BITCOIN FALLACIES

This claim is disputed!

@anilsaidso

"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

“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

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

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.

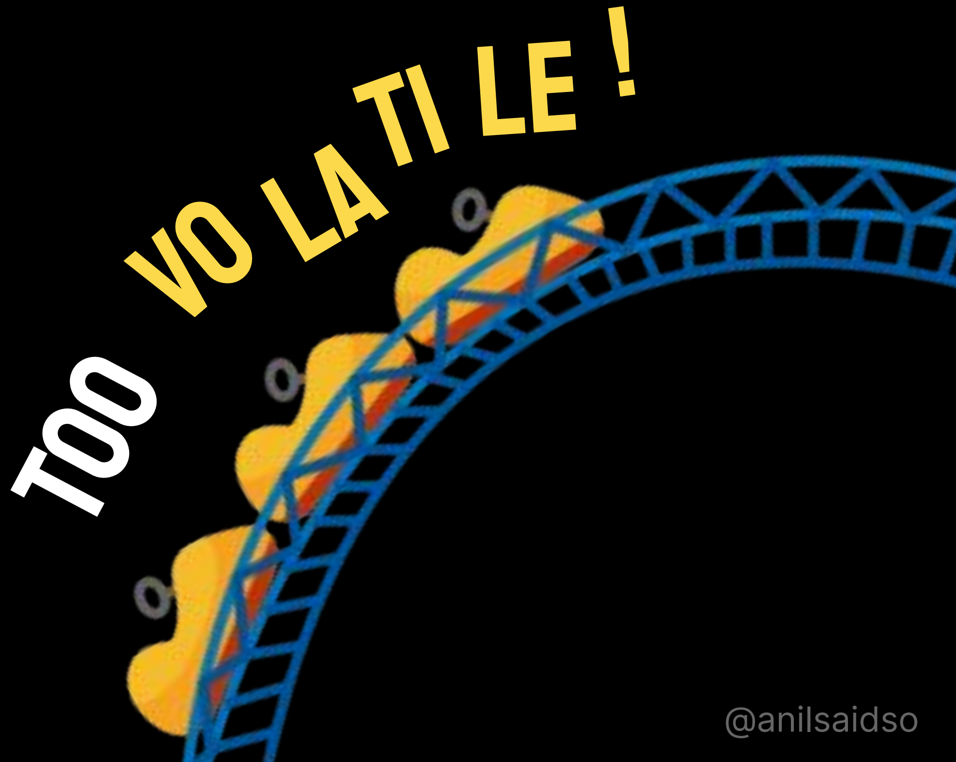
Critics proclaiming the *death* of bitcoin after each market cycle are thankfully running out of analogies and have been revealed for what they are—**wrong**.

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.

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



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

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

EXCESSIVE CONSUMPTION OF ENERGY

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

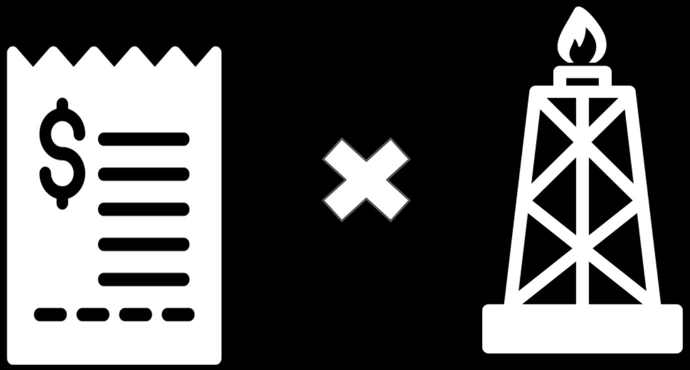
With an estimated four billion people currently living under some form of authoritarianism, bitcoin offers a way to send, receive, save, and transport wealth. Ask yourself—what is the exact amount of energy such a monetary network should consume? And more crucially, why are you the person to best judge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

"Imagine a topographic map of the world, but with local electricity costs as the variable determining the peaks and troughs. Adding Bitcoin to the mix is like pouring a glass of water over the 3D map – it settles in the troughs, smoothing them out. As Bitcoin is a global buyer of energy at a fixed price."

