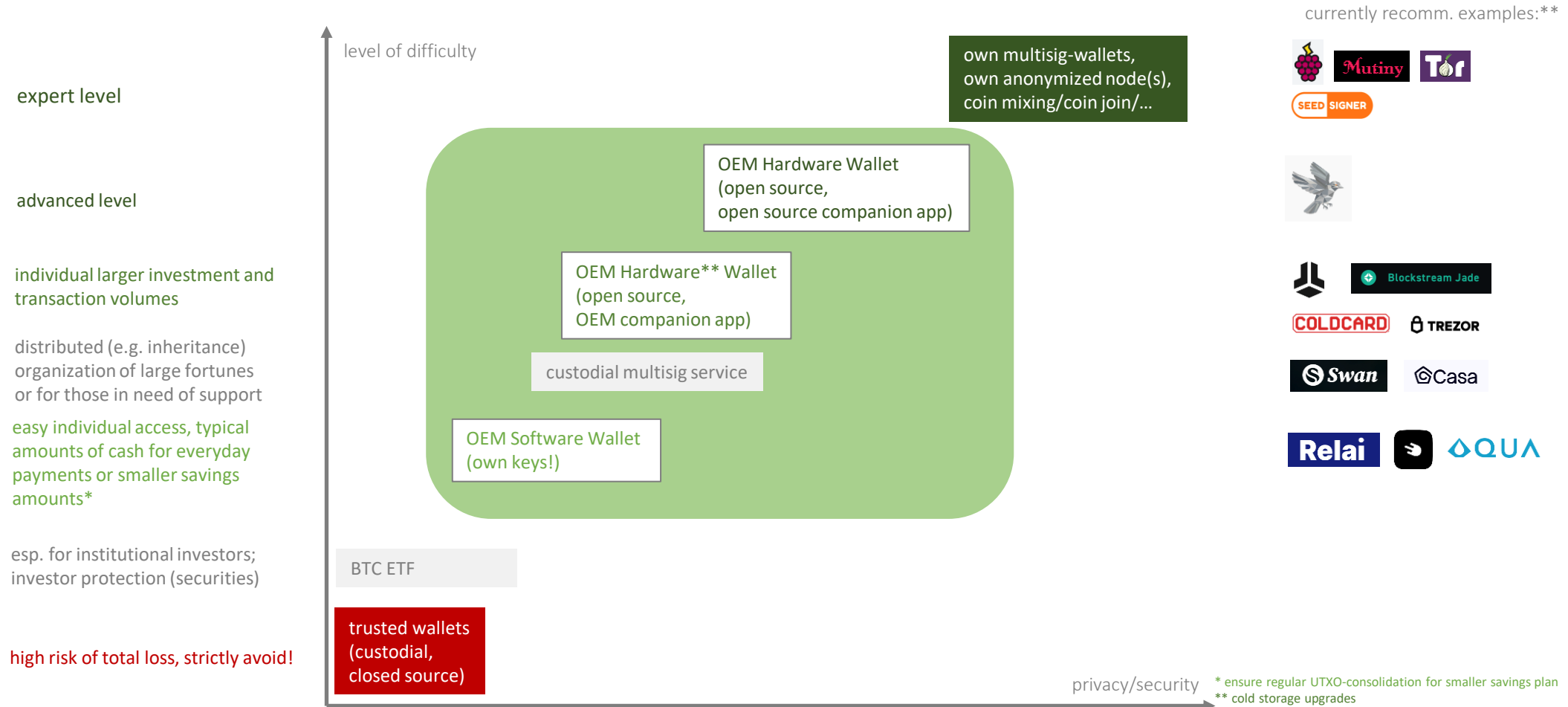
abandon ability able about above absent absorb account access accident account accuse achieve acid acoustic acquire across act action actor actress actual adapt add addict address adjust admit adult advance advice aerobic affair afford afraid again age agent agree ahead aim air airport aisle alarm album alcohol alert alien all alley allow almost alone alpha already also alter always amateur amazing among amount amused analyst anchor ancient anger angle angry animal ankle announce annual another answer antenna antique anxiety any apart apology appear apple approve april arch arctic area arena argue arm armed armor army around arrange arrest arrive arrow art artefact artist artwork ask aspect assault asset assist assume asthma athlete atom attack attend attitude attract auction audit august aunt author auto autumn average avocado avoid awake aware away awesome awful awkward axis baby bachelor bacon badge bag balance balcony ball bamboo banana banner bar barely bargain barrel base basic basket battle beach bean beauty because become beef before begin behave behind believe below belt bench benefit best betray better between beyond bicycle bid bike bind biology bird birth bitter black blade blame blanket blast bleak bless blind blood blossom blouse blue blur blush board boat body boil bomb bone bonus book boost border boring borrow boss bottom bounce box boy bracket brain brand brass brave bread breeze brick bridge brief bright bring brisk broccoli broken bronze broom brother brown brush bubble buddy budget buffalo build bulb bulk bullet bundle bunker burden burger burst bus business busy butter buyer buzz cabbage cabin cable cactus cage cake call calm camera camp can canal cancel candy cannon canoe canvas canyon capable capital captain car carbon card cargo carpet carry cart case cash casino castle casual cat catalog catch category cattle caught cause caution cave ceiling celery cement census century cereal certain chair chalk champion change chaos chapter charge chase chat cheap check cheese chef cherry chest chicken chief child chimney choice choose chronic chuckle chunk churn cigar cinnamon circle citizen city civil claim clap clarify claw clay clean clerk clever click client cliff climb clinic clip clock clog close cloth cloud clown club clump cluster clutch coach coast coconut code coffee coil coin collect color column combine come comfort comic common company concert conduct confirm congress connect consider control convince cook cool copper copy coral core corn correct cost cotton couch country couple course cousin cover coyote crack cradle craft cram crane crash crater crawl crazy cream credit creek crew cricket crime crisp critic crop cross crouch crowd crucial cruel cruise crumble crunch crush cry crystal cube culture cup cupboard curious current curtain curve cushion custom cute cycle dad damage damp dance danger daring dash daughter dawn day deal debate debris decade december decide decline decorate decrease deer defense define defy degree delay deliver demand demise denial dentist deny depart depend deposit depth deputy derive describe desert design desk despair destroy detail detect develop device devote diagram dial diamond diary dice diesel diet differ digital dignity dilemma dinner dinosaur direct dirt disagree discover disease dish dismiss disorder display distance divert divide divorce dizzy doctor document dog doll dolphin domain donate donkey donor door dose double dove draft dragon drama drastic draw dream dress drift drill drink drip drive drop drum dry duck dumb dune during dust dutch duty dwarf dynamic eager eagle early earn earth easily east easy echo ecology economy edge edit educate effort egg eight either elbow elder electric elegant element elephant elevator elite else embark embody embrace emerge emotion employ empower empty enable enact end endless endorse enemy energy enforce engage engine enhance enjoy enlist enough enrich enroll ensure enter entire entry envelope episode equal equip era erase erode erosion error erupt escape essay essence estate eternal ethics evidence evil evoke evolve exact example excess exchange excite exclude excuse execute exercise exhaust exhibit exile exist exit exotic expand expect expire explain expose express extend extra eye eyebrow fabric face faculty fade faint faith fall false fame family famous fan fancy fantasy farm fashion fat fatal father fatigue fault favorite feature february federal fee feed feel female fence festival fetch fever few fiber fiction figure file film filter final find fine finger finish fire firm first fiscal fish fit fitness fix flag flame flash flat flavor flee flight flip float flock floor flower fluid flush fly foam focus fog foil fold follow food foot force forest forget fork fortune forum forward fossil foster found fox fragile frame frequent fresh friend fringe frog front frost frown frozen fruit fuel fun funny furnace fury future gadget gain galaxy gallery game gap garage garbage garden garlic garment gas gasp gate gather gauge gaze general genius genre genuine gesture ghost giant gift giggle ginger giraffe girl give glad glance glare glass glide glimpse globe gloom glory glow glue goat goddess gold good goose gorilla gospel gossip govern gown grab grape grass gravity great green grid grief grit grit grocery group grow grunt guess guide guilt guitar gun gym habit hair half hammer hamster hand happy harbor hard harsh harvest hat have hawk hazard head health heart heavy hedgehog height hello helmet help hen hero hidden high hill hint hip hire history hobby hockey hold hole holiday hollow home honey hood hope horn horror horse hospital host hotel hour hover hub huge human humble hummer hundred hungry hunt hurdle hurry hurt husband hybrid ice icon idea identify idle ignore ill illegal illness image imitate immense immune impact impose improve impulse inch include income increase index indicate indoor industry infant inflict inform inhale inherit initial inject injury inmate inner innocent inquire inquiry insane insect inside inspire install intact interest into invest invite involve iron island isolate issue item ivory jacket jaguar jar jazz jealous jeans jelly jewel job join joke journey joy judge juice jump jungle junior junk just kangaroo keen keep ketchup key kick kid kidney kind kingdom kiss kit kitchen kite kitten kiwi knee knife knock know lab label labor ladder lady lake lamp language laptop large later latin laugh laundry lava law lawn lawsuit layer lazy leader leaf learn leave lecture left leg legal legend leisure lemon lend length lens leopard lesson letter level liar liberty library license life lift light like limb limit link lion liquid list little live lizard load loan lobster local lock logic lonely long loop lottery loud lounge love loyal lucky luggage machine mad magic magnet maid major make mammal man manage mandate mango mansion manual maple marble march margin marine market marriage mask mass master match material math matrix matter maximum maze meadow mean measure meat mechanic medal media melody melt member memory mention menu mercy merge merit merry mesh message metal method middle midnight milk million mimic mind minimum minor minute miracle mirror misery miss mistake mix mixed mixture mobile model modify mom moment monitor monkey monster month moon moral more morning mosquito mother motion motor mountain mouse move movie much muffin mule multiply muscle museum mushroom music must mutual myself mystery myth naive name napkin narrow nasty nation nature near neck need negative neglect neither nephew nerve nest net network neutral never news next nice night noble noise nominee noodle normal north nose notable note nothing notice novel now nuclear number nurse nut oak obey object oblige obscure observe obtain obvious ocean october odor off offer office often oil okay old olive olympic omit once one onion online only open opera opinion oppose option orange orbit orchard order ordinary organ orient original orphan ostrich other outdoor outer output outside oval oven over own owner oxygen oyster ozone pact paddle page pair palace palm panda panel panic panther paper parade parent park parrot party pass patch path patient patrol pattern pause pave payment peace peanut pear peasant pelican pen penalty pencil people pepper permit person pet phone photo phrase physical piano picnic picture piece pig pigeon pill pilot pink pioneer pipe pistol pitch pizza place planet plastic plate play please pledge pluck plug plunge poem poet point polar pole police pond pony pool popular portion position possible post potato pottery poverty powder power practice praise predict prefer prepare present pretty prevent price pride primary print priority prison private prize problem process produce profit program project promote prop property prosper protect proud provide public pudding pulp pulp pulse pumpkin punch pupil puppy purchase purity purpose purse push put puzzle pyramid quality quantum quarter question quick quit quiz quote rabbit raccoon race rack radar radio rail rain raise rally ramp ranch random range rapid rare rate rather raven raw razor ready real reason rebel rebuild recall receive recipe recode recycle reflect reform reject regular reject relax release relief rely remain remember remind remove render renew rent reopen repair repeat replace report require rescue resemble resist resource response result retire retreat return reunion reveal review reward rhythm rib ribbon rice rich ridge rifle right rigid ring riot riddle risk ritual river road roast robot robust rocket romance room rose rotate rough round route royal rubber rude rug rule run runway rural sad saddle sadness safe sail salad salmon salon salt salute same sample sand satisfy satoshi sauce sausage save say scale scan sarcasm scatter scene scheme school science scissors scorpion scot scrap screen script scrub sea search season seat second section security seed seek segment select sell seminar senior sense sentence series service session settle setup seven shadow shaft shallow share shed shell sheriff shield shift shine ship shiver shock shoe shoot shop short shoulder shove shrimp shrug shuffle shy sibling sick side siege sight sign silent silk silly silver similar simple since sing siren sister situate six size skate sketch ski skill skin skirt skull slab slam sleep slender slice slide slight slim slogan slot slow slush small smart smile smoke smooth snack snake snap sniff snow soap soccer social sock soda soft solar soldier solid solution solve someone song soon sorry sort soul sound soup source south space spare spatial spawn speak special speed spell spend sphere spice spider spike spin spirit split spoil sponsor spoon sport spot spray spread spring spy square squeeze squirrel stable stadium staff stage stairs stamp stand start state stay steak steel stem step stereo stick still sting stock stomach stone stool story stove strategy street strike strong struggle student stuff stumble style subject submit subway success such sudden suffer sugar suggest suit summer sun sunny sunset super supply supreme sure surface surge surprise surround survey suspect sustain swallow swamp swap swarm swear sweet swift swim swing switch sword symbol symptom syrup system table tackle tag tail talent talk tank tape target task taste tattoo taxi teach team tell ten tenant tennis tent term text thank that theme then theory there they thing this thought three thrive throw thumb thunder tick tide tiger tilt timber time tiny tin tired tissue tile tobacco today toddler toe together toilet token tomato tomorrow tone tongue tonight tool tooth top topic topple torch tornado tortoise toss total tourist toward tower town toy track trade traffic tragic train transfer trap trash travel tray treat tree trend trial tribe trick trigger trim trip trophy trouble truck true truly trumpet trust truth try tube tuition tumble tuna tunnel turkey turn turtle twelve twenty twice twin twist two type typical ugly umbrella unable unaware unbecome uncover under undo unfair unfold unhappy uniform unique unit universe unknown unlock until unusual unveil update upgrade uphold upon upper upset urban urge usage use used useful useless usual utility vacant vacuum vague valid valley valve van vanish vapor various vast vault vehicle velvet vendor venture venue verb vessel veteran viable vibrant vicious victory video view village vintage violin virtual virus visa visit visual vital vivid vocal voice void volcano volume vote voyage wage wagon wait walk wall walnut want warfare warm warrior wash wasp waste water wave way wealth weapon wear weasel weather web wedding weekend weird welcome west wet whale what wheat wheel when where whip whisper wide width wife wild will win window wine wing wink winner winter wire wisdom wise wish witness wolf woman wonder wood wool word work world worry worth wrap wreck wrestle wrist write wrong yard year yellow you young youth zebra zero zone zoo

