BTCTKVR



LISTEN ON

twitch YouTube twitter



Table of Contents

Foreword	04
The Long Road to Taproot	06
Are You Here For The Pump Or For The Revolution?	10
Can Bitcoin Work As Paper Money?	12
Introducing Bitcoin Takeover Radio	14
When Are Nation States Ready to Adopt Bitcoin As Legal Tender?	18
The Music on Bitcoin Takeover Radio	24
Why Bitcoin Incentivizes Sustainability & Environmental Care	26
Explaining the Lightning Network So Even A 10 Year-Old Can Understand It	28
Bitcoin in 2021: Principles vs Number Go Up	32
Can't Withdraw To Your Own Wallet? It's Not Your Bitcoin	38
How & Why Michael Saylor & MicroStrategy Can Become Bitcoin Villains	46
Bitcoin Public Key, Receiving Address, UTXO: What's the Difference?	50
On Taking Bitcoin Mining to the Moon. . . Literally	54
How to Make Bitcoin Transactions Environmentally-Friendly	58
The Significance of Satoshi Nakamoto's Coins	66
Comic Strip: Bitcoin Eating Popcorn #1	70
How to Pay Lower Bitcoin Transaction Fees (Full Guide)	72
Listen to the Bitcoin Takeover Podcast on Sphinx, Breez & More	80
We Need to Start Denominating Bitcoin in Bits	82
It's Time to Replace BTC-USD with BTC-Gold	86
Companies Can't Wait to Buy Your Bitcoins To Opt-out from Inflation & Taxation	88
At 12 Years Old, Bitcoin Is Turning Into a Rebellious Teenager	90

Foreword

What type of Bitcoin-related magazine is more successful: the one which sells thousands of copies in a handful of developed countries, or the one which can be acquired for free by anyone who wants it, regardless of location, nationality, and income? When I decided to start working on the Bitcoin Takeover Magazine project, I've spent a lot of time pondering on the following issue: do I want to be just another guy who delivers content to an echo chamber and entertains the minds of those who most likely already know a lot about Bitcoin, or should I also search for ways to reach wider audiences?

Correspondingly, I set my mind on getting to the individuals who need to learn about Bitcoin, but can't afford to purchase a magazine subscription, don't have the time or commitment to go through long internet articles, and/or feel a degree of skepticism which doesn't allow them to spend money on any kind of educational material on the topic.

In order to accomplish my goal, I needed to:

A. Produce content that is interesting to both newbies and well-versed bitcoiners;

B. Publish it in a way which makes it available to anyone around the world (all the articles can be found for free on btctkvr.com and by the time you start reading this, a PDF version of the magazine will have been published as well);

C. Print it on high-quality, beautiful and durable paper which facilitates borrowing and guarantees that nobody is going to throw away the magazine even if they dislike the topic or the author;

D. Pay for the printing, graphics, and distribution without going bankrupt;

Luckily for me and my project, I found a handful of companies and individuals who believed in my mission and provided financial support. My pitch was very simple: it costs me about 10 euro to bring to life another high-quality copy, so whatever amount of money you're giving me is going to get spent on making the magazine printer go BRRRR. The more donations and sponsorships I receive, the more copies I'm going to print and distribute for free to individuals who want and need to learn about Bitcoin.



What do I offer in exchange? A full-page ad for every company, individual, or entity which helps me subsidize the Bitcoin Takeover Magazine (abbreviated BTCTKVR for convenience). The amount really doesn't matter: it can be 10, 100, or 1000 euro. Regardless of this financial factor, every sponsor you will be seeing throughout this issue has received ad space. I did it because I like their product/service and I'm the kind of guy who would rather receive a small amount of money from a handful of sources than sell out to some big entity that would make me feel like I've made compromises with my core values.

Furthermore, I have nothing but respect for those who support educational work without trying to impose their agenda on the nature of the content. None of the companies was interested in vetting the articles that I will be publishing in the magazine and nobody asked for a favorable article to get featured – all of them chose to believe in my project and support the mission of printing and distributing magazines.

I would like to thank Bitcoin Takeover Podcast sponsors Vaultoro and Wasabi Wallet for unconditionally believing in my work throughout the first half of 2021. Without them, I wouldn't have had the peace of mind to write all these articles and pursue the topics that I find interesting. Then, in no particular order, I would like to thank LNBits, Bitrefill, Trezor, Start9, and Mallorca Blockchain Days for allowing this first print to get delivered to you in a timely manner. All of these companies and entities (as well as the individuals who run them) have believed in me and my work before anyone else did and didn't ask too many questions about ROI, statistics, target audience, and everything else that marketing departments like to talk about. For this, I am grateful.

