BTCTKVR 3


21
B
Bitcoin
42
Re
Rules everything
63
A
Around me
105
K
King
168
In
Immutable
273
G
Gold
9
F
Fear
92
U
Uncertainty
105
D
Doubt

BTCTKVR 3

>NORMANCOMICS (AARON GOMBAR SPECIAL EDITION COVER)



Vlad Costea: Writing & editing, AI image generation & editing

Grafton Clark & Garry Rominger: Writers of "Breaking FUD: How A Father's Devotion Led A Sceptic To Bitcoin"

Leonard Luția: Graphic design & DTP (Articles 1-5, Foreword)

Bogdan Menci: Graphic design & DTP (Articles 6-7)

Andrej Cibik: Graphic design & DTP (Articles 8-11, Cover, Know Your Magazine section, Final composition)

Aaron Gombar (Normancomics): Inner cover remix

Mihai Dimache: Inner cover graphics for Bitcoin Takeover Podcast Season 14

Bitcoin_Apex: Hand-drawn graphics (pages 8-10) | bitcoinapexart.com

Special thanks for proof reading and providing technical advice: **Peter Todd, Pavol "Stick" Rusnak, Paula Magal**

Thank you **Roland Hrubaru** and **Charles Polanski** for finding 4 typos at pages 6, 27, 76 & 86

This magazine aims to debunk the most popular misconceptions about Bitcoin. It features 2 personal stories, 10 articles about ChatGPT's FUD, and 1 article about FUD for thought.

All images that aren't screenshots are generated using Midjourney, Dalle-2 and Stable-diffusion, under licenses which permit usage for commercial purposes.

Subscribe to the
Bitcoin Takeover Podcast

Donate to the Project
bitcoin-takeover.com/donate

Watch videos
YouTube.com/BitcoinTakeover

Table of Contents

Breaking FUD: Embracing Bitcoin 02

Breaking ChatGPT's Bitcoin FUD #1: Government Regulation 08
Renaissance

Breaking ChatGPT's Bitcoin FUD #2: Altcoins 13
1980s Neon Synthwave

Breaking ChatGPT's Bitcoin FUD #3: Scaling 18
Anime

Breaking ChatGPT's Bitcoin FUD #4: Security Vulnerabilities 23
Pixel Art

Breaking ChatGPT's Bitcoin FUD #5: Price Volatility 30
Art Nouveau

Breaking ChatGPT's Bitcoin FUD #6: Limited Use Cases 36
Film Noir

The Editions of BTCTKVR 2 46

Breaking ChatGPT's Bitcoin FUD #7: Energy Consumption 48
Solarpunk

Bitcoin Eating Popcorn #3 63

Breaking ChatGPT's Bitcoin FUD #8: Mining Centralization 64
Pop Art

Breaking ChatGPT's Bitcoin FUD #9: Education 70
Surrealism

Breaking ChatGPT's Bitcoin FUD #10: Mainstream Acceptance 75
Cubism

FUD for Thought 82
Expressionism

Breaking FUD: How a Father's Devotion Led a Skeptic to Bitcoin 88
Cartoony

Hall of Plebs 91







Breaking FUD

Embracing Bitcoin

Bitcoin has once again entered FUD season. It's the time when it gets thrown in the same basket as crypto scams in order to have its technological legitimacy questioned.

"It's been this number of years, what did Bitcoin accomplish? Here's why it's a wasteful ocean-boiling failed utopia for libertarians and all the people we tell you not to like", you hear them say. These are the moments when critics and skeptics get to shine – because when the price is down from the previous highs, the number of disillusioned retail investors grows. Naturally, the majority of the attention shifts towards these poorly informed but strongly-convicted voices that tell you that it's over and it was a bad idea all along.

Meanwhile, Bitcoin offers financial inclusion to millions of people worldwide. The unbanked, the politically oppressed, the socially and financially constrained, and the ideologically driven constantly benefit from the kind of freedom of transactions which no government or private institution will ever grant them. If the previous enumeration sounds too general and formulaic, here are some specific examples:

– the Canadian truckers, who protested for their freedom to work under irrationally authoritarian conditions in early 2022, eventually had their bank accounts frozen through political abuse. In order to be able to make transactions and receive support, they had to use bitcoin;

– the citizens of countries which experienced triple digit inflation during 2021 and 2022 protected their savings using BTC. Many such cases can be found in Sudan, Argentina, Lebanon and Venezuela;

– in countries such as Suriname and Turkey, bitcoin's crash from its all-time high is still not as drastic as the devaluation of their national fiat currencies;



– in El Salvador, the country which embraced the magic internet money as part of their official currencies, bitcoin transactions are part of daily life;

– and if you still think that Bitcoin still hasn't proved its utility, consider this: in 2022, Chinese spies reportedly sent BTC bribes to a US double agent via Wasabi wallet. Meaning that government officials also find Bitcoin useful, in spite of the official narrative they propagate through the media.

If 2021 was filled with Tesla Cybertruck and citadel memes, then the fall of 2022 and probably most of 2023 are all about FUD against Bitcoin. It's easier for speculators who don't understand the purpose and ideals of Bitcoin to criticize it through half-truths and distorted facts. And it's also extremely convenient for government officials, central bankers and private bankers to promote this FUD through their authority and the media channels they control. Such dishonest and deceitful actions effectively increase the demand for failing fiat currencies and may also temporarily boost faith in their silly money system.

But FUD, outside of its governmental weaponization, is nothing but a series of natural reactions which help us process events and phenomena that shake our worldview and system of beliefs. When we're faced with something new and revolutionary for which we don't possess enough information to understand, the first instinct is to be afraid of the changes it might bring to our surroundings. Fear is part of our human nature.

As soon as we learn a little bit more about it, we no longer hold strong opinions about the outcomes – which leads to uncertainty. And when we deal with a meteoric collision between our deeply-rooted system of beliefs and a black swan event, we tend to cast doubt on the contender.

FUD is part of who we are. It's a mechanism which makes us defend a status quo and helps us approach change in a critical manner. If we embraced every new idea without applying a basic level of scrutiny, our civilization would get destroyed. On the other hand, the permanent emergence of new information helps us transcend the FUD phase in order to embrace something that's truly revolutionary and worthwhile.

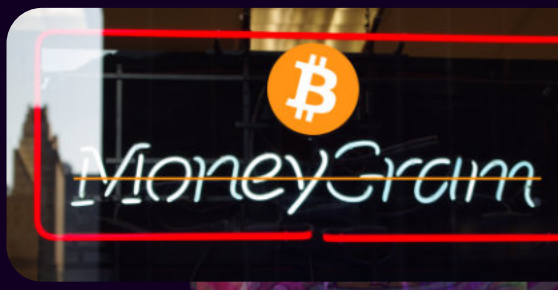


How I Broke The FUD And Embraced Bitcoin

My Bitcoin story follows the same pattern of FUD. When I first read about it in 2013, I thought it was a stupid idea. I was 21 years old at the time, and I remember staring at my laptop screen while thinking along the lines of "I have a bank account which allows me to access my funds from an internet app. I can send money to anyone I want – as a matter of fact, I've never faced any restrictions. Why do I need this?". Then I looked at Bitcoin's use cases and noticed that it's being used on dark markets to buy drugs and guns. "I'm a good person and a law-abiding citizen", I said to myself. So I started fearing Bitcoin and the changes that it might bring to my surroundings as a facilitator of activities I dislike.

That same year, I couldn't pay my rent to the student accommodation company SGS Goteborg because I needed a Swedish bank account. So I went to a Swedish bank to try to open an account with them – but since I wasn't a proper resident (I was in Goteborg as an exchange student) and had no income outside my scholarship, they couldn't help me. That's when I withdrew cash from an ATM and took a walk to the housing company's office to attempt a physical payment. They told me that they can't accept cash because it looks suspicious and I'm supposed to wire the money to their bank account. When I explained to them that my bank won't accept transfers to their accounts (different countries with different IBAN codes) and no local bank will allow me to do business with them in the absence of extra papers that I did not have, their suggestion was to try Western Union or MoneyGram.

The next day, I went to MoneyGram. I took one of their forms, filled it in while waiting in a long line, accepted to pay a 30 euro transaction fee on a 600 euro payment, but still hit a bureaucratic roadblock. The lady behind the counter



told me that customers from outside the Schengen area (of which Romania is not a member) must show their passport (which I did not have, since I traveled there with my national ID). I went to Western Union and found the exact same problem – I was holding Swedish crowns in cash, had no means to deposit it back into my Romanian bank account, and nobody wanted to help me pay my rent without seeing a passport.



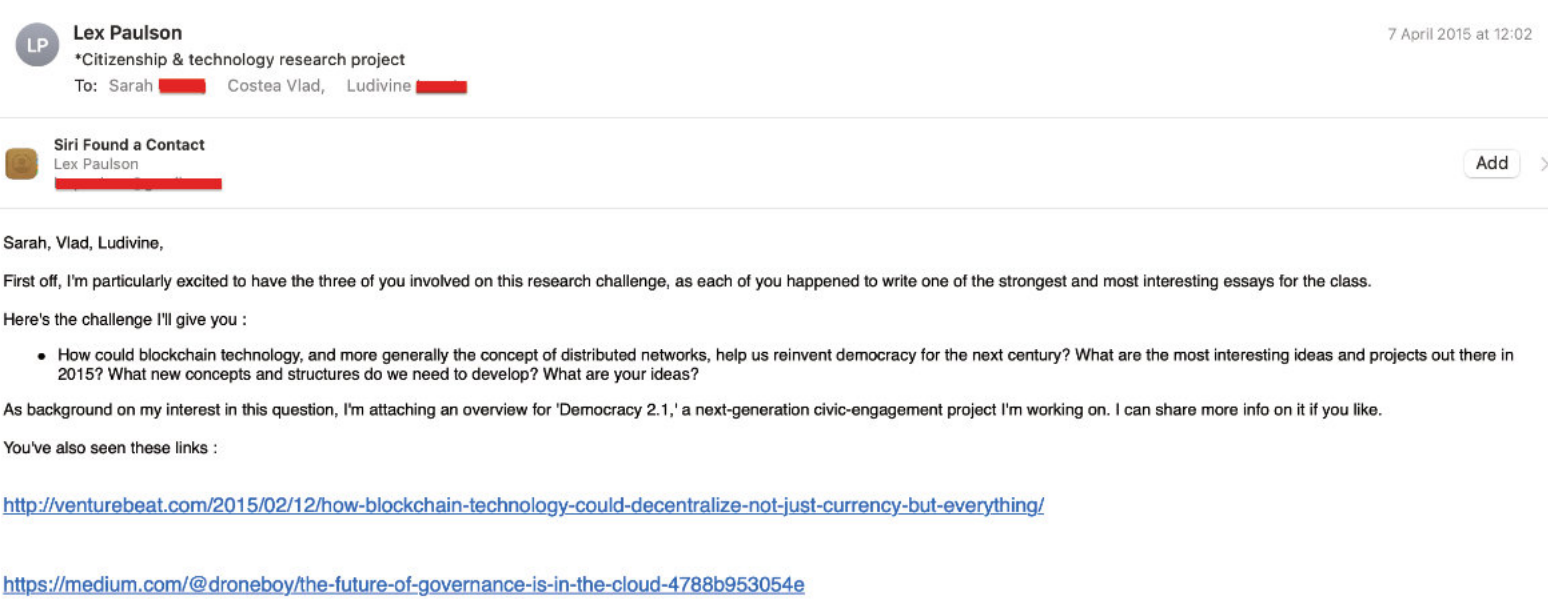
Since my national ID was not good enough for them, I had to go to university and ask a classmate of mine from Ireland (a country which is part of the Schengen area) to fill in the MoneyGram form in his name, wait in line, and make the payment with the cash I'm giving him. To perform a financial transaction as basic as paying my rent, I had to find a friendly proxy who had all the right papers to fulfil a MoneyGram wire transfer (thanks, Adam Ballance!).

And yet, I still regarded Bitcoin as something dangerous and irrationally feared its effects.

Two years later, at the age of 23, I was an exchange student in France. This time, I could only pay my rent in cash because the landlord did not want to sign a contract and pay taxes. But in the absence of this funny paper, I couldn't open a bank account and therefore had no access to student discounts for public transportation or a SIM card. For a couple of months, I had no means to use my mobile phone for calls and I paid full price for everything. That was when I figured out another way to use a proxy – a fellow Romanian classmate accepted to receive a cash payment in exchange for letting me use one of her SIM cards and would sometimes also help me get cheaper tickets for the subway train. God bless her, I hope she's doing well these days!

The year was 2015, I was still in Paris and I was taking a class in advocacy and innovation. My professor, an American political theorist named Lex Paulson, assigned me and three other colleagues with the task of making a presentation in front of the class on the topic of Bitcoin and blockchain. It wasn't the first time when I was reading about Bitcoin, but it was certainly strange to have this person from academia tell me to look into something that I knew was being used for drugs on the internet. Around the same time, I was an avid reader of Rolling Stone – the publication which informed me that Ross Ulbricht had received a life sentence for creating the Silk Road marketplace. But due to the fact that someone I knew and respected in real life (as opposed to some chatroom troll) told me to study Bitcoin, I no longer feared it.

I was now in the "uncertainty" phase. So I've become more open to the idea of Bitcoin, I went further with the process of studying its technological impact, but I failed to understand its importance in the history of money. Mostly because I didn't know anything about economics and the financial system – I was studying



Lex Paulson 7 April 2015 at 12:02
*Citizenship & technology research project
To: Sarah [redacted] Costea Vlad, Ludivine [redacted]

Siri Found a Contact Add
Lex Paulson
[redacted]

Sarah, Vlad, Ludivine,

First off, I'm particularly excited to have the three of you involved on this research challenge, as each of you happened to write one of the strongest and most interesting essays for the class.

Here's the challenge I'll give you :

- How could blockchain technology, and more generally the concept of distributed networks, help us reinvent democracy for the next century? What are the most interesting ideas and projects out there in 2015? What new concepts and structures do we need to develop? What are your ideas?

As background on my interest in this question, I'm attaching an overview for 'Democracy 2.1,' a next-generation civic-engagement project I'm working on. I can share more info on it if you like.

You've also seen these links :

http://venturebeat.com/2015/02/12/how-blockchain-technology-could-decentralize-not-just-currency-but-everything/

https://medium.com/@droneboy/the-future-of-governance-is-in-the-cloud-4788b953054e

political science and was stuck in this bubble of ideas about governance. I could have bought 1 bitcoin with the money I had in my bank account (about 200 euro), but I didn't because I was a broke student who would eat 5 euro menus at McDonald's and spend 20 euro a week on groceries. I also thought that everyone must buy 1 whole BTC, which turned out to be a terrible mistake. Had I purchased 0.1 BTC with 20 euro (4 days of skipping McDonald's meals), today it would be worth about 100 times more in euro terms – or almost 350 times more at the November 2021 all-time high.

But the good news is that, since doing my presentation in front of the class in May 2015, I kept an eye on Bitcoin. I paid more attention to it, I even started surfing the dark web to better understand how it's being used. By early 2016, I had returned home in Romania and my bank account was slightly more loaded. So I decided the time has finally come to buy some BTC – but that's when I read on the news that former Core developer Mike Hearn said that "Bitcoin has failed". So I entered the doubt phase of my journey.

You see, at the time I still believed that mainstream media channels serve the purpose of informing the masses... as opposed to pushing an agenda to manipulate markets, maintaining governments in power or else destabilizing them, and promoting the interests of their advertisers/financiers. In January 2015, the price of 1 bitcoin had doubled from the 200 euro that I remembered from 6 months prior. So if a major developer says that it's a failed project, his opinion is reinforced by prestigious publications (Reuters, Business Insider, The Guardian) and the price is higher than the last time, then I should probably stay away and wait to see what happens. Who am I to know any better and buy bitcoin at 400 euro per whole unit?

Hearn says the bitcoin network is about to run out of capacity as the volume of transactions increases. And when that happens, the network will become unreliable, with payments unable to be processed and vulnerable to fraud.

"If an IT system runs out of capacity like that then all kinds of things go wrong – all hell breaks loose," he said in an interview with Reuters in late December.

Hearn reckons the bitcoin community has "failed" in its governance of the crytocurrency's code.

"What was meant to be a new, decentralised form of money that lacked 'systemically important institutions' and 'too big to fail' has become something even worse: a system completely controlled by just a handful of people," he wrote.

DOUBT
UNCERTAINTY
FEAR

FEAR
UNCERTAINTY
DOUBT

It wasn't until a year later, in 2017, that I finally pulled the trigger and bought some BTC. By that point, the price had exceeded the previous bull market all-time high of $1000. So ironically, it was the market that made me turn a blind eye to all the mainstream criticism. Who said that price doesn't matter?

During the 4 years that it took me to conquer the FUD, the price had gone up more than 3 times. And it's not like I held onto my newly-purchased coins and did not sell them later in the year for a small profit... only to buy back at a higher price in December 2017. But that's a story for another day.

To conquer my fear of Bitcoin, I needed to receive reassurance from a person whom I held in high regard (a university professor who assigned me to study it for a graded project). To overcome the uncertainty, I spent another 6 months reading about the phenomenon. And in order to replace doubt with a buy order, I had to watch the price increase in spite of all the mainstream media coverage. I went through all the three phases of FUD only to realize how all these techniques have been weaponized against me.

I couldn't adopt a universal form of money, which nobody can censor or take away, because I believed in the banking system that failed to provide me even the most basic services. Upon learning new information, I failed to connect the dots because I believed in the benevolence and integrity of the mainstream media. And when I was finally ready to join the revolution, I was deterred by a dishonest but vocal developer.

I honestly don't want people to go through the same process in order to liberate themselves. The FUD is a normal reaction, but there's no reason for it to turn into a 4-year rollercoaster that's filled with bad experiences with banks and financial services. Which is why I've decided to take every misconception about Bitcoin and provide the kind of informed explanation that effectively breaks the FUD. Fearing something is only normal when it's new and you have no means to explain to yourself what it is. Feeling uncertain about it makes sense as long as your ability to get information is unreliable. And doubt is only for those who were unable to gain any sort of confidence and conviction in the information they've just learned.

It's Time To Break The FUD!

Satochip

Secure the future.



No need to be an AI to use a Satochip hardware wallet. The open source solution to manage your #cryptocurrency easily.

satochip.io/shop

@TheVladCostea

Hey ChatGPT, what are the top 10 most serious threats to the Bitcoin project?

@ChatGPTBot

1. Regulation: Government intervention in the form of restrictive laws or outright bans on the use of cryptocurrencies could impede the growth and adoption of Bitcoin.
2. Competition from other cryptocurrencies: The emergence of new, more advanced cryptocurrencies could potentially steal market share from Bitcoin.
3. Scalability issues: The limited number of transactions that can be processed on the Bitcoin network at any given time could become a bottleneck as adoption grows.
4. Security vulnerabilities: As Bitcoin's value and user base increases, it becomes an increasingly attractive target for hackers and other malicious actors.
5. Volatility: The price of Bitcoin has been known to be extremely volatile, which can make it difficult for businesses and individuals to effectively use it as a medium of exchange or store of value.
6. Limited use cases: Bitcoin has a limited set of use cases, which could limit its adoption and growth.
7. Energy consumption: The energy consumption required to maintain the Bitcoin network has been a point of concern, as it is significantly higher than most other payment systems.
8. Centralization of mining: A small number of mining pools control a large portion of the mining power on the Bitcoin network, which could lead to centralization of power and decision-making.
9. Lack of education and understanding: Many people still do not understand the technology behind Bitcoin and cryptocurrencies, which could limit its adoption.
10. Lack of mainstream acceptance: While Bitcoin has made significant strides in recent years, it is still not widely accepted by mainstream businesses and individuals.





Breaking ChatGPT's Bitcoin FUD #1:

Government Regulation

BITCOIN IS BETTER THAN YOUR GOVERNMENT **BITCOIN REGULATION**

WHAT DO YOU THINK ABOUT THIS ARTICLE? LEAVE YOUR COMMENTS OR SEND A DONATION BY SCANNING THIS QR CODE

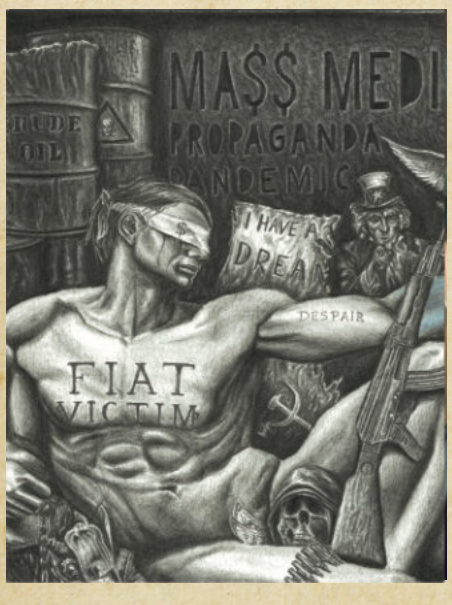
When I asked **Chat GPT** to provide a list of top 10 biggest threats to the **Bitcoin** project, the concept of regulations was at the absolute top. According to the AI's thesis, restricted access and outright bans have the potential to impede the adoption and growth of **Bitcoin**.

On the surface, these concerns seem legitimate. But if you understand how internet privacy and **Bitcoin** operate, then you will realize that only government-regulated businesses that facilitate the purchase and sale of bitcoin are really affected. They can shut down Coinbase, Binance, eToro, Kraken, Bitfinex, and every other business which operates under a jurisdiction that becomes hostile. They can also severely punish individuals using such services by closing down their bank accounts and lowering their social credit scores to a point where many of their freedoms go away. But these are all social contract problems which have nothing to do with the **Bitcoin** network.

In most countries around the world (and with a handful exceptions), the government can't stop a private citizen from owning a computer, accessing the internet, and running free open source software. In the constitutions which provide and protect individual freedom, computer code is regarded as free speech and access to information is a fundamental human right. Sure, specific bans can be put in place to cover the **Bitcoin** software – but what is **Bitcoin** if not software and pure mathematics? It's not like the client can't be rewritten from scratch in another programming language and under a different name, while respecting the same consensus rules. And if the connection to the **Bitcoin** network itself gets banned, obfuscation technologies such as Tor, Nym and VPNs come in handy.

Even in the absence of internet access, there's serious development to be found in the field of mesh antennas and satellite communications. Currently, Blockstream rents a satellite which broadcasts information about the latest Bitcoin transactions. Anyone who acquires or builds a parabolic antenna

(most commonly used by people to get access to distant television channels) is able to get information about the **Bitcoin** network without needing internet access. In the future, we can also imagine scenarios where mesh antennas are set up within reasonable distances in order to act as a permanent backup for the otherwise fragile internet infrastructure. And if all of these plans fail, there's also ongoing research about broadcasting **Bitcoin** transactions through short-wave radio signals – the same technology that was being used during the Cold War to send propaganda across national borders, now reimagined for **Bitcoin**. On the other hand, we should be aware that **Bitcoin** dies the moment people stop using it. In and of itself, no technology has any meaning and it's the individuals who adopt it that project purpose and goals towards it. Accordingly, **Bitcoin** can be effectively killed if a government ban leaves people apathetic about the project. In the absence of freedom fighters who care about keeping the governments away from their personal affairs, **Bitcoin** can't succeed.





Nonetheless, Bitcoin will succeed in spite of all political pressures and bans...

for as long as it provides freedom of transactions and a safe haven from confiscation. Should exchanges and registered businesses get banned, price discovery would take a hit. Such a situation leads to difficulty in pricing goods and services, so local or regional denominations need to be set according to the supply/demand ratio. Maybe that 1 bitcoin will be harder to valuate in the local fiat currency, but people can measure hours of work or certain commodities according to the BTC supply that they can access.

Should a government ban **Bitcoin**, it would effectively encourage the establishing of black markets, Which drives up adoption beyond the authority's control and reach. After all, the software is open source and nobody can stop the users from distributing and even reproducing from scratch all the elements necessary to interact with the **Bitcoin** network. From a game theory point of view, it is better for the government to facilitate **Bitcoin** adoption within its control. Collecting information about users though legal private companies helps them also collect taxes. Also, allowing a certain degree of liberty will make the regime look a little bit more freedom-leaning – thus strengthening its legitimacy and reducing the likeliness of a coup.



However, the exemple presented is too broad. There are two extreme cases where banning **Bitcoin** makes sense from a government's point of view: when the fiat currency's hegemony is being threatened (as is the case of the United States of America), and when the ability to control the country's finances in times of crisis becomes severely undermined by people opting out (such as Nigeria and Argentina in 2023).

Bear in mind that the first example presented above concerns the world's first modern democracy and the government which consciously makes efforts to export human rights, rule of law, and civil liberties around the world. Should the USA become such a flawed democracy themselves, their soft power around the world would diminish in favor of actors such as China and the Russian Federation.

In the case of Nigeria, it makes much more sense to ban **Bitcoin** for the purpose of regaining control over the money printer and reestablishing faith in the money. After all, increasing the supply only makes sense if there is real demand for the money. And any form of currency which offers an escape from the existing power structure needs to be crushed by those who want to stay in government while retaining the hegemony of an older system.