→ e.g. key=00110010100010000110100111000100000110011011101100001101001000000010101100000101111011001110110001100101010110100111100011000011000000111011111011001100010100111011110101010010011010011100000111010001001100100111000011101000100110010011100001110100010011001001110001000101110001
→ hex: 328869C419B80D203582F629167F4E5569E18607BF6629EF549A6E1D132788B8
→ in hexatridecimal (base 26): 19CA603HVNWNZNPHDTMB48AEV7E3MU43JHUGK4WFMULKLBHOEY3



Bitcoin Starter Package

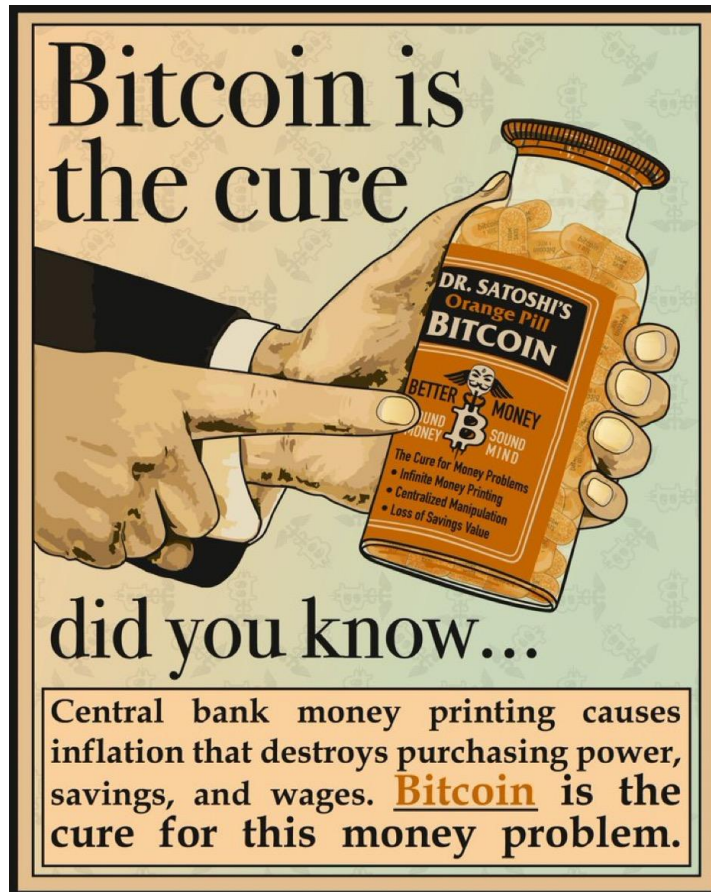
Base Layer: »Not your keys, not your coins.«





»Bitcoin fixes this«

21 = 42/2: Bitcoin as the answer to half of all questions...



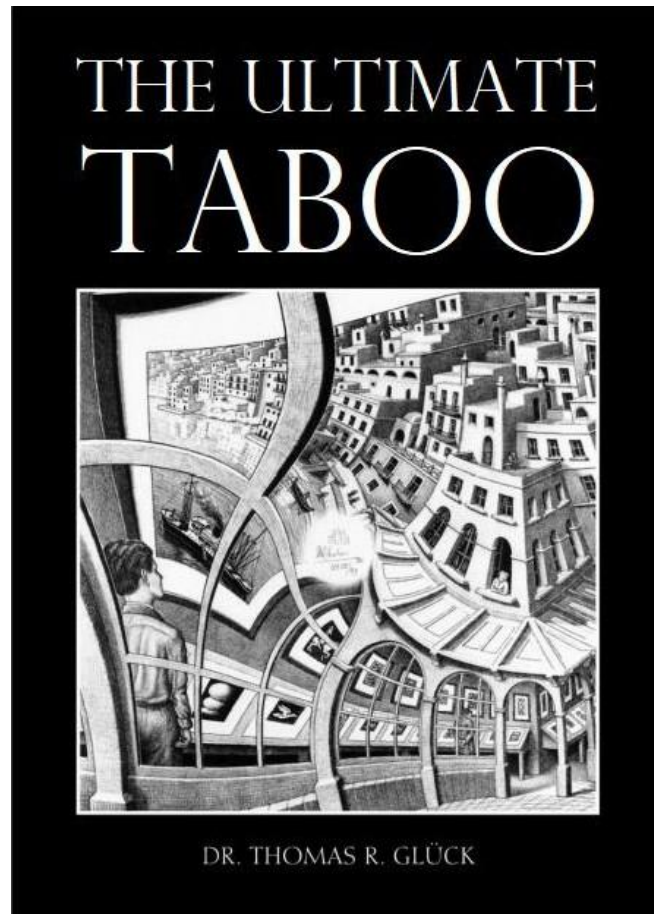


Part 2: Rational Cybernetics



Rational Cybernetics

What is information?



»The real truths are heresies. They cannot be spoken. Only discovered, whispered, and perhaps read.«
Naval Ravikant

Hard question:

How can we fundamentally improve information quality?

Radical simplification and pragmatic solution by *inversion*:

In order to draw a boundary to knowledge, one must know both sides of this boundary (i.e. one must know what one *cannot* know).

Only by considering the empirical phenomenon of *Passive Disinformation*, knowledge quality becomes concretely treatable.