—Nic Carter

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

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 connected device via SMS, passing around physical wallets containing a one-time use tamper-evident private key, or even receiving the latest blocks via satellite.

TRANSACTING BITCOIN OFFLINE

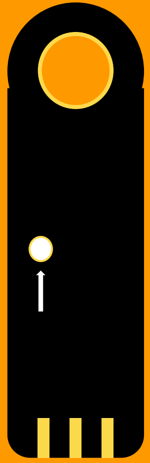
SATELLITE (BLOCKSTREAM)

SHORTWAVE RADIO

SMS

MESH NETWORKS

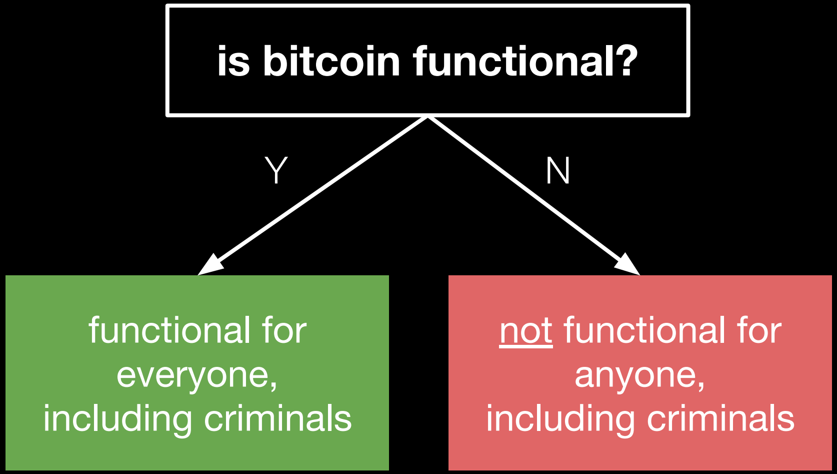
PHYSICAL BEARER INSTRUMENTS



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

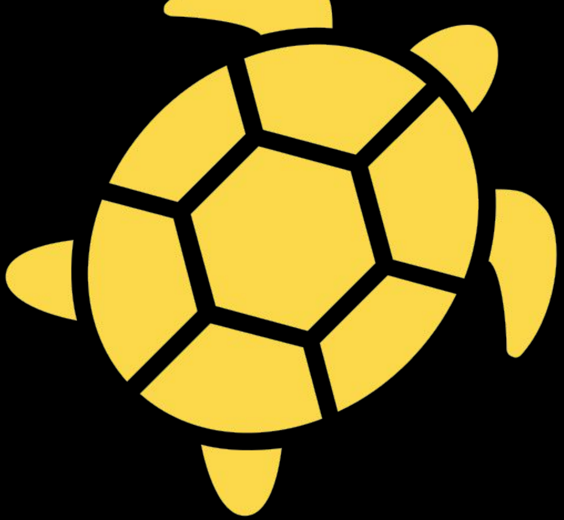
Calling bitcoin a ponzi scheme lacks an understanding of both bitcoin and the definition of a ponzi scheme.

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.