I would also like to thank:

– Mihnea Niță for creating this beautiful magazine layout, handling most of the graphics for my articles, and also designing the cover under pressure and in record time (it only took about one week to put my articles in this beautiful graphical enclosure and I'm extremely satisfied with the collaboration. If you need graphic design or video editing services, feel free to contact Mihnea at: nitamihnea@outlook.com);

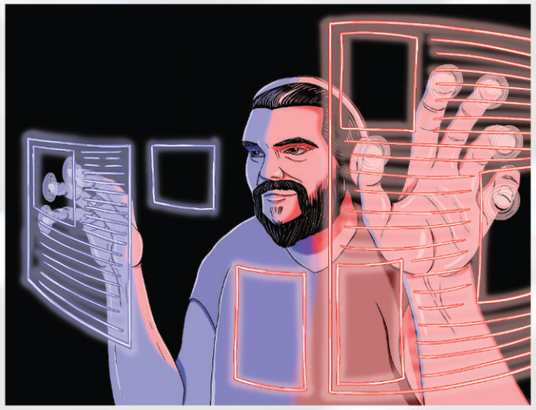
– My parents and my brother for providing emotional support while also questioning the extent to which my work is actually "work" (as opposed to a hobby which consumes all of my time and money). Their input always keeps me grounded and low on hopium;

– My government for keeping me locked down for months in 2020 and constantly instilling fear in all of the friends with whom I used to hang out. Being indoors for such a long time might have ruined my social life, but it turned me into a mad yet surprisingly productive workaholic who wrote lots of articles;

– Bitcoin Magazine for treating me like an expendable freelancer who could get overworked and underpaid, was never good enough to get promoted to staff writer status, and got replaced shortly after rage quitting over editorial differences during the daily morning call. I wouldn't have found the drive to publish my own magazine if it wasn't for a couple of their staff members.

Last but not least, I know that you find it funny or strange that I talk so much about a money system without looking to make any actual money off of my work. But as somebody who has greatly benefitted from free educational resources both before the internet age and during it, I think that it is my duty to give back to the world by sharing my knowledge with people from all around the world.

You can still support me with a donation. But you should be warned that I will most likely use your money to print more magazines that I give away for free, produce more content (articles, videos, podcasts),



open more Lightning Network channels with curious strangers, and buy pizza around lunchtime.

Donate BTC on-chain to this address: bc1qxszcuhscawhjys25ts87em9fvmunkdfat9rj5y

Send a Lightning Network donation via LNBits: https://btctakeover.lnbits.com/lnurlp/2

Dump your infinitely inflationary fiat on Patreon (recurring monthly payments): https://www.patreon.com/bitcointakeover

This is the free and open source version of the BTCTKVR magazine. Under the CC BY 4.0 license, you are free to share the content, print your own copies, and even sell them if you want. Since my goal with the BTCTKVR project is to spread knowledge and education, this is a great opportunity to help others learn about Bitcoin with physical and visually-pleasing content. Let the magazine printer go BRRRR!



Taproot is the most significant refinement that the Bitcoin code has received in recent years. It follows the same soft fork activation route that SegWit has used in 2017, except this time the trial involved securing 90% of the blocked mined throughout a 2016-block epoch (approximately 2 weeks).

From a technical point of view, Taproot takes the best of three major improvement proposals: Schnorr signatures (as described by BIP 340), Merkle branches (also known as MAST or Merklelized Abstract Syntax Tree, as described in BIP 114 and BIP 117), as well as new opcodes (Taproot, Grafroot, G'root, and cross-input aggregation).

As explained by Bitcoin Core developers Pieter Wuille, Jonas Nick, and Anthony Towns in their final BIP 341 Taproot proposal, their work is not an encapsulation of all previous ideas – as adding too many code changes would result in a more difficult review process and higher chances of adding undesirable bugs. At the same time, it's not an attempt to separately push previous proposals either – too many upgrades would exhaust independent node operators, while also reducing the benefits of this selective approach. The authors of the BIP called it a "tradeoff" which "strikes balance", but I like to think of it as a refinement which prioritizes the best features available and makes everything efficient.