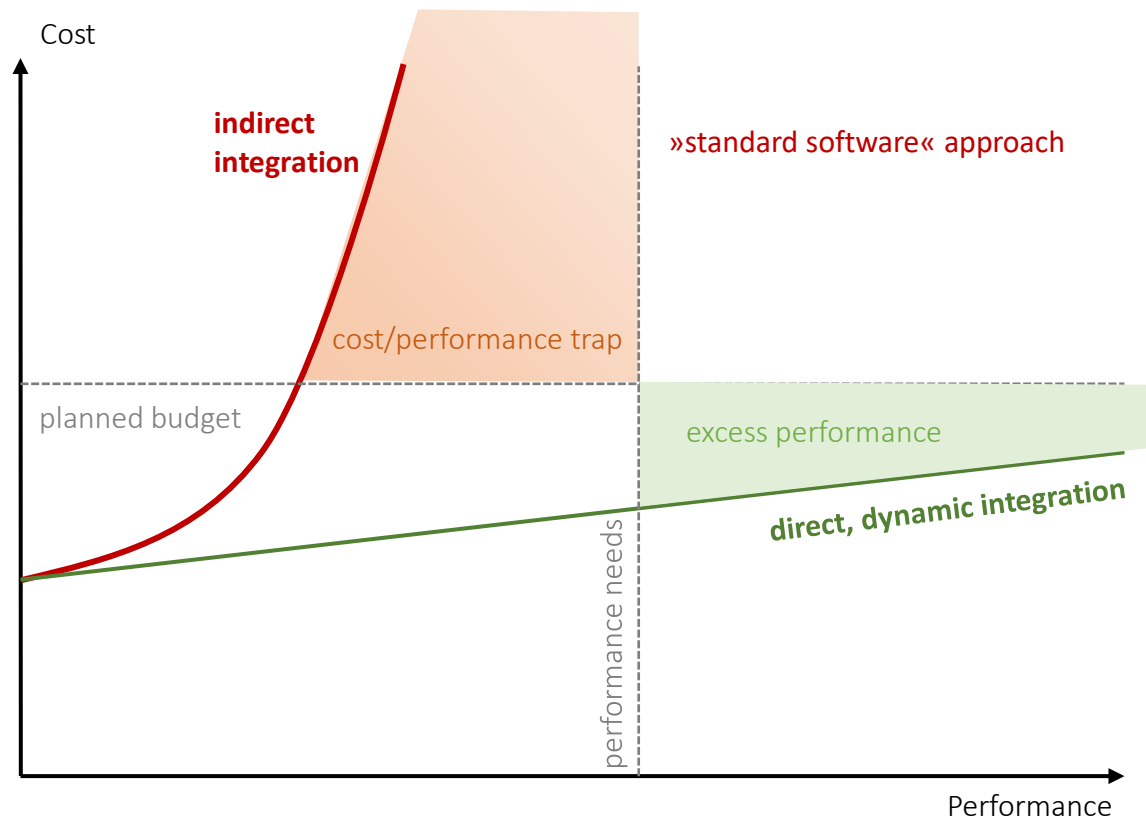
However, far-reaching improvements in the quality of knowledge can be at least as disruptive as »the separation of money and state«: a potential separation of power and collective control systems.



Part 3: Technical Cybernetics

Technical Cybernetics

cyberCortex® - how do you control control systems?



cyberCortex® *fully* meets the specific practical requirements, so there is no need to adapt to a predefined »standards«:

- No process changes necessary
→ *lossless, uncompromising solution implementation*
- Smooth, dynamic adaptation to changing requirements
even during operation

Technical Cybernetics

cyberCortex® - how do you control control systems? In case of AI:

- **Macro-perspective:** Integration and coordination of different AI systems with shared, seamless data utilisation and the option of real-time (even structural) change interventions with »immediate« feedback.
- **Micro-perspective:** Enabling »hypernatural« plasticity and direct networking of neural networks.

In the context of deep learning, countless artificial neurons (variables) are currently being trained in layered, relatively rigid architectures. More complex n:m architectures cannot be effectively and dynamically controlled without a process like implemented by cCortex®, and thus cannot be implemented »plastically« like in natural neural networks.

cCortex® enables, among other things,

- the effective integration and control of *more complex than layer-oriented/static neural base architectures*,
- a real-time architectural adaptation of neural network structures as an additional training element (*real plasticity*), even in *distributed training*
- a *lossless decomposition of large neural networks* and a *reduction in the number of artificial neurons with the same or higher internal mapping complexity*,
- the development of *more energy-efficient training procedures* (by increasing the information content while reducing the number of variables), as well as
- *improved controllability* of AI systems: the artificial neural networks are directly controllable at the technical architecture level (e.g. enabling targeted (de)activation of sub-areas of »artificial brains«).

?



Thank you :-)





Recommended internet sources

Collection of **original documents** by Satoshi Nakamoto: <https://satoshi.nakamotoinstitute.org>

Bitcoin **history**: <https://www.lopp.net/bitcoin-information/history.html>

Bitcoin **discussion forum**: <https://bitcointalk.org>

Deep dive presentations:

Jack Mallers: BTC as *neutral payment infrastructure*: https://youtu.be/dkXZx-eB_Uk

Michael Saylor: BTC from an asset perspective (demonetization of asset classes): <https://youtu.be/8SQBly5yG-s>

Id.: Bitcoin for *Corporations*: <https://youtu.be/S3T4nhtHxOA>,

Id.: Paradigm shifts and strategic scenarios from the individual to the nation state: <https://youtu.be/O9KnBcWMkpw>

Bitcoin and **ethics**: <https://youtu.be/oksraL7wN6Q>

Edited, very good **source collection** around BTC: <https://www.hope.com>

»**Bitcoin University**«: http://www.youtube.com/@Bitcoin_University; esp. on *information security aspects*: <https://youtu.be/AI0os5JPUQY>

Various **tools**:

Bitcoin distribution statistics: <https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html>

Explorer: <https://mempool.orangepill.ovh/de/>, <https://mempool.space/de/>, <https://blockstream.info>

Fees: <https://feemultiple.bullbitcoin.com/chart/index>

BTC-Map: <https://btcmap.org>

Hashrate: <https://mempool.space/graphs/mining/hashrate-difficulty>

Estimate of the distribution of directly reachable nodes: <https://bitnodes.io>

Market capitalizations: *Crypto*: <https://coinmarketcap.co>; *Fiat*: <https://fiatmarketcap.com>; *Assets*: <https://companiesmarketcap.com/assets-by-market-cap/>

International currency valuations in BTC: <https://sorukumar.github.io/ChartingExperiment/btcath/>

ETF-tracker: <https://heyapollo.com/bitcoin-tracker/overview>, <https://blockworks.co/bitcoin-etf>

Hodl-Waves: <https://unchained.com/hodlwaves>

Final settlement comparison: <https://howmanyconfs.com>

Graphanalytics for blockchain transactions: <https://oxt.me>

Collection of original financial/valuation models: <https://nakamotoportfolio.com/>

Bitcoin Improvement Proposals (BIP), esp. Seed-Wordlist: <https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki>

Uncensorable social media platform: <https://nostr.com>

Bitcoin uptime tracker: <https://bitcoinuptime.com>



Recommended reading

Bitcoin from an *economic perspective*:

Ammous, Saifedean: **The Bitcoin Standard** – The Decentralized Alternative to Central Banking, 2018, Wiley

Id.: **The Fiat Standard** – Debt Slavery Alternative to Human Civilization, 2021, Scribe Media

Booth, Jeff: **The Price of Tomorrow**, 2020, Stanley Press

Bitcoin from a *technical perspective*:

Antonopoulos, Andreas: **Mastering Bitcoin** – unlocking digital cryptocurrencies, 2014, O'Reilly

Bitcoin from an *ecological perspective*:

D. Campbell, A. Larsen: **Bitcoin and the Energy Transition**: From Risk to Opportunity, IRM Energy and Renewables Group, <https://www.theirm.org/news/bitcoin-and-the-energy-transition-from-risk-to-opportunity/>

Bitcoin from a *strategic perspective*:

Lowery, Jason: **Softwar**: a novel theory on power projection and the national strategic significance of Bitcoin, 2023, Massachusetts Institute of Technology

Study on *disinformation* around BTC: Collins, S: **Runaway Citations and the Persistence of Bitcoin Misinformation**, www.da-ri.org, <https://drive.google.com/file/d/1L3TwwwjP7s3cDYFD7TtlqY20kpNghyJL/view>

Gold- vs. fiatstandard:

Lips, Ferdinand: **Gold Wars** – the battle against sound money as seen from a Swiss perspective, 2001, fame.org

Bestseller (fiction) on the failure of fiat money systems:

Shriver, Lionel: **The Mandibles** – a family, 2029-2047, 2017, The Borough Press



Price history to date

»There is no 2nd best.«

VanEck

INVESTMENTS FUND CENTRE LEARNING HUB INVESTOR CENTRE INSIGHTS

Figure 1: Bitcoin has been the best performing asset class in 8 out of the past 11 calendar years