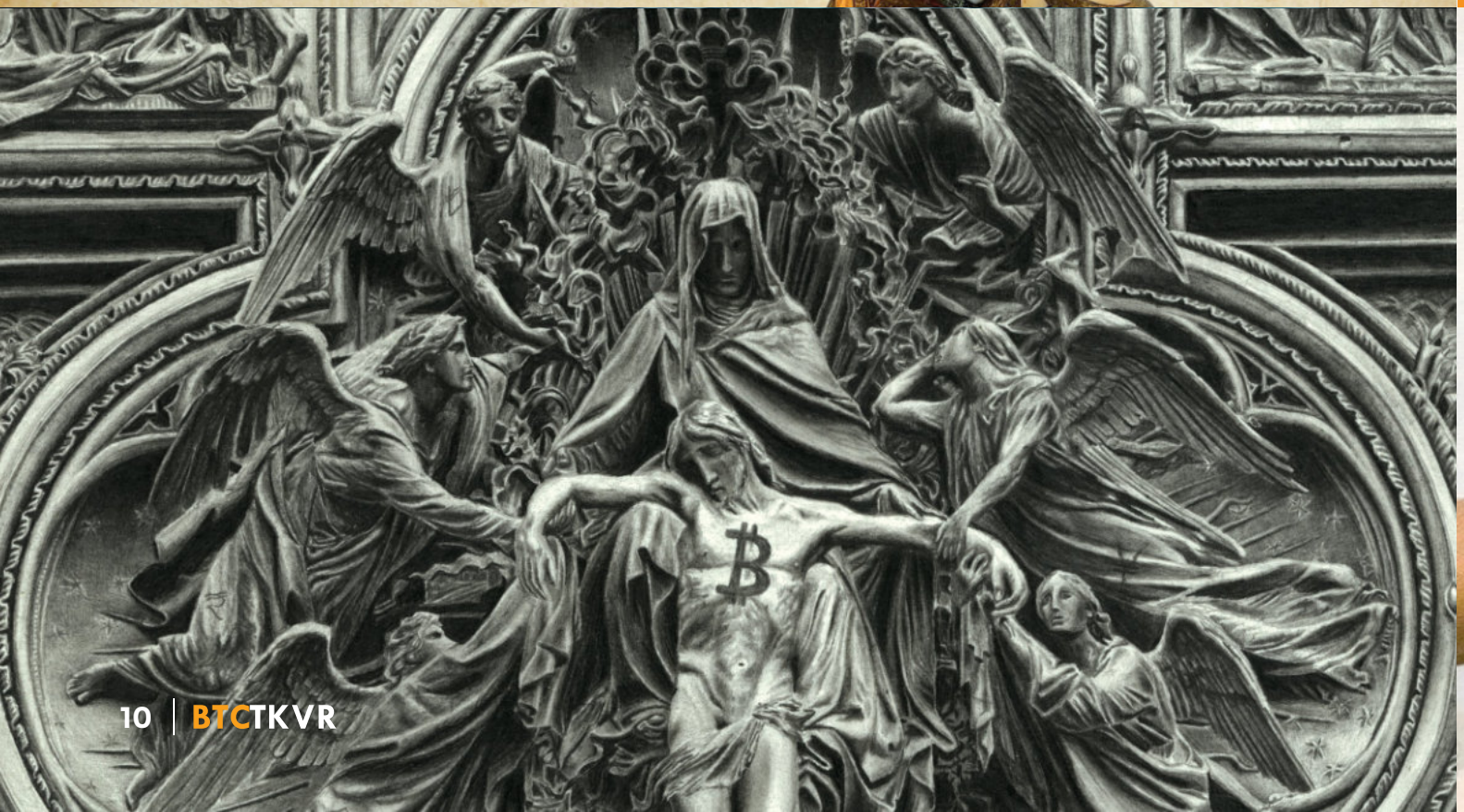
Nevertheless, it is also in Nigeria's best interest to receive capital inflows



and be a part of the global economy. And for thousands (if not millions) of freelancers, there's a real opportunity to work remotely and get paid in a better form of money – which of course would get exchanged in the local currency to buy food and pay for living expenses. Therefore, even if central banking policies would suggest that a strict ban on **Bitcoin** is temporarily the best alternative, the economic dynamics of supply and demand say otherwise. So it's better for developing nations like Nigeria to actually allow the youth to use **Bitcoin**, as long as the central bankers can maintain popular faith in their funny money. Otherwise, the situation turns into a full-blown **Bitcoin takeover** (pun intended) in which the non-governmental digital currency is the Trojan horse for freedom of transactions and the collapse of central banking.



From a geopolitical point of view, Bitcoin is an instrument for blackmail.



Nation states are under permanent threat that, if they don't allow it to exist, their neighbors will – and therefore these nations will absorb a greater degree of capital from the global markets and develop at a higher pace. Nobody wants to fall behind in the race for innovation. And if the price governments must pay is that of enabling **Bitcoin** to exist, then they would much rather make this compromise.

There's also a case to be made for regional alliances, international trade federations, and confederations. On a surface level, these forms of government are more likely to collaborate towards achieving a common goal. If they decide that **Bitcoin** is a big threat, then they will find ways to ban it. However, there are two facts that deem such an agreement unlikely:

1. First of all, even federation/confederation/alliance members compete with each other from an economic point of view and it's hard for the lesser developed territories to simply give up on extra means for wealth creation only to comply with the will of the others. In order for an agreement to be made, the more developed and wealthy members of the supranational body would have to make serious compensatory concessions to the others. This scenario is unlikely to work over the long term, though;

2. Secondly, no international government organization (including the United Nations) has a membership large enough to cover all sovereign nations. Palestine, Kosovo, Taiwan, Hong Kong, and Western Sahara are only five examples of countries that are not part of the UN. For as long as at least one of them remains neutral from global policies (which is very likely, granted the tax haven status of many of them), **Bitcoin** will continue to work as designed. And the fact that one nation benefits from the prosperity that **Bitcoin** brings will only accelerate the adoption race among its neighbors.

The best time to ban **Bitcoin** was probably in the first 4 years of its existence. Before users discovered the virtues of self-custody after the Mt. Gox fiasco, before node operators showed their resilience against big companies that wanted to increase the block size via hard fork in 2017, and before miners successfully migrated out of China in 2021. All of these are examples of resilience and persistence. At this point, **Bitcoin** is a global financial phenomenon. It has changed people's lives to the extent that these individuals are willing to fight to defend the network. It's also the kind of honest money that holds governments and central bankers accountable by making them aim to print less money... granted that they care about the long-term survival of their fiat currencies.

As the Nakamoto consensus dictates, it's more economically rational to become an honest actor in **Bitcoin's** mission than to fight against it. Governments are not exempt from this axiom – which is why they use FUD to buy themselves more time (and program AI software to push their agenda).

Sorry ChatGPT, you've lost this one!

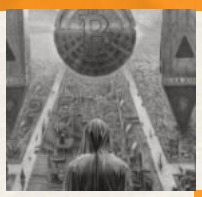




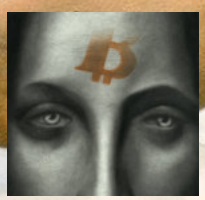
SCORE

Vlad C. 1

ChatGPT 0







Mallorca Blockchain Days

Be part of the Mallorca Blockchain Days IV experience

July 13 - 16 2023

Palma, Mallorca, Spain

GET YOUR TICKET ONLINE







WWW.MALLORCABLOCKCHAINDAYS.COM



Breaking ChatGPT's Bitcoin FUD #2:

Altcoins

WHAT DO YOU THINK ABOUT THIS ARTICLE? LEAVE YOUR COMMENTS OR SEND A DONATION BY SCANNING THIS QR CODE!



ALTCOINS GOING TO ZERO

According to **ChatGPT**, the emergence of new and more advanced cryptocurrencies could steal market share from **Bitcoin**. Generally, these alternatives to Bitcoin are referred to as "altcoins" – and they mostly comprise of modified **Bitcoin** clones that are neither original, nor "advanced".

Altcoins are essentially **Bitcoin's** experimentation layer – parallel networks which test features that were first proposed on **Bitcoin**, but did not get enough support from the community or from developers. Since the **Bitcoin** codebase is entirely open source, anyone can copy it, modify it, change it to include new features, and then deploy an entirely new network which focuses on a specific use case.

The reason why the **Bitcoin** network can't accommodate all use cases is best described by Zooko's triangle – a trilemma model in which system architects must choose two of three fundamental qualities: security, decentralization, and user meaningfulness (in our case,

scalability). **Bitcoin** is definitely secure and decentralized. However, its model doesn't scale too well. If the block size was to get increased arbitrarily (as forks such as **Bitcoin** Cash did), then this upgrade would come at the expense of lower decentralization and therefore cause potential security threats.

A reasonable equilibrium must be maintained in order to make sure that the network doesn't end up getting validated by computers in large data centers (as is the case of Ethereum and other networks which store large amounts of data). In the case of **Bitcoin**, blocks can't be larger than 4 megabytes – an arbitrary value which was deemed a reasonable compromise to enable more scalability without damaging the other fundamental qualities.

This is why altcoins exist: they take advantage of a limitation in **Bitcoin**, they identify a solution, and they deploy a new network to see what the free market thinks about it. Sometimes this experimentation is useful by providing empirical evidence on the various pros and cons of certain proposals, but most of the times these projects are deceitful about their tradeoffs by pretending to be 1000x faster or more secure than Bitcoin without simultaneously being decentralized.

As history shows, more than 90% of these projects fail. They rarely stick around for longer than a bull-bear market cycle and they lose relevance specifically because they don't get the expected traction and new improved proposals come along. This is good news for scientific experimentation, but bad news for investors who believe in the hype and hold worthless bags.

There are technical, social, and economic reasons why these altcoins fail while

Bitcoin continues to prosper.

From a technical point of view, it's the most reliable, secure, and decentralized network which attracts sustainable long-term investors. **Bitcoin** works well for its intended purpose, and its shortcomings can be overcome by building layers on top of it (such as Lightning network) or moving some of the activity on parallel chains (sidechains such as RSK, Statechains, Drivechains, and Liquid).

The economic reasons why **Bitcoin** thrives concern the increasingly fairer distribution of wealth and the resulting greater adoption. **Bitcoin** had no premines, Satoshi never spent a single coin and most likely left his stash as a honeypot for hackers, and the monetary policy is very simple to understand. There are only 21 million coins which get issued according to a well-timed and comprehensive inflation schedule that lowers rewards over time. Sure, you can argue that early adopters had easier access to BTC – to the point that they could mine with their laptop's CPU or get free coins from Gavin Andresen's June 2010 faucet. But at the same time, **bitcoin** had no monetary value at the time and it took a few years for markets to develop.



This argument leads to the social consideration as to why **Bitcoin** continues to prosper. First and foremost, **Bitcoin** had an immaculate conception and existed in a nascent phase for several years before big money came pouring in. Nowadays, in the middle of an entire blockchain industry which throws money at projects and demands for investor-centric pre-sale events, this feat is extremely difficult to pull off. Grin is one rare example of an altcoin that did everything right and remained pure – but it failed to get traction to the point where developers couldn't get paid. And this is another big problem: expectations and the constant pressure that ideologically-driven developers must endure while they know they could be making a lot of money elsewhere.

The first **Bitcoin** adopters had no financial expectations from the project, they just liked the idea of non-governmental digital money with no single point of failure. They built wallets, applications, and established traditions long before there was even a proper exchange system to trade BTC for USD. And they are also the ones who stuck around for purely ideological reasons, without caring too much about getting rich (even if they did get wealthy).

We should also talk about the wave of libertarian adopters who embraced **Bitcoin** between 2011 and 2014. They are the ones who built most of today's businesses and wrote many of the metaphors that describe **Bitcoin**, from

"Bitcoin is the honey-badger of money" to "Everything is good for Bitcoin".

Their greatest merit is that of making it "safe" to be a bitcoiner: they fought the legal battles, lobbied to regulators, and made use of their narratives to explain to politicians why banning **Bitcoin** could be detrimental for the greater economic landscape of the future. And they did it long before holding BTC turned them into USD millionaires.

Then there's the generation of bitcoiners that fought to protect the integrity of the network during the fork wars. Attackers assumed that **Bitcoin's** value can be diluted by creating dozens of modified copies which divide the users and take away some of the activity. They were wrong specifically because the social layer protected the original **Bitcoin** chain, kept the largest amount of economic activity on it, and therefore deterred both users and miners from supporting forks.

As of 2023, it's very unlikely that another cryptocurrency would truly compete with **Bitcoin**. Ethereum can burn as much as they want of the supply, they won't undo the harms of their premine of 70 million coins and



their financial policy will always resemble a central bank making short-term decisions for ever-changing goals. Monero can flaunt its superior privacy, but it can't survive without XMR/BTC swaps which enable merchant adoption and acceptance in the greater economy. And if something radically better comes along, which uses an entirely different architecture that gets rid of the blockchain, it would take years for it to get to **Bitcoin's** level of recognition and adoption.

A secure and decentralized **Bitcoin** whose scalability and privacy get upgraded in layers is very close to ideal money. However, it's going to take a few more years until the technology gets polished to the extent that it becomes accessible to non-technical users who also don't speak English. Which is enough time for bad actors to test the market with half-baked solutions that may indirectly damage **Bitcoin's** reputation and slow down adoption.

Ultimately, **Bitcoin** is the culmination of three decades of research in cryptography and computer science. It's an interesting marriage between game theory, technology, and economics which was never bettered. It's the network which survived every wave of FUD and perpetually hit new all-time highs against gold and the US dollar. And it's the currency which remained number one in terms of adoption and market capitalization for a decade and a half.

Today, nobody speaks about Peercoin, Vertcoin, and NXT anymore. Nobody still believes that DASH, Nano and Decred will replace **Bitcoin**. Today, we have coins with similar ambitions but different names – they will most likely follow the likes of Vertcoin into the graveyard of failed crypto experiments. The amount of people who truly believe that the politically-fragile Ethereum is a real contender is also small – let's not forget that the Ethereum ICO raised BTC and was a financial event that mostly bitcoiners attended and backed.

The longer **Bitcoin** exists and the more people learn about it, the more resilient it gets. And the fact that it has an immaculate conception, humble beginnings, and an organic growth makes it even harder to reproduce as a phenomenon. It takes the right historical context, the right technological innovation, and the fitting economic environment to create and launch something like **Bitcoin**. Which is why it will probably never get replaced by another cryptocurrency.

Sorry ChatGPT, but you and your programmers are once again wrong.

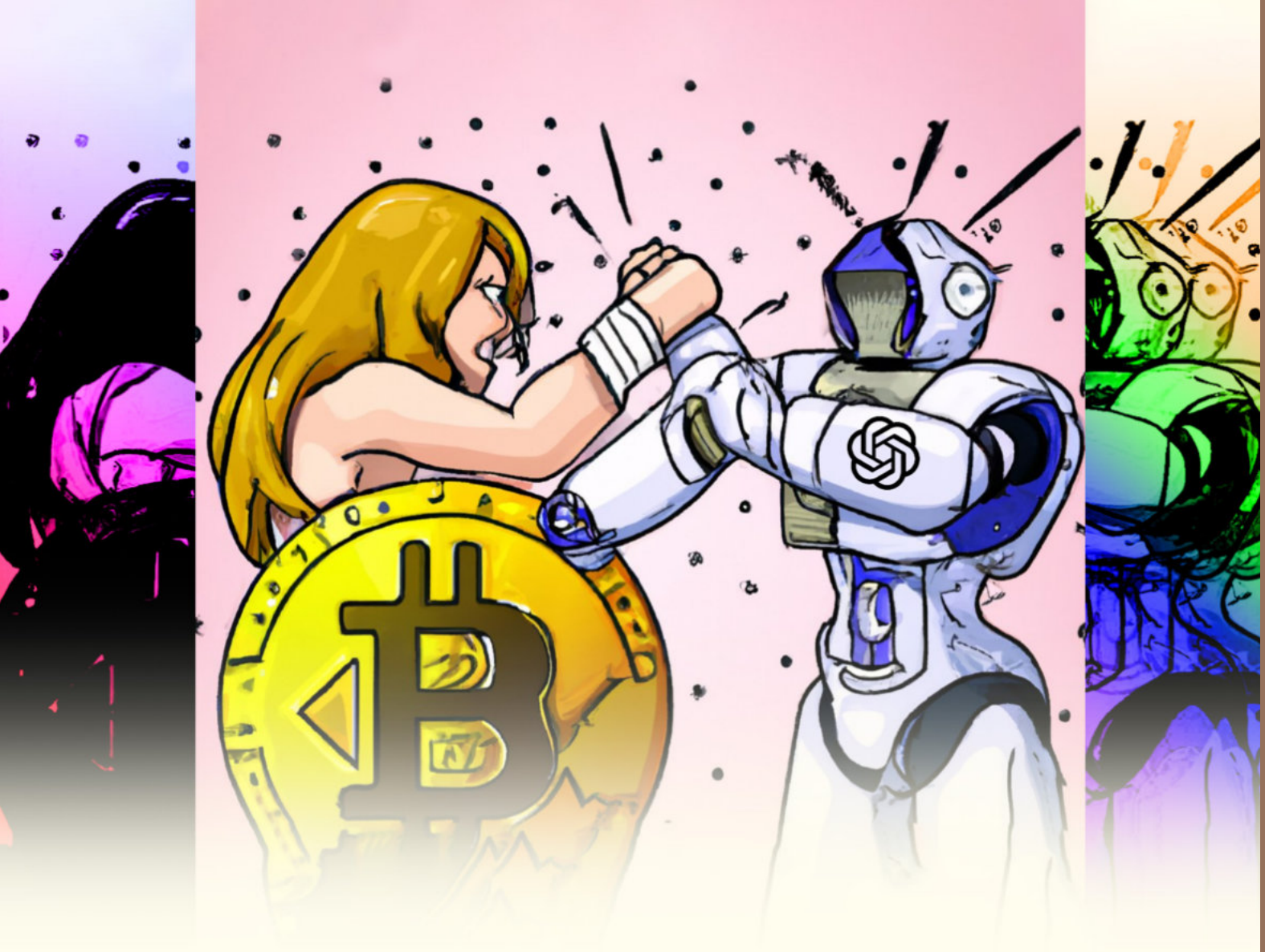


SCORE
Vlad C. 2
ChatGPT 0






HODL HISTORY
WASABI WALLET
DOWNLOAD NOW AT
WASABIWALLET.IO



Breaking ChatGPT's Bitcoin FUD #3:

Scaling

HOW BITCOIN SCALES | SEGWIT | SCALABILITY

WHAT DO YOU THINK ABOUT THIS ARTICLE? LEAVE YOUR COMMENTS OR SEND A DONATION BY SCANNING THIS QR CODE!

According to **ChatGPT**, the limited number of transactions that the **Bitcoin** network can process might become a bottleneck as adoption grows. This is a really valid criticism for **Bitcoin**, as no blockchain can scale. As a matter of fact, James A. Donald first said it to Satoshi Nakamoto on the cryptography mailing list back in November 2008: "it does not seem to scale to the required size". This was the first public feedback that Satoshi Nakamoto received about **Bitcoin** and it concisely outlined the limitations of the system.

Interestingly, the same e-mail from James A. Donald also gave away a potential solution for wider adoption and scalability: "a file trading network akin to Bittorrent". In other words, another layer that's fast, direct in the way that it connects peers, and capable of handling a number of transactions which is only limited by every user's bandwidth. Something that doesn't need a blockchain and doesn't become bloated and

centralized if there's too much activity going on. Also, a system that's very much like Bittorent in its design and therefore doesn't make every user store, verify and validate everyone else's data. This all sounds an awful lot like the Lightning network, doesn't it?

Re: Bitcoin P2P e-cash paper

James A. Donald | Sun, 02 Nov 2008 17:55:45 -0800

Satoshi Nakamoto wrote:

> 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

We very, very much need such a system, but the way I understand your proposal, it does not seem to scale to the required size.

For transferable proof of work tokens to have value, they must have monetary value. To have monetary value, they must be transferred within a very large network - for example a file trading network akin to bittorrent.

To detect and reject a double spending event in a timely manner, one must have most past transactions of the coins in the transaction, which, naively implemented, requires each peer to have most past transactions, or most past transactions that occurred recently. If hundreds of millions of people are doing transactions, that is a lot of bandwidth - each must know all, or a substantial part thereof.

The Cryptography Mailing List
Unsubscribe by sending "unsubscribe cryptography" to

James A. Donald's technical criticism was truly visionary, as he predicted both the scaling wars that would take place in **Bitcoin's** first decade of existence and he also suggested a way to increase the velocity of the currency. However, this 2008 statement alone doesn't break **ChatGPT's FUD** – a proper contextualization is required in order to highlight the current strategy for scaling Bitcoin and why it's very likely to work.

First of all, why does **Bitcoin** deal with scalability issues at all? It's all in the nature of decentralization and how blockchains work. The first instinct is to make the network mine larger blocks at a faster rate – but doing so only makes it more difficult for regular users around the world to validate their own transactions like every sovereign bitcoiner should. Conversely, the other side effect of increasing the block size is the requirement for more powerful hardware – with a slippery slope which ends at servers and industrial-grade computers which effectively defeat the purpose of decentralization. Once you get to a certain block size (as BSV did), you might as well use PayPal.

The ideal network needs to be secure, decentralized, and scalable. But according to Zooko's popular triangle, computer networks can only have two of them and must choose their tradeoffs – with the intention to complement them in some other way. By far, security is most important. Without it, financial transactions have no finality and are therefore worthless. But physical cash and gold also have good finality. So it's decentralization that represents **Bitcoin's** main value proposition – it accomplishes to offer access to a global financial network without the need for banking institutions and with no controlling third party actor in the middle. Anyone can participate in mining and validation, anyone can download a wallet and receive coins even if they delegate validation to another node (SPV, or Simple Payment Verification). Nobody can censor a transaction, confiscate the funds, or restrict specific individuals from using the network. Without these qualities, **Bitcoin** is no different from PayPal.

But all of these come at the expense of limited scalability. Bitcoin mines a new block at an approximate rate of 10 minutes



and adds about 2000 new transactions that receive confirmation. The system is not terrible for this early stage of adoption. Its design, with an arbitrarily limited block size, is supposed to enable a burgeoning and competitive fee market which supports the miners' revenue. However, **Bitcoin** must be able to accommodate all financial transactions of the world in an uncompromising way – and it accomplishes this feat through layers.

In time, using the base layer will become too expensive for most people around the world. Thankfully, everyone will have a Lightning channel or sidechain to use with various tradeoffs: for the sake of speed and cost-efficiency, these higher **Bitcoin** layers can be more centralized. Since security must remain a constant and the highest level of decentralization is also the most expensive way to transact, it will be the latter value that gets lowerred in order to increase scalability and convenience.
Though lowering the decentralization is not ideal and might become dangerous in some instances, what matters the most is that users get to choose between competing layers and they also benefit from the option to not rely on a trusted third party. For example, users can already opt for custodial Lightning solutions – which offer cheap, instant, and private transactions at the expense of trusting the custodian. What keeps entities such as Wallet of Satoshi, Alby, Tippin and BottlePay honest is the competition from other similar and non-custodial services, as well as the looming threat that users will open their own Lightning channels and therefore stop supporting the service with their transaction fees. The same goes for sidechains, federations, Chaumian mints, and other parallel chains. Since it's in their best economic interest to have a large user base and stay competitive, they are far less likely to exit scam. Of course, this doesn't sound ideal – but it's better than **Bitcoin**'s current dominant scalability option which involves centralized over-regulated exchanges that act as banks and alternative blockchain networks which make use of experimental features and onboard newbies in a way that provides education with both using wallets and getting scammed.
Increasing the blocksize to fit more transactions is not completely off the table in the distant future, but no reasonable size can accommodate all financial transactions around the world. When storage gets even cheaper and 5G internet connections become common with affordable data plans even in the least developed nations, the community might decide to hard fork in order to increase the block size and therefore allow more users to open Lightning channels and peg into sidechains at lower costs. For example, 32 or 64 megabyte blocks might be reasonable in 2040. But if on-chain transactions keep on getting smaller and more efficient via soft forks (as was the case with SegWit in 2017), we might not need any kind of hard fork.
The biggest issue with increasing the block size is not storage or bandwidth, but social consensus and the slippery slope theory. Some will argue that making such a significant change will only prove that it's possible to coordinate to arbitrarily change **Bitcoin** – and therefore generate more such similar events to the point where the block size either gets unreasonably big or else the community gets too fragmented while supporting different versions of the chain. It's much easier to deal with parallel chains and second layers, whose potential failures do not break the base layer's security and decentralization.



Furthermore, increasing the block size does not guarantee that the blocks will get filled all the time. Such an action directly generates lower transaction fees for miners due to lower competition to get into the next block. During times of low demand for block space, when the coinbase rewards will already have been cut in half a few times, this can effectively pose a security threat to **Bitcoin**.

To directly address **ChatGPT's FUD**, **Bitcoin** is scaling and will get better at scaling as more layers get developed. The limited number of transactions that can fit into a block can be Lightning channel openings and sidechain peg-ins which endow users with the ability to transact in a fast, affordable, and scalable way. The only issue is that these layers come with various decentralization tradeoffs. But they're still more decentralized than altcoins, centralized exchanges, and other forms of trying to poorly replicate or else replace **Bitcoin** with awfully designed systems.

The criticism is valid, but it lacks context and nuance. So once again, ChatGPT takes an L.

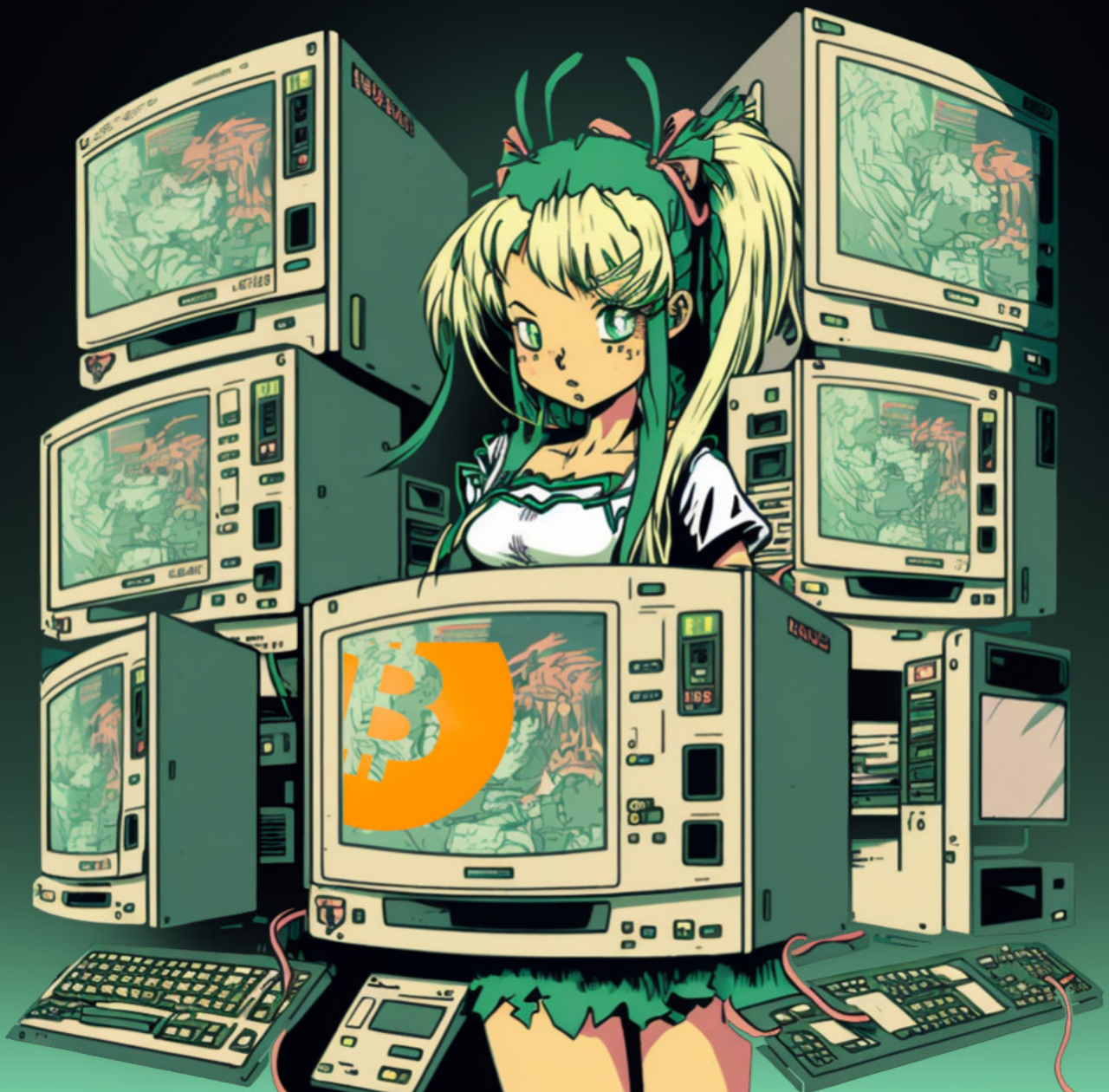


SCORE

Vlad C. 3

ChatGPT 0






YOUR
SEED
PHRASE
cryptosteel
cryptosteel



YOUR BACKUP

THE ORIGINAL SINCE 2013

cryptosteel



Breaking ChatGPT's Bitcoin FUD #4:

Security Vulnerabilities

BRUTE FORCE SHA256

WHAT DO YOU THINK ABOUT THIS ARTICLE? LEAVE YOUR COMMENTS OR SEND A DONATION BY SCANNING THIS QR CODE!