Taproot is like combining three dishes without eating too much, while retaining the taste and nutritional value. And it's another significant breakthrough in the process of making Bitcoin more efficient – instead of scaling through bigger blocks like many existing altcoins, the network seeks to make the existing small blocks more efficient and private for all users.

In a previous article, I've praised the activation mechanism and argued that the path to upgrade completion reflects the kind of decentralization that Bitcoin really needs to succeed as a project. In this article, I'm going to use Pieter Wuille's short thread to tell the story of how Taproot got activated and also explain what's next.

Taproot – from 2018 diner talk to June 2021 lock-in

As of block height 687284 (mined by F2Pool on June 12th 2021), the Taproot soft fork has been signalled by more than 90% of the miners which discovered blocks throughout an epoch. This means that Taproot will finally get activated at block height 709632, an event that is estimated to take place in the month of November.

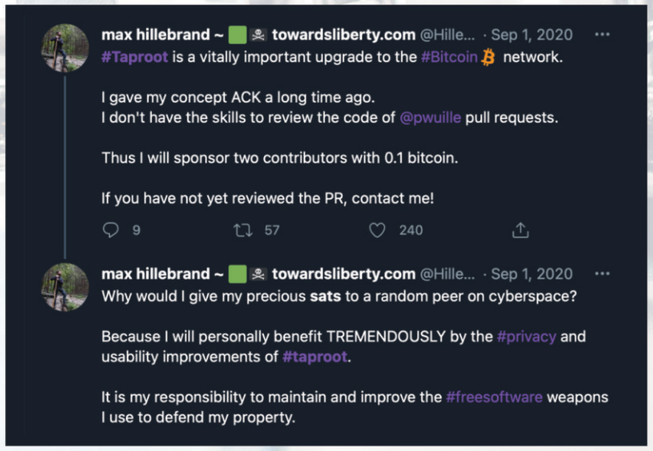
However, the Taproot phenomenon didn't happen over night. The idea of replacing Bitcoin's ECDSA (Elliptic Curve Digital Signature Algorithm) with Schnorr signatures has been debated within the community for years. Satoshi Nakamoto chose the lesser efficient ECDSA because there was still a patent which prevented him to use Schnorr until 2008, and the more popular open source standard had more libraries anyway. So while his design was not ideal, it was the most practical and reasonable for its time.

Yet bitcoiners have been dreaming of adding Schnorr signatures for quite some years. A proposal has been formalized by Greg Maxwell in January 2018, just a few months after SegWit got successfully activated via UASF (User-Activated Soft Fork). Around the same time, Maxwell met with fellow developers and cryptographers Pieter Wuille and Andrew Poelstra in a diner from Los Altos, California. As described by Wuille, his peers had come up with a "really cool idea to hide Merkle roots in P2PK-like outputs" while he briefly left the table.



But in Bitcoin, the process between a successful brainstorming session and the creation of a thoroughly-reviewed proposal takes 3 years or more. Wuille formalized the first Taproot proposal in May 2019 – it was only a short message to the mailing list of Bitcoin developers, but the text already described the main features of the soft fork. Contributors to this proposal include Jonas Nick, Anthony Towns, and Tim Ruffing – all of whom stuck around throughout the entire development cycle.

After some careful testing and observation, a refined version of Taproot was created by Wuille in October 2019. This time,



Wuille and his collaborators figured out more parts that may cause unnecessary complications and stand in the way of the desired efficiency (most famously, 1 byte from the initial 32 byte public key design was dropped because it "provably does not contribute to security"). Also, they quadrupled the depth of the Merkle trees for the sake of optimizing the code. The name of the Bitcoin development is efficiency, and this second version was nothing short of its goal.

The Taproot received its final changes in August 2020, when the quadratic residue tiebreaker was removed. Once again, this was all about improving efficiency. And when one feature does not provide the expected benefits and causes extra sophistication, it gets removed. This is part of the Bitcoin development ethos, according to which every line of code matters. It's not just minimalism, but a constant quest for maximum efficiency.

By October 2020, a final version of Taproot was available for testing. Developers merged it in a preliminary testnet version of Bitcoin Core 0.21, and it was around the same time that the debates about activation became serious.