2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	YTD 2024
Bitcoin 6823.60%	A-REITs 27.04%	Bitcoin 51.96%	Bitcoin 125.13%	Bitcoin 1495.00%	Gold 10.07%	Bitcoin 86.66%	Bitcoin 258.36%	Bitcoin 77.48%	Gold 7.68%	Bitcoin 155.04%	Bitcoin 73.15%
Global Equities 48.03%	Global Equities 15.01%	A-REITs 14.32%	A-REITs 13.16%	EM Equities 27.09%	Australian Bonds 4.54%	Global Equities 27.97%	Gold 13.52%	Global Equities 29.58%	Cash 1.25%	Global Equities 23.23%	A-REITs 16.75%
Australian Equities 20.20%	Global Bonds 10.37%	Global Equities 11.80%	Australian Equities 11.80%	Global Equities 13.38%	A-REITs 2.91%	Australian Equities 23.40%	EM Equities 7.77%	A-REITs 26.14%	Australian Equities -1.08%	A-REITs 17.59%	Global Equities 14.06%
A-REITs 7.11%	Australian Bonds 9.81%	Global Bonds 3.35%	EM Equities 11.72%	Australian Equities 11.80%	Cash 1.92%	A-REITs 19.36%	Global Equities 5.73%	Australian Equities 17.23%	Australian Bonds -9.71%	Gold 13.89%	Gold 11.43%
EM Equities 13.03%	Gold 9.46%	Australian Bonds 2.59%	Gold 8.62%	A-REITs 5.72%	Global Bonds 1.65%	EM Equities 18.61%	Global Bonds 5.09%	EM Equities 3.44%	Global Bonds -12.28%	Australian Equities 12.42%	EM Equities 7.07%
Cash 2.87%	EM Equities 6.93%	Australian Equities 2.56%	Global Equities 7.92%	Gold 4.30%	Global Equities 1.52%	Gold 18.61%	Australian Bonds 4.48%	Gold 1.54%	Global Equities -12.52%	EM Equities 9.15%	Australian Equities 5.33%
Global Bonds 2.27%	Australian Equities 5.61%	Cash 2.33%	Global Bonds 5.24%	Global Bonds 3.68%	Australian Equities -2.84%	Global Bonds 7.26%	Australian Equities 1.40%	Cash 0.03%	EM Equities -14.33%	Global Bonds 5.31%	Cash 1.09%
Australian Bonds 1.99%	Cash 2.69%	Gold -1.14%	Australian Bonds 2.92%	Australian Bonds 3.66%	EM Equities -5.10%	Australian Bonds 7.19%	Cash 0.37%	Global Bonds -1.53%	A-REITs -20.46%	Australian Bonds 5.06%	Australian Bonds 1.03%
Gold 1.99%	Bitcoin -56.83%	EM Equities -4.30%	Cash 2.07%	Cash 1.75%	Bitcoin -69.23%	Cash 1.50%	A-REITs -4.61%	Australian Bonds -2.87%	Bitcoin -62.52%	Cash 3.89%	Global Bonds -0.31%

Source: Morningstar, as of 31 March, 2024. Bitcoin is represented by MarketVector Bitcoin PR USD; Cash is Bloomberg AusBond Bank 0+Y TR AUD; Gold is LBMA Gold Price PM USD; Emerging markets is MSCI EM NR AUD; Global equities is MSCI World Ex Australia NR AUD, Australian bonds is Bloomberg AusBond Composite 0+Y TR AUD; A-REITs is S&P/ASX 200 A-REIT TR; Australian equities is S&P/ASX 200 TR AUD. Past performance is not indicative of future results. You cannot invest directly in an index. The value of bitcoin is highly volatile.

Bitcoin #1

56.419,80 \$



▲ 91.238.986,92 %

↑↓ 1,0000 ₿

1 Std 24Std 7 T 30 T 90 T 1 J Alle



09/2012 10/2014 10/2016 10/2018 10/2020 11/2022



Luddite gaslighting & disinformation

What can be done against a dominantly better, antifragile technology?


 **World Economic Forum** 
@wef

In 2020 Bitcoin will consume more power than the world does today
wef.ch/2odVW4z







8:41 AM · 16/12/2017 ·  [Twitter](#)


114 Retweets 24 Quote Tweets 114 Likes



Why Printing Trillions of Dollars May Not Cause Inflation

1.1M views · 1 yr ago [#CNBC](#)

 12K  Dislike  Share  Download  Saved

 **CNBC**
2.7M subscribers

[SUBSCRIBE](#)

09:28    26

 **Carl B Menger** 
@CarlBMenger

When your salary depends on not understanding [#Bitcoin](#)  - [@ecb](#)

The truth is that the Euro has already lost 99.45% of its value against [#Bitcoin](#) 

[Post übersetzen](#)

Market Summary > Euro
0,000018 BTC
-0.00 (99.45%)  all time
1 Mar, 02:42 UTC · [Disclaimer](#)

1D 5D 1M 6M YTD Max 

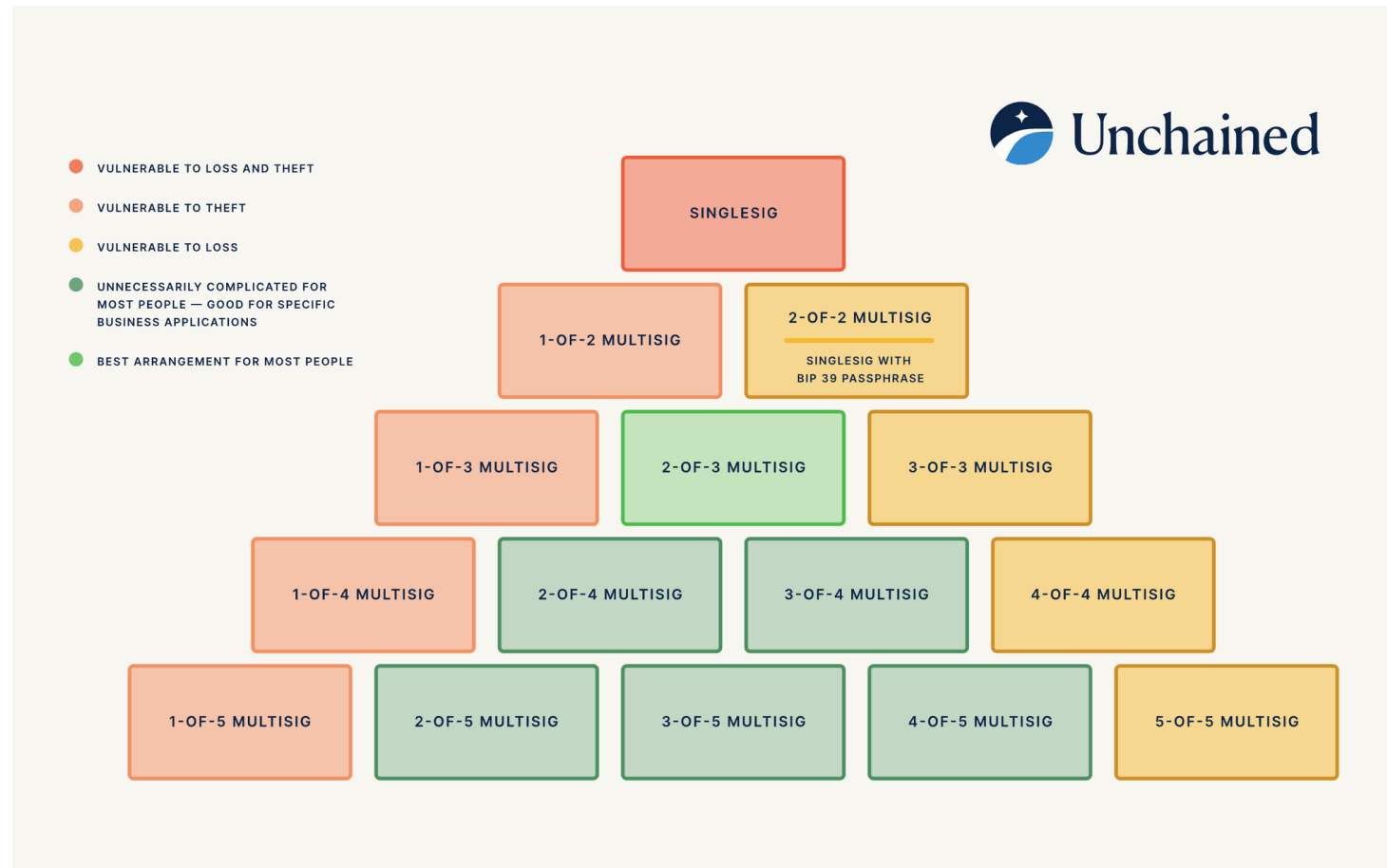


 **Gunther Schnabl** [@GuntherSchnabl](#) · 20h
Bitcoin-Preis manipuliert?
„Wert ist null, lockt Ahnungslose an“ – #EZB-Papier rechnet mit dem [#Bitcoin](#) ab