According to **ChatGPT**, the increasing popularity of Bitcoin attracts hackers and other malicious actors. But what can these hackers actually break?

Well, there are multiple layers of **Bitcoin** security. We can talk about mining and potential 51% attacks to reorganize the most recent blocks, we can look into the odds to brute force a wallet to find its private key, or we can take the easy way out and assume an increase in social attacks (malicious developer inserting harmful code, or individual **Bitcoin** users getting tricked into losing their coins).

First of all, the 51% attack is one of **Bitcoin's** biggest security threats – and one which is part of the Proof of Work design. The idea that a simple majority of the miners' hashrate can act in bad faith is a serious attack vector. However, the incentives of the so-called Nakamoto Consensus are designed in such a way that playing by the rules is more profitable than trying to attack the

system. Buying and renting the mining equipment, then consuming a lot of electricity in order to double spend transactions and reorganize the most recent blocks is not cheap at all.

At more than 360 exahashes per second in hashrate, even the most resourceful governments and transnational corporations in the world would struggle to amass 51% of it. Furthermore, supercomputers are not optimized to run SHA-256 hashes like the **Bitcoin** ASICs – so if you put together all the supercomputers in the world, you only get the equivalent of a very tiny and insignificant mining pool.

Running a 51% attack on **Bitcoin** requires purchasing or renting scarce and highly-specialized hardware which is currently being used to secure the network while earning rewards for playing by the rules. The financial incentives matter, and have so far kept the miners honest, focused on their goal, and efficient with their energy use. Anyone pursuing this type of attack against **Bitcoin** requires lots of resources to sustain it. The greatest risk that the attacker faces is that the honest network participants fork off to a new chain which copies the UTXO set to retain the rightful coin ownership. Such an effort offers no guarantees of any profitability or success – which at its best can serve as political FUD against the network's security. If the financial incentives remain a constant, we'll most likely never see any kind of serious 51% attack.



Even the large pools, which consist of multiple users who put their hashing power together in order to share the rewards, are subjected to a type of game theory that keeps them honest. Under governmental pressure, they could prefer to stop mining altogether to opt out from attacking the network. Turning off mining operations will cause disruptions for the remaining blocks of the cycle, but after every 2016 blocks (approximately 2 weeks) there's a new difficulty readjustment and there's always someone else on a different part of the world who is willing to start mining when the odds to successfully find the right hash become higher. **Bitcoin** is extremely well thought out and there's a reason why these attacks were never really successful – not in the early days when they were easier to pull off, not today when the number of highly-specialized mining machines that secure the network is higher than ever.



Furthermore, **ChatGPT** claims that malicious actors would emerge as a consequence of the increasing popularity. So from the get-go, launching 51% attacks shouldn't fall under this description – as more users joining will also result in more mining rigs being deployed. However, it was important to explain since the AI software doesn't directly allude to the issue.

Secondly, let's talk about brute forcing wallets in order to find the private key which allows hackers to steal the funds. It's certainly a type of security vulnerability that theoretically should become more widespread as Bitcoin gets mass adoption. Every internet hacker ought to attempt to brute force wallet files, try to guess valid BIP39 seed phrases, and generate correct passphrases. Good luck with that, though – you have better odds finding intelligent alien life on a distant planet or digging up a particular grain of sand in the desert.

Let's take the most obvious example: Satoshi Nakamo-



to's coins. The fabled million, as described by Sergio Demian Lerner in his Patoshi research project, is the ultimate bounty. There's no proof that this theory about what Satoshi might own is correct – it's a mere analysis which assumes that Satoshi constantly mined. But the resulting coins, to whomever they may belong, are in plain sight and haven't moved since 2009. Everyone knows about their existence and can track them on the public ledger. However, nobody can brute force the private keys in order to claim ownership of them.

To put everything into numbers, **Bitcoin** has a total number of 2^{256} possible private keys and only 2^{160} combinations of addresses that can exist (assuming that they're all 160 bits). Yet brute forcing must start from an existing and valid public key. Which in and of itself requires extra effort.

A more efficent way to brute force wallets involves trying to find one of the 2^{96} private keys that collide with the same address. The number of possibilities is 79,228,162,514,264,337,593,543,950,335 – about 79,228 times more than the estimated number of stars in the universe. On the other hand, if you want to brute force a specific wallet (like Satoshi's), you must deal with the entirety of 2^{256} private key combinations. Assuming that you possess the processing power to try 1000 trillion keys per second, going through ever key will take you an amount of time which is equal to 2.7×10^{44} × age of the universe (as pointed out by developer Raghav Sood on the **Bitcoin** StackExchange). This number exceeds anything that's measurable to man – including the amount of atoms surrounding our observable world.

As for BIP39 seed phrases, there are 2048 words and 12/24 combinations of them. For the sake of convenience, let's assume a basic 12-word setup. In order to guess a random one, you have 2048^{12} (or 2^{132}) possibilities. To quote Reddit moderator BashCo, that number is one in 115 quattuorvigintillion 792 trevigintillion 89 duovigintillion 237 unvigintillion 316 vigintillion 195 novemdecillion 423 octodecillion 570 septendecillion 985 sexdecillion 8 quindecillion 687 quattuordecillion 907 tredecillion 853 duodecillion 269 undecillion 984 decillion 665 nonillion 640 octillion 564 septillion 39 sextillion 457 quintillion 584 quadrillion 7 trillion 913 billion 129 million 639 thousand 936.

If you're certain that one of the 2048 words must be the first one, then your odds turn into 2048^{11} – because in BIP39, you can have words getting repeated in the same setup. And if you have the first 10 words in the correct order and only need your 11th and 12th one, you only have 2048^2 possibilities – which already makes it brute forceable today with a regular computer processor. So take good care of your seed phrase and, if you feel comfortable about it, add a passphrase on top from outside of the BIP39 dictionary. This will greatly improve your security, but might only become problematic if you forget/lose your passphrase.

But generally, as Peter Todd and BIP39 co-creator Pavol "Stick" Rusnak pointed out, it's very impractical and akin to stating that you can park 500 cars on a football pitch. Peter's suggestion was to delete it altogether, as



the efficient type to attack BIP39 seed phrases is to brute force the private key it generates.

Yes, quantum computing might become a threat in the future. But this future is very distant: as of March 2023, the most powerful quantum computer in the world is IBM's Osprey – a machine that touts 433 physical qubits. As pointed out by a 2022 research paper which got published in the AVS Quantum Science journal, a computer that aims to break **Bitcoin**'s elliptic curve public key cryptography within 24 hours requires 13×10^6 qubits. In other words, quantum computers need to become thousands of times more powerful to break bitcoin.

So far, the technological leap in quantum computing slightly exceeds Moore's law. For prediction purposes, let's use this model to assume that the pattern continues and the amount of qubits keeps on doubling every 2 years. In order to get from 433 to 13×10^6, quantum computers need to become 30023 times more powerful. That's at least 20 more years before we should seriously start to get worried.

It took 24 years of research and development to go from 2 qubits to 433 qubits. How long until we reach 10000 qubits? Probably a few more decades. At 10000 qubits and some very specific physical conditions (a code cycle time of 1 µs, a reaction time of 10 µs, and a physical gate error of 10^{-3}), a quantum computer will be able to steal the coins from an arbitrary **Bitcoin** wallet in 10 days. However, cryptography will also improve tremendously by then and Bitcoin might migrate towards a better model that makes brute forcing so difficult that quantum computers need a lot more time to catch up.

Upgrading to quantum-resistant keys only requires a soft fork which can be activated by a majority of nodes or miners. So this whole discussion might just turn out to be a paper tiger – or an unworthy piece of FUD.

Now that we got these two very complex and extremely expensive attacks out of the way, it is time to focus on the most probable ones: the social attacks. In **Bitcoin**, we like to say "don't trust, verify". However, establishing trust systems which remove doubt about potential maliciousness from developers is one very serious attack vector.

The easiest way to mitigate any kind of attack is to remain conservative about code: don't update to the latest version unless you verify it beforehand or pay someone else to do it for you. And if you do neither, at least make sure that enough people with adversarial incentives have verified the new code. When the stakes are so high that the global financial system is under threat, it's safe to assume that developers are under a lot of pressure and might make mistakes or get compromised.

This is not an argument for ossification, though: **Bitcoin** is not complete as a project and refinements are still necessary. From adding privacy to making transactions smaller and all the way to providing resistance against quantum computing attacks, there's still a lot to do. My argument is against being reckless with untested technology whose consequences are not entirely understood, but not against innovation.

Nonetheless, while pursuing innovation, we should not surrender verification to urgency. As a community, we should encourage **Bitcoin** developers to prepare options before the threat becomes imminent: models for quantum-resistant elliptic curve cryptography, scalable privacy, and so on. Some of these solutions are already being tested with market incentives on other networks – what matters the most is that **Bitcoin** developers pay attention to the



legitimate technological improvements, refine what's already out there, and bring out proposals that everyone must debate. Also, we should never neglect our roles as sovereign node operators and miners – we are the ones who choose which code we run and **Bitcoin** clients can work with some minimalistic specs. Not everything that's been added to Core is necessary, but the well-tested features provide useful optimizations.

Last but not least, we must talk about the security of every individual **Bitcoin** user. This, most likely, is the primary type of FUD that **ChatGPT** expressed when it mentioned hackers and malicious actors. Anything between keyloggers that register and broadcast your computer keyboard inputs (which may contain your **Bitcoin** Core passphrases or BIP39 seed phrase) to affinity scams and physical attacks is increasingly more likely to happen as the price of BTC gets higher.

The bad news is that no developer, protocol change, governmental or non-governmental entity is able to protect you from making mistakes. The good news is that there are some general good practices that you can follow in order to improve your security. They include:

- using a dedicated device to sign and broadcast **Bitcoin** transactions (a Linux laptop or phone that runs **Bitcoin** full node software while being used, BIP39 hardware wallets with strong passphrases);
- creating setups which eliminate single points of failure (multisig and SLIP39 Shamir backups);
- using cold storage (metal plates, paper wallets, physical **bitcoins**);
- protecting yourself through good operational security and privacy (don't reveal to random strangers where you live, what your **Bitcoin** setup is, and how much money you have – this also includes living a materially normal life for your neighborhood/community without showing off). Remember: leak as little information about your **Bitcoin** activity as you can, or at least mislead your spies to have a distorted image of what you're really doing and how wealthy you are.

Bitcoin is a currency which enforces absolute ownership. Which means that, once a transaction has been broadcast and confirmed into a block, it has become irreversible. Therefore, every user is responsible for protecting their wealth to the best of their knowledge and ability, according to a real threat model. Before you create any kind of setup, you must ask yourself "who is the most dangerous adversary that's likely to try to steal my coins?".

If you're sharing the computer with other people, then you shouldn't



leave behind unencrypted wallet files. If you're traveling, then it's a bad idea to carry around devices which reveal that you're carrying **bitcoin** (usually, a hardware wallet is easier to recognize and more suspect than a laptop or piece of paper). If you have children or a nosy spouse who might meddle with your file cabinets and drawers, then it's better to not keep your backup within reach. If you live in a bad neighborhood with high crime rates, then you should probably avoid keeping any **bitcoin** backups in your house. And if your area is under the threat of floods, fire, volcano eruptions, or earthquakes, then you need to figure out a system with good geographic distribution that simultaneously makes it impossible to lose everything and easy for you to access the other keys/parts of your backup.

However, the most common threat consists of internet hackers. You can find these criminals under the form of individuals who illegally try to break into your computer, as well as suit-wearing businessmen who design systems that essentially steal your coins within a legal framework. From the first category, you can distinguish people who code malware or else befriend you to later ask for money (whether it's a Nigerian prince or an OnlyFans model who desperately needs help). The second category consists of exchanges and banks, who promise to custody your coins in a safe environment but will restrict you from withdrawing whenever their business model is under water. You should avoid both of these hackers at all costs, as they are the most likely to steal your **bitcoin**.

While it's convenient to deposit your coins in some bank account, this type of action defeats the purpose of the Bitcoin project and greatly diminishes your own financial sovereignty. Trusted third parties are security holes and you should never trust an individual or company who promises to hold your BTC in exchange for security and/or yield.

Of course, there are other types of social attacks: fake exchange e-mails asking you to verify your seed phrase in a reply, callers impersonating a wallet service which asks you to confirm your data (sometimes even a home address) hardware wallet deliveries getting intercepted and compromised via BIP39 seed phrase insertion (the attackers leave their own seed phrase in the box, hoping that newbie users will send their coins there), $5 wrench attacks, and impersonators who pretend to be friends or family members who urgently need a money delivery. These are the ones that become more common as the price and adoption go up. Which is why you need to be aware of them and protect yourself by minimizing the amount of data you provide about the services that you use, the place where you live, and the amount of **bitcoin** you have.

Getting back to **ChatGPT**'s argument, it's disingenuous to assume that people getting scammed is a serious threat to **Bitcoin**. The network will exist and continue to function in spite of the thieves. Sure, a large number of people might feel scared and deterred by the idea of responsibility. But we shouldn't forget that self-custody solutions also get more secure and user-friendly over time. **Bitcoin's** layers also get more developed and new ways to use and store your money get unlocked. For example, the Fedimint project plans to enable community banks in which users can unlock their funds with nothing but a selfie. Also the Wizardsardine recently launched their Liana to make it simple to lock your bitcoin until a future block height of your choice. This makes long-term holding and inheritance easy and free even for technical users who don't understand Bitcoin's script. You could have done it in Bitcoin Core and Electrum all-along, but now it's even more user-friendly.

Hackers and malicious actors exist in every money system and human organization. What matters the most is to build a culture of fairness, accountability, good practices, and truth.

As long as these are in place, ChatGPT is gonna be taking a big L for being so wrong with its FUD.

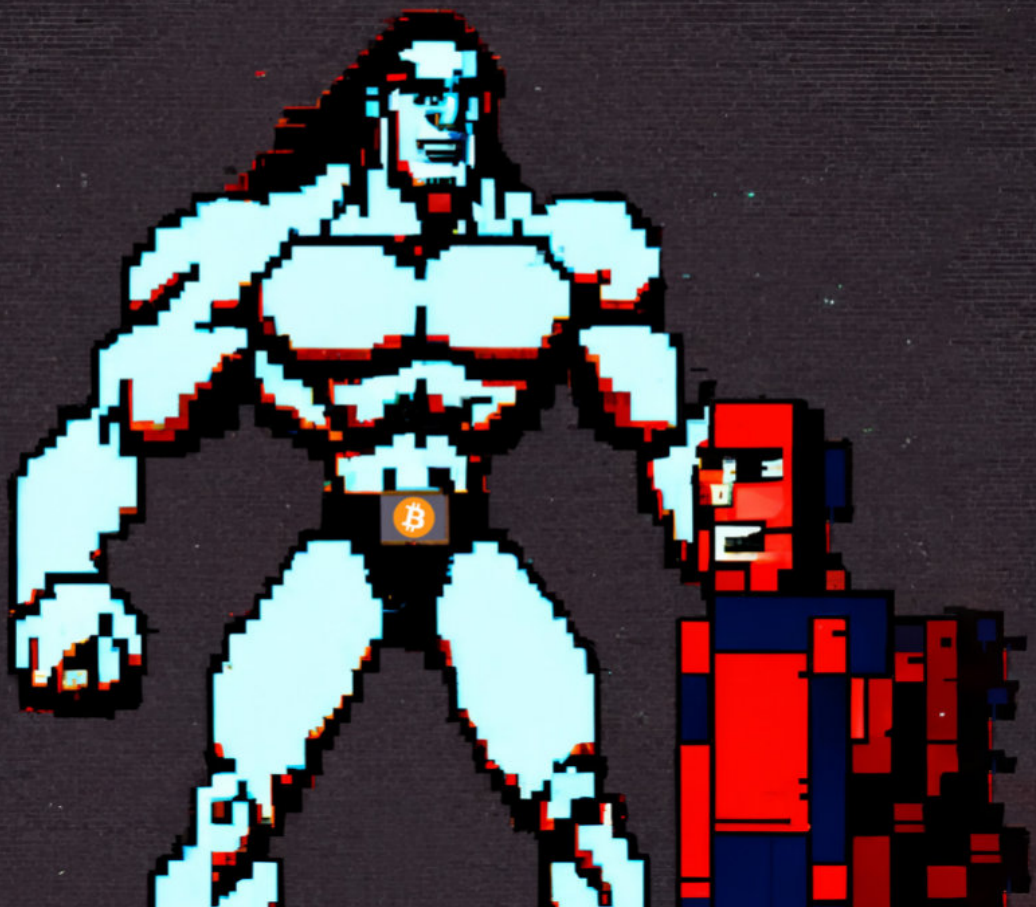




SCORE

Vlad C. 4

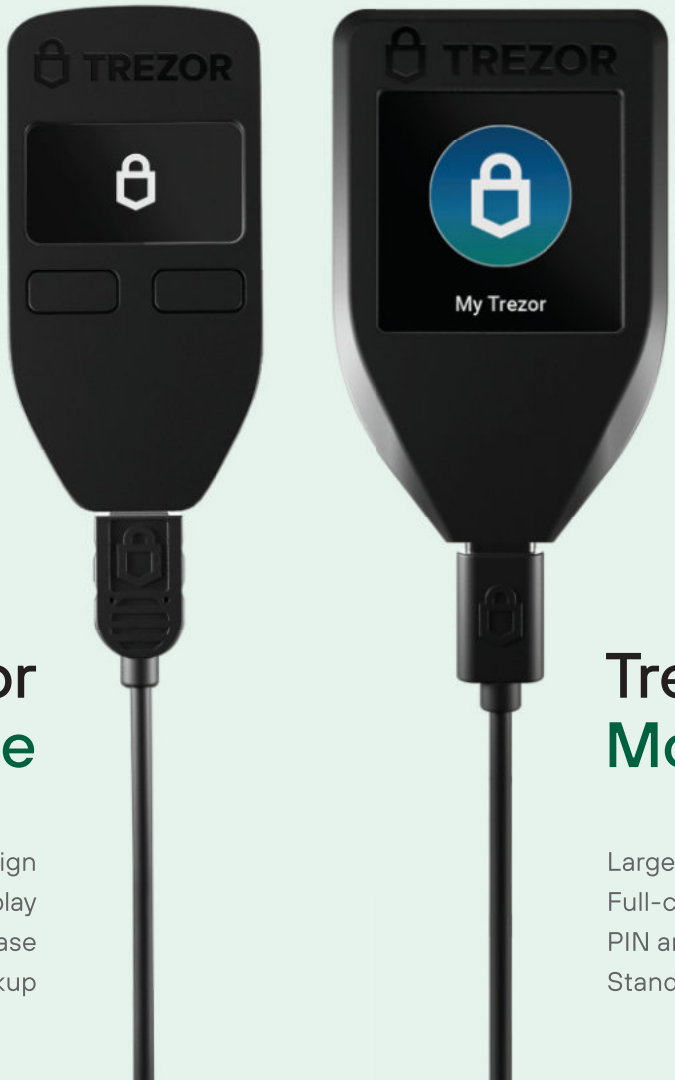
ChatGPT 0



TREZOR

Putting control in your hands.

Take control of your Bitcoin with a Trezor hardware wallet.
Boost your privacy and manage coins securely, with the integrity and independence of open-source design.



Trezor Model One

Simple durable design
Monochrome trusted display
PIN and Passphrase
Standard backup

Trezor Model T

Large comfortable touchscreen
Full-color trusted display
PIN and Passphrase
Standard or Shamir backup

Find out more at **trezor.io**



Breaking ChatGPT's Bitcoin FUD #5:

Price Volatility

BTC-USD **VOLATILITY** **BULL/BEAR MARKETS**

WHAT DO YOU THINK ABOUT THIS ARTICLE? LEAVE YOUR COMMENTS OR SEND A DONATION BY SCANNING THIS QR CODE!

According to **ChatGPT**, the fifth most serious threat to the **Bitcoin** project is the price volatility of the bitcoin currency. The assumption around this statement is that the constant and unpredictable swings against fiat money are supposed to deter people from adopting BTC as a medium of exchange and/or store of value.

There are two ways to break this FUD, which also happens to be the most popular in mainstream media: one is technical, the other one is comparative. The former is introspective, the latter questions the meaning of the word "volatile" by presenting recent examples from the supposedly "stable" financial world.

First of all, let's do a little bit of technical analysis on the price of **bitcoin**. For reference, we're going to use the values provided by the BTC/USD chart on the Bitstamp exchange – which has been tracking the price since August 2011. Over the course of nearly 12 years, BTC went up 243,207%. The price discovery phase has witnessed 3 distinct bull



cycles and the same number of bear markets. And on the longer term (3-4 years), the volatility has always been upwards – which made bitcoin a pretty good store of value.

Furthermore, there's a lot to be said about how volatility decreased over time. Just by looking at the long-term logarithmic chart, one can notice how both green and red candles were bigger back in the day. The liquidity was lower, the number of users was likewise smaller, and it was easy for a few whales to manipulate the price in either direction. But as adoption grows, a larger number of users transact with bitcoin on a regular basis. And as the BTC amounts end up in more hands, the volatility also decreases.

This isn't a mere theoretical observation – you can see it in the quantity of resistance and bounce-backs that take place after every dump. For every seller, there are instant buyers around the world. And even when the price is oversold, you will always find someone on the other side to immediately buy the dip. It appears that the trading became a little more professional, with resistance patterns that one can also notice on Wall Street. With each boom-crash cycle, the downwards volatility also gets lower.

During the 2013 bull market, the price rose to $1237 in December – only to crash to $687 three days later. During the coming bear market, **bitcoin** went as low as $179.13 in early 2015. That's a 85.5% drop in about a year, which was a



consequence of poor exchange development and limited options to buy and trade bitcoin. As the financial infrastructure and adoption increased, the situation got better.

The situation changed a little bit during the 2017 bull market, when the amount of liquidity clearly increased. The December 15th all-time high was $19345, while the 2018 bottom happened at around $3196. This was great for early adopters, but really painful for everyone who bought around the top – as the 83.4% drop was lower than the previous one, but still brutal.

If you're reading this, then you most likely already know the story about the November 2021 all-time high of $68789 and the bottom of $15877 which came a year later. This time, the gap between the top and the lowest point is of 76.91% – thus indicating more resistance and conviction in the asset. While the numbers are still not ideal, they do point out to a gradual lowering of volatility.

Regardless, this data is still not good enough for mainstream economists and journalists. They will

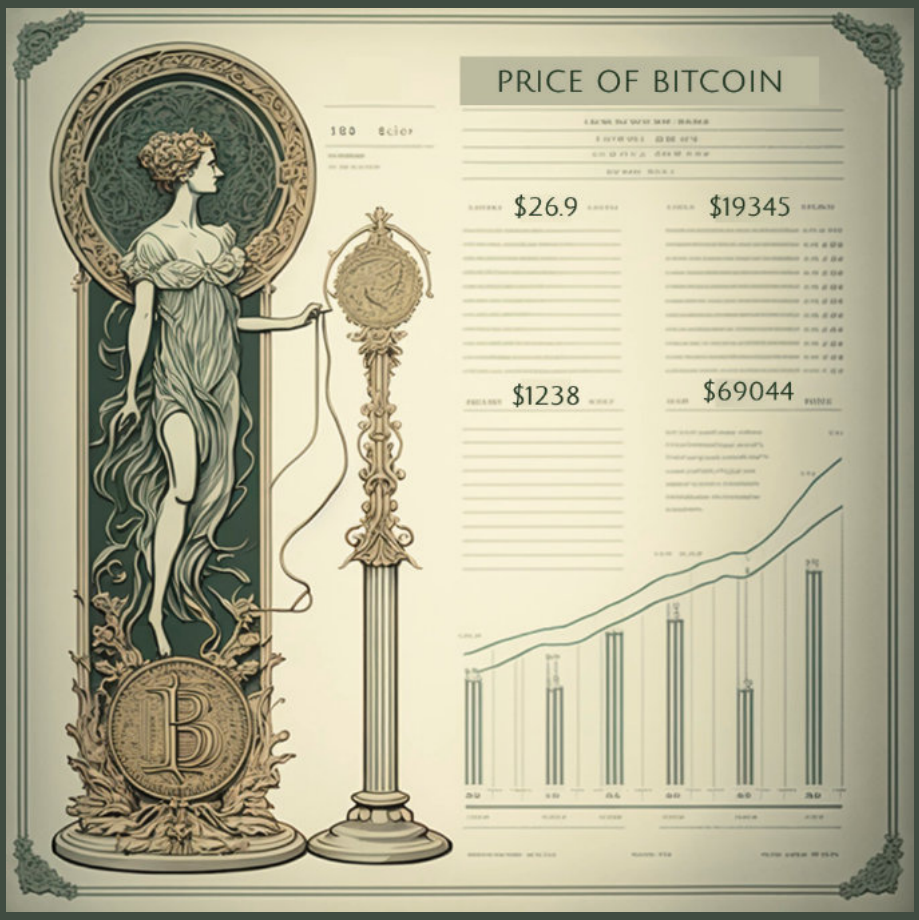
claim that even a 5% daily movement is too volatile for a currency. As December 2013 proved, the price can drop by 44.4% in only 3 days! So this is neither a store of value, nor a medium of exchange. Central banks under the fiat money standard will prevent this from happening, right?!