Meanwhile, all throughout the development process, independent auditors would take a look at the open source code. After all, the future of money is at play and nobody wants to allow a terrible mistake to damage the functionality of a system like

[bitcoin-dev] Taproot activation proposal "Speedy Trial"

David A. Harding dave at dtrt.org
Sat Mar 6 03:43:43 UTC 2021

- Previous message: [bitcoin-dev] Supermajority then simple majority Taproot Activation
- Next message: [bitcoin-dev] Taproot activation proposal "Speedy Trial"
- **Messages sorted by:** [date] [thread] [subject] [author]

```
On the ##taproot-activation IRC channel, Russell O'Connor recently
proposed a modification of the "Let's see what happens" activation
proposal.[1] The idea received significant discussion and seemed
acceptable to several people who could not previously agree on a
proposal (although this doesn't necessarily make it their first
choice).  The following is my attempt at a description.

1. Start soon: shortly after the release of software containing this
   proposed activation logic, nodes will begin counting blocks towards
   the 90% threshold required to lock in taproot.[2]

2. Stop soon: if the lockin threshold isn't reached within approximately
   three months, the activation attempt fails.  There is no mandatory
   activation and everyone is encouraged to try again using different
   activation parameters.

2. Delayed activation: in the happy occasion where the lockin threshold
   is reached, taproot is guaranteed to eventually activate---but not
   until approximately six months after signal tracking started.
```

Bitcoin. Bitcoiners like Max Hillebrand offered bounties to code reviewers to take a look at every line of code and make sure that nothing contentious or poorly-optimized would get included. This is part of the beauty of a decentralized and open-source system, where everything is visible and anyone around the world can contribute.

If you recall the events, it was all about showing support for LOT=true or LOT=false: in the former case, sovereign nodes could step in and reject the blocks of miners that don't signal Taproot activation at the end of the trial period; in the latter case, there would be no consequence if miners refused to update to Taproot (thus giving them a veto power). Either way, the signalling period would have lasted an entire year.

Most of all, users were aware of the 2017 situation with SegWit. At the time, the miners refused to signal the softfork activation before the given trial time. Therefore, sovereign nodes took it upon themselves to adopt the transaction malleability fix – thus leading to the successful UASF movement.

But in the middle of these heated debates, David Harding presented a proposal for a "speedy trial" which lasts only 3 months and requires a supermajority of 90% of blocks mined during an epoch (1815/2016). This seemed like the ideal way to proceed, as everybody else seemed to agree that the Taproot code was ready and activation was only a matter of agreeing to update the Bitcoin Core client.

The speedy trial had a rocky start, with only a couple of mining pools (including Slush Pool and Foundry USA) signalling the activation of Taproot. But bitcoiners were relentless and they kept on demanding miners to signal their support. Users on Twitter went tribal and displayed their advocacy for Taproot by using the green block emoji next to their name – but after the first epoch, the situation didn't look so good. Though F2Pool was the big player that joined the activation camp, it still wasn't enough.

The second epoch of the trial didn't succeed either, but it was pretty close. Around the time, mining pools such as Poolin, Antpool, BTC.com and Binance Pool were pressured into joining the signalling camp. During the final dozens of blocks of this epoch, it became clear that the third time's a charm: unless the miners decided to backpedal on their decision to support Taproot, the activation would get imminently locked in. And that's exactly what happened on June 12th 2021.



What's next for Taproot?

The Taproot activation is going to take place in November 2021, at block height 709632. But until then, there's a lot of work to be done. On the developers' side, wallets need to be upgraded and standardized. To take advantage of the privacy advancements of multisigs, the MuSig2 format needs to receive a standard that all wallets can use. Also, the PSBT extensions need to get improved to communicate with keys, scripts, or signatures.

On the users' side, they must update their node clients to a version which supports Taproot – the most recent being 0.21.1. This is the most important step, as all the coding and activation efforts are futile if they don't get used to their full potential. Obviously, everything is optional and relies on the best interests of the sovereign node operator. But there are unquestionable advantages to upgrading at both the individual and the network level.

I read about Taproot for the first time in 2019, in Aaron van Wirdum's article. It took approximately two years for the code to get refined and reviewed by the community, and another half a year until the speedy trial succeeded in locking up the soft fork for the November activation. It feels like a long time, but this is how progress is made on a decentralized and truly deliberative ecosystem. Everything must be optimized to the slightest details, while efficiency is much more important than the speed of activation or the pressure coming from market actors during various phases.

Bitcoin is the perfect example of a decentralized system which takes into account the opinions of all users and gives everybody enough time to voice their concerns and criticism. Going forward, it's unlikely that anything will change – miners and node operators will always demand the highest standards of rigor before running a new version of the client, while developers will seize every opportunity to stand out with constructive additions or valuable criticism.