BTC Starter Package

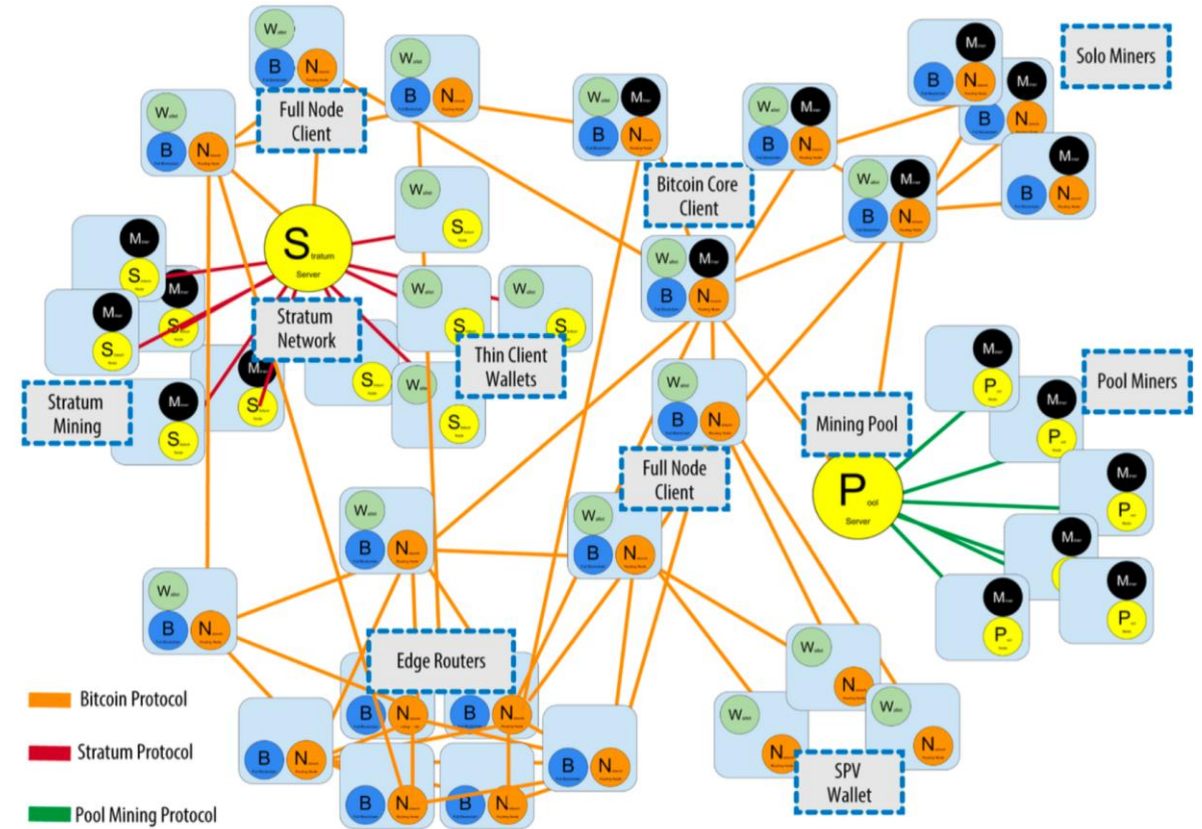
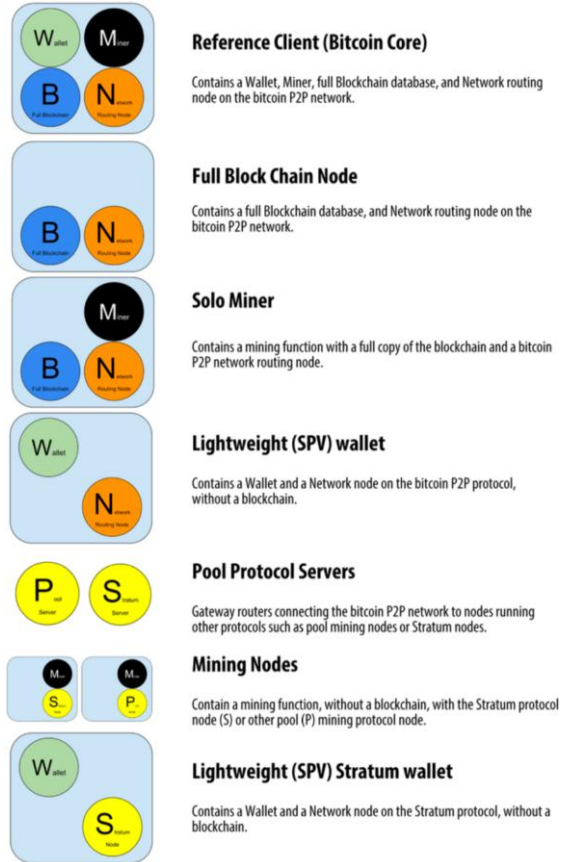
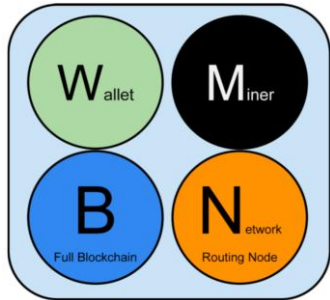
Evaluation & recommendation of multisig variants





BTC Components

cf. A. Antonopoulos: Mastering Bitcoin





Fiat-Interregnum

Confusion of confusions vs. shockingly simple facts



Bernstein: »The US government can't go bankrupt because we can print our own money.«

Interviewer: »[...] Why exactly are we borrowing in a currency that we print ourselves [...] Why do we borrow our own currency in the first place«?

Bernstein: »well um the uh so the I mean again some of this stuff gets some of the language that the em some of the language and concepts are just confusing.

I mean the government definitely prints money and it definitely lends that money which is why the government definitely prints money and then it lends that money by uh by selling bonds uh is that what they do they they um they yeah they they um they sell bonds yeah they sell bonds right because they sell bonds and people buy the bonds and lend them the money yeah so a lot of times a lot of times at least to my year with MMT the the language and the concepts can be kind of unnecessarily confusing but there is no question that the government prints money and then it uses that money to um uh uh so um yeah I I guess I'm just I don't I can't really talk I don't I don't get it I don't know what they're talking about like because it's like the government clearly prints money it does it all the time and it clearly borrows otherwise we wouldn't be having this debt and deficit conversation so I don't think there's anything confusing there.«



»The real problem is not the high taxes themselves but the fact that they are not even really funding the government [...]

The government is financed by treasury bonds, paper.

And who buys the treasury bonds?

Mostly the FED.

And how does the FED buy them?

By printing money.

But what backing does the FED have for that money being printed?

The treasury bonds themselves.

So basically you finance the government by printing money out of thin air.

Someone could ask: well, so if the government can print unlimited amounts of money out of thin air, why did they collect taxes? [...]

The answer is simple but it's very shocking:

The real problem is that **you pay high taxes only to uphold the illusion that you are funding the government, which you are not.**«

The Evolution of Accounting Technology

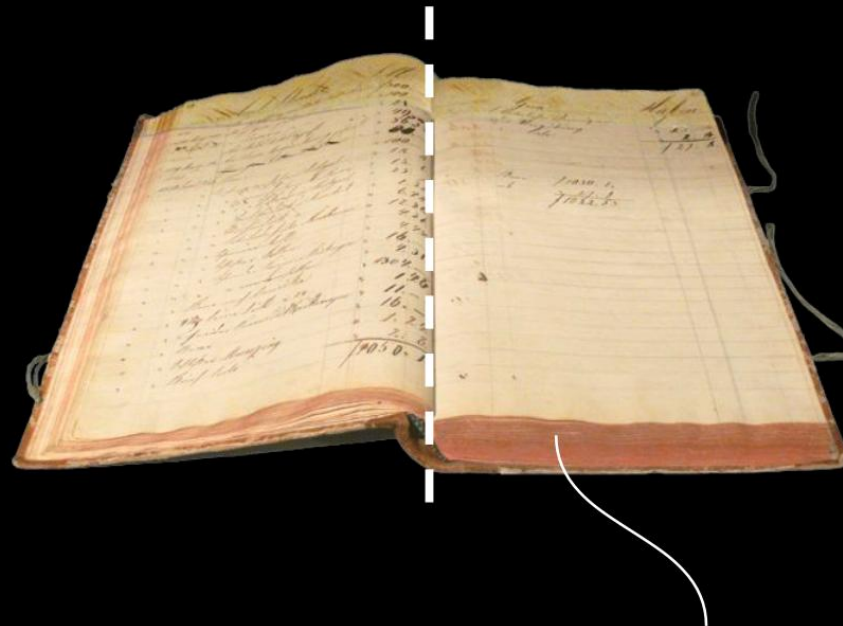
Single-entry



2000 B.C.

Mesopotamia
Sumerian cuneiform describing
the receipt of oxen

Double-entry



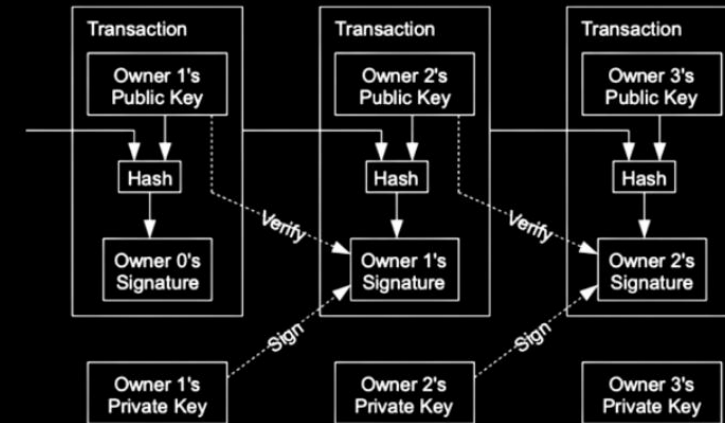
70 A.D.

Rome, Italy
System of *Tabulae Rationum*
described by Pliny the Elder

1299

Nîmes, France
Earliest recorded use
by Amatinio Manucci

Triple-entry



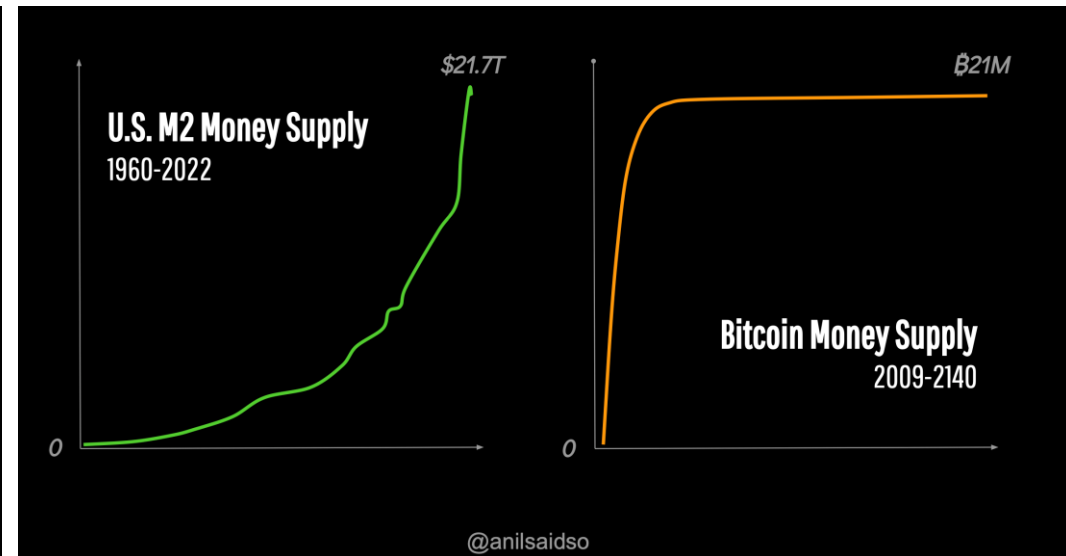
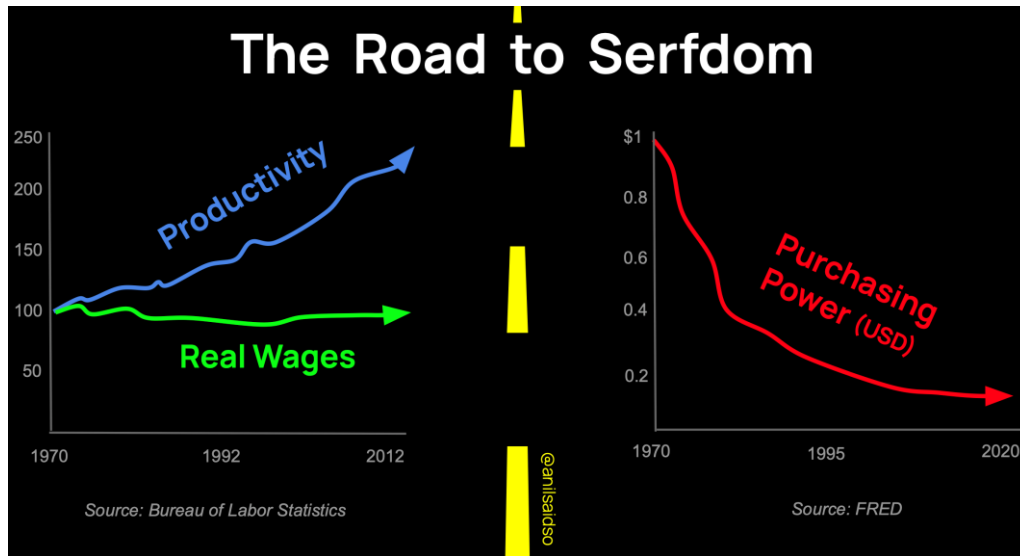
2008