SLOW

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

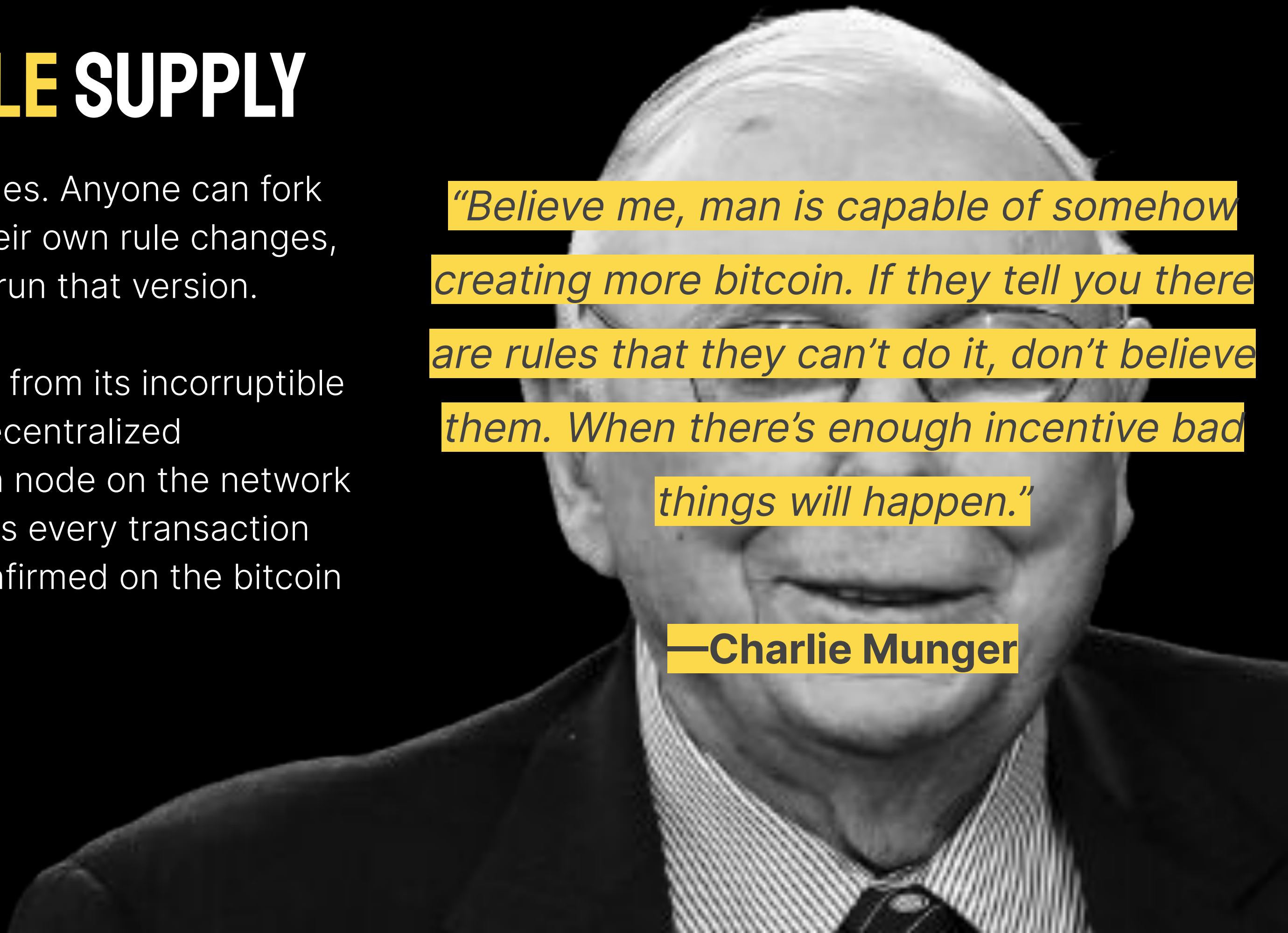
"Using bitcoin for consumer purchases is akin to driving a Concorde jet down the street to pick up groceries: a ridiculously expensive waste of an astonishing tool."
—Saifedean Ammous

@anilsaidso

CORRUPTIBLE SUPPLY

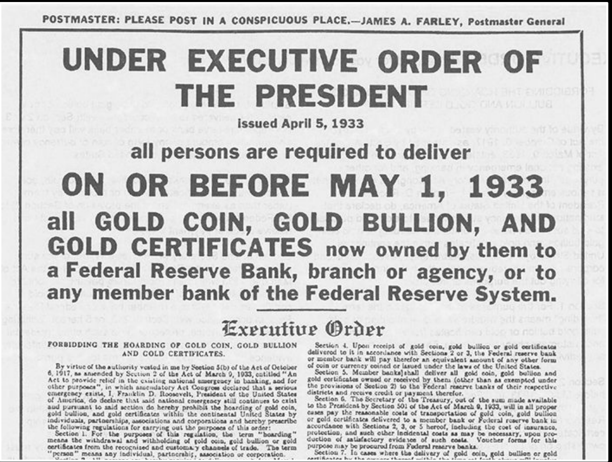
Opting in to a set of rules. Anyone can fork the code and insert their own rule changes, but no one is going to run that version.