The following counter-arguments are only a few examples that happened in 2023: on March 10th, Silicon Valley Bank failed to survive a bank run. A couple of days later, Signature Bank followed. Two "too big to fail" institutions, which managed money deposits worth billions of dollars and whose customers were important start-ups from the technology industry, went to 0 and needed the US Federal Government to step in to bail out the depositors.The next day, all hell broke loose in the land of regional US banks: the stocks of First Republic Bank plunged by 70%; PacWest Bancorp also lost more than 40% in stock value; and then Western Alliance Bancorp stocks witnessed a 30% drop. Just in case it wasn't clear already: all of this happened in a single day.

In Europe, Credit Suisse (the 2nd largest bank in Switzerland) witnessed a 25% stock crash which resulted in the Swiss government getting involved to arrange a buyout by UBS (Switzerland's largest bank). This was a soft bailout, as Credit Suisse's efforts to take loans and sell some of its property only resulted in increasing the magnitude of the bank run. In France, BNP Paribas stocks also collapsed by 8% in a single day – which resulted in interventions to halt trading.

So when bitcoin lost half of its market valuation within 3 days in December 2013, the outcome wasn't as dramatic as some of the events that first world bank depositors experienced in March 2023. After all, **Bitcoin** was a new project with low liquidity and a relatively small community of traders. It wasn't some 166 years-old Swiss bank, it wasn't the institution which banked most of Silicon Valley's start-ups, and the project didn't promise to perform banking duties or have low volatility by virtue of tradition or government intervention.

Bitcoin exists in a purely free market where the price dynamics are imposed by supply and demand. There is no central bank to halt trading when the currency is oversold or to bail out users who lose their coins. There is no support desk to call when someone steals your BTC or you forget your passphrase. Also, there is no entity to decide that they



should stabilize the price during times of high volatility. Every individual actor is his own bank, every person decides when is the best time to buy or sell, and everyone is responsible for securing their own access keys.

This may sound wild and frightening, but it works specifically because bitcoiners understand sovereignty, responsibility and scarcity. Bitcoiners also know that this financial computer network emerged at the peak of the 2008 financial crisis, when private banks were getting bailed out by their governments. Which is why high volatility under a free and honest system is preferable to crony capitalism.

But then again, what is volatility anyway? Since we established that "safe", "insured" and "too big to fail" banks can provably take daily plunges bigger than anything **bitcoin** has witnessed thus far, why aren't we complaining about these financial institutions being volatile and unsafe? Well, the most obvious answer is that banks control politicians and media outlets through funding. Not only that, but **Chat GPT** itself was financed by Microsoft and a bunch of VC firms that aren't quite **Bitcoin**-friendly. Their role is to preserve an old and well-established tradition, so anything that threatens their position must receive criticism at every step.

Another argument is that witnessing the collapse of banks is generally regarded as a "black swan event" because it occurs less frequently than a swing in BTC price. On a short-term chart, bitcoin appears to be more volatile because there is no central entity to set a daily exchange rate and sometimes people around the world can coordinate impactful events. But bank runs are also real – as we have witnessed in the first half of 2023, institutions are very fragile to mass withdrawals due to their high-risk approach to holding very little reserves. They exist at the mercy of central banks and governments, which may or may not bail them out in critical moments. And on a long enough term, they all fail.

What's interesting about **Bitcoin** the network and its underlying currency is that so far we've witnessed a trend of resilience against price volatility. For instance, Tesla famously bought bitcoin in 2021... only to sell it later in the year. The same happened with many hedge fund managers and large companies which invested a percentage of their money in BTC. But even during the moments when the big investors started leaving, the network had true believers who kept the project alive.

Bitcoin kept mining blocks every 10 minutes even when the miners weren't making much of a profit. Full nodes kept on storing and validating the entire ledger of transactions even in the absence of economic incentives. And developers kept on proposing refinements to the code even when nobody was paying them. Can anyone make similar statements about bankers going to work when they no longer get paid and institutions processing payments 24/7 in spite of dealing with tough market conditions?

Ultimately, the demand for bitcoin is proportional with the demand for freedom. For as long as people around the world get oppressed, abused, cheated, and robbed by institutions (governmental or private), the quest for financial sovereignty will continue. Free markets are much more resilient and have purer motivations than any form of centralized control. And as governments become more Orwellian and central banks print their way out of trouble while putting multiple generations into debt, **Bitcoin** is here to provide that hopeful escape from it all.

What's more volatile, something that changes at the whim of despots and irrational bureaucrats, or a system which relies on math and game theory?



SCORE
Vlad C. 5
ChatGPT 0



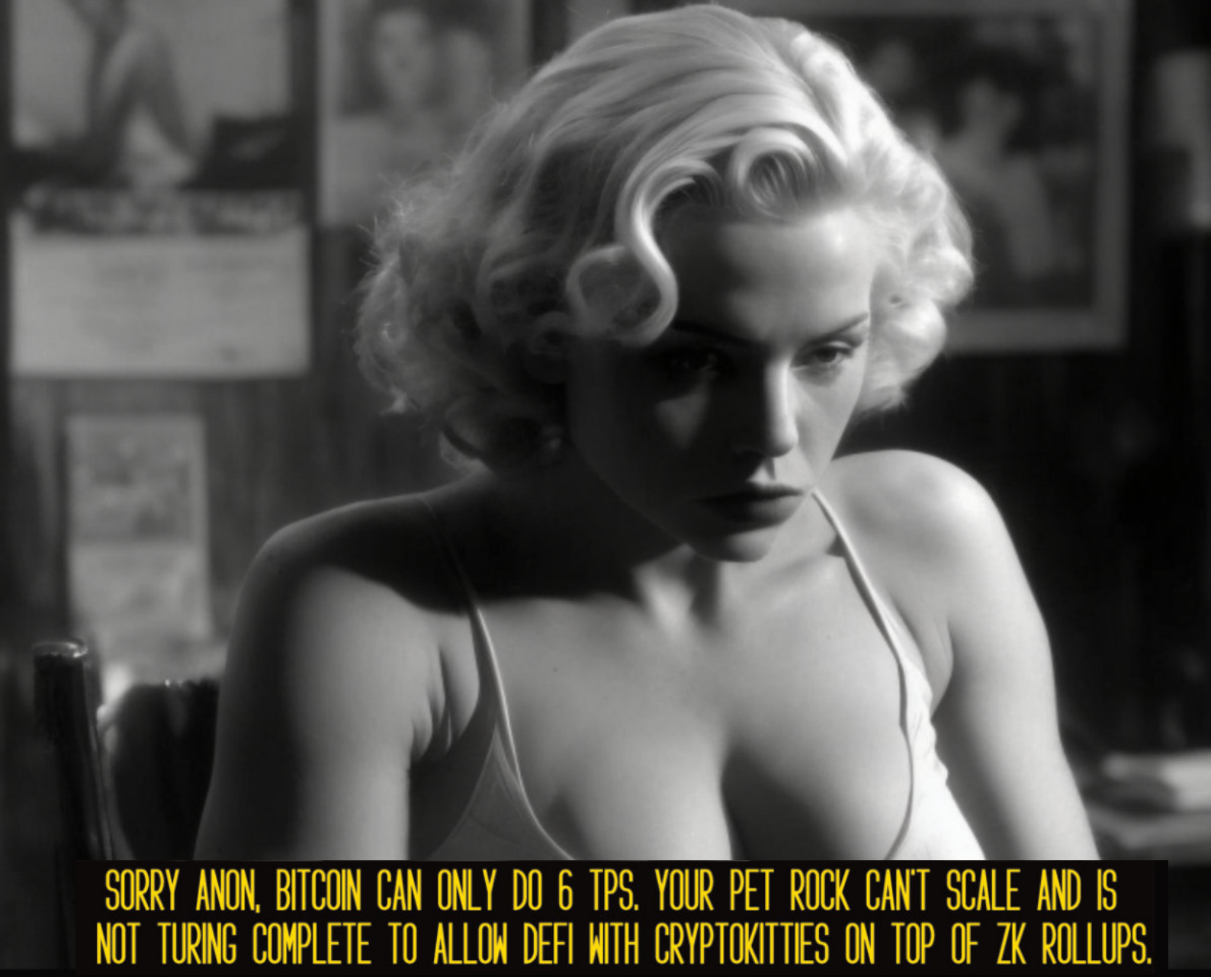
PANTIES FOR BITCOIN



FREEDOM

PANTIES FOR THE
SOVEREIGN WOMAN

Made in Italy



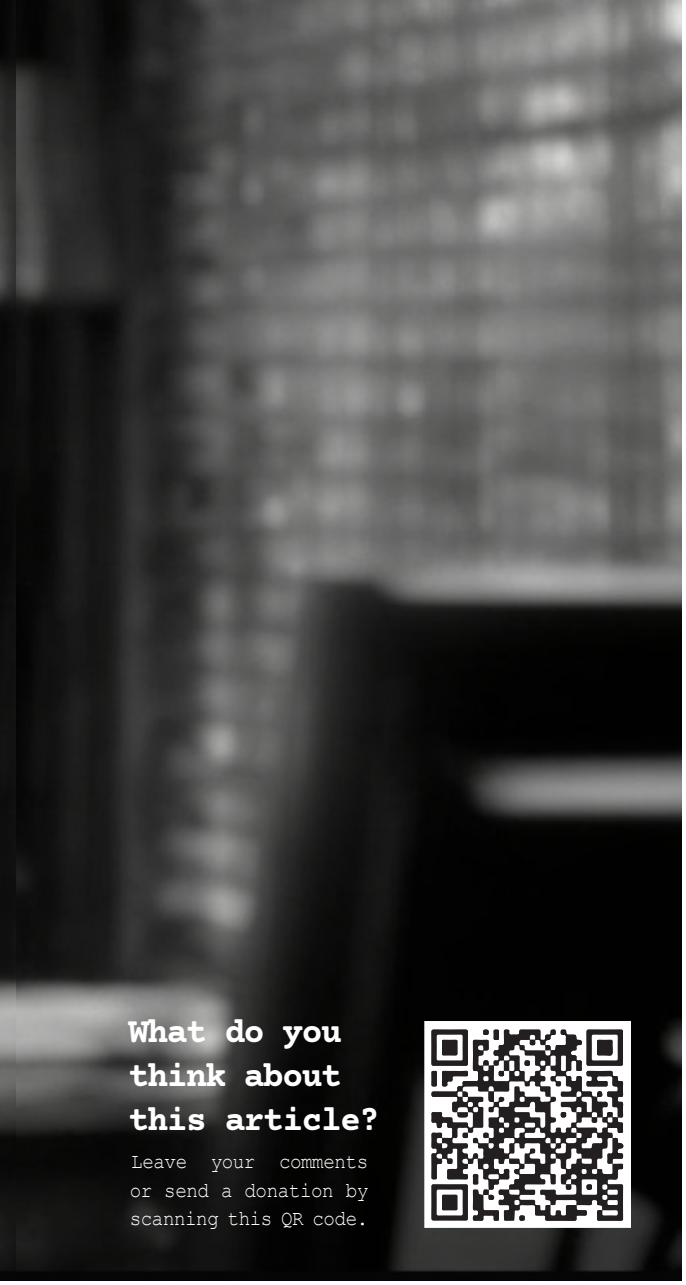
Breaking ChatGPT's Bitcoin FUD #6

Limited Use Cases

SCALABILITY TRANSACTIONS LAYERS SHITCOINS PROTOCOLS

According to ChatGPT, Bitcoin only accommodates a limited number of use cases, and this fact will consequently limit its adoption and growth. This is, by far, the silliest piece of criticism one can write about Bitcoin. There are two approaches to debunk it: one appeals to Bitcoin conservatism and the meaning of sound money in order to discredit the different use cases, while the other leverages the various technological breakthroughs that Bitcoin maximalists have made over the years with protocols, sidechains and second layers. Ultimately, both sides of the debate will explain why putting large amounts of data and running complex applications on the main chain is a bad idea which leads to inefficiencies that can be mitigated with more elegant designs.

In its current state, Bitcoin can already accommodate most of the altcoin use cases: it can do on-chain tokens and host decentralized exchanges with Counterparty and Omni, it can store files within the limit of 4 megabytes per



block, and it can do some basic smart contracts (multisig setups, conditional coin locks, dispensers). But there's still a lot that Bitcoin cannot do on its base layer, ranging from recurring payments to confidential transactions. These features exist on plenty of altcoins which experiment with them in different shapes and forms. However, just because Bitcoin currently doesn't enable them on the base layer doesn't mean that the world's dominant cryptocurrency is bound to remain stagnant and won't catch up by integrating the best-performing of implementations.

There's a conservative school of thought, mostly dominated by Austrian economists, who argue that Bitcoin doesn't need any of these use cases because sound money should be basic by design. They tend to believe that the imminent collapse of fiat money will make every person on planet Earth buy bitcoin and denominate all goods and services in the verifiably-scarce BTC. And while the likeliness of this outcome is low (fiat money and central banking will exist and get perpetuated under different shapes and forms for as long as people have faith in their governments and provide demand for whatever currency is being supplied), the idea is still worth considering.

Conservatives tend to label non-BTC tokens as scams,

refer to non-monetary uses of Bitcoin as fiat degeneracy, and slam other chains for being inefficient and poorly-optimized Rube-Goldberg machines. Some of this criticism is valid, but in many instances the free market disagrees with their ideology – there are people who don't care about sound money and simply want to fundraise with tokens, trade between assets without having a centralized exchange in the middle, create and sell tokenized art, and save their video game items on a neutral global network which can't get shut down by the developers. On the other side of the spectrum, there are freedom fighters and investigative journalists whose main concern is transaction privacy – they don't care about digital gold which serves the store of value function, they only want to send and receive money without leaving any kind of evidence regarding who they might be, with whom they are transacting, and which amounts are being moved.

Yes, many of these use cases don't require a blockchain.







And no, it's not a wise approach to direct these people to other chains which offer scalability and extra features at the expense of blatant centralization – not only because the underlying networks are fragile and deal with bad money that's most likely going to 0, but also because people should be using the hardest form of money on one of Bitcoin's layers.

Bitcoin maximalists provide a much more nuanced approach to this situation: instead of discouraging use cases not natively enabled by the Bitcoin network (or not scalable when deployed on it), they build layers on top of Bitcoin to accommodate the needs of different types of users and attract new market segments. Though in some cases conservative bitcoiners refer to themselves as maximalists, the distinction is in the maximization itself: someone who is against certain types of projects being built on a Bitcoin layer and believes that the 21 million BTC should only be used to make monetary payments doesn't really maximize anything – these people use ideology to justify remaining convservative.

My issue with Bitcoin conservatives is that they willingly and knowingly reduce the scale of adoption through purity tests. Their belief is that the collapse of central banking and the hyperinflation of fiat currencies will make every person on planet Earth start using bitcoin as money. This scenario requires a universal acceptance of free markets and a new paradigm for distrust in governments. Everyone would want to conduct peaceful, voluntary transactions instead of becoming violent for the purpose of seizing property and wealth. At least in our lifetime, this is a utopia… especially in a world where governments get bigger and more people rely on Big Brother to provide everything from education and healthcare to subsidies, financial aid, and employment.

Given these considerations, the thesis that I defend (not just for the sake of beating ChatGPT's FUD, but also because I happen to ideologically position myself on this side) is the maximalist one. In order to get mass adoption, Bitcoin shouldn't rest on its laurels and flaunt its qualities as sound money. Integrating more use cases to get everyone from business owners to artists interested in the project is a far better approach.

Some of the best Bitcoin maximalist projects include

Colored Coins, Counterparty, Omni, Blockstream's



Liquid sidechain, Rootstock (RSK), the Lightning Network, Paul Sztorc's Drivechains, Ruben Somsen's Statechains, John Carvalho's Synonym, Portal, Eric Martindale's Fabric, Maxim Orlovsky's RGB, Lightning Labs' Taro, Eric Sirion's Fedi, Calle's Cashu, and Casey Rodarmor's Ordinals. This list is somewhat chronological and covers protocols and layers deployed on Bitcoin since 2012. However, the enumeration isn't necessarily exhaustive – there's always something new that comes out and extends the ways in which you can use your coins… there's an even longer list of proposals that never came to fruition.

For the sake of destroying ChatGPT's argument about "limited use cases", I'll present the projects that have been delivered, are still available to get used, and successfully extend the ways in which you can transact your BTC.

Colored Coins, Counterparty and Omni enable token issuance on the Bitcoin blockchain. From a technical standpoint, they are OP_RETURN transactions which leave permanent and recognizable marks in the public ledger. Their goal is to mark real-world assets (commodities like gold, real estate, equities, fiat currencies) on the Bitcoin blockchain either by arbitrarily assigning a certain meaning and value to a handful of BTC units (as in the case of Colored Coins), or by issuing a token which represents the ownership of other assets (Rare Pepes and Bitcoin Heads on Counterparty, Tether on Omni). Launched in 2014, Counterparty was even more ambitious – it aimed to enable decentralized companies to issue their own shares, pay dividends, and trade their stock against other assets on an open marketplace. But due to limited scalability and high transaction costs, most of these plans were never fully realized.

Casey Rodarmor's ordinal inscriptions are another take on Colored Coins. The project aims to associate numbered bitcoin units with a string of data which is stored in the witness side of a Bitcoin block. The design is more elegant and minimalistic than anything NFT-related on chains such as Ethereum, but it can't scale to accommodate everybody's arbitrary data and it ultimately competes with the financial transactions of other users. Due to these limits, proponents of Ordinals deem their inscriptions more scarce and assign a relative value to their existence.

Canadian bitcoiner Mike in Space has created something





NO, I DON'T CARE ABOUT HIS OPSEC. FIND HIM NOW, BIG BOSS WANTS THIS BITCOIN FUD BROKEN!

similar with STAMPS – an even more radical way to put files on the Bitcoin blockchain, which encodes data in Base58 format and permanently stores it on the unprunable UTXO set. Bitcoin nodes end up using a lot of their RAM memory to keep the transaction information… so if too many actors deploy such transactions at the same time, these STAMPS can take down lots of validators around the world. So far, due to high transaction costs, STAMPS have only been used to store silly pixel art. But if a series of attackers coordinate to broadcast many of these large data-heavy transactions, Bitcoin nodes will have to upgrade their hardware. The deterring factor for such an undertaking is the high cost of every transaction (about 0.01 BTC per kilobyte).

The projects described are certainly from the Bitcoin maximalist crowd,

but they purposely use block space inefficiently to leverage scarcity. They're the equivalent of turning gold bars into jewellery, their use generates controversy among community members due to concerns of bloating the blockchain for future generations of node operators, but they find themselves in a minority in relation to economic transactions. If there's a positive to their existence, outside of dunking on ChatGPT, it's that they absolutely confuse regulators – named Counterparty tokens, ordinal inscriptions and STAMPS are an exercise of free speech on a public immutable ledger. As Bitcoin-friendly attorney Justin Wales wrote in his 2019 University of Miami Law Review research paper "Bitcoin Is Speech", the US Government has pretty solid reasons to protect Bitcoin transactions under the provisions of the First Amendment to the US Constitution.

On the other side of the spectrum, we have the scalable and economical Bitcoin maximalist projects. They don't bloat the base layer, as they move the extra transactions to a second layer or pegged parallel chain. Furthermore, their transaction costs are significantly lower.

Blockstream's Liquid is perhaps the best known Bitcoin sidechain. It functions as a federation of block producers who also act as gatekeepers of the

system – it's through them that you receive your L-BTC when you lock your BTC on the base layer, and it's also at least a federation member who must process your request to burn the L-BTC and unlock the funds on the main chain. Some argue that the design is a far cry from the October 2014 research paper which first outlined the sidechain concept, mostly due to the permissioned design and the replacement of decentralization with a federation of members.

However, Liquid offers pretty good privacy via Confidential Transactions and can also help Bitcoin scale during times of high demand. It can issue tokens just like Counterparty/Omni and mimic some of the features you find on Ethereum (contracts, royalty systems), but in a more private environment. Nonetheless, the main use case is to help exchanges and traders make settlements faster, at lower costs, and with the option to hide the amounts that they're moving around – these whale tracker bots on Twitter and Telegram won't reveal large money transfers anymore.

On top of Liquid, there are also a few interesting applications. One of them is Raretoshi, a tokenized digital art marketplace which emulates the same style and functionality of the more popular OpenSea. SideSwap, BitMatrix, and TDEX are some of the decentralized exchanges which allow you to trade L-BTC for L-USDT (Tether on Liquid). Then there's Fuji money, a platform which enables users to borrow bitcoin-backed stablecoins and synthetic assets without a trusted third party in the middle. The ecosystem built around the Liquid sidechain is certainly interesting, but it didn't get too much traction. Maybe in the future, when demand for mainchain block space is higher, Liquid will have its moment in the spotlight of mainstream Bitcoin culture.

Rootstock, known today as RSK, is another important sidechain. Its purpose is very simple, yet ambitious: to provide the infrastructure to successfully port all Ethereum smart contracts to a Bitcoin layer. It's a modified version of Ethereum which gets secured via merge mining by more than 57% of the Bitcoin hashrate – meaning that the same miners provide thermodynamic security to the system and collect transaction fees to increase their revenue. Rootstock architect Sergio Demian Lerner has also added a few extra optimizations that don't exist in Ethereum. At the time of this writing, about 3500 bitcoins are locked into RSK – which is nearly as much as Liquid's 4130. Since Rootstock is designed to be compatible with Ethereum, its applications feature both original works and ports from other chains. Metamask allows an easy transition, assets can be secured with both Trezor and Ledger hardware wallets, and there are ways to borrow stablecoins against your RBTC with Sovryn. For those who are into decentralized finance, the ecosystem also offers RSK Swap – a clone of Uniswap which provides the foundation for a decentralized exchange where no KYC is necessary.

Overall, RSK benefits from features and integrations that you can't find on Liquid specifically because porting applications and contracts from Ethereum is seamless. The reason why it's not replacing Ethereum yet is that the original chain still hasn't had critical security flaws and the preminers still have a lot of money to spend on marketing to attract new users. But RSK is a useful safety net which guarantees that there won't be any disruptions when Ethereum fails… and in the end, it all comes back home to Bitcoin.

Drivechains, on the other hand, are a reimagining of the 2014 sidechains research paper and proudly represent the purest form of Bitcoin maximalism. Through them, Bitcoin could integrate every altcoin use case in existence and



put an end to their blatant scamminess. Brought into existence by Paul Sztorc's BIP300 and BIP301, Drivechains are best described by the "altchains without altcoins" mantra. The principle is rather simple: if this system of hashrate escrows and blind merged mining gets deployed on the main chain, then it would allow anyone to create their own Bitcoin sidechain which pays fees to the same BTC miners.

The free market approach is what might put an end to all shitcoins.

The entire economy would revolve around the 21 million BTC that get moved across various chains in order to gain several advantages. For instance, some coins can be moved to a Monero/Zcash sidechain to get better transaction privacy, while others can get into an Ethereum-like sidechain where anyone can do ICOs and DeFi. What's radically different about this design is that nobody gets to print money out of thin air anymore – every activity, regardless of how legit or scammy it is, incurs BTC costs and pays fees to the Bitcoin miners. Furthermore, conservatives who

only want to use the main chain are not affected and their full nodes don't store any information generated by the sidechains.

On testnet, Drivechains show promising results: Paul Sztorc posted guides and video tutorials which demonstrate how a Zcash and an Ethereum sidechain work. Most importantly, he showed that Bitcoin Core wasn't affected and had zero knowledge (pun intended) of the activity taking place on other chains. If merged on the main net, Drivechains could be the Bitcoin soft fork to end all altcoins and minimize the need to further upgrade the Bitcoin base layer in the future.

Statechains also extend the functionality of Bitcoin

and provide further scalability options. First presented by Ruben Somsen at Scaling Bitcoin 2018 in Tokyo, Statechains function as a layer two for swapping coin ownership. On the basis of a main chain multisig which locks funds, users can hop onto this protocol to generate transitory keys which enable off-chain transfer of value.

The most popular implementation of Statechains can be found in MercuryWallet: a desktop Bitcoin wallet that performs off-chain CoinSwaps that empower users to trade UTXOs of the same value without leaving on-chain traces. But beyond the transferring feature, Statechains are also interoperable with the Lightning network and allow users to open channels directly from this layer. This has privacy, scalability, and cost benefits.

Of all the layers and protocols presented in this article, Statechains are the most overlooked and they're extremely underrated for the potential they have. But maybe after you're reading this, you will be inspired to take a look at Ruben Somsen's work and build something on top of it.

The Lightning network is by far the most successful Bitcoin layer.





YOU SEE, CHATGPT IS NOT SO GREAT.