System of a independently verifiable
chain of digital signatures
by Satoshi Nakamoto



The road to serfdom...

... and BTC as »escape hatch«



BITCOIN FALLACIES



@anilsaidso



This claim is disputed!

IT'S A BUBBLE

Bitcoin has been called a bubble many times, by many people, over many years. While the price of bitcoin has experienced several severe declines that might warrant the label, the overall trend has been spectacularly up and to the right.

Critics proclaiming the *death* of bitcoin after each market cycle are thankfully running out of analogies and have been revealed for what they are—**wrong**.



@anilsaidso

@anilsaidso

WILL BECOME OBSOLETE

Bitcoin represents the singular discovery of absolute scarcity. It's a one-time event like the discovery of fire, electricity or the field of mathematics. Competing with bitcoin along this dimension is both illogical and impossible. There is no level of scarcity above *absolute* scarcity.

Criticisms over bitcoin's current perceived limitations or drawbacks assume that trade-offs in security and incentive design do not exist or that bitcoin's current form doesn't already provide immense benefit to millions of participants.

As an exponentially growing permissionless network with an uptime of 99.98% over more than a decade, transacting trillions of dollars in value and secured by billions of dollars in hardware, displacing bitcoin as the dominant digital monetary network is, at this point, improbable.

"There's never been an example of a \$100B monster digital network that was vanquished once it got to that dominant position."

—Michael Saylor



"Bitcoin is a radical break from the past, so understanding the way traditional money works doesn't help you understand bitcoin. If anything, it hinders it."

The people who understand bitcoin the least are monetary economists. They cannot wrap their heads around it."

—Andreas M. Antonopoulos

Volatility is subjective. Expecting the price of bitcoin to keep within some imagined range is groundless.

Bitcoin trades 24/7/365 across almost every country on Earth. There are no registration requirements, bank holidays, circuit breakers, or bailouts. It is a truly free market. Any and all volatility is the product of buyers and sellers reaching agreement in real-time, without government intervention.

Bitcoin is on a journey to becoming the primary global store of value of the Information Age. Bootstrapping from zero, the notion that such a trajectory would occur in a straight line is delusional.

EXCESSIVE CONSUMPTION OF ENERGY

Bitcoin is globally-accessible sound money that is censorship resistant as a product of its Proof of Work mechanism.

With an estimated four billion people currently living under some form of authoritarianism, bitcoin offers a way to send, receive, save, and transport wealth. Ask yourself—what is the exact amount of energy such a monetary network should consume? And more crucially, why are you the person to best judge this?

"It ought to be outlawed."
—Joseph Stiglitz

"Bitcoin's volatility renders it unattractive for most corporations to hold in lieu of cash reserves."

—Steve Hanke

"Bitcoin has bootstrapped to \$1 trillion in market cap, almost like returns to counterfeiting,"

—Jeffrey Sachs

As adoption grows, bitcoin becomes further de-risked, further potential upside diminishes, and volatility declines.



@anilsaidso

@anilsaidso

UNBACKED



The concept of *backed* money is an oxymoron given that the thing *backing* it would then simply be considered money.

Money derives part of its value from scarcity. Bitcoin doesn't require the backing of some other scarce thing because it is absolutely scarce in and of itself. Independently verifiable and auditable, bitcoin is completely free of counterparty risk. There is no third party somewhere that must be trusted to store and secure some quantity of commodities or assets. If anything, the future will likely be backed by bitcoin.

*"Ultimately, bitcoin is backed by something, and it's the only thing that backs any money: the credibility of its **monetary properties**."*
—Parker Lewis

SCARCITY
DIVISIBILITY
PORTABILITY
DURABILITY
RECOGNIZABILITY

@anilsaidso

USE CASE

MONETIZATION OF STRANDED ENERGY

Bitcoin mining offers a highly portable solution to energy assets located in regions for which there is no current local demand nor possibility for transportation. Through the use of onsite hash-generating equipment, bitcoin can be produced. This asset can then be held for future value appreciation or sold into its highly liquid and globally-accessible free market.



"Bringing the market to the molecule is very powerful."
—Marty Bent

@anilsaidso



THE 3 BUCKETS OF CRITICISM

SPECULATIVE/UNFAIR

- BUBBLE
- TOO VOLATILE
- UNBACKED
- HOARDING
- CENTRALIZED OWNERSHIP

WASTEFUL/USELESS

- OBSOLETE
- ENERGY INTENSIVE
- SLOW
- EXPENSIVE FEES
- INTERNET DEPENDENT

DANGEROUS/SCAM

- CRIMINAL USE
- PONZI/PYRAMID
- GOVERNMENT BAN
- INFLATION BUG
- DUPLICABLE

INTERNET DEPENDENT

The risk of losing access to the internet due to infrastructure failures, natural disasters or intentional outages is a legitimate concern. Fortunately there are several methods for transacting bitcoin offline and via other telecommunication networks.

In the case of sending bitcoin on-chain, a signed transaction need only reach a single node in order to be broadcast the network for inclusion in a future block by miners. Some of the different methods one can use to achieve this relaying transactions to an internet



@anilsaidso

TRANSACTIONING BITCOIN OFFLINE

SATELLITE
(BLOCKSTREAM)

SHORTWAVE
RADIO

SMS

MESH
NETWORKS

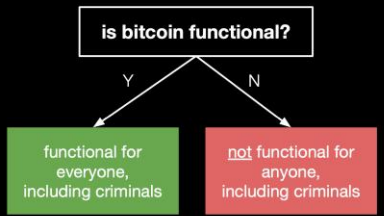
PHYSICAL
BEARER
INSTRUMENTS

@anilsaidso

FACILITATES CRIME

Bitcoin is a neutral tool for communicating value. It has no intrinsic beliefs, opinions or values. People give meaning to bitcoin through their use of it.

The argument that bitcoin's properties has resulted in an increase in criminal activity overall does not hold up under scrutiny. Criminality doesn't stem from access to tools, but individual circumstance.



source: Bitcoin Is Not For Criminals (2019)

"There is nothing inherent about the tools used to facilitate crimes that makes them criminal in themselves. Despite criminal use, no one is calling for the ban of roads, the internet, mail, etc."

—Parker Lewis

@anilsaidso

PONZI SCHEME

Calling bitcoin a ponzi scheme lacks an understanding of both bitcoin and the definition of a ponzi scheme.

A key element of a ponzi requires that there be some kind of **promise of above market returns** for investors. As a permissionless network, bitcoin does not have a central authority from which such promises can be made. More fundamentally, bitcoin is not an investment scheme, it is itself **money**.

Additionally, unlike opaque investment opportunities promoted to the unwitting individual, bitcoin's code is open-source and its supply independently verifiable at all times.



@anilsaidso

S L O W

Settling a bitcoin transaction on the main chain is not the same as using your credit card to pay for a taco. Even then, although your payment may seem instantaneous, it's actually passing through several counterparties and only gets deposited into the merchant's bank account after several days of processing. With bitcoin, you are not sending some IOU. You're sending hard money **directly** to the recipient, without any intermediaries, risk of censorship, and can be assured of final settlement once the transaction is confirmed. Six blocks doesn't sound like such a long time after all.



"The proper comparison would be between bitcoin and the Fed as currency issuer and as a clearing mechanism."
—Parker Lewis

"Using bitcoin for consumer purchases is akin to driving a Concorde jet down the street to pick up groceries: a ridiculously expensive waste of an astonishing tool."
—Saifedean Ammous

@anilsaidso

CORRUPTIBLE SUPPLY

Opting in to a set of rules. Anyone can fork the code and insert their own rule changes, but no one is going to run that version.

Bitcoin's appeal comes from its incorruptible supply, achieved by decentralized consensus where each node on the network independently validates every transaction that has ever been confirmed on the bitcoin network.

"Believe me, man is capable of somehow creating more bitcoin. If they tell you there are rules that they can't do it, don't believe them. When there's enough incentive bad things will happen."

—Charlie Munger

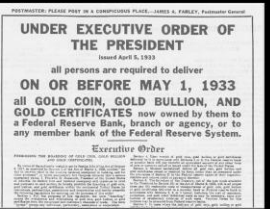


@anilsaidso

WILL BE BANNED

In all fairness bitcoin *can* be banned. It's the enforcement of the ban that is a lost cause. This is because bitcoin has turned money into pure information (a private key is simply a 256-bit random number). Banning bitcoin would mean preventing random numbers from being generated. Best of luck with achieving this!