There are still improvements to be made to Bitcoin's base layer and there are plenty of proposals, ranging from Drivechains to OP_CheckTemplateVerify. The developers are hard at work doing what they do best: making the most out of Bitcoin and extending its limits in creative and efficient ways.





Are You Here For The Pump Or For The Revolution?

During moments of extreme exuberance or pain, it's easy to lose focus and forget why you got involved in the Bitcoin space. High prices make you forget about all the struggles which laid the foundations for the glorious moments, while dramatically-low dips might make you think that it's all over.

But like the legend of the phoenix, Bitcoin has a long history of dying and coming back to life in the least expected moments. And it's very likely that we're going to $100.000 and beyond – given the irrationality of fiat inflation, bitcoin's appreciation against the dollar is almost certain – though it's impossible to time the market and figure out when something happens, you can look at the fundamentals and figure out why it will happen.

The problem is that humans are greedy and tend to act irrationally. This is how bubbles get formed and burst. This is why we switch from extreme bullishness to the anecdotal "blood on the streets" within a few days. This is why the volatility is so wild. And this is when the differentiation happens between the winners and the losers of the trading game – the winners always do their fundamental analysis and know WHY they are holding onto an asset.

Now that I've written a brief explanation of market psychology, it's time to get to the subject matter of this article: conviction and a good understanding of what Bitcoin is. Because as soon as you figure out how the Bitcoin network works and what the bitcoin currency can do for the world, you will stop worrying about fiat evaluation and focus more on accelerating this goal.

And no, Bitcoin was not created to help corporate CEOs like Michael Saylor and Elon Musk get richer. They were only among the first of our current financial elites who understood the potential of a truly decentralized, uncensorable, unconfiscatable, and disinflationary form of money. But to their credit, they are most likely here for the revolution because they want to spearhead it – they already have all the fiat riches and may make even more from stock market investments, but it's likely that they see something that the rest of us cannot or do not.

Bitcoin is not just a revolutionary tool, it is THE revolution. It's the kind of system that cannot be stopped and benefits from every mistake of central banking. It's a bearer asset which empowers every individual with all the virtues and advantages of self-custody. And it's the kind of money whose supply anyone can verify and audit (aka run a node), while anyone can voluntarily participate in the process of inflating the supply according to the planned schedule (aka mine).



From a monetary point of view, bitcoin is a major step up from gold (better divisibility, portability, durability and scalability, as well as provable scarcity). Its Achilles' heel is the reliance on electricity and the internet – though one could argue that modern banking is exactly the same, while also highlighting the efforts to make the Bitcoin network available via physical bearer assets, and through satellite, dish antennas, and even radio short waves.



It's easy for shitcoin peddlers to point at Bitcoin's apparent slowness and suggest that their new and very centralized currency network is better and handles more transactions. But they willingly ignore all the development that's happening on top of Bitcoin via layers: the Lightning Network, as well as sidechains such as Liquid, Drivechain, Statechain, RSK, and more. Basically everything that exists in altcoins can be done on top of Bitcoin to benefit from a more solid monetary base and better network security.

The reason why it's not happening faster is that bitcoiners demand rigorous testing before moving their hard money in one direction or the other. And the developers working on Bitcoin projects tend to be more honest than their altcoin counterparts: they wouldn't recommend something unless they themselves are sure that it works as designed and is safe for everybody else to use.

But in the long-term, Bitcoin will deem altcoins pointless and also make fiat central banking undesirable and obsolete. This is the goal to which Satoshi Nakamoto hinted in the message that he wrote in the genesis block and this is why most old-time bitcoiners have stuck around the space. Most of them are already fiat wealthy and have moved past the speculative investment phase. The goal is not to be rich, but to be free and help the rest of the world achieve this civilizational goal.

So next time you feel like capitulating and get gloomy feelings about the state of the objectively volatile market, ask yourself once again: why are you here? If the answer is "for the pump", then it's all good: take your profits in fiat and return whenever you figure out what Bitcoin actually is.

On the other hand, if you're here for the revolution, then you're going to need to spend a little more time educating yourself and others than watching price charts. You need to be willing to learn beyond the qualifications written on your degree and outside of your comfort zone. Revolutions don't happen because the people starting them are foolish and poorly educated – you can claim that their ideals are naive, but you can never question their intellects.



Can Bitcoin Work As Paper Money?