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



POSTMASTER: PLEASE POST IN A CONSPICUOUS PLACE.—JAMES A. FARLEY, Postmaster General

UNDER EXECUTIVE ORDER OF THE PRESIDENT

Issued April 5, 1933

all persons are required to deliver

ON OR BEFORE MAY 1, 1933

all GOLD COIN, GOLD BULLION, AND GOLD CERTIFICATES now owned by them to a Federal Reserve Bank, branch or agency, or to any member bank of the Federal Reserve System.

Executive Order

FORBIDDING THE HOARDING OF GOLD COIN, GOLD BULLION AND GOLD CERTIFICATES.

By virtue of the authority vested in me by Section 5(b) of the Act of October 6, 1917, as amended by Section 2 of the Act of March 9, 1933, entitled "An Act to provide relief in the existing national emergency in banking, and for other purposes", in which amendatory Act Congress declared that a serious emergency exists, I, Franklin D. Roosevelt, President of the United States of America, do declare that said national emergency still continues to exist and pursuant to said section do hereby prohibit the hoarding of gold coin, gold bullion, and gold certificates within the continental United States by individuals, partnerships, associations and corporations and hereby prescribe the following regulations for carrying out the purposes of this order:

Section 1. For the purposes of this regulation, the term "hoarding" means the withdrawal and withholding of gold coin, gold bullion or gold certificates from the recognized and customary channels of trade. The term "person" means any individual, partnership, association or corporation.

Section 4. Upon receipt of gold coin, gold bullion or gold certificates delivered to it in accordance with Sections 2 or 3, the Federal reserve bank or member bank will pay therefor an equivalent amount of any other form of coin or currency coined or issued under the laws of the United States.

Section 5. Member banks shall deliver all gold coin, gold bullion and gold certificates owned or received by them (other than as exempted under the provisions of Section 2) to the Federal reserve banks of their respective districts and receive credit or payment therefor.

Section 6. The Secretary of the Treasury, out of the sum made available to the President by Section 501 of the Act of March 9, 1933, will in all proper cases pay the reasonable costs of transportation of gold coin, gold bullion or gold certificates delivered to a member bank or Federal reserve bank in accordance with Sections 2, 3, or 5 hereof, including the cost of insurance, protection, and such other incidental costs as may be necessary, upon production of satisfactory evidence of such costs. Voucher forms for this purpose may be procured from Federal reserve banks.

Section 7. In cases where the delivery of gold coin, gold bullion or gold

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

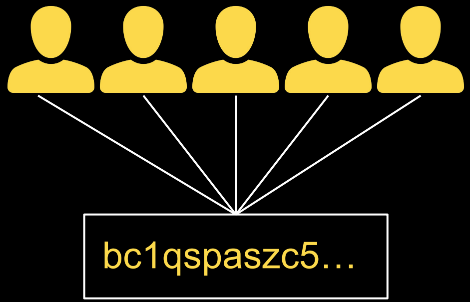
CONCENTRATED OWNERSHIP

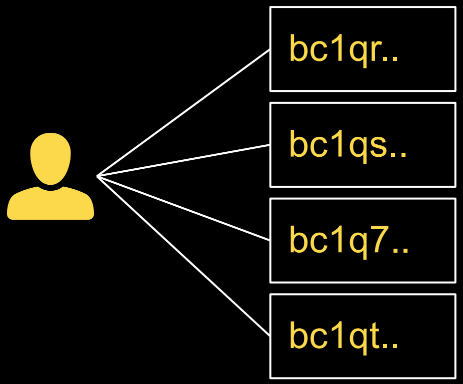
How many times have you heard the same old line:
"a handful of wallets hold the majority of all bitcoin!"