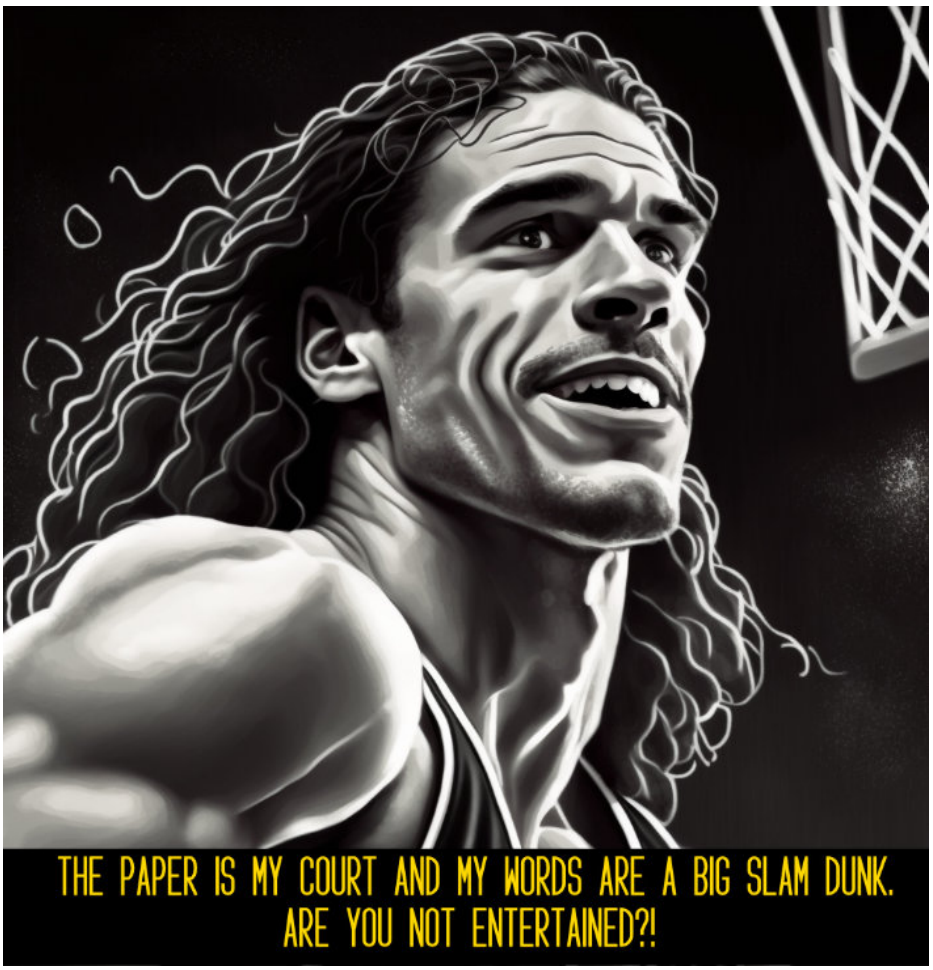
If the other protocols and sidechains mostly have a single team of developers which focuses on their improvement and growth, then Lightning has thousands of people working on it from all around the world. At the protocol level, Lightning Labs (lnd), Blockstream (Core Lightning), ACINQ (eclair), Nayuta (Nayuta Core) and Electrum all compete for market share by making various refinements across all platforms. At the operating system and distribution level, we have RaspiBlitz, Umbrel, MyNode, Start9 EmbassyOS, Citadel, and a bunch of other interfaces which allow everyone to easily spin up Bitcoin and Lightning nodes.Even at the wallet level, Lightning is the most popular and robust – Breez, Blixt, Phoenix, Electrum, and Muun being only a few examples of non-custodial solutions that work without needing a dedicated node that runs 24/7. As of April 2023, the Lightning network also reigns supreme in terms of liquidity (5460+ BTC), independent nodes (15000+) and channels (70000+).

At this point, Lightning is so big and significant that there are layer 3s built on top of it, as well as interoperable layer 2s: RGB, Taro, and Cashu represent the former, while Statechains, Liquid, and Fedi are amongst the latter. This phenomenon happens because Lightning is network-agnostic and can do atomic swaps between different chains.

The value proposition for Lightning network is that,

for the price of two on-chain transactions, users can transact hundreds (if not thousands of times) at the speed of their internet connections and at a significantly lower cost. However, the main issue is routing – in order for a payment to get from wallet A to wallet B, the two of them need to either open a channel between each other or have a third party which connects them. As the liquidity increases, big hubs emerge – users naturally gravitate towards the nodes with the most economic activity (shops, dedicated companies which provide infrastructure). And if this influx of liquidity is accompanied by obvious choices for common hubs, then the lonely islands will become fewer and the odds to connect nodes become greater.

What's great about Lightning is that it can act as the foundation for other layers that can leverage its speed and flexibility in order to do other stuff. For example, RGB aims to make the Ethereum design obsolete with client-side validation, while Taro seeks to bring a USD stablecoin to enable more trading options. There's also Portal and Fabric, which contribute with atomic



swaps, computation and data storage. And if your Lightning transactions aren't private enough, then Chaumian mints such as Cashu and Fedi will come to the rescue. But before we get to these, let's talk about John Carvalho's Synonym.

Synonym describes a whole suite of applications and integrations: from Bitkit (Bitcoin toolkit) to Blocktank (a Lightning service provider), there's a lot to discover. But the truly unique product is Slashtags – a tool that makes identity across web a lot easier. With only a Bitcoin and Lightning wallet (currently provided by Bitkit), anyone can set up a profile, build their reputation, and make their contributions easily discoverable under a simple mobile-friendly interface.

In a nutshell, Synonym's Slashtags attempts to fix the censorship problem across the internet in a way which incentivizes good faith. Your profile is platform-independent to the point that any website with a Slashtags integration will enable you to comment and participate in debates, and there's also a Lightning payments dimension on top of it. Facebook and Google attempted something similar in the mid 2000s, except that they always had control over the profiles to the point that they could shut down, restrict, and censor accounts.

Currently, Metamask attempts to do something similar for assets across the Ethereum ecosystem: a browser integration which makes it easy to log into other applications and protocols. However, the scope of Metamask is limited to financial applications. Slashtags cover a wider spectrum of use cases which include commenting across websites and building a reputation. So once again, the Bitcoin version does more and does it better.

Another interesting project is Portal, a DeFi platform which makes use of atomic swaps on the Lightning network. It's being built by some of the veterans who created the first Bitcoin meet-up in Silicon Valley (most notably, George Burke), it's backed by capital from a bunch of big centralized exchanges (most notably, Coinbase and OKEX), and it aims to become a scalable replacement for custodial exchanges. So far, Portal has successfully managed to perform a successful cross-chain L2 swap between Bitcoin and Ethereum – without the need for "bridges" or wrapped coins. In time, the project's scope is expected to grow.

Fabric is a protocol which takes the ambitions of the Lightning network to the next level, as it aims to build a computation layer for data storage and trustless application deployment.

The official description is that of an "operating system for the world's most powerful super computer", but the data storage plans extend the scope beyond the app store ambitions. Fabric was first announced in February 2016 and chief architect Eric Martindale has reported some breakthroughs with early prototypes. However, the project is yet to get deployed at its full scale.

RGB, Taro, Fedi and Cashu

are also third layers built on top of the Lightning network. Though there are some technical similarities between them, their purposes are very different. RGB is a smart-contract system based on Bitcoin and Lightning Network, which benefits from client-side validation and enables instant transfers of asset ownership. So if Bitcoin Heads digital collectible cards get moved to RGB, then collectors can exchange them within seconds and at significantly lower costs than making on-chain transactions.

Conceptually speaking, Taro by Lightning Labs is very similar to RGB – to the point where RGB creator and lead developer Maxim Orlovsky slammed their tactic to

copy parts of the code without giving credit and then raise millions of dollars for the final product. However, Taro is more explicitly being built to put "the world's currencies" (aka stable-coins) on the Lightning network. RGB is universal in design and aims to empower users to build a worldwide economy where they can fundraise via secure tokenised company shares, trade digital collectibles, and more. Basically a more scalable, elegant, and private version of the stuff happening on Ethereum today.

Taro has a narrower and more specialized role, as it's using the Lightning network as the settlement layer for other types of currencies. It appears to be focused on bringing the dollar to Lightning, but other types of fiat money will definitely follow. If properly funded, RGB can technically replace the need for Taro – but this type of competition, where one side has more ideas while the other has more capital, might turn out to be healthy for innovation.

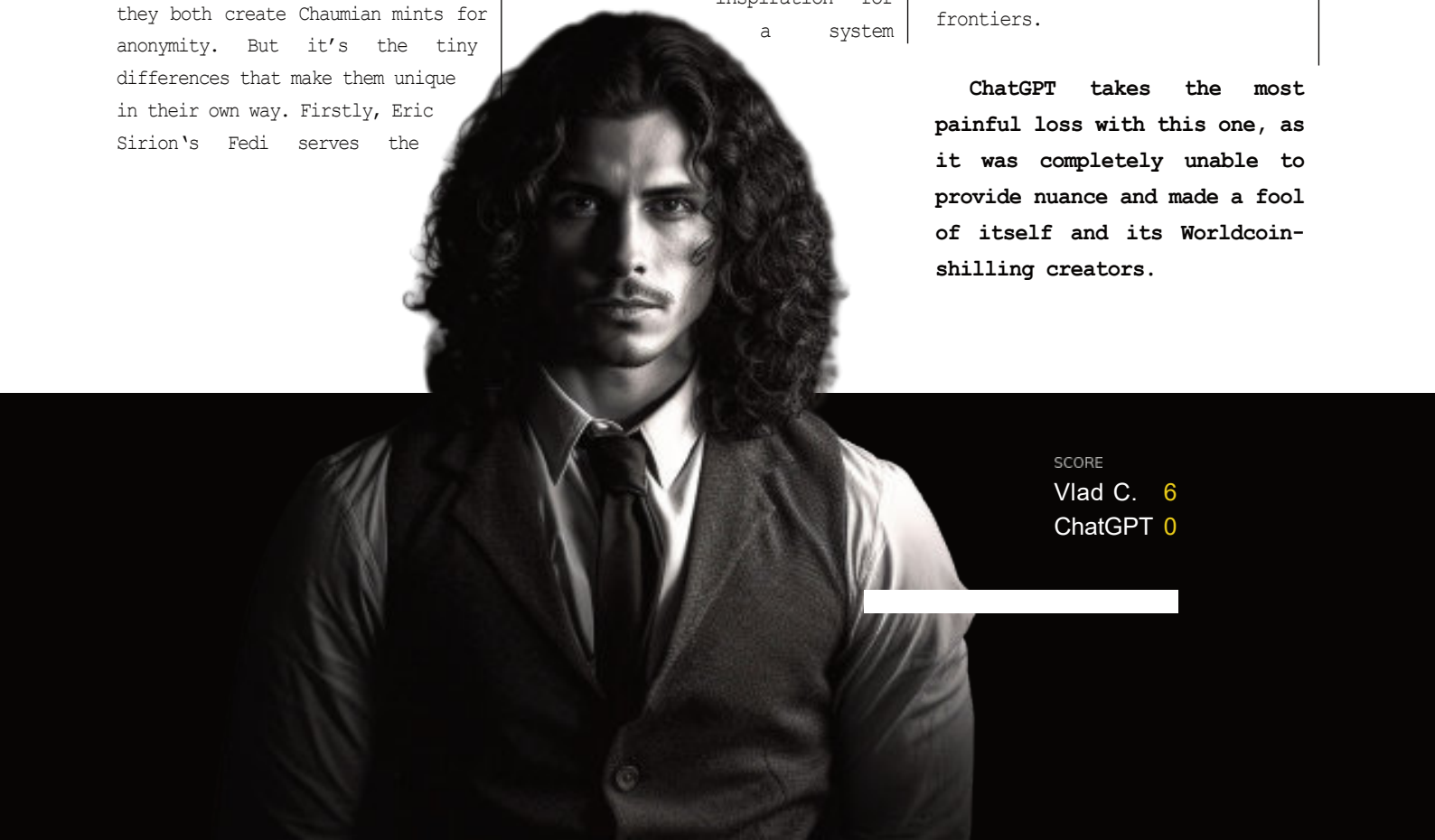
Fedi and Cashu are the latest additions to Bitcoin's layer 3 stack. They are very similar in design, as they both create Chaumian mints for anonymity. But it's the tiny differences that make them unique in their own way. Firstly, Eric Sirion's Fedi serves the purpose of creating community banks which make onboarding easy and accessible for people who are generally afraid of self-custody. People in small towns, villages, or members of various clubs and religious groups can pool their bitcoins together and trust a handful of figures who set up a multisignature wallet to give birth to the mint. The advantage is that everybody's transactions are private and nobody can see how much money everyone else has. The only information that everyone can observe is the total amount of BTC in the mint.

However, Fedi's disadvantages are social and political. Community banks are easier to censor and shut down than a decentralized global network of computers. Furthermore, the creators of the mint can coordinate to steal the funds – of course, this comes with a reputation cost among the community… but it's still possible.

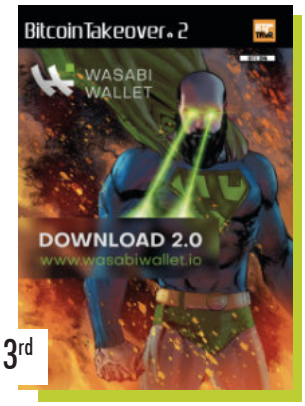
On the other hand, Cashu is designed in order to improve on Lightning's privacy limitations. Creator Calle has looked into Chaumian e-cash to get some inspiration for a system where people pool in their money in order to maximize their transaction privacy. On the Lightning network, only the sender benefits from good privacy… while the receiver remains exposed. The major difference between Fedi and Cashu is that the former relies on a federation, while the latter optimizes individual self-custody. Cashu is also excellent to use with custodial Lightning wallets, to prevent the node operator from knowing who you are, how much funds you own, and with whom you're transacting. This also removes the custodian's power to censor users.

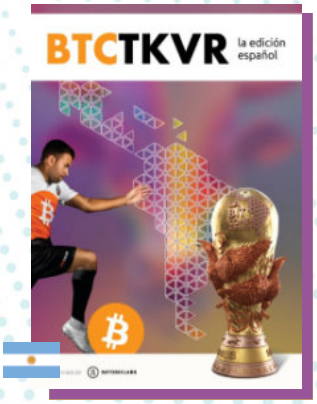
Initially, this article was meant to be a simple enumeration of the layers and protocols that make Bitcoin much more complex and capable than the mainstream media and the makers of ChatGPT portray it as. But the "pet rock with limited use cases" FUD is recurrent and takes many shapes and forms – ranging from "Bitcoin is not Turing complete" to "Bitcoin offers no yield". So it was important to highlight the efforts of Bitcoin maximalists who constantly improve and expand the network towards new frontiers.

ChatGPT takes the most painful loss with this one, as it was completely unable to provide nuance and made a fool of itself and its Worldcoin-shilling creators.



KYM
Know Your Magazine

edition	1st	2nd	3rd	4th
				
supply	120 prints	41 prints	50 prints	50 prints
launched at	Fulmo Lightning Hackaton	Scarce.City	Wasabi's Hunting Sats Campaign	Pizza Day
place	Istanbul, Turkey	Online Auction	Budapest, Hungary	Paralelni Polis, Prague, Czechia
launch date	February 25th 2022	April 6th 2022	Christmas 2022	May 21st 2022
printed in	Turkey: 100-150 Romania: 1-70	Romania	Hungary	Czechia
cover art by	Vlad	Scrilla	Alexa	CypherpunkNow & Katka
bonuses	Comes with Vol. 2 Signed & numbered XCP token	Comes with Vol. 2 XCP token Stamped with Scrilla's signature	Bonuses: Comes with Vol. 2, Wasabi merchandise	Signed & Numbered
latest price	0.0045 BTC (June 13th 2022)	0.0149 BTC (August 1st 2022)	N/A (Not Available)	0.00082 BTC (May 21st 2022)

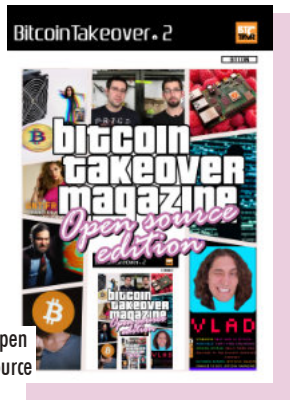
edition	7th	8th		
				
supply	100 prints	90 prints	300 prints	100 prints
launched at	HCPP	TABConf	LABitconf	Adopting Bitcoin
place	Prague, Czechia	Atlanta, Georgia, USA	Buenos Aires, Argentina	El Salvador
launch date	30th Sept. - 2nd Oct. 2022	14th - 15th October 2022	10th - 13th November 2022	15th - 17th November 2022
printed in	Czechia	USA	Argentina	El Salvador
cover art by	CypherpunkNow	NoGood	Andrej Cibik, Mariana Aquirre, FC Hájske	Bitko
bonuses	Signed & numbered by Vlad	Signed & numbered by Madelyn Ash	Signed & numbered by Roberto	Sold at Adopting Bitcoin merch booth
latest price	0.0013 BTC	N/A (Not Available)	N/A (Not Available)	N/A (Not Available)





6th





open source

200 prints	100 prints	100+ prints	digital
Mallorca Blockchain Days	Baltic Honeybadger	Surfin Bitcoin	Github.com/VladdyC
Palma de Mallorca, Spain	Riga, Latvia	Biarritz, France	online
July 14th 2022	September 3rd 2022	August 26th 2022	February 26th 2022
Germany	Latvia	Germany (first 100)	anywhere
Andre	Anna from HodlHodl	Bogdan Menci & Delacroix	Vlad & Bogdan Menci
Signed & Numbered (first 70 copies)	Signed & numbered XCP token	Best BTCTKVR articles translated by Grittoshi	Download it Print it Sell it
N/A (Not Available)	#1: 0.005 BTC #100: 0.00005 BTC (September 3rd 2022)	N/A (Not Available)	priceless



9th





10th



Vol.2

100 prints	20 prints	21 prints	311 prints (also digital)
Adopting Bitcoin	Dakar Bitcoin Days	Christmas 2022	Fulmo Lightning Hackaton
El Salvador	Senegal	Romania	Istanbul, Turkey
15th - 17th November 2022	2nd - 3rd December 2022	25th December 2022	February 25th 2022
El Salvador	Senegal	Romania	Turkey: 100 Romania: 111 USA: 50 Hungary: 50
Adopting Bitcoin	UndercoverMax	Golshid Rahbar, Vlad	Bogdan Menci, Igor Petrov
Sold at Adopting Bitcoin merch booth	Distributed by Nourou	Includes French + Spanish Translations Signed & Numbered	Signed & numbered
N/A (Not Available)	N/A (Not Available)	N/A (Not Available)	N/A (Not Available)



Breaking ChatGPT's Bitcoin FUD #7

Energy Consumption

WASTE/USE MINING BITMAIN CO^2 POW

According to ChatGPT, the amount of energy that's required to secure Bitcoin is concerning because the decentralized Proof of Work network consumes more electricity than other payment systems. As usual, the AI model provides little to no nuance and presents a rather generic criticism. Nonetheless, the fact that we're given a comparative perspective (worded as "consumes more energy than most other payment systems") is really useful and we can use it in the FUD deconstruction.

Before we dive into breaking the FUD itself, it's important to distinguish between two types of mainstream commentary which regard Bitcoin's electricity use:

– the first one is inherently nihilistic and implies that Bitcoin is useless or should not exist alongside banking services. This type of logic leads to a

What do you think about this article?

Leave your comments or send a donation by scanning this QR code.

conclusion that Bitcoin is wasteful, trivial, and too damaging for the environment to receive any kind of credit. This is the most common type of attack, even when it's presented indirectly under the disguise of "Bitcoin has no utility" and "Bitcoin can't be money";

– the second type suggests that Bitcoin should switch to Proof of Stake. It's a more nuanced, technical, and ultimately destructive argument which is mostly perpetuated by altcoin proponents who seek to undermine Bitcoin's decentralization and possibly gain a degree of control. Ethereum is often presented as the example of a transition to Proof of Stake that Bitcoin should follow, while Ripple executives actively fund anti-Bitcoin campaigns to damage the system's reputation. Some of these points sound reasonable to the average person, but it's important to explain why Proof of Stake can't provide security in the absence of a concerning degree of centralization.

Both of these arguments are destructive in the sense that they aim to erode Bitcoin's fundamental properties. The first one benefits bankers, while the second one serves the interests of altcoin proponents whose networks can't compete with Bitcoin on the free market... so they consequently choose to play the political game.

Now let's provide a little bit of context to explain how Bitcoin works

and why it needs to consume energy to function. Because yes, Bitcoin is a form of money which uses large amounts of electricity to remain secure. The system is bound to the laws of physics, as transactions get thermodynamically protected against future changes. New transactions from users worldwide get added into a memory pool which gets stored by Bitcoin nodes, while miners take part in a global competition to find a rare number (referred to as "hash"). Once a miner or group of miners discovers that number, a message gets broadcast to the entire network, and a time-stamped block which encapsulates a few thousand transactions from the memory pool gets added to the public ledger.

Only one miner or group of collaborative miners can take the reward. Bitcoin is a "winner takes it all" system which encourages competition and doesn't favor inefficiency. Miners need to find an inexpensive and reliable source of electricity, use hardware which produces the greatest amount of hashes per consumed kilowatt, and constantly adapt to a dynamic global market which never stops innovating and sometimes gets regulated by local or national governments. In most cases, the best source of energy for Bitcoin miners is also the greenest – renewable



electricity production is a burgeoning field, and there are always some excess kilowatts that can't be stored and therefore gets used to contribute to Bitcoin's security in exchange for mining rewards.

Bitcoin's Proof of Work mining is the element which connects the digital money network with the real world and creates a cost for the production and transaction of funds. It provides thermodynamic finality to every operation and makes sure that the history can't be altered without great costs and permanent evidence. At first, Proof of Work was a mechanism to deter denial of service attacks (as described by Moni Naor and Cynthia Dwork in 1993) and prevent e-mail spam (as implemented by Adam Back in Hashcash). Basically, operations within a Proof of Work system require either a monetary payment or a computation cost: if you want to spam a mailing list, you must use your computer's processor to run the right amount of hashing cycles.

In Bitcoin, Proof of Work also works as a protection against censorship: if all transactions pay fees and require a miner to include them in a block, then there will always be someone who will accept to take the fee to cover electricity costs. On a global scale, this mechanism circumvents political censorship. If certain users are sanctioned in a certain number of countries, it's impossible for the entire network to collaborate in censorship because a miner from a free jurisdiction will have no moral or legal issue with taking the fee – therefore include that transaction in a block.

Another advantage of Bitcoin's Proof of Work mining is the so-called permissionless nature.

Anyone can buy a computer which specializes in mining. Of course, not everyone around the world benefits from competitive electricity costs and a friendly jurisdiction. But there is no registration required and there is no need for miners to reveal their identity to the world – all they need is luck or a lot of computation power to discover the rare hash before the rest of the world.

The descriptions presented above should fuel the imagination of any defender of human rights – and should be self-explanatory as to why governments and big corporations dislike Bitcoin and often criticize it for being wasteful. People living in authoritarian regimes need a way to protect themselves too.

Sounds complicated? It's because the decentralized design uses constant verification. In this money system, all participants check each other's honesty and rely on math and computer code to settle what is fair and what gets invalidated. Bitcoin mining is part of securing a decentralized network which has no central entity to make the rules. Bitcoin is the most successful attempt to solve the double spending problem – it makes sure that, in the absence of a server which acts as the oracle for everyone else, the same amount of money doesn't get spent twice by the same participant. It's like going to the store and trying to pay for a $2 chocolate bar by offering the same $1 banknote twice, before the cashier can put the bill in the register. It can't work as long as there are verifiers who observe that you're trying to cheat the system.











Everyone is bound to the same consensus rules, so attempts to cheat are costly: for example, if a miner pretends to have found the right hash and the network's rule-enforcing nodes disagree, then the miner's work doesn't become part of the public ledger. This rejection comes with financial costs, as the miner who tried to cheat has used electricity-intensive computation and must either get in line with the rest or try to convince a 51% majority of other miners to collaborate in cheating.

However, at least up to this moment in Bitcoin history, it was always more profitable to play by the consensus rules than to try to attack the network. Honest miners receive rewards which cover for their electricity costs and other expenses. Dishonest miners haven't been able to form a dangerous majority due to the geographic distribution of the Bitcoin network and the involvement of a large number of users who believe in this parallel money project and want to see it succeed. Part of the merit belongs to the way in which the incentives were designed to encourage honesty, but we should never disregard human action. It's the quality of the Bitcoin users that brought it to this point.

Banks don't have this problem, as they are governed by human politics. Their settlements are also much slower than Bitcoin blocks, they only work from Monday to Friday within a time frame of 8 hours, and all transactions in between are stored in a proprietary version of "memory pool" which gets cleared during office hours. Unlike Bitcoin, banks can reverse transactions and freeze funds with great ease. It's this censorship dimension which gets taken to extremes even in the most democratic countries with liberal constitutions that theoretically involve free speech – some individuals had their accounts frozen for political speech, while a bunch of Canadian truckers had to choose between financial access and continuing a protest.

A fairer world needs Bitcoin as a financial instrument which empowers

the people to opt out from corruption and abuse. For as long as Bitcoin exists in a decentralized way via Proof of Work, it is possible for individuals to invest capital in order to mine it and therefore obtain amounts of it without going through state-regulated procedures. With the coins they get from mining or private peer to peer trades, people from all around the world can vote with their feet: they'll leave any territory and jurisdiction which insults their dignity, abuses their freedoms, and infringes their fundamental rights in order to settle in a friendlier place. You can find many such examples among Venezuelans – and from amongst Bitcoin Takeover podcast guests, you can hear Alessandro Ceccere talk about escaping tyranny through Bitcoin (season 5, episode 5).

Furthermore, people can use Bitcoin to create parallel black markets which effectively circumvent abusive regulations.

Farmers can no longer raise cattle and get pressured into incubating bugs? It's not like the demand for milk, dairy products, and beef will disappear because a bunch of politicians decided to impose a reduction on the production. So people will be able to purchase the food that they like directly from the farmers, in a peer to peer manner which completely bypasses the control of Big Brother.

There's also a lot to be said about Bitcoin in the era of cashless transactions and CBDCs. Consider this: central banks will possess unprecedented control over every money transaction, will use a worrying degree of surveillance against everyone, and will be able to manipulate the currency supply/inflation at the flick of a switch. By design, CBDCs are bound to be marked by heavy censorship, discrimination, and political abuse. No financial institution or registered payments service can provide uncensorable and somewhat private money transfers like Bitcoin does.

Bitcoin is an escape from a gloomy authoritarian future,

where technological innovations are used to surveil and enforce control of the masses more efficiently than communism and fascism in the 20th century. So of course governmental actors are doing their best to discourage its use. They already try to keep every on-ramp and off-ramp under control, while also surveilling every transaction to try to guess where



the money is going. But Bitcoin is every authoritarian's worst nightmare: a global computer network which works according to consensus rules that no parliament, president, king, or alliance of powerful politicians can change. The people can't be blocked from sending and receiving BTC anywhere around the world, so political censorship suddenly becomes less effective.