Though Bitcoin finds itself ahead of the financial innovations of our times, it is not part of the cashless society agenda. Correspondingly, its purpose is not to replace the concept of paper money or the physicality assets, but to change their underlying backing. Instead of having paper money that's backed by a nation's debt, in the future we might make day to day purchases with pieces of paper that can be redeemed for BTC at the nearest exchange.

Turning bitcoin into a bearer asset is essential for the expansion of the currency's use as medium of exchange and unit of account. By virtue of cryptographic innovations and lessons that we have learned from centuries of issuing banknotes, we can successfully make bitcoins more liquid, more private, and less reliant on an internet connection or network interactions.

Cash is the most private and fungible form of money that we have. It can change owners without leaving any kind of trace and it's the ultimate instrument for preserving the economic rights of the individual. While transacting on Bitcoin's base layer leaves permanent records and sending Lightning transactions generates cryptographic proofs that get verified by participants routing transactions, cash leaves no permanent trace and can't be identified.

But in order for bitcoin to work as paper money, it needs to fulfil these criteria:

- the bill must contain distinct elements that make it unfalsifiable, while counterfeit money should easily get detected;
- the bill shouldn't contain the private key like in the case of paper wallets. Instead, it should have a distinct cryptographic proof (such as an Open Time Stamp) to prove the issuance by a certain entity (exchange, government, or any other issuer). Based on this unique identifier, the issuing entity must enable bearers to redeem the bitcoins;
- the bill must be provably backed by an equivalent amount of bitcoin. One bill equals one distinct UTXO. To guarantee that the corresponding amount was not redeemed at a bank/exchange, a scannable public key should get printed on the piece of paper;
- in the event that the bill gets irreversibly lost or destroyed, it should be easily replaceable by the issuer. This can be established by setting a custom to replace the bills every 5-10 years – everyone should have enough time to trade their banknotes, and after an arbitrary deadline the old paper money should get replaced;
- the verification should include the entire bitcoin reserves which back the paper notes. This would make sure that there is no arbitrary printing outside the existence of reserves.

Historically and traditionally, paper money requires an issuer that can be held accountable. Though bitcoin is a permissionless and decentralized currency which can be held for an unlimited amount of time, the transition to paper money can't be practical without breaking some of these rules. Just like sidechains and second layers, there will be trade-offs. In the case of paper money, users will appreciate the untraceable privacy and the ability to make bitcoin payments without using the internet.



Correspondingly, bitcoin paper money can get issued by exchanges, banks, or governments. The subsequent trading should be frictionless, instant and voluntary. And just like in the case of Liquid peg-outs or Tether withdrawals, the party which redeems the bitcoins must undergo a more thorough identity verification process (and the redeemers will most likely be businesses, organizations, and other legal entities that want to hold real bitcoins instead).

When merchants receive a bitcoin cash (pun intended) payment, they will make use of a free open source application which verifies the UTXO, the greater funds which backs the banknotes, the unique serial number of the bill, and the unique design elements which guarantee authenticity.

The verification shouldn't take longer than a quick scan – and the message on the screen should describe the status of the verification. Certainly, it's not as frictionless as cash and still requires an internet connection on the side of the merchant (for further verification, the payer should also run the same software to avoid fraud attempts). But it's still a great way in which bitcoin can be used under the shape of paper money.

Previous proposals for bitcoin paper money

Other similar proposals go back to August 2010, when Bitcoin developer Gavin Andresen described how "printing bitcoins" would work (though he described the creation of paper wallets).

In 2013, Sergio Damian Lerner (who later went on to design the RSK sidechain) described a more advanced and technical system which he called BitBanknotes. And the proposal for bitcoin cash (pun intended) seems to be recurrent during bull markets, as Andreas Antonopoulos tweeted a picture of the $5 bill with a "5 mBTC tag" when the price of bitcoin hit $5000 in October 2017.

More recently, Charlie Lee suggested that El Salvador should print paper currency backed by corresponding bitcoin amounts. Though newer bitcoiners acted on gut instinct and vehemently rejected the idea, applied cryptography expert and early Bitcoin Core developer Peter Todd confirmed that the idea is possible by virtue of cryptographic proofs (having worked on Open Timetamps and Proofmarshall, he is definitely one of the most knowledgeable people on the matter).





Introducing Bitcoin Takeover Radio

Meet Jane: a 21 year-old who lives in a futuristic metropolis and is slowly beginning to discover the advantages of sound money. She's impatient, finds it hard to resist the temptation to trade, and yet she is willing to learn the fundamentals that strengthen her conviction.