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

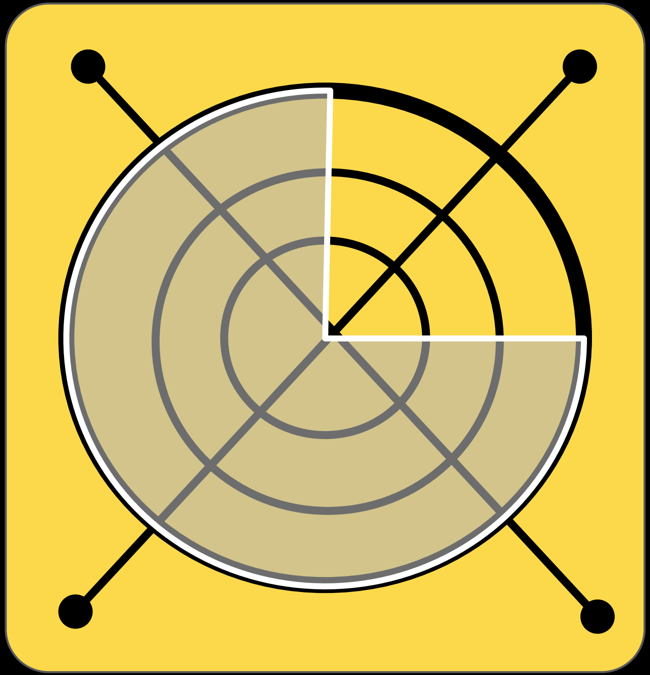
@anilsaidso

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.

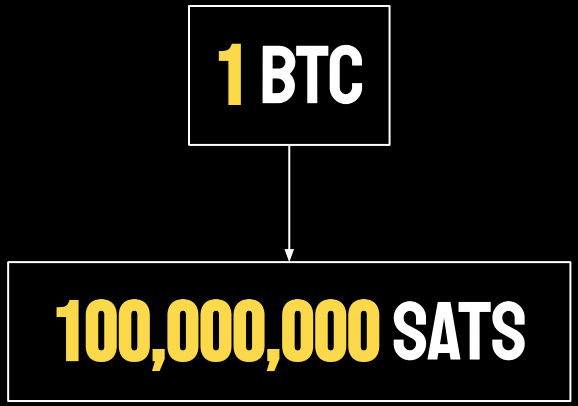
*"A majority of hashing power **cannot**:*

-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!*"



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."*

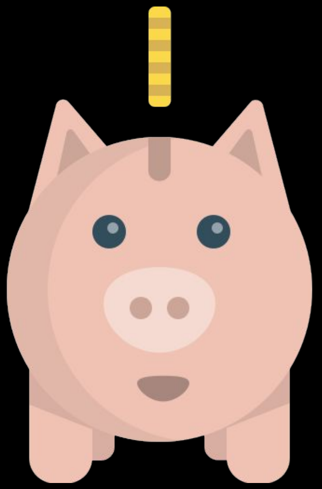
—Saifedean Ammous

(The Fiat Standard)

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 demonzies 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 was the logic prior to banks loaning money into existence).



"People hold money to hedge against future uncertainty.

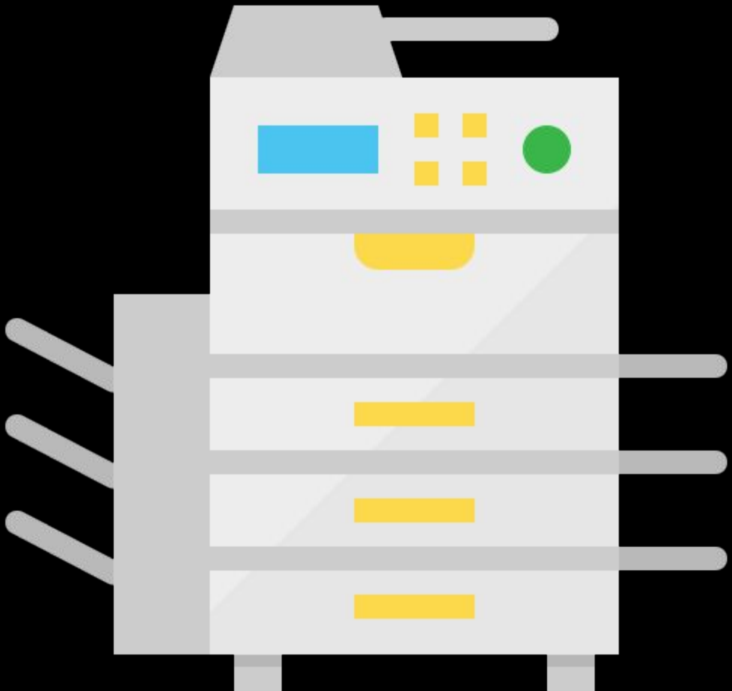
Yes, holding bitcoin is using bitcoin. All bitcoin are always held by someone, payments only change who is holding it."
—Pierre Rochard