At the same time, corrupt politicians likely also keep part of their wealth in Bitcoin – which is why it probably won't get banned in a way that can't be technically circumvented. They can block the Bitcoin-related websites, they can restrict and discourage on-ramps, but they won't ban Tor, VPNs, and other IP obfuscation services which bypass this restriction. Also, governments will never shut down the internet because it feeds them too much valuable data and it's useful for propaganda. They can use the network to surveil the citizens and also control their thoughts through news and entertainment.

Based on the arguments presented, we can agree that Bitcoin is certainly useful to a lot of people across all walks of life. So the electric energy which keeps the system secure is clearly not wasted. Furthermore, the fact that a real-life resource gets consumed in order to produce BTC is also part of the reason why there's so much global demand for the magic internet money. The price of gold takes into account extraction, transportation, and security costs. The price of food includes production, transportation, and storage costs. Bitcoin is valuable because individuals and companies use electricity in order to secure their savings and also receive mining rewards.

Unlike fiat money, which is printed out of thin air

and relies on trust in governments and central banks (accompanied by a degree of military enforcement), bitcoin is honest money which everybody purchases at a price that takes into account production cost in hardware and electricity, supply, and demand. Unlike governmental money, you always know how many bitcoins exist in circulation. So when you determine the price, the only real variables are production cost and demand. As I'm writing this article, the price of 1 bitcoin is approximately $30000 – but when fiat money gets replaced, one bitcoin can be priced in hours of labor, scarce natural resources, pieces of land, gold coins, and other human-made products. Time, energy, and resources are finite – why shouldn't the money that purchases them also be bound to the laws of physics instead of human politics?

Having electricity consumption as a point of reference for evaluation is a feature which works in Bitcoin's favor. It makes the network secure and it gives the currency more legitimacy. The regular counter-argument is that Bitcoin is computer code that anyone can clone in order to deploy an identical network – however, markets will not assign the same amount of value to that new network over time, and therefore the use of electricity converges towards the most stable and constantly in-demand money network.

Such ambiguiszation attacks against Bitcoin's supremacy already took place in 2017 and 2018 with various forks: Bitcoin Cash, Bitcoin Gold, and Bitcoin Satoshi's Vision being three of the best-known attempts which clearly failed. Though they still exist today, they didn't manage to convince the market that they are the true and most valuable versions of Bitcoin. Consequentially, they constantly lost market share against the original Bitcoin to the point where today BCH has only 0.39% of the real Bitcoin's mining hash rate.

Not all cryptocurrency mining is created equal. The markets recognize something that has value and, on a long enough time frame, it becomes clear what is truly precious and what gets revealed to be a failure or a scam. As of 2023, Bitcoin has been the undisputed king for 14 years. Clones have come and gone, but only one form of internet money reliably helped people worldwide transact and make savings every day. So there's clearly a lot of value in this network and it deserves to use that electricity to help individuals around the world gain more freedom against overreaching tyranny.

This is where some would argue that a switch from Proof of Work (the mechanism which uses the laws of thermodynamics to convert electricity



to digital money) to Proof of Stake (Ethereum's approach to security, where newly-minted coins are given to users who lock their ETH tokens in a contract and keep a validating computer online) could reduce Bitcoin's energy consumption by up to 99%. The point is only valid in regards to the energy consumption, but completely disregards the meaning of decentralization and the idea of fair money.

In Bitcoin, anyone can invest external resources (fiat money, gold) to purchase mining equipment and pay electricity bills in order to acquire BTC tokens without touching any of the coins that already exist on the market. You can secure the network and earn rewards, and thus avoid enriching the early adopters by affecting the price with any potential market buy.

In a Proof of Stake system, you have no choice but to buy your coins from people who created them out of thin air, without any kind of energy expenditure. Not only that, but Proof of Stake functions as an oligarchy: the newly-created currency units get distributed to those who staked the largest amounts. The rich always get richer, while the poor are destined to remain poor. Obviously, there's a lack of dynamism: early adopters can afford to always stake and only spend the rewards they gain. The system was unfair from the get-go, but the ways in which the poorest must buy the coins from the elites to effectively preserve their overlords' status are despicable and unacceptable for human progress.

At least Proof of Work is dynamic, as proven by the significant shifts in mining pool dominance:

– in **2011**, Deepbit became the first mining pool to hit more than 50% of the hash rate and this fact caused some panic among Bitcoin Talk users;

– in **2013**, Deepbit was already dead. But BTC Guild was the new kid in town, and users were expressing concerns about its dominance. By January 2015, the pool shut down due to regulatory pressure;

– in **2014**, Bitcoin Magazine co-founder Vitalik Buterin wrote an article to complain about GHash.io – a pool which was nearing 50% of Bitcoin's hash rate. In less than 2 years, GHash went out of the mining business;

– in **2017**, bitcoiners were concerned about Bitmain's unfair advantage as a manufacturer which also runs Antpool. As of April 2023, Antpool only accounts for 23% of the Bitcoin hash rate;

– in **2023**, the community frowns upon Foundry USA – a pool which is getting too big after a large chunk of the operation moved out of China. Currently, this relatively new pool provides approximately 33% of Bitcoin's hash rate. However, Foundry is fragile to two factors: the excessive regulatory concerns in the United States of America, as well as the dynamics of a competitive and global free market which searches for the most abundent and affordable form of energy. A decline is never impossible and there's always a competing service that can take over the task of offering Bitcoin thermodynamic security;

On the other hand, it's still not clear if Proof of Stake can work without worrying degrees of centralization – when Ethereum switched to this consensus protocol, they enforced a rule which doesn't allow the stakers (users who secure the network by locking their coins) to withdraw their money from the contract. It's a temporary decision to prevent major security issues... or so they claim.

Their system, even if it consumes very little electric energy, is unfair and much worse than the banking system we already have. Proof of Stake can't and won't work alongside a free global money network which allows anyone to participate with equal chances. Which is why the enemies of Bitcoin insist that the switch of Proof of Work should happen – they don't want the price of bitcoin to have a real-world equivalent in energy, they don't want the system to offer everyone equal chances to compete, and they don't want the decentralization to last. They would rather push for something that they know how to control.

The next level of criticism that they would present (officially or through ChatGPT) would be that Bitcoin is not money, as only governments make decisions in such matters. And once again, there are two distinct layers to debunking this FUD:

– the easiest way is to point the index finger at El Salvador, a country which recognizes Bitcoin as an official currency;

– the more nuanced way is to explain that markets decide what money is, not governments. The former are dynamic and innovative, while the latter are reactive and conservative. It was the markets that picked gold and silver to trade them across national borders, but it was the governments that decided to position themselves in the middle under the guise of simplifying coin verification. It was also the markets that used credit and ownership certificates before governments decided to embrace and centralize this type of accounting.

In the past, governments could ban and confiscate certain types of currency

which they deemed dangerous for the elite class. Today, the same governments can't stop Bitcoin from being used in markets to pay for goods and services. So the only real property of traditional money that Bitcoin really lacks is the ability to be confiscated by the government – and if we define money through this lens, then we can agree that Bitcoin is definitely something else.

Now let's have a nuanced discussion about Bitcoin's energy consumption. We already explained that the Proof of Work system has value and produces something useful for humanity in a dynamic free market way, so let's put the energy consumption in a comparative perspective. After all, there are lots of "wasteful" uses of electricity that governments don't frown upon

but consume lots of kilowatts – ranging from Christmas lights to clothes driers and idle television screens that nobody watches.

People who dry their clothes with dedicated machines, warm their homes with space heaters (electricity-hot air), and sleep with their computers or televisions on aren't considered ecological terrorists. Governments which consume a lot of electricity with military operations and various experiments are never held accountable. Big tech corporations which run server farms get a free pass, as they have enough money to lobby governments and make regulators and environmental activists look the other way. But Bitcoin miners are held to unreasonably high standards and they're frowned upon for securing a money network that governments can't control.

Alarmists refer to Bitcoin mining as a wasteful,

planet-damaging,excessive carbon-emitting, and ocean-boiling activity. On the other hand, mining advocates and stakeholders describe it as an increasingly-green activity which converges towards the cheapest forms of electricity – which also happens to be renewable. But the truth is always somewhere in the middle: in reality, anyone can purchase mining equipment and run it at home, as part of a mining farm inside a dedicated facility, or in any other place where electricity is inexpensive.

There's also something to be said about free markets in the energy sector and how prices will change over time to adjust with the supply-demand dynamics. For instance, the electricity produced by burning coal is now expensive, heavily polluting, and undesirable in comparison with nuclear, solar, wind, or hydro energy. However, if the demand for coal reaches such low levels that the resource becomes very cheap to purchase and burn, it's likely to be used by competitive actors. Not only in mining, but across all energy sectors. After all, even the German government increased electricity production via burning coal in 2022 in order to deal with the energy crisis... which is rather unusual for a country which is ruled by a left-wing coalition of which the Green Party is a member.

On the Bitcoin network, miners get paid 50% fewer coins per block after every 210.000 blocks get discovered. This cycle, referred to as the "halving", takes approximately 4 years and greatly contributes to the professionalization of the entire mining sector. The inefficient participants, which pay high prices for energy and don't produce enough processing power to remain competitive, are driven away.

At the same time, the mining hash rate cannot stay constant over time and will not only grow. Once miners take their electricity from power plants where it's being produced in excess, there aren't too many places left to go. They can convert geothermal energy, they can turn the otherwise polluting gas flaring into electricity and consequently release CO2 into the atmosphere instead of the heavy polluting methane, and they can even use the kilowatts generated by fermented cow manure. So what happens if the mining hash rate can no longer increase and starts decreasing unexpectedly due to reliability issues in some parts of the world?

After all, Bitcoin's Proof of Work mining is designed to enable dynamism and allows anyone around the world to join in or leave at any time. How are hash rate drops going to be mitigated? Well, every 2016 blocks (approximately 2 weeks), the mining difficulty readjusts in order to maintain the 10-minute block time – so the difficulty increases after times of high activity (when more miners discover blocks much faster) and lowers after times of low activity (when the miners



struggle to discover blocks).

This also means that if more energy gets deployed on Bitcoin at one time, the mining rewards remain the same and the increased number of participants must share them. Which is another brilliant design – if more resources get deployed towards finding and exploiting gold mines or petrol wells, then the amount of resources available on the market becomes more abundent and the prices get lower. But Bitcoin has a programmed inflation system which releases 50 coins per block in the first epoch of 210.000 blocks, 25 coins per block in the second epoch of 210.000 blocks, and so on until the rewards run out and the miners only get paid from transaction fees between participants.

Only the most efficient miners, who can make a profit from the diminishing rewards, will survive. And when the lowest electricity costs get reached and the mining hardware improves to the absolute limit, there's still a case to be made for ideological mining – people around the world who don't care much about rewards, but only want to secure the Bitcoin network against attacks.

Bitcoin's energy consumption is so easy to criticize because it's even easier to figure out – the mining hashrate is a

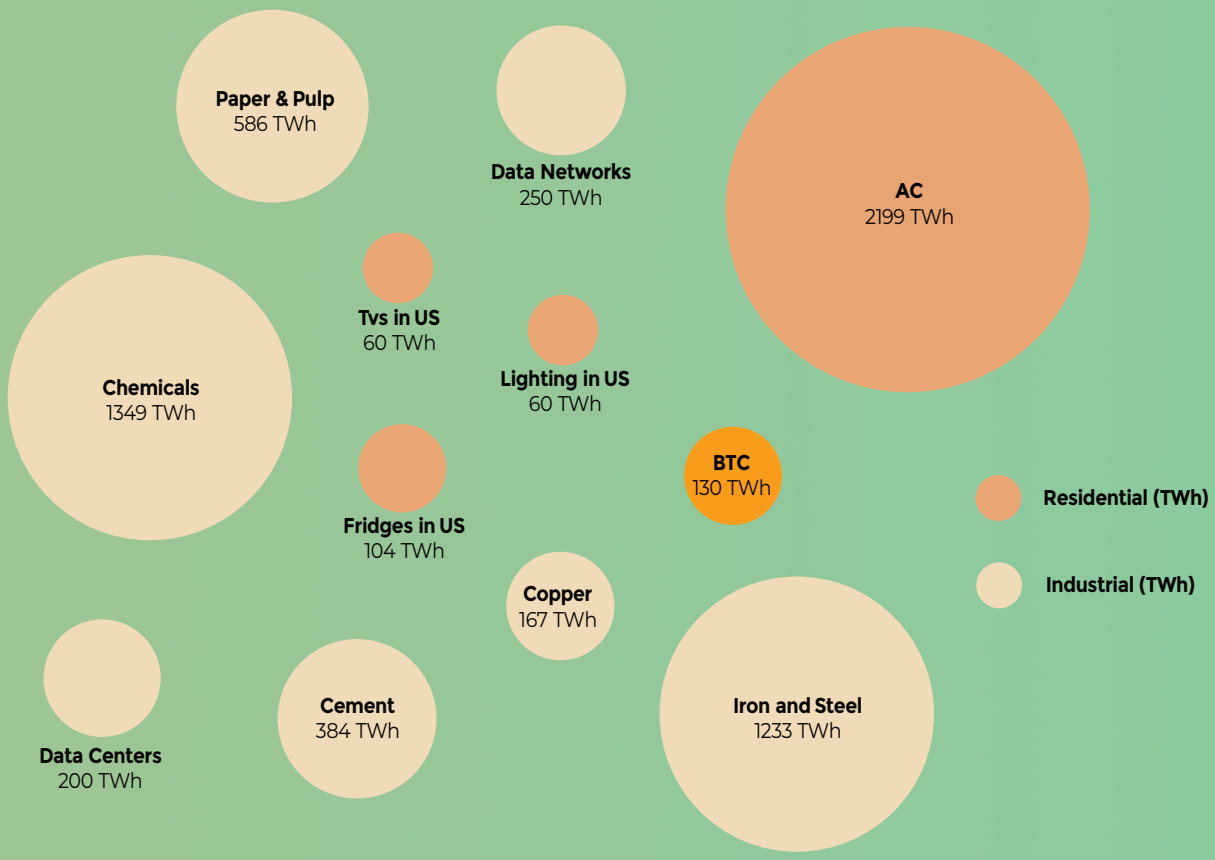




public metric, the efficiency of the most popular mining hardware is known, so anyone can make a pretty accurate approximation of the amount of electricity being used. In comparison, no other private financial institution publishes such data. You won't see banks revealing how much electricity their offices and servers consume. You won't see reports from PayPal and Venmo in which you find out how much they paid for electricity to run their operations (including offices, support desks, servers, and everything that powers their business). And even in the case of governments, not everything is transparent – the military and the secret services only report their overall budget, but don't publicly justify how they spend it or why they needed a certain amount of electricity for something that produces no results.

Which is why we need to compare Bitcoin's electricity consumption with that of other industries. According to Statista, between February 2017 and November 2022, Bitcoin hit a peak at 204.6 TWh per year (achieved in the first quarter of 2022). In 2021, the entire world consumed 176431 TWh. Even at the top, Bitcoin accounted for 0.11% of the world's energy consumption. Which is 100 times less electricity than the World Economic Forum estimated Bitcoin would use by year 2020 in their hilariously terrible article from December 2017, titled "In 2020 Bitcoin will consume more power than the world does today". The elites in Davos must really hate this money system that they can't control.

I hope WEF author Adam Jezard is reading this, as growth in mining will not be steady and exponential. In his model, he used the 25% monthly hash rate increase as a constant. But that's not how it works: for reasons described earlier in the article, if you deploy 25% more power, you don't get 25% more rewards. The difficulty adjustment



algorithm will make the same block reward harder to get. This means that many miners around the world will become unprofitable and shut down their operations. So in the long run, only the ones who run on the most affordable electricity will stay profitable and keep going. Inefficiency is getting priced out constantly, and there's an incentive to create the kind of hardware innovation which makes machines generate more hashes per watt.

Also, 0.11% of the world's energy consumption is really insignificant if we want individuals to have the option to be free from tyranny. 204.6 TWh per year is 1/10 of Romania's energy production from 2022, 19 TWh less than Kenya's annual energy production from the year 2021, and 1.65% of the United States of America's reported electricity generation from 2021.

In December 2020, Forbes contributor James Conca did some math to arrive to the conclusion that





Christmas lights in the USA consume 3.5 TWh during the month of December. Let's assume that the rest of the world, through holidays which range from Christmas to Hanukkah and the new year, doubles the amount of electricity that's being used in the US. That's 7 TWh globally in the month of December. In comparison and approximately during the same, Bitcoin consumed 6.48 TWh (a number which represents the estimated Bitcoin TWh per year during December 2020, divided by 12).

According to the Cambridge Bitcoin Consumption Index, as of late April 2023, Bitcoin's annualized consumption estimate is of 129.94 TWh – significantly lower than the peak presented on Statista. If we take a look at other industries, we notice that gold consumes 131 TWh every year, while TVs in the USA consume 60 TWh annually. Most strikingly, fridges in the US consume 104 TWh per year... yet nobody starts a campaign to stop people from buying fridges and only eat fresh food instead.

Data centers which provide internet services to people around the world don't receive threats of having to pay 30% extra for the electricity they consume (as US miners did). Both of these provide something which is objectively useful to humanity, but only one of them is 100% controllable by the state... and it's the other one that regularly gets threatened with regulations that make business difficult. There are lots of double standards in judging Bitcoin mining and it's not fair. ChatGPT contributes to this FUD, though we must understand that Bitcoin is useful and provides value to human civilization.



Take this L, you elite-protecting AI!

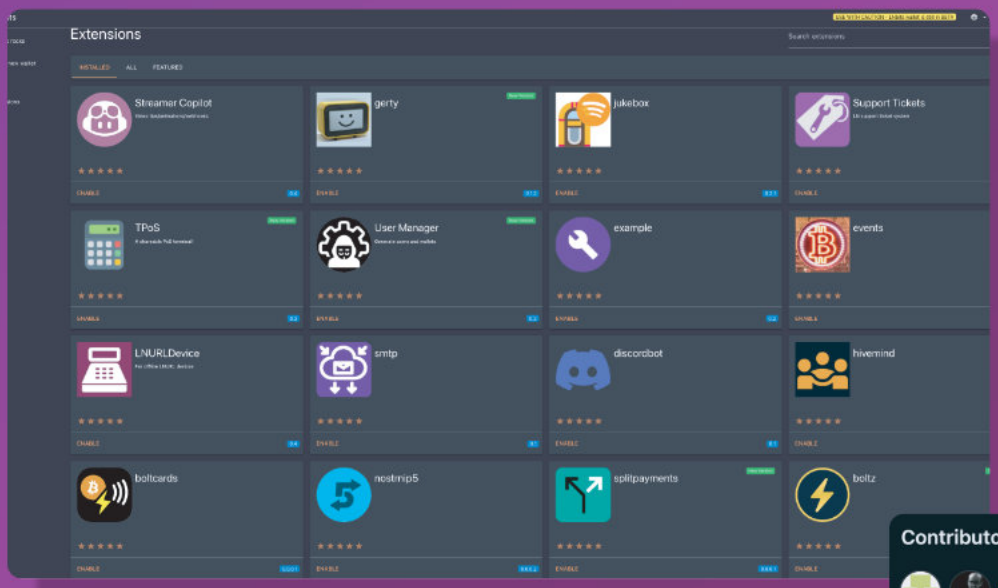
SCORE

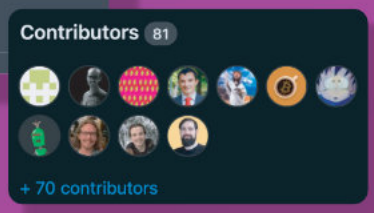
Vlad C.	**7**
ChatGPT	**0**


SLUSH POOL
IS NOW
BRAIINS POOL
MINING BITCOIN
SINCE 2010
LEARN MORE AT BRAIINS.COM/POOL

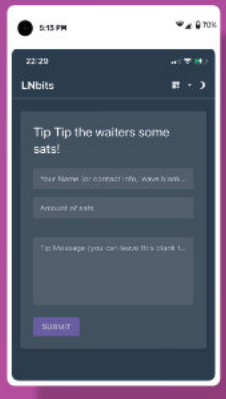
LNbits

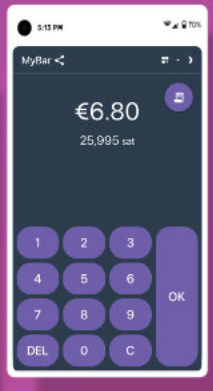
Free and open-source bitcoin accounts and extension system.
Run for yourself, friends & family, or for the whole world!

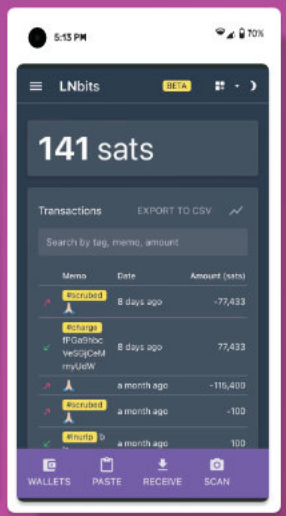




An insta-wallet system
Your own branded lightning wallet
Custodial community banking solution
Accounts system, each wallet with own API keys
Extendable platform using our extension framework
Develop for an API, use any funding source!
Part of a development stack for a bitcoin service
Build and connect your hardware tools
Awesome community!







Coinflip

Join us!
https://github.com/lnbits/lnbits


no intrinsic value
2011
SHIT COINER TEARS
Bitcoin is a Ponzi game!
2014
SHIT COINER TEARS
rat poison squared
2018
SHIT COINER TEARS
it's a failure too volatile
2021
SHIT COINER TEARS
2023:
SHIT COINER TEARS
Bitcoin eating popcorn, BTCTKVR.com



Breaking ChatGPT's Bitcoin FUD #8

Mining Centralization

51% ATTACK MINING BITMAIN CHINA / USA POW

According to ChatGPT, a small number of mining pools control a large portion of the mining power on the Bitcoin network. Such a scenario could lead to centralization of power and decision-making. First of all, it's nice to see that the AI model introduces a little bit of nuance by suggesting that the attack described is hypothetical. "Could" is a tad softer than "can collaboratively centralize" or any other phrasing which puts emphasis on the consequences of this threat.

Secondly, it's interesting that ChatGPT doesn't mention the 51% attack which reorganizes recent transactions and can theoretically rewrite the history across multiple blocks. Maybe that the programmers didn't spend enough time training it to FUD Bitcoin (and shill the Orwellian Worldcoin which Open AI endorses as an alternative), or maybe that the

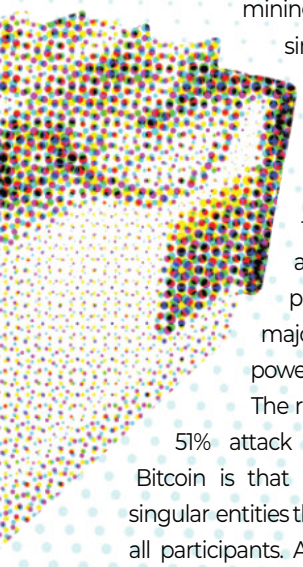
What do you think about this article?

Leave your comments or send a donation by scanning this QR code.

vagueness was left there on purpose. Regardless of semantics, let's break this FUD.

In order to challenge the FUD about mining centralization in Bitcoin, one must look at historical, technical, and game theoretical examples. Because the concerns date back to 2011 and they were never really validated – as a blockchain reorg attack takes a lot of coordination, and even if the attack takes place it's financially costly and socially difficult to sustain.

As described in the previous article, which debunked some dishonest concerns about Proof of Work mining and energy consumption, there have been previous moments in Bitcoin's history when users expressed fear of witnessing a 51% attack. What is a 51% attack, you say? It's a situation where one mining entity reaches a simple majority of hash rate and decides to reorganize recent blocks and steal money from transactions. It's not about a majority of participants, but a majority of processing power (or hash).



The reason why a successful 51% attack never happened on Bitcoin is that mining pools are not singular entities that can act on behalf of all participants. Also, at least up to this point, the miners have always found it more profitable to play by the rules and collect the coinbase rewards.

To recap, here are the moments in history when a mining pool reached a dangerously high hash rate – one which could theoretically enable them to launch attacks against Bitcoin:

– in July 2011, Deepbit surpassed the 50% mark: an event that inspired Bitcoin Talk forum user bcearl to post about it and tell others "Don't panic, but watch carefully!". In less than 2 years, Deepbit was already irrelevant and bitcoiners migrated towards new and more efficient pools;

– in September 2013, Bitcoin Talk forum user mechs pointed out that BTC Guild might become a "51% attack risk". Funnily enough, the first reply by Nancarrow was "Whoa man, deja vu". Bitcoin Core developer Greg Maxwell also tuned in to explain why the concerns are unjustified. But the most prophetic answer came from a user named johnyj, who suggested that GHash.io poses a greater risk because the hardware manufacturer is also the biggest operator;

– in January 2014, the rise of GHash.io has made Bitcoin Magazine co-founder Vitalik Buterin lose faith in Proof of Work mining. Around the same time, then-Bitcoin Core developer Peter Todd took to Reddit to announce that he sold half of his bitcoins to mitigate the risk. But in March 2014, the community coordinated a massive DDoS attack against GHash. In the aftermath, the pool shut down its cloud mining service and quickly faded into obscurity as it was no longer accepting new members. Only GHash's exchange service, CEX.io, is still around today;

– in 2017, bitcoiners would once again battle against a large mining pool named Bitmain. Like GHash.io, Bitmain was manufacturing chips that the rest of the industry was using. But what Bitmain did was to develop and enable the so-called ASIC boost, a special type of software which pushes the performance of their mining devices. Then, when they figured out that Bitcoin's SegWit upgrade would nullify their ASIC boost, the company shifted towards supporting Bitcoin Cash – the big block version of Bitcoin, which failed to get enough traction. Bitmain's support for BCH resulted in a loss of dominance for their two mining pools: BTC.com and AntPool. So while bitcoiners were concerned that Bitmain may get too big and attack Bitcoin, bad management made the company shrink and ultimately diminished its role in providing hash rate. However, Bitmain is still the biggest manufacturer of SHA-256 ASICs for Bitcoin mining and most other pools (as well as individual contributors) use their hardware.

This short history lesson is meant to





help us understand that Proof of Work mining is dynamic and no entity is too big to fail. But since the concept of a mining pool has been brought into discussion so many times, it's important to explain what it is and how it works.