This is why Jane is listening to the Bitcoin Takeover Radio: a project which combines education and entertainment is order to promote both the content and its creators. There are hundreds of articles, dozens of podcasts, and at least a handful of songs that get released every day on the topic of Bitcoin. And even though many of them tend to be great, there are times when some really good ones get buried by social media algorithms or the short attention span that we get forced to develop in our information era.

Bitcoin Takeover Radio curates the best content that you may have missed, from creators who are most likely too busy working on their next project to spend every day spamming you with self-promotion posts. Podcasts that may have been buried by the Twitter newsfeed receive their chance to get in the spotlight and get introduced in a playlist which combines fun with learning.

There is something special about the radio format, as it exposes you to a degree of randomness. Normally, if you were to create your own playlist, you would only choose the content that you know is good. But if you allow somebody else to surprise you, there are high chances that you will discover a great podcast or song that you would have never found in your daily routine.

These are some of the practical and philosophical considerations behind the Bitcoin Takeover Radio project: the idea is to promote both the content and elevate the creator. Bitcoin is such a broad topic and it can be presented from so many points of view, that we often discover unique perspectives. So it's always a good idea to step away from the comfort zone or information bubble and expose ourselves to something new. You think you know it all, until a new voice takes you down a whole new rabbit hole.

Where does the Bitcoin Takeover Radio get streamed?

By virtue of a very nice piece of software that's called Restream, I will broadcast the weekly playlist on YouTube, Twitch, and Twitter. Make sure that you follow/subscribe all of these channels.

In the future, if there is enough demand, I can also stream the broadcast on Facebook. But according to my observation, there isn't enough Bitcoin-only activity going on and the groups tend to be flooded with uninteresting shitcoinery.

Furthermore, you can talk about the content with other enthusiastic listeners on the dedicated Bitcoin Takeover channel on Telegram. Become a member and join the conversation.

If you're on Sphinx chat, you can also chat in the Bitcoin Takeover tribe.

Rewarding excellence in Bitcoin podcasting and music

Every broadcast will feature a QR code in the description. If you choose to make a donation, then the funds will get divided equally between all content creators involved in the episode. If you want the donation to only go to one or a handful of them, then please write me an e-mail and mention your preference. But it would be ideal if you contacted the podcasters and musicians personally and sent them the donation directly, to minimize the friction, the costs, and the blockspace occupation.

In the event of a small base layer donation which needs to get split in a dozen of tiny amounts, I'll most likely use the Lightning Network

Anyway, these individual efforts deserve recognition and the kind of rewards which encourage content creators to keep going. And if I'm able to facilitate the process, then I will gladly do it.

In a perfect world, hard work and excellence should always get better results than relentless marketing and engagement tactics. Unfortunately, the reality is different and we often allow hype to steal our time and attention. Though I probably won't be able to make a significant change, I will do my best to provide better incentives for Bitcoin podcasters and musicians.

Why are there sponsors?

Producing an online radio show requires an investment in equipment and production. Curating the best content around also takes time. And last but not least, there are electricity costs involved in keeping a computer online all the time – and a low-powered Raspberry Pi won't be able to handle the task.

This is why I've decided to start looking for sponsors. They help me break even in financial terms, and also make use of their marketing teams to promote the project. I see it as a huge win-win opportunity. Not only that, but I'm very strict when it comes to selecting sponsors and only choose true Bitcoin believers who are in this space for all the right reasons.

No, the content creators who allow me to use their podcast episodes and music will not benefit from any sponsored financial compensation. But it's likely that someone from the company that sponsors the show will listen to their show or at least share the broadcast on social media channels and make it easier for the work to get discovered. To compensate for this inconvenience, I've created the donation system that I described in the previous section.

Also, I will use the sponsorship opportunities to give back to the community. I'll try to do giveaways and organize all sorts of engaging events that give everyone more reasons to listen to the entire stream and pay attention to some fine details.



How often does the radio content change and how can you submit your own work?

I'll do my best to create a different show every week and replace the ongoing stream with new podcasts and music. If, for whatever reason, I can't do the replacement in a week, then I'll let the existing broadcast get looped until I put together all the fresh content. Though I like to think that I'll be consistent about it, I'd rather make pleasant surprises than break promises.