CAN BE DUPLICATED 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



A BITCOINER'S JOURNEY

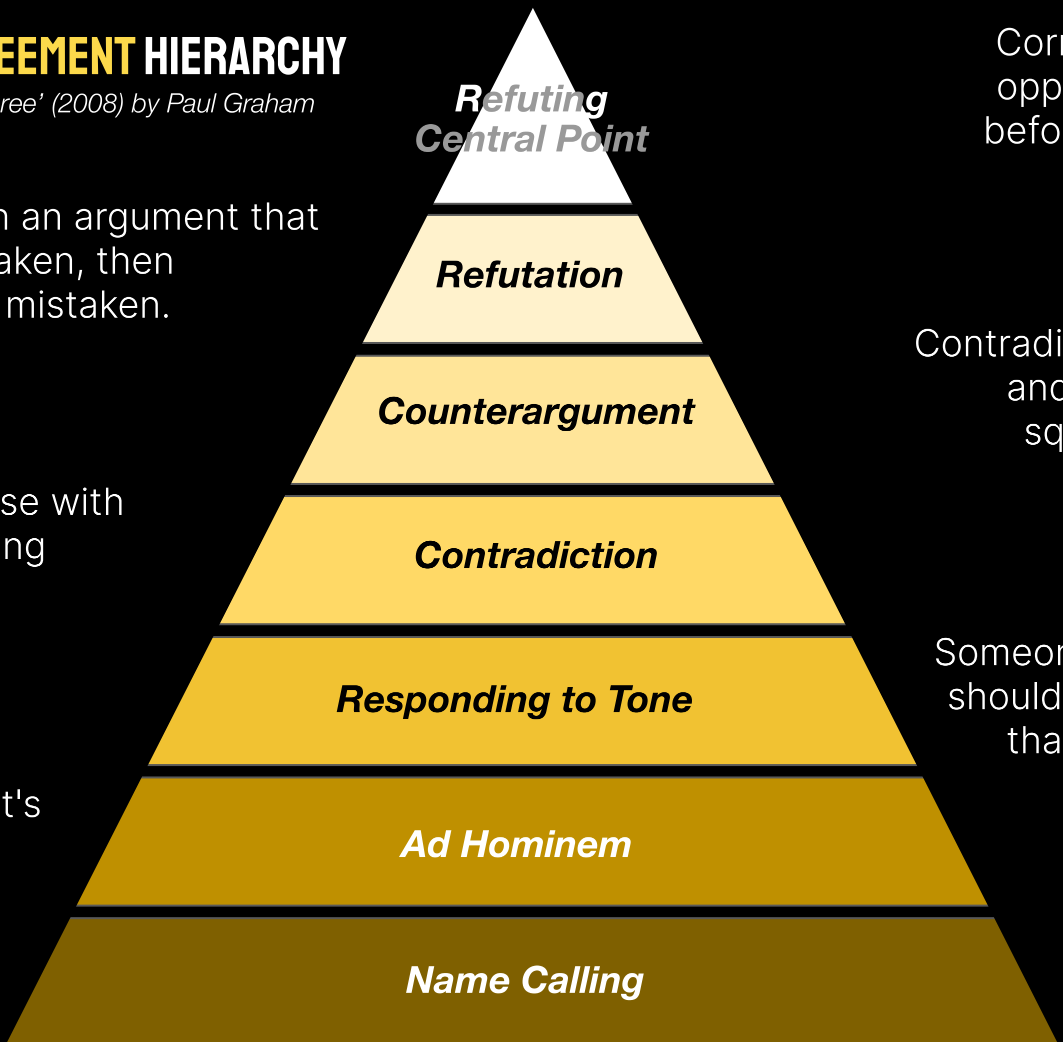
It takes little talent to come up with **100 reasons** why bitcoin will fail.

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**.

GRAHAM'S DISAGREEMENT HIERARCHY

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



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

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

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

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

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

Attacking opponent's **character**

The **lowest** form of disagreement.

@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.”

@anilsaidso

Thanks for reading!

Leave a review on Gumroad and help reduce bitcoin FUD by ensuring others can find it.

**You may use these slides with attribution for non-commercial educational purposes.*