While bitcoin transactions may be highly visible on the blockchain, the location of the private keys that control their access remains largely undetectable. Additionally, the infrastructure required to access the bitcoin network in order to trustlessly verify transactions is trivial provided basic computer hardware is sourceable.



"Banning bitcoin is not much different from trying to ban math. It will just prove its utility & drive more people to it."
—Saifedean Ammous

@anilsaidso

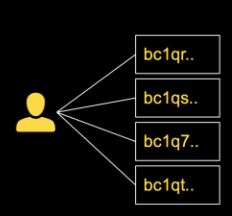
CONCENTRATED OWNERSHIP

How many times have you heard the same old line: **"a handful of wallets hold the majority of all bitcoin!"**

It's true, but there's a key clarification missing. Those are generally wallets of exchanges, each with millions of customers. In an ideal world, people wouldn't leave their bitcoin on an exchange, but that's a topic for another day.

A single bitcoin address can may contain bitcoin belonging to many users and a single user can control multiple wallets. In fact, best practices for maintaining privacy include avoiding address re-use, where a new address is generated for each receiving transaction.

Many users, one address



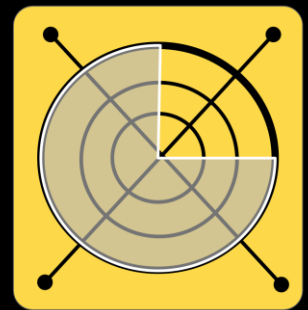
One users, many addresses

@anilsaidso

CENTRALIZED MINING

The threat of mining pools colluding to somehow disrupt the network, censor transactions, or double-spend bitcoin comes from a lack of understanding of the incentives of miners and their control over the network and the blockchain.

"A majority of hashing power **cannot**:
-take coins you already possess away
-change the rules of bitcoin
-hurt you without hurting themselves"
—Jimmy Song



TOO EXPENSIVE

Comparing bitcoin's unit price to the unit price of other assets (e.g. 1 bitcoin to 1 oz of gold) demonstrates **unit bias**. It's more accurate to compare the entire market cap of bitcoin to that of other asset classes. And besides, a single bitcoin is divisible into **100 million smaller units (satoshis)**. As the maxim goes: "you can buy a fraction of a bitcoin!"



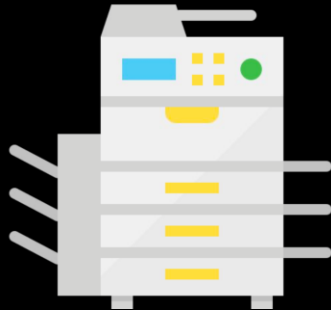
@anilsaidso

CAN BE DUPLICATED

Critic: Bitcoin is not scarce because there are 1000's of other cryptocurrencies out there and besides, anyone can copy the code and create their own version.

Bitcoin is an open source protocol for transferring value. Yes, anyone can fork it or attempt to launch an identical version. But you cannot take all of the developers, miners & hash power, users, node operators or suite of products and services with you. Bitcoin attracts people and resources precisely because of its transparency and rigorous development process.

"Open source is very much a meritocracy. You've got the hive mind building solutions. You get all that scrutiny and that comes back to security. Bitcoin Core is probably one of the most heavily scrutinized code bases in the world."
—@BTCSchellingPt



GRAHAM'S DISAGREEMENT HIERARCHY

Adapted from "How to Disagree" (2008) by Paul Graham

Finding evidence in an argument that you believe is mistaken, then explaining **why** it's mistaken.

State **opposing** case with little or no supporting evidence.

Attacking opponent's **character**

Refuting Central Point

Refutation

Counterargument

Contradiction

Responding to Tone

Ad Hominem

Name Calling

Correctly **identifying** an opponent's central point before arguing against it.

Contradiction **plus** reasoning and/or evidence. Aimed squarely at the original argument.

Someone with **chip** on their shoulder, offended by tone that others find neutral.

The **lowest** form of disagreement.

@anilsaidso

PROHIBITIVE TRANSACTION FEES

Confirmed transactions on bitcoin's main layer provide a level of certainty as to their finality that cannot be matched in the legacy financial system. Hence, while transaction fees may spike at certain times due to the limited capacity in each block, the bitcoin network remains an incredibly efficient and reliable settlement layer for high-value transactions. Smaller transactions (incl. microtransactions) continue to migrate to secondary layers (e.g., lightning, liquid or federated side-chains) where fees remain an order of magnitude below anything a retail bank can afford.



"Between October 2010 and July 2021, the average daily transaction fees came up to around **0.02%** of the value of the transactions."

—Saifedean Ammous
(The Fiat Standard)

@anilsaidso

A BITCOINER'S JOURNEY

It takes little talent to come up with **100 reasons** why bitcoin will fail.

But it takes genuine curiosity to independently and systematically debunk these reasons, one-by-one, from first principles.

This is how a bitcoiner is **forged**.



HEADLINE GENERATOR

Select technology ▼

Bitcoin

The Internet

Artificial Intelligence

Robots

Select hysteria ▼

Taking our Jobs

Boiling the Oceans

Facilitating Crime

A Speculative Bubble

@anilsaidso

WILL BE HOARDED

An argument that has seen a resurgence in an era of cheap debt, is that a fixed supply money incentivizes *hoarding*, whereby holders will not spend their bitcoin into the economy but simply sit on their hands and watch its value rise.

There are a few issues with this logic, mainly that it demonizes an activity more commonly known as *saving* (the excess of income > spending). Rebranding *saving* as *hoarding*, is quite literally advocating for living paycheck to paycheck. As any significant investment first requires saving capital to be able to later deploy (at least that was the logic prior to banks loaning money into existence).

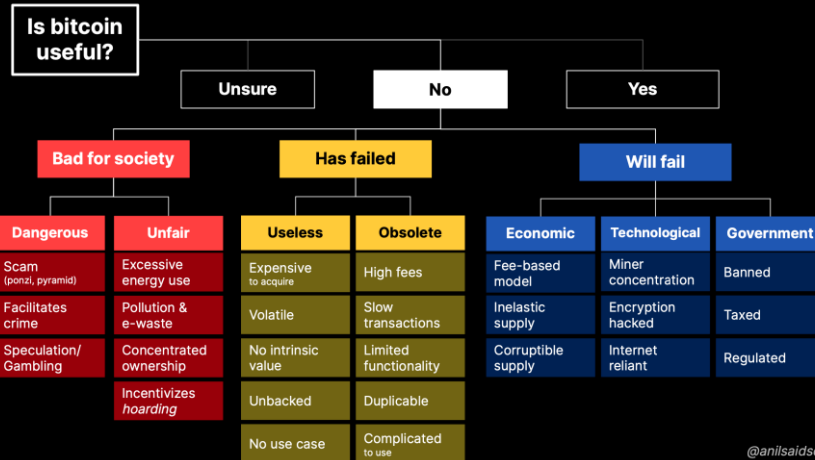


"People hold money to hedge against future uncertainty."

Yes, holding bitcoin is using bitcoin. All bitcoin are always held by someone, payments only change who is holding it."
—Pierre Rochard

@anilsaidso

@anilsaidso



THE FOUR CRITICS OF BITCOIN

According to Alex Gladstein

"You might be an exception but virtually all Bitcoin critics fall into one of these four categories:"

The Salty Hater

"You heard about Bitcoin years ago, but never bought, and are now salty."

The Desperate Statist

"You believe money can only be created by the state, so Bitcoin breaks your worldview."

The Dishonest Intellectual

"You haven't done the work to understand Bitcoin so you wish it would just go away."

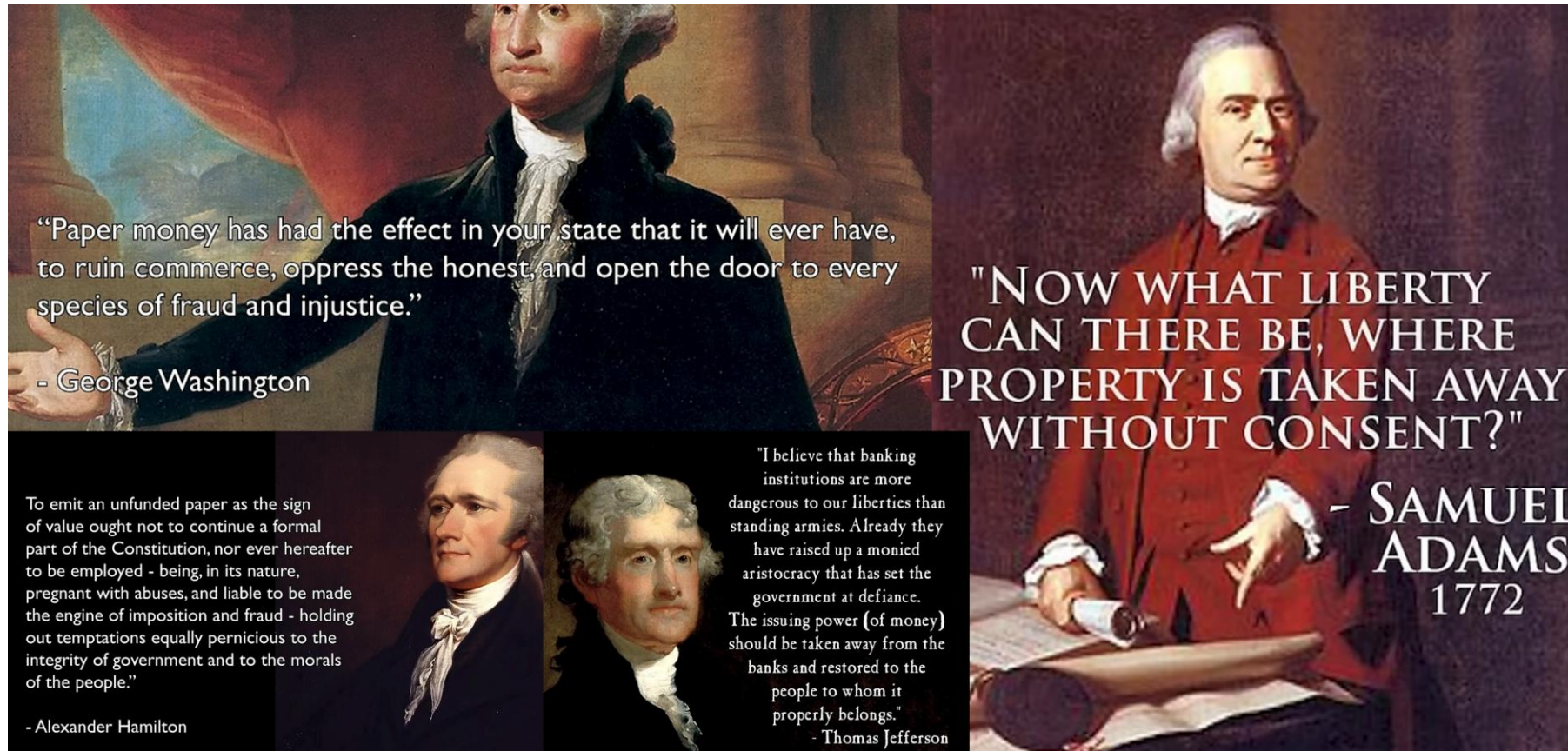
The Prisoner of Sunk Cost

"You are invested in an altcoin and feel the need to criticize Bitcoin to defend your life choices."