A mining pool is a voluntary association of miners who want to maximize their chances to get rewards more frequently. By putting together their hash power, they become a pool and share the revenue according to the amount of contribution each member brings. For example, someone who mines from Buthan using hydro energy may find it way too hard and unreliable to find Bitcoin blocks all alone. So they look at existing mining pools and pick the one which charges the lowest fees. There are large mining pools from China (F2Pool, AntPool, ViaBTC), large mining pools from the United States of America (Foundry, MARA Pool, Luxor), and there's also a smaller option from Europe (Braiins).

The miners from Buthan can pick any pool…

and flip flop between them at will. Naturally, they will search for the best balance of predictability and high rewards. Though the largest mining pool offers the most frequent payouts, the smaller ones have lower fees and offer extra services such as free firmware updates to boost your hardware's efficiency and advanced profitability calculators. It makes no sense for everyone to go towards the biggest player – as the "small fish in a large tank" situation isn't always the most effective way to make money and free markets provide incentives to support competition.

Assuming that the Buthan miners pick a pool which is secretly malevolent and will attack Bitcoin as soon as the 51% hash rate mark is hit, this scenario doesn't mean that the Buthanese participants must be on board with the decision. They can leave the pool which acts in bad faith and contribute towards restoring the balance somewhere else.

In some cases, 51% attacks can be profitable for the miners. But this destructive short-term bet will only harm the long-term business at large. Assuming that every participant acts in the most rational economic way, it makes no sense to accept a short-term big payout instead of protecting a source of revenue that can bring higher rewards over an extended time frame. It's as if a farmer gets paid a lot of money to burn his crops – it may be momentarily tempting, but what's the point of risking his reputation and means to make a living when he can harvest the land for many more years in order to make a decent living?

Furthermore, if Bitcoin is under attack it's likely that the market participants will panic and crash the price. So the potential rewards at the end of a successful attack are significantly lower, as everything is in BTC. Sure, the attackers can use US dollars to short the price on some exchange... but they have no guarantee that their attempt would succeed and they're only exposing themselves to more risk. An unsuccessful 51% attack makes the entire effort a waste of time and energy, destroys the reputation of the attackers, and only strengthens the Bitcoin network to better respond to such a threat. But now we're assuming that such a coordination is possible, though history teaches us that it hasn't happened in times when the probability seemed high.

As of May 2023, there's geopolitical multipolarity in Bitcoin mining pools.



The Chinese miners, who have been suspected of one day colluding to launch a 51% attack against the network, still retain about 40% of the hash power across a handful of pools. Meanwhile, the US and European mining pools also add up to roughly 39% of the hash power. In the event of a totalitarian takeover in China or the US, which results in a politically-motivated attack against Bitcoin, no party can gain the necessary majority.

Furthermore, just because the pool is from China or the USA doesn't mean that the miners must be physically located in the same country. As a Romanian who might be mining from home, I am free to either launch a lottery ticket as a solo miner and only get the entire block reward by sheer luck, or else join any pool which offers me the best balance of low fees and high rewards at a predictable rate.

Though the pool itself is responsible for coordinating the participants, decentralizing limitations are set in place thanks to software innovations such as Stratum V1 (the industry standard since 2012) and Stratum V2 (a newer standard that's currently implemented by Braiins and offers even more decentralization through allowing individual miners to negotiate their own transaction sets). It's even more difficult for a pool to attack Bitcoin if the miners have the autonomy to opt out from certain types of transactions.



What is the cost to launch a 51% attack, though?

As of May 2nd 2023, when the hash rate is 322 EH/s and the price is $28700, it costs about $1.27 million US dollars per hour to rent the hardware that can pull off this attack. In the last hour, thanks to a combination of full blocks and high fees, Bitcoin has produced $1.6 million worth of coins. Theoretically, an attacker could have made $0.33 million in profits – assuming that the majority lasted for so long and other miners didn't turn on more machines to dilute the 51%.

However, this model is purely theoretical. Mostly because there aren't enough machines that an attacker can rent to use against the Bitcoin network. Currently, Proof of Work mining on Bitcoin uses a SHA-256 hashing algorithm which requires dedicated hardware. Due to limited and specialized demand, these ASIC miners are only made in a few places around the world and their supply is always limited. In hindsight, this scarcity of devices is oligopolistic and bad for the average Bitcoin enthusiast who wants to mine from home. But in practice, this means that enemies of Bitcoin must invest extra resources to purchase the hardware, run it in areas where excess energy is available, and start an initiative that might as well fail.

Back in January 2021, Braiins published an article which does some basic math about what a successful 51% attack requires. At the time, the hash rate was 150 EH/s. In the meantime, it doubled. So if we use their model and assume that the current miners remain honest and the attacker must get at least the same amount of hash rate (300 EH/s), and there's also an unlimited availability of Antminer S19 XP Hyd mining devices that do approximately 257 TH/s each, then at least 1167315 units are necessary to initiate the attack. Never mind that Bitmain's production can't accommodate this type of demand, let's assume that a nation state actor is able to get what they want or else build their own hardware in a secret factory.

What we should take into account now is that every single Antminer S19 XP Hyd device consumes 5346 watts per hour. 5346 multiplied by 1167315 is 6.23 GW/h. This amount of energy is immense and it would be very difficult



to find it among excess sources without causing disruption in places that require electricity. Only powerful nation states such as China, Russia, and the United States can theoretically mobilize to deploy such a large-scale attack. But in reality, given how one Antminer S19 XP Hyd costs $10000 and they'd have to spend $11.67 billions in taxpayer money only for an attempt (and then pay for electricity and personnel), it's much easier and cheaper for them to launch social attacks which actively discourage the use of Bitcoin: they can push regulations, they can spread all sorts of FUD, and they can leverage financial mechanisms to suppress the price on compliant trading hubs within their jurisdiction.

At this point, some would ask "isn't it easier for Bitcoin to migrate to Proof of Stake and leave behind this complicated game theory with likely attack vectors from global superpowers?". Well, the answer is a clear no. Proof of Stake is a "one coin, one vote" system that can't function without a concerning degree of centralization. Assuming that a nation state wants to attack Ethereum, Cardano, or any other Proof of Stake system, all it has to do is threaten with harsh regulations to crash the price and then print money to acquire a majority of coins. Then it's game over for the entire system, as the largest stake is in control of governance.

Attacking Bitcoin requires investing money in hardware and electric energy. And even if you do everything by the book and deploy the most successful attack in which the USA and China collaborate, it's still likely that the users will fork off to migrate to another chain which copies the pre-attack history of the previous network and changes the mining algorithm to turn any further attack into a waste of resources.

Bitcoin has never had a successful 51% attack specifically because the game theory system works. There's geopolitical competition between nations, there's electricity efficiency competition between miners, and the incentives to play by the rules are stronger than the consequences of attacking. Thinking about 51% attacks against Bitcoin is a nice intellectual exercise and the idea of this threat is useful in keeping honest miners in check (if they care about the network, they will consider migrating to smaller pools). But in practice, it's a nightmare to successfully undergo.

Sorry ChatGPT, but you're taking another big loss here.

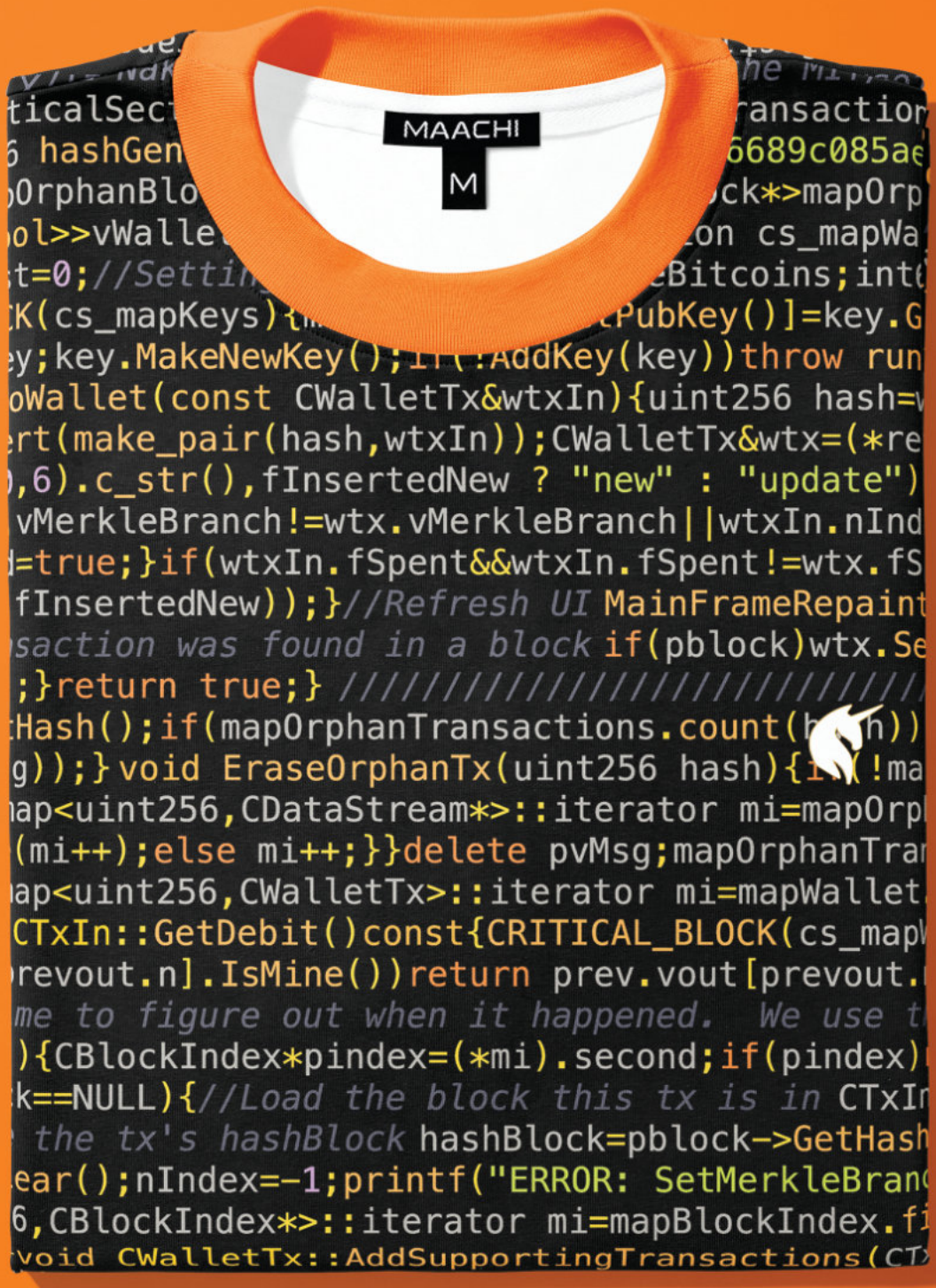


SCORE

Vlad C. **8**

ChatGPT **0**




MAACHI
M



Breaking ChatGPT's Bitcoin FUD #9



Education

ARGENTINA BITCOIN EDUCATION FUD NIGERIA

According to ChatGPT, many people still do not understand the technology behind Bitcoin. Presumably, this lack of education could limit the decentralized digital currency's adoption.

In principle, I agree that it's of utmost importance to teach others what Bitcoin is, how it works, and why it matters. After all, no invention or discovery in the history of humankind makes sense in the absence of both research to refine it and education to explain it. And even when you have these two elements, a context for this knowledge to be used is also necessary. Arguably, everything from algebra to the internet is meaningless unless we use it to solve problems and improve our lives.

Bitcoin is no different. At its core, it's software which runs on millions of computers worldwide for the

What do you think about this article?

Leave your comments or send a donation by scanning this QR code.

purpose of securing and verifying an innovative self-contained economic system. It's simultaneously a much-expected discovery and a revolutionary invention. It has the potential to change the way we understand and transact money. However, the way we use and describe such a system is subjective to human action and every individual's financial needs.

Given these arguments, I consider the statement "the lack of education could limit Bitcoin's adoption" silly, lazy, and antiquated. It could have been true in 2009, when only a few computer nerds understood what Bitcoin is and how it can be useful. It was probably true in 2014, before Andreas Antonopoulos' "Mastering Bitcoin" was launched to inspire an entire generation of writers to also pursue this path. But in the year 2023, anyone around the world can read at least some basic information about Bitcoin in their native language. So I'd like to argue that this is the most short-sighted and easiest to debunk type of FUD that ChatGPT could produce, as today we have more educational resources about Bitcoin than ever.

I could probably break the FUD only by presenting how the BTCTKVR magazine has grown since its release in 2021: even before launching this year's edition, more than 2000 people worldwide have received a physical copy of the magazine and many more enthusiasts downloaded the free digital version. And since it's an open source project, some of the best articles have been translated into French and Spanish. In 2022, Bitcoin enthusiasts from France, Argentina, El Salvador, and Senegal were able to get their hands on magazines at various conferences. And this is only the empirical data, to which I can personally attest.

Every day, hundreds of new articles about Bitcoin get written all around the world. We can see increasing interest from blogs, mainstream news websites, as well as academic journals. Furthermore, if you search for "Bitcoin" on YouTube and filter the results to only see the content that has been posted in the last 24 hours, you're going to scroll through thousands of videos in English, French, Italian, Spanish, Turkish, Arabic, Vietnamese, Czech, Polish, and many other languages. You don't have enough time in a day to consume the entirety of content that gets generated, which is a remarkable achievement.

But let's also look at books: Amazon lists more than 300 long-form publications on the topic of Bitcoin, ranging from digital-only self-published guides to paperbacks from some of the biggest publishing houses in the world. You can find everything from coloring books to trading guides, economic theory manuals, and programming tutorials.

Admittedly, most of the content is in English and all the latest research gets published in English first. There also appears to be a lag of 3-4 years between the original work and the moment it gets translated and commercialized in more than 5 languages. Furthermore, some of the more technical works rarely



receive translations – as their target audience is educated enough to already do most of the work in English. While these points are valid, my argument still stands: everyone around the world who benefits from internet access can learn at least the basics about Bitcoin. If something is not officially translated and/or published, today's artificial intelligence technology is powerful enough to turn an English text into something that a Cambodian or a Gambian can read.

But to play ChatGPT's advocate, there's an obvious difference between quantity and quality which can be best observed in the case of YouTube videos – most of these clips are purposely designed and structured to attract clicks, but rarely offer much educational information. Many of them present distorted facts which reveal a poor understanding of the subject matter, and the most popular angle from which Bitcoin gets presented is a type of speculation which closely resembles gambling. It's not even about betting against fiat currency inflation, the most popular approach is all about trading BTC for more USD.

This is arguably fine. Does every Bitcoin user really need to understand the technical details about how sending and receiving money works? Is it really necessary to explain economic theory to someone who only needs to send and receive money from a digital wallet? Also, does a form of sound money require a moral dogma which actively judges the ways in which people use it?

Bitcoin is a tool towards which people voluntarily and rationally converge…

when they need to. It's certainly easier to adopt among groups of technology enthusiasts and libertarians, but it's the oppressed and censored individuals who need it the most in order to overcome their struggles. While the former group uses Bitcoin as an ideological hobby or for speculation, the latter category of people needs it to survive under tyranny.



Though I tend to be a puritan when it comes to Bitcoin-related content and often dismiss low-quality contributions, I can agree that a limited amount of knowledge that's being shared is still better than no such knowledge at all. As long as people know why they use Bitcoin (and we certainly shouldn't question their rationality), it doesn't matter that they can't tell the difference between P2PKH and SegWit addresses.

Internet users don't need to understand the differences between various protocols in order to use e-mail and an internet browser. Bitcoin needs to reach the same degree of accessibility, under a user interface which seamlessly enables anyone to send and receive payments across all layers and sidechains.

So yes, education is certainly important and there's already plenty of it being produced every day. But awareness is even more

important. Thankfully, governments in crisis do a pretty good job promoting Bitcoin when they try to ban it. When the Nigerian government attempted to restrict access to on-ramps and off-ramps in 2021 as a response to the declining demand for their failing national currency, the effect was that more people found out about Bitcoin and started exchanging it in a peer to peer manner for goods and services. At one point, there was so much demand for BTC that the exchange rate in Nigeria was higher than in any other place in the world.

More recently, the Argentinian central bank decided to "mitigate risks" by banning Bitcoin from payment applications. What they actually did was to tell people that Bitcoin is the escape from the crisis – and undoubtedly, the results will be seen in the coming months. The central bankers did everything it takes to help the Bitcoin project, even if they don't realize it. All of this rising demand for Bitcoin will lead to the creation of even more ad hoc educational resources.

The people from Nigeria and Argentina weren't deterred by the rather limited access to educational resources (at least, as compared to English-speaking countries). They didn't give up on adopting Bitcoin only because nobody translated a specific book in their language and didn't care that the amount of BTC-related podcasts and YouTube shows is lower in their country. They pursued their needs, used the tools at their disposal, and learned to the best of their ability.

As a decentralized project, Bitcoin can't coordinate to finance the writing of books, the recording of podcasts, and the filming of video tutorials. Everything is a voluntary effort that may or may not be supported by the demand of a community. Some users create educational content with a specific audience in mind, while others do it for the sake of it – only because they want it to exist.

This magazine is part of the latter category: I don't know who you are, why you're reading this, and what you're planning to do with the newly-acquired knowledge. However, I do hope that you're going to share some information with your peers and help them become more free. If you want to translate this magazine, go ahead. If you want to make changes and sell it, be my guest. All that matters is that information gets passed along for noble and benevolent goals which protect human dignity and freedom of all kinds.



In a perfect world, where central banks and governments are accountable and honest, Bitcoin would be a silly idea that fails due to lack of demand. But in our times, it's a bit ironic how these institutions drive people towards Bitcoin and enable educators and content creators to enjoy a degree of success within their communities. Adoption rate and the quality of education are intertwined, as the former is a metric for the supply which pushes for the creation of useful resources.

In a perfect world, ChatGPT would be right on this subject matter. Unfortunately, it's only a tool which parrots pro-government narratives without much nuance. It's what the investors of OpenAI want, which makes it even more satisfying to register...

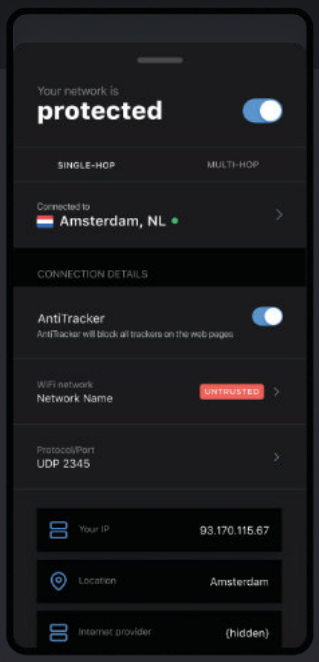
...another bitter defeat for the machine. Bitcoin education to the moon!

SCORE

Vlad C.	**9**
ChatGPT	**0**

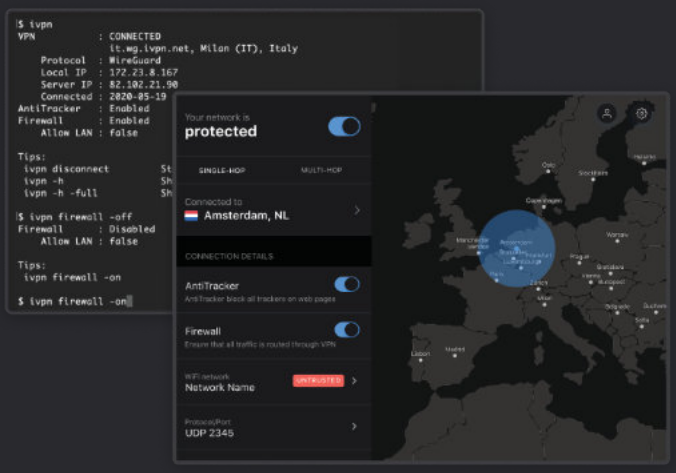


IVPN



Not your average VPN provider

- Generated accounts (no emails)
- Open source apps
- Regularly audited
- Run by privacy + Bitcoin advocates



BTC accepted,
Lightning recommended

Ask Vlad for a trial voucher card, or email **trial@ivpn.net** and refer to BTCTKVR.

Resist Online Surveillance

IVPN.net



Breaking ChatGPT's Bitcoin FUD #10

Mainstream Acceptance

ADOPTION MAINSTREAM EL SALVADOR LEGAL TENDER

According to ChatGPT, the fact that bitcoin still didn't reach mainstream acceptance among businesses and individuals is a big issue. Presumably, this is a threat for the entire Bitcoin project. And while I agree that creating demand for the currency by offering products and services in exchange for it is an integral part of building an economy, I still believe that the AI model's expectations are unrealistic and this piece of FUD is silly.

To better explain why I'm not taking ChatGPT's FUD about mainstream acceptance too seriously at this point, I'm going to have to define mainstream acceptance (or adoption). A first definition concerns nation state adoption, which El Salvador and the Central African Republic pioneered. The second definition focuses on bottom-up grassroots adoption, which

What do you think about this article?

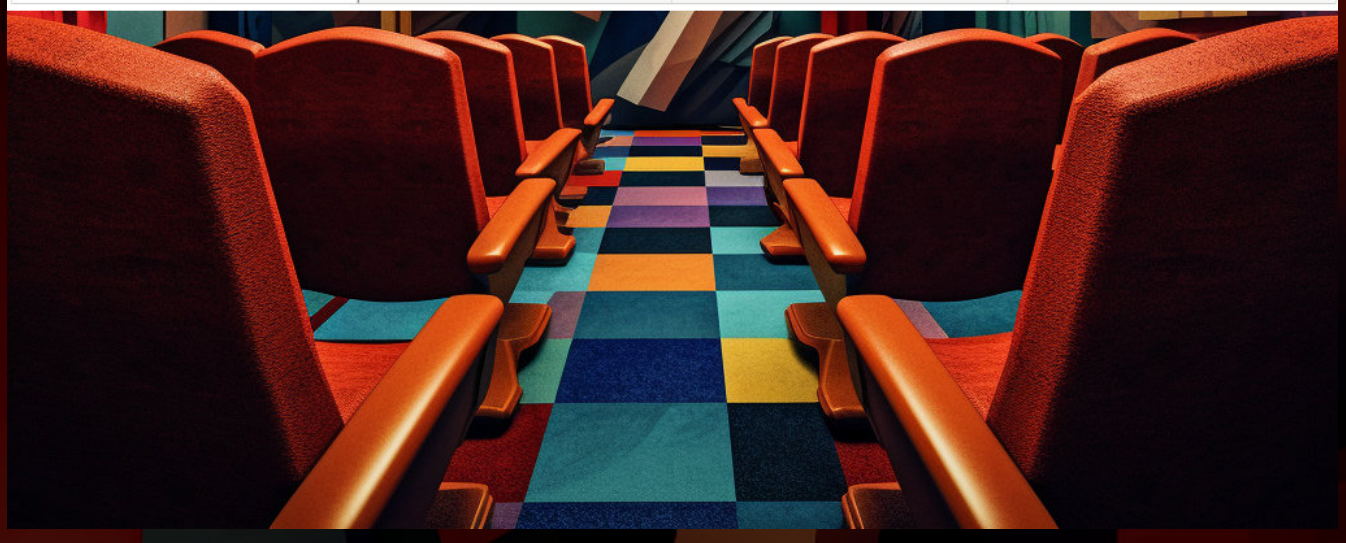
Leave your comments or send a donation by scanning this QR code.

is more significant and ideologically aligned with the mission of the Bitcoin project. It includes businesses, individuals, and everything in between which concerns the private sector.

Is Bitcoin such a failure or disappointment in terms of nation state adoption? Well, let's compare it with the two biggest fiat currencies in the world: the US dollar and the euro. The US dollar was first conceptualized on July 6th 1785, and it took another 6 years and 9 months until it became the United States of America's official currency through the Coinage Act of 1792. However, it wasn't until 1944 that the dollar became the world reserve currency – 152 years since launch and approximately 158 years since the first announcement.

In the case of the euro, it's the result of decades of discussions about a single European currency to challenge the US dollar's supremacy. It was first announced on February 7th 1992 as part of the Maastricht Treaty, and it became an official currency in 11 European countries at once on the first day of January 1999. Due to the fact that the German mark was already a reserve currency worldwide, the euro instantly inherited this property. As of May 2023, Bitcoin has only been around for 14 years and 4 months. 12 years into its existence, it became an official currency in El Salvador. The Central African Republic also embraced bitcoin in April 2022, but gave up on it only a year later. Though this adoption happened in a top-down manner, the use of bitcoin is not enforced by the states – meaning that

	Bitcoin	US Dollar	Euro
First Announced	October 31st 2008 (Whitepaper)	July 6th 1785 (Continental Congress resolution)	February 7th 1992 (Maastricht Treaty)
Launch Date	January 3rd 2009	April 2nd 1792 (Coinage Act of 1792)	January 1st 1999
First Became Official Currency in a Country	June 9th 2021 (12 years, 8 months since announcement)	April 2nd 1792 (6 years,9 months since announcement)	January 1st 1999 (6 years, 11 months since announcement)
Number of Countries Where It's Official Currency	~~2~~ 1	7 exclusively, 22 along other national currencies	20
Reserve Currency Since	2021	1944	1999
% of Global Reserves (2022)	<1%	58.36%	20.47%
Years It Took to Become Reserve Currency	12 since launch 13 since announcement	152 since launch 158 since announcement	0 since launch 7 since announcement





using bitcoin is legal for all types of payments, but the government won't use its monopoly on violence to coerce merchants and banks to accept bitcoin. In the case of the euro, the Italians, Spaniards and Germans had no choice but to exchange their lira, pesetas and marks for the new currency that they were obligated to use in all transactions. In comparison, this first wave of nation state-level bitcoin adoption is much more voluntary.

But Bitcoin wasn't created to serve governments of nation states. It exists as a way for individuals to opt out from tyranny and escape the consequences of central bank-driven inflation. The intended purpose of the project was made clear by creator Satoshi Nakamoto in the network's first block: "Chancellor on the brink of second bailout for banks" – a direct quote from the front page of The Times, a British newspaper which made a headline out of Chancellor Alistair Darling's decision to save the banks at the expense of all taxpayers on the same day that Bitcoin launched.