Founding Fathers...

... on the risks and side effects of fiat money





Central banks as essential basis for communism

»If socialists understood economics, they wouldn't be socialist.«

Communist manifesto:

1. Abolition of property in land and application of all rents of land to public purposes.
2. A heavy progressive or graduated income tax.
3. Abolition of all rights of inheritance.
4. Confiscation of the property of all emigrants and rebels.
5. Centralisation of credit in the hands of the state, by means of a national bank with State capital and an exclusive monopoly.
6. Centralisation of the means of communication and transport in the hands of the State.
7. Extension of factories and instruments of production owned by the State [...]
8. Equal liability of all to work. Establishment of industrial armies, especially for agriculture.



Not even Germans could make it work...

Severe cybernet(h)ical deficiencies vs. Galt's Gulch



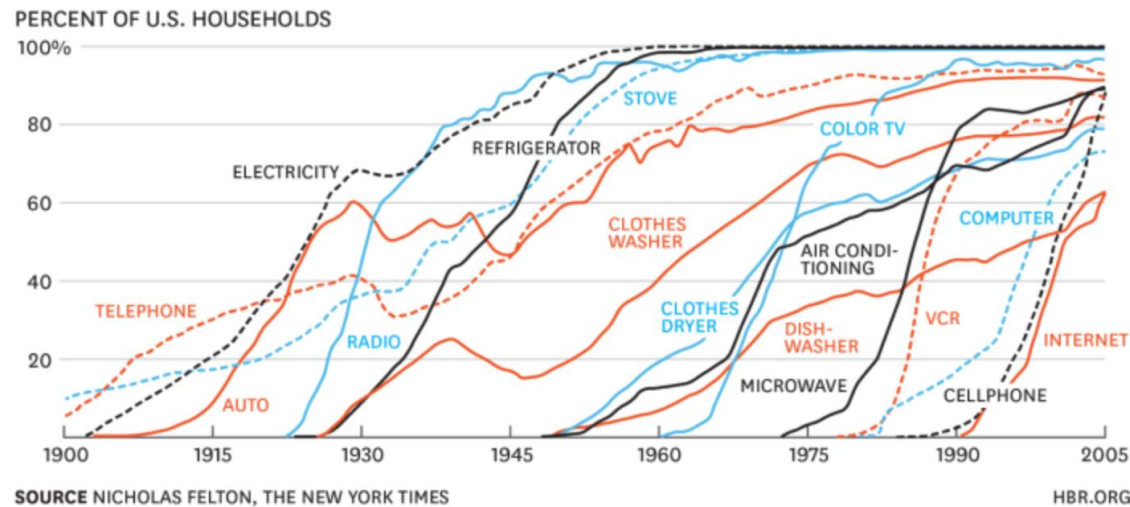
"Even a broken clock is right twice a day."

Socialist Clocks:





2024 US presidential elections

BTC has come a long way in a short time...



Bitcoin Voter Checklist

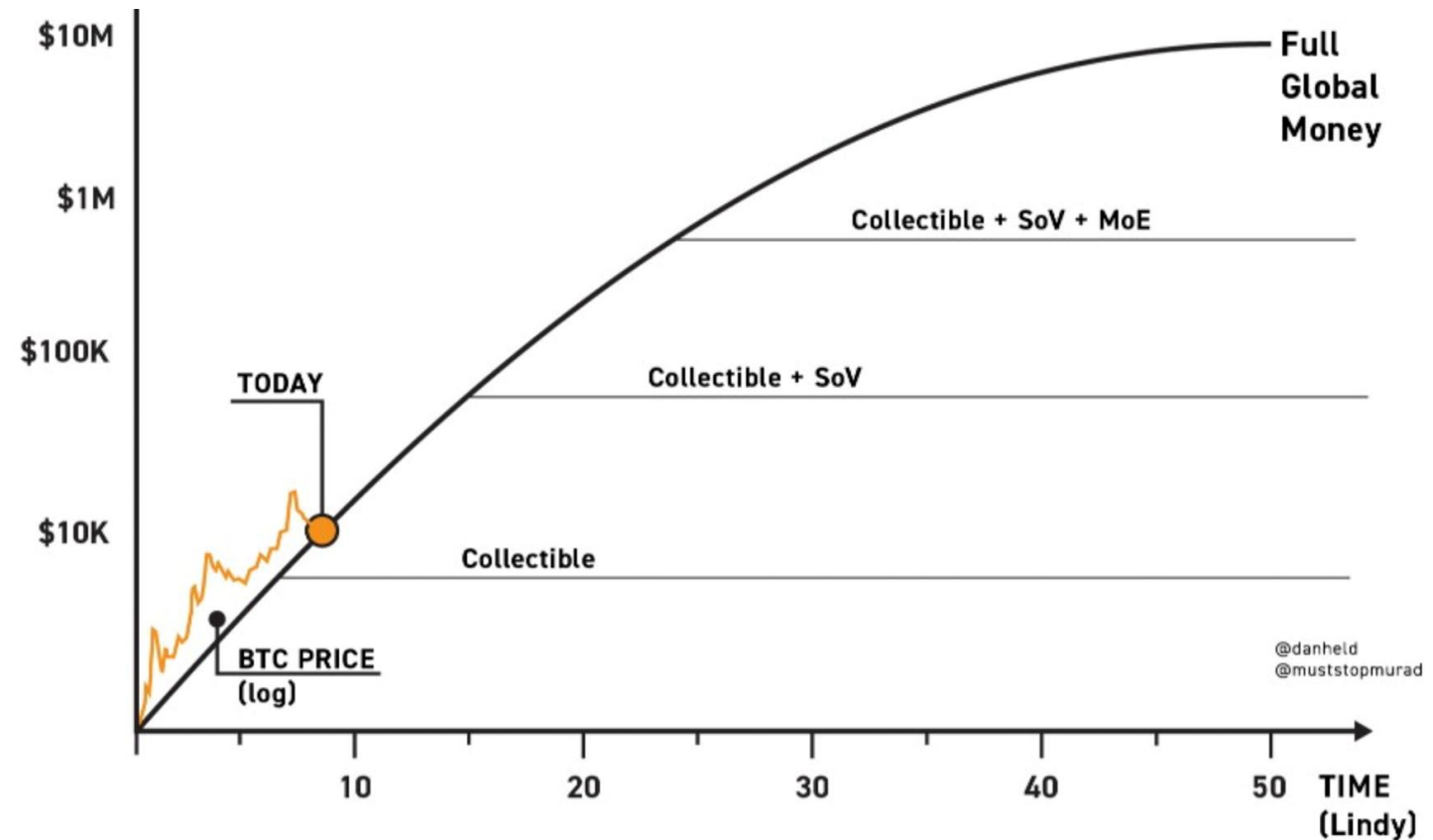
Policy	 Kennedy	 Trump	 Harris
Transfer ~200,000 Bitcoin from the US DOJ to the US Treasury for strategic reserve	✓	✓	
Purchase 4 million Bitcoin	✓		
Direct IRS to issue guidelines that all transactions between Bitcoin and US dollar are unreportable to protect the 4 th amendment right to privacy	✓		
Make the conversion of Bitcoin to dollars tax free	✓		
Direct IRS to treat Bitcoin as eligible asset for 1031 exchange into real property	✓		
Support Bitcoin self-custody	✓	✓	
Support running Bitcoin nodes at home	✓		
Block government and Fed from issuing a CBDC	✓	✓	
Understand MIT SoftWar thesis and how Bitcoin is a power projection weapon	✓		
Support Bitcoin mining to incentivize green energy investments	✓		
Shut down the Fed	✓		
Promise to never sign a law that taxes direct ownership of Bitcoin	✓		
Supports a Treasury Secretary from the Bitcoin community like Michael Saylor or Caitlin Long	✓		
Pardon Ross Ulbricht on day 1	✓	✓	
Pardon Julian Assange on day 1	✓		
Pardon Edward Snowden on day 1	✓		



Lindy Effect

Tik tok, next block.

The screenshot shows a Google search interface with the query "can bitcoin be stopped". Below the search bar, the "All" tab is selected. The search results display a text snippet: "To even have a chance to stop Bitcoin, every government in the world would have to successfully coordinate simultaneously to shut down the entire Internet everywhere and then keep it off forever. Even in that improbable scenario, the Bitcoin network can be communicated over radio signals and mesh networks." The phrases "every government in the world would have to successfully coordinate simultaneously to shut down the entire Internet everywhere and then keep it off forever" are highlighted in blue.



BTC meme wars



**FTX IS THE
BIGGEST SCAM
IN CRYPTO**



CARL B MENDER

**THE BIGGEST
CRYPTO SCAM
SO FAR**





Unfortunately, Prometheus didn't know how to use cryptography...