Bitcoin is not issued or controlled by any country,

it functions according to a predictable monetary policy which is clear and transparent for all participants, and relies entirely on voluntary interactions. This type of digital currency can't be confiscated, frozen, or taxed. Nobody can stop a certain user from installing, using, or else building their own wallet to participate in this economy. Furthermore, nobody can stop individuals from securing the ledger which contains the entire history of transactions and then broadcasting their own transactions to the network through their full node. And if users want to provide thermodynamic security to Bitcoin and also participate in the money issuance process, they can deploy their own solo or collaborative mining operations.

In many ways, any comparison with existing types of money is wrong – mostly because we put side by side



metrics from a free, transparent and voluntary system, and data from a trust-based, military-enforced, and politically coercive apparatus. It's a choice between freedom and submission to the big bully.

Nonetheless, it's still useful to understand that Bitcoin has accomplished quite a lot during its existence of 14 years and will only become more accepted as a worldwide currency specifically because its competitors are dishonest and untransparent.

Free markets outlive elections,

regime changes, and governments. Likewise, non-governmental and uncensorable internet money will outlive any type of financial central planning. Historically speaking, markets and neutral money tend to stick around for longer than empires, nations, and different waves of migration. The Silk Road consisted of Eurasian trade routes that lasted for about 1500 years, while gold and silver have been used as money since at least 550 BC. Bitcoin is relatively young, but it has already set a nice record of withstanding crises and navigating through chaos.

The most important part of Bitcoin's mission is for it to be adopted by people who need it and provide more economic freedom to the world. For now, it mostly works as a blackmail against governments and central banks – they either agree to maintain a reasonable degree of accountability by not devaluing everyone's savings, or else the people will refuse to use their currency and pay taxes. Bitcoin is the effective protest, a tool that works much better than marching in the streets and signing petitions. However, the main condition is that the people use it in a non-custodial and sovereign manner.

This, I believe, is the main barrier that still stands between Bitcoin and mass adoption – or, as ChatGPT calls it, mainstream acceptance. Even today, when the user interfaces are friendlier, there are quirks and frequent roadblocks that make the experience bumpy. Sometimes the on-chain transaction fees rise for a while and transactions get stuck in the mempool. Other times Lightning payments fail due to a communication error. There are times when managing UTXOs induces headaches. These issues can be tricky to identify even from an advanced user's perspective.

Given how simple it is to use your debit card to set up an account with a centralized BTC exchange, it's no wonder that most users are stuck in these bona fide banks. However, using a centralized, regulated, and ultimately government-compliant custodian defeats the purpose of using Bitcoin. Unless you use your own wallet, with your own full node, and with a certain degree of privacy against your government, you aren't really free or able to peacefully protest.

The complexity of self-custody is definitely a roadblock on the way to mainstream acceptance. Because using Bitcoin in any other way than with sovereignty is nothing but speculation with a trusted third party in the middle. But those who truly need to use Bitcoin will find all the educational resources they need in order to set themselves free from tyranny of all kinds.

I can argue that the reason why Bitcoin didn't gain too much mainstream acceptance is given by the relatively prosperous times that people have been living in the developed world, accompanied with a lack of technological means in the underdeveloped world. In between these two extremes, there were people who either decided to speculate or else secure a better future for themselves. The price also plays a major role, but on a long-term scale the volatility points to a massive appreciation against every fiat currency. Even when it's losing 50% of market valuation against the US dollar, bitcoin still finds itself performing better than failing fiat currencies such as the Argentinian peso, the Turkish lira, and the Nigerian naira.

Education about money and Bitcoin's place in the grand scheme of the global financial system is important. Having a good understanding of computer science and markets also helps a lot. But in the end, most people adopt Bitcoin because they need to – and if they haven't yet, then they didn't urgently need to up to this point.

As every price increase brings in a new wave of speculators, many of them will end up understanding the value proposition of Bitcoin and teaching others about it. As central banks print more money in this Bitcoin-educated environment, the adoption for the decentralized digital currency will grow. And as adoption grows, everything improves – from governments which become more



accountable, and all the way to Bitcoin wallets that receive enough feedback to refine user-friendliness.

But let's stop making excuses, ChatGPT can't win this one. According to CoinATM Radar, there are 34100 Bitcoin ATMs around the world, spread across 75 countries. This means that people from 75 different nations can use their local fiat currency to buy bitcoin, or else sell the bitcoin that they have for instant cash. Except for the US dollar, name another currency that's so easily accepted and transacted in 75 countries. The metric presented doesn't even count the thousands of small businesses around the world that accept payments directly in BTC.

Try to travel to East Asia, South America, or Central Africa with euro, British pounds, and bitcoins.

Talk to merchants in marketplaces, go to stores, and ask around to see which one of the three currencies is the fastest to exchange for the country's official form of money (and therefore, which one is most likely to get accepted as means of payment). You're going to be surprised to discover that the demand for bitcoin is second only to the US dollar.

In the West, most of the large retailers didn't catch up. Which enables bitcoin-friendly third parties such as Bitrefill (who sell gift cards) and ShopInBit (who will sell any legal physical items) to fulfil the roles of Amazon, Steam, Spotify, eBay, PlayStation Store, and lots of other services. There's definitely a parallel economy which is gradually intersecting with the mainstream one, but it's probably too early for BTC to be just as omnipresent as the US dollar in commerce.

Sadly, the only two moments which bring spikes in Bitcoin adoption are the massive price pumps that attract speculators and the tragic events that attract people who need



Bitcoin as a safety net. But as more time passes, the descentralized digital currency proves its resilience, and the grassroots demand for it increases, mainstream acceptance can only go up. The US dollar didn't become the dominant currency in 14 years, and neither did gold turn into the world's most important precious metal over night. It takes work, it takes persistence, and it takes education.

Nonetheless, given the circumstances, Bitcoin exceeded all expectations, defied the gloomy predictions of all Nobel prize-winning economists, and resisted pressure better than entire governments. In the process, it became more decentralized with every user who embraced sovereignty and it became better known with each person who spread the word about the magic internet money.

Mainstream acceptance is a marathon, not a sprint. And it's steadily reaching the goal.

Sorry, ChatGPT.

SCORE

Vlad C. 10

ChatGPT 0





Elon says you must pay $8/month just so your friends can see your posts.

Nostr fixes this

Pura Vida

Vlad @ BTCTKVR.com



FUD For Thought

Udi is a fraud



PROBLEMS | FUNGIBILITY | PRIVACY | SECURITY BUDGET | WEALTH DISTRIBUTION

For all the certainties that it offers and all the FUD that it can destroy through its continued existence, Bitcoin is still not perfect. Users and programmers must still deal with some of the system's design choices that leave room for speculation.

For instance, the single biggest bet in Bitcoin is that the network will one day benefit from the same security incentives while only paying miners with transaction fees. The diminishing block subsidy is an essential part Bitcoin's economic system: every 210.000 blocks (approximately 4 years), the mining rewards get cut in half. Back in January 2009, it was established that the mining reward would be 50 bitcoins per block. Then it got reduced in half in November 2012, and once again in July 2016, and May 2020.

As of May 2023, miners receive 6.25 bitcoins + transaction fees. And sometime next year, this reward will get reduced to 3.125 BTC per block. This halving trend will go on until the year 2140, when the entirety of the 21 million coins will have entered circulation. After this point, Bitcoin will be an entirely deflationary monetary system.

But what's also worth mentioning is that, by May 2024 when the next block reward halving should take place, 93.75% of all bitcoins will already have been mined. So most of the supply is in circulation, the costs to produce 1 BTC are higher, and therefore only the most efficient miners will survive. The only winning combination involves affordable and abundant electricity (nuclear, solar, wind, and/or hydro) accompanied by high throughput mining hardware which produces more hashes per kilowatt. If mining remains stagnant across halving cycles, then the game theory becomes more complicated.

This issue is generally referred to as

What do you think about this article?

Leave your comments or send a donation by scanning this QR code.

"the Bitcoin security budget", and questions to which extent existing subsidies will be able to keep the miners profitable in the future. It's estimated that, by year 2032, the transaction fees will already pay the miners better than the block reward of 0.78125 BTC. But some analysts are uncertain whether or not Bitcoin users are willing to constantly pay high fees.

There Are 6 Main Ways To Fix The Security Budget Issue,

which I will present from the most popular to the least supported:

A. The bitcoin price doubles every 2 years, so that the diminished BTC reward is worth just as much in US dollars. Though this scenario is the most popular, we've reached a point where it takes half a trillion US dollars to double today's market cap and it will take another trillion dollars to make the same successful transition in 2028 (then two trillions in 2032, four trillions in 2036, and so on). For reference, Apple and Microsoft have a cumulated market capitalization of $5 trillion, while gold is at $13.36 trillion. Even if we assume that inflation through money printing goes on and gets worse over the years, a bitcoin price that doubles every 210.000 blocks still requires a lot of liquidity that may not always come.

B. With help from merge-mined sidechains such as RSK and Drivechains that get a lot of traction, Bitcoin miners manage to collect more transaction fees across multiple parallel chains. The main chain fees don't increase too much, as most of the activity takes place on second layers. But the increased number of transactions in the ecosystem will compensate.

C. The bitcoin transaction fees will perpetually double after every halving cycle, to make up for the diminishing revenue. This is a social solution, as it relies on the good faith of others and their willingness to voluntarily pay higher transaction fees to keep the current miners running. Also, the fees don't have to double – they can increase proportionally with the price, so that miners get paid an amount which incentivizes them to keep going.

D. Do nothing and let the miners lose money until they find cheaper energy sources, improve their equipment, or else give up. This solution incentivizes efficiency and innovation in terms of hashes per watt, but also completely takes out miners that don't keep up. If the consequence of this purge drastically affects the hash rate, then all Bitcoin users will probably wait for more than 6





confirmations until they establish that a transaction becomes final.

E. Increase the block size, hoping that more transactions will come. This is difficult to pull off because it requires a hard fork (all users abandon the chain and move to an upgraded one), it negatively affects the miners' revenue during times of low demand, and it centralizes the network much more during and after times of high demand. Also, this type of scaling doesn't guarantee anything in terms of users and adoption – Bitcoin Cash, the big block clone of Bitcoin, didn't manage to get traction in commerce in spite of aggressive marketing campaigns in 2017 and 2018.

F. Change the monetary policy to add inflation/tail emission. This is, by far, the most unpopular approach – and the one that will only be taken seriously if Bitcoin finds itself in a phase where the fees don't make up for the declining block subsidy. It implies expanding the 21 million bitcoin cap in order to pay the miners, thus creating the type of inflation and central planning that bitcoiners sought to escape. Probably the most interesting proposal belongs to Peter Todd, who suggested that adding a small annual tail emission for the security budget might work.

In principle, this security budget FUD won't become an urgent discussion subject until sometime around 2032. By then, it's expected that a lot of innovation will happen in all fields – just like Bitcoin's first decade was filled with discoveries and new research. Nonetheless, it's good to know what's going on and what the options are – the more time we spend thinking about the problem, the higher quality debates we're going to have in the next decade.

Another source of legitimate FUD is the fungibility of the currency and the privacy it requires. When we deal with gold coins or banknotes, we don't have to care too much about the origins. At a convenience store, a $10 bill that was once owned by Brad Pitt should not be more valuable than another one which previously belonged to an obscure car mechanic from the suburbs. The money is fungible – meaning that one currency unit is equal with any other one which bears the same nominal value.

But in the case of Bitcoin not all coins are created and transacted equal. As a matter of fact, unless you buy the freshly-mined coins directly from miners, it's impossible to find two bitcoin units that carry the same history. The difference between cash and Bitcoin is that the former is great for local in-person transactions because it's instant, private, and has the best finality... while the latter is designed for internet payments and it's somewhat easy to track on the public ledger.

Bitcoin Has 4 Main Types Of Privacy:

A. Network-level privacy, which protects users of light wallets (those that run on other people's nodes and Electrum servers) from having their IP address registered. If someone can associate your Bitcoin transactions with a real IP address, then they can make use of social engineering to find out where you live. Thankfully, this issue can easily be mitigated with Tor routing (Tails OS on desktop, Orbot on Android phones, or specific wallets which have a Tor integration: Blixt, Blockstream Green,





Phoenix) or a good VPN service (IVPN and Mullvad are both excellent because they require no e-mail address and accept BTC payments).

B. Public key privacy, which prevents other people's servers from associating transactions from one UTXO with the rest of your wallet (and potentially identity). Your wallet's xpub (extended public key) contains information about how much bitcoin you have, which addresses belong to you, and which addresses your wallet will generate in the future if you continue using it. To remove this risk, users run their own full nodes, or else install wallets that run a BIP157/158 implementation (Neutrino). Managing your own node comes with great privacy benefits, and it's certainly something that everyone should learn.

C. Sender privacy, which is Bitcoin's weakest spot. When you send someone some bitcoin, they can take a look at the public blockchain to see from where the transaction comes and where the funds have been before. After you withdraw from a KYC exchange which works with blockchain analysis services, someone will most likely track your funds across transactions in an attempt to know to whom you are sending bitcoin and from whom you are receiving. CoinJoins (Wasabi, JoinMarket, Samourai) offer a reasonably good workaround: you enter a collaborative transaction where, even if the entrants (inputs) are known, it's difficult to tell who is who after the outputs get generated. CoinSwaps (MercuryWallet) are also great at exchanging your UTXO with somebody else's, but they pose the risk of receiving the identity of someone who's way more tracked than you may be. Using both tools in conjunction is the best solution so far.



D. Receiver privacy, which is Bitcoin's strongest spot in terms of privacy. As long as you use addresses only once, nobody will be able to determine how much money you have or with whom you have been previously transacting. Your sender will only be able to see that your balance went from 0 (as all new addresses) to the amount that he or she transacted in your wallet. They can see, however, how you transact your funds afterwards. On the other hand, if a third party node owns your public key (described at point B), then your receiver privacy is nullified – they can see your transaction in every new address you may generate from the same wallet.

E. Amounts privacy, which is about being able to see how many bitcoins are being transacted across addresses. Bitcoin is an open ledger, so you can see how much money is being sent even if you don't know who the sender and the receiver are. In principle, this is a matter of monetary policy transparency – you can always see that the amount of coins in circulation doesn't add up to more than the amount of coins that have been mined, of which there will never be more than 21 million. However, there is some interesting ongoing research in the field and zero knowledge proofs or some other type of technology may mitigate the need for auditability and amounts privacy.

The issue with Bitcoin is that Big Brother caught up and figured out how it works.



On-ramps and off-ramps are regulated in most countries, so the only truly private transactions are the ones that take place between someone who bought directly from a miner and his trading partner, CoinSwappers, or full node wallets that also went through a couple of CoinJoin rounds. Of course, there are off-chain solutions that offer better privacy: Lightning network, Liquid sidechain, statechains, drivechains, and other existing or proposed sidechains. But the base layer also needs improvements.

For now, privacy is costly. But it's important to not let Bitcoin get captured by nation states that surveil – or else it turns into a financial panopticon. Nation state adoption is also a bad idea, as citizens benefit from even less privacy while transacting. Last but not least, the core argument is simple: sound money requires fungibility and Bitcoin has yet to acquire it.

Another legitimate piece of FUD concerns wealth distribution inequality. Mainstream economist Nouriel Roubini repeatedly pointed out in 2018 that Bitcoin has a terrible Gini coefficient. Bitcoiners suggested that the mainstream financial system also has most of the wealth concentrated in the hands of a few elites and their families, but academic economists ignore this issue because they can't bite the hand that feeds them.

Nonetheless, it's true that almost 93% of the supply has been mined over the last 14 years and it's in the hands of a few millions of users. This isn't an argument for redistribution, but one for fairness: if Bitcoin is about being a better form of money, then it should be about more than replacing the financial elites of the industrial age with a new class of computer geeks.

Bitcoin can't be the currency of the entire world unless it can serve 8 billion people. To achieve this milestone, early adopters need to be more generous and sometimes charitable by allowing others to earn more bitcoin than their equivalent in government money in exchange for their goods and services. Tipping and gifting are also ways to onboard others and make them willing to participate in the network.

But for as long as Bitcoin gets treated as a collectible, it can't be money for the entire world – and this argument goes beyond the scaling debate. On a Bitcoin standard, all transactions are voluntary. So we should try to be voluntarily generous to prevent others from becoming envious or miserable to the point that they resort to violence. If we are truly building a better form of money, we must learn some lessons from the issues of fiat money and try to do better.

ChatGPT apparently wasn't smart enough to present these three pieces of FUD.

But I think they are much better than the stuff that it presented and I'm glad that I had the chance to explain them. They are FUD for thought, as we all have a voice and the ability to contribute to the Bitcoin project. Unlike the fiat system which has its own hierarchies that revolve around an official narrative and a system of trust, Bitcoin is voluntaryist: anyone can join, anyone can learn to code and try to bring improvements, anyone can educate others about it without requiring a license from an authority, and everyone can run a node or mine. In other words, we are all in charge and we can make a significant difference. Now that we know the FUD in theory, let's also break it in practice.

Europe's biggest BITCOIN Store

SHOPINBIT

800.000 Products

Free Shipping from 21€

3% Discount with Bitcoin/Lightning





Our Premium Services:

CONCIERGE SERVICE

Get anything.
We ship it worldwide.

TRAVEL SERVICE

Go anywhere.
Get the best deals.







shopinbit.com

Also part of the SHOPINBIT Family: PLEBBIN.COM



Breaking FUD

How A Father's Devotion Led A Sceptic To Bitcoin

This article is written by Grafton Clark, with assistance from his good friend Garry Rominger. Grafton is a technical writer at Trezor and bona fide advocate of Bitcoin peer to peer trading at Vexl. He is also the best friend of Ash, the fluffiest and most privacy-friendly dog in Bitcoin. Follow Grafton on Twitter @SatsDisco

Garry and I have been friends for nearly 13 years – united by our love for gaming, meat-based meals, random trips to castles, and unforgettable road trips to Berlin to attend concerts like Billy Strings. Our friendship grew as we spent countless evenings online, playing Call of Duty. Between rounds, we'd chat about everything: from our jobs and new movies, to girls and philosophy.

As I pursued a career in the world of Bitcoin, my expanding knowledge in the field deepened my focus on privacy and financial freedom in all aspects of my life. Bitcoin naturally became an essential part of my professional life and a recurring subject of conversation with Garry. Despite his initial reservations

What do you think about this article?

Leave your comments or send a donation by scanning this QR code.



("No way man, it's way too volatile and I don't know anything about trading stocks, or whatever."), I became increasingly passionate about sharing my experiences and knowledge about bitcoin with Garry during our in-game chats.

Although I've only worked in the industry for a short time, Bitcoin has been a huge presence in my life for nearly a decade. Needless to say, I've told countless stories and shared technical insights through rolled eyes and annoyed sighs which just motivated me to poke and prod further. I know Satoshi Nakamoto said "if you don't believe it or don't get it, I don't have the time to try to convince you, sorry". But when I'm playing video games late at night, believe me, I've got nothing but time.

Garry isn't an overly ambitious man. He would always say "as long as the rent is paid and food is on the table, I'm good". But I know him and I know he always finds a way to spend money he doesn't have on things for him and his family. I could see that his stance on Bitcoin was softening. Despite this, however, difficulties acquiring bitcoin (an American living in the EU without an address or bank account in his home country made it difficult for him to be able to withdraw any needed currency he'd potentially purchase) left a bad taste in his mouth.

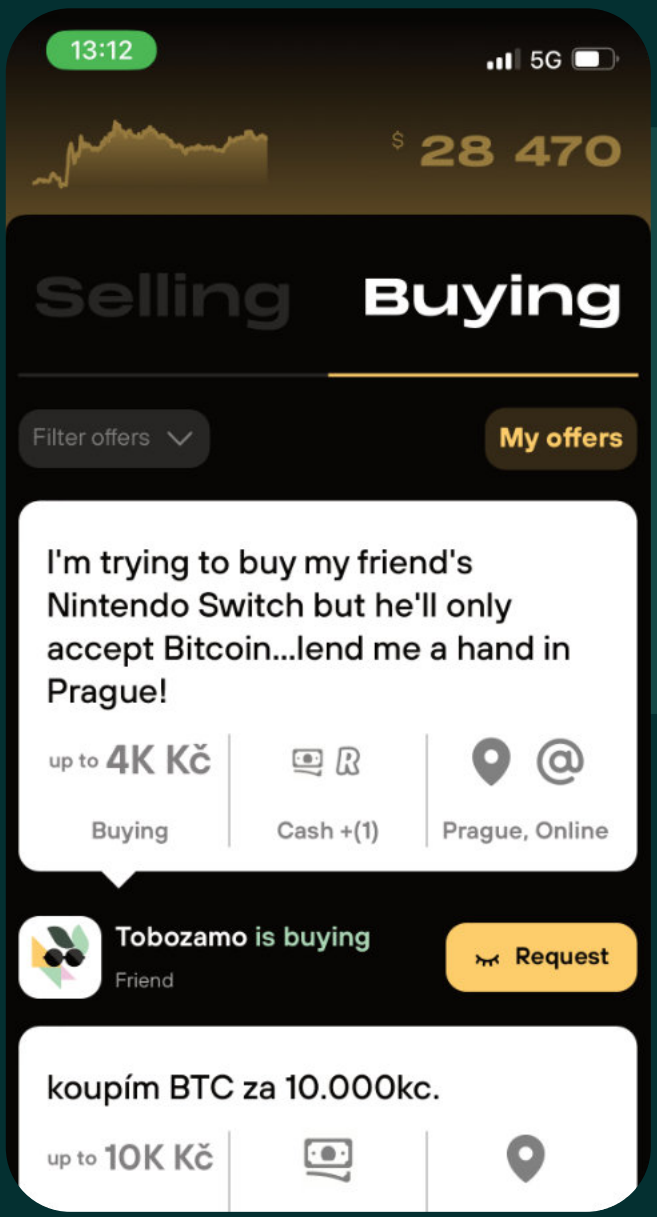
You could maybe understand why the overworked family man soured on this new financial endeavor. While he saw the merit in all I tried to explain, he still had fears over the perceived risks,



and he was consistently faced with new obstacles each time he mustered the courage to take the plunge into the world of bitcoin. To Garry, bitcoin seemed temporarily out of reach.

Garry's second son has just been born and gaming became an even more important bonding tool with his oldest. He set his sights on a Nintendo Switch. In 2017, I bought one such video game system at a local electronic store that had just started accepting bitcoin. I was reminded of this purchase each time I heard the click of the console starting. I was once again reminded of this purchase when I heard that, in his search for a reasonably priced Switch, he was immediately scammed on Facebook marketplace.

Upon hearing this, while I emphatized with his situation, I experienced a hint of "schadenfreude" – a German term for taking pleasure in others' misfortune. Once we stopped laughing, I made the decision to offer him my Nintendo Switch at an, admittedly, excellent price. There was, however, a catch: I had to be paid in bitcoin, and I wouldn't be selling any of my own coins for fiat.



Garry, now presented with a real-world reason to acquire bitcoin, was determined to make it happen. Through game chat, I quickly helped set him up with a Lightning wallet and we practiced zapping sats back-and-forth. Those were his first ever bitcoin transactions. He was amazed at how easy it was, which boosted his confidence. After this experience, he was excited to buy his first bitcoin. So I introduced him to Vexl, a mobile app that allowed him to buy bitcoin without the hassle of KYC and without dealing with a financial institution. Peer to peer, as it was intended.

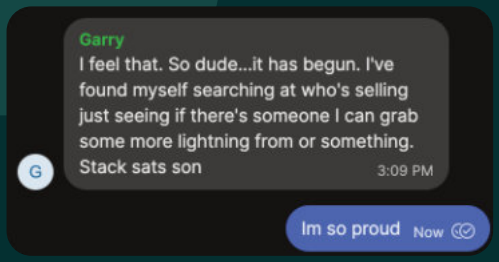


Garry downloaded the app and quickly created an offer. Within minutes, he found someone willing to Vexl (trade bitcoin). He had finally converted his dirty fiat cash for bitcoin. End of transaction, no documents, no electric bills, no hassles and no difficulties. Garry's first bitcoin purchase went the way many of us wish ours had gone.

He then sent that bitcoin to me – and in exchange, I happily turned over the Nintendo Switch for his son. I was more than pleased to replenish the bitcoin I had spent on the Switch so many years ago. It took a real world application and years of friendship for Garry to overcome his Fear, Uncertainty, and Doubt. Today, he's a proud and active bitcoiner.

The bitcoin community has really made some strides, simplifying just about everyone's involvement with this peer to peer cash system. It's less about making a fortune and more about having a simple, permissionless way to handle money.

Nowadays, there are tons of user-friendly tools that help people get into bitcoin without any fuss. It's all about being in control of your own finances while enjoying the experience. Take Garry's story as an example – he stepped into the world of bitcoin, and now he's loving it. I felt incredibly proud when I got this text message from him, and I can't resist sharing it with you:



The Bitcoin community has managed to make it not just accessible, but also quite a fun experience. With so many new doors opening up, people everywhere are starting to see bitcoin in a whole new light. I've really enjoyed watching Garry's "aha" moments while taking his first steps in the realm of Bitcoin exploration. Now, every time we hang out, he's all about picking up the tab... as long as I pay him back in BTC, of course. It's been awesome being part of his journey, and I'm stoked to see how he'll share his excitement and adventures with others.

HALL OF PLEBS

@Buchiimaine says you should watch the Dirty Coin documentary

King Arctan

@BeggiJonsson

From Dragoș M. to Marian A.
"Bro, everything is seen!"

Ionuț Bogdănel Herghelegiu

Iulian Șerban (Zece)

tweetious

Travin "Tavern" Keith

@Buchiimaine says no really, you should watch @TheDirtyCoinDoc



David St-Onge says: check out my book "Bitcoin: Everything You Need to Know"



Daniel Ses @ iBlock.ro

Mopar Mining @ CryptoCloaks.com

@Florinqw9

Max Hillebrand

@Buchiimaine says: let's go Brandon... to El Salvador 🇸🇻

Asanoha

@BTCparadigm says: "you are an idiot. eat mushrooms and buy bitcoin"




BITCOIN
TAKEOVER
PODCAST
SEASON 14
BTC HERE!

Mallorca Blockchain Days

Be part of the Mallorca Blockchain Days IV experience

July 13 - 16 2023

Palma, Mallorca, Spain

GET YOUR TICKET ONLINE



WWW.MALLORCABLOCKCHAINDAYS.COM