If you want your podcast or music to get featured on the Bitcoin Takeover Radio broadcast, then send me an e-mail or Twitter DM. Attach your best work and I'll give it a fair evaluation. If it's really good, then I'll make sure to add it to the next livestream and mention something nice about you and your work in the introduction.

Since the livestream plays in a loop, theoretically there isn't a time limit for how long it can be. However, I'll try to keep it under 24 hours because otherwise it's gonna require more work than I can handle in a week. You'd be surprised how long it takes to edit or clean up only a few minutes of audio.

When launch?

On Wednesday, May 12th 2021, 8 PM CET (1PM EST for Americans), I will start streaming the first broadcast. It includes podcasts from 9 other content creators (some of whom you know and most of whom you'll love) and music from myself and another artist.

This first broadcast is sponsored by Vaultoro and ShiftCrypto's BitBox02. The former will give you the chance to win 100 bits (10000 sats) through a Lightning faucet at the end of every episode, while the latter will teach you about Bitcoin history and might just do a hardware wallet giveaway.

I will also promote Wasabi wallet (their podcast Wasabikas is also part of the playlist and I can't praise their product enough) and THNDR Games (I'm a big fan of Jack Everitt's Bitcoin Bounce and Turbo 84 and we're doing a cross-promotion).

Is Jane single?

Yes, she is! But then again, she hasn't met you yet.



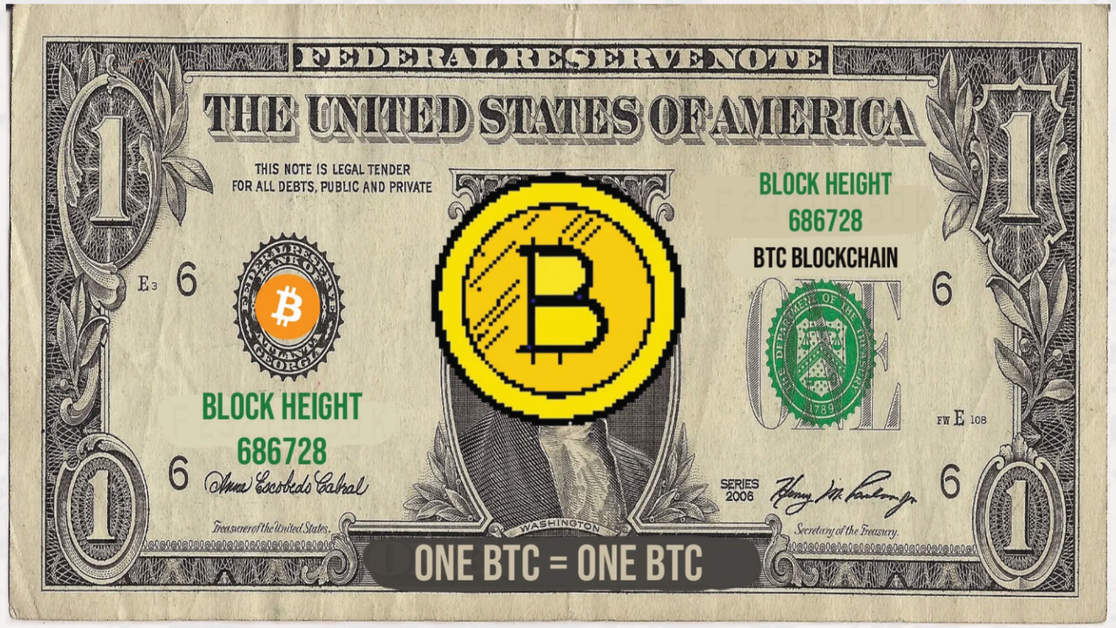
Secure Your Funds

Your Gold at Vaultoro is secured in your name as your legal property within top-tier vaulting facilities in Switzerland, fully insured and audited by one of the largest auditors in the world, BDO.
Buy gold with Bitcoin with confidence.

Trade from Bitcoin to investment-grade bullion and back. Crypto can bring large gains, Gold is to preserve those gains without dealing with banks or fiat.

Vaultoro™
The European Alternative Asset Exchange

VAULTORO.COM



When Are Nation States Ready to Adopt Bitcoin As Legal Tender?

In my previous article, I've tried to explain why adopting bitcoin as legal tender in El Salvador is a bad idea whose risks outweigh the benefits: poking Uncle Sam from a Latin American country whose official fiat currency is the US dollar, which has a 90% debt to GDP ratio, and whose 20th century history is filled with coups and even had a 13 year-old civil war cannot end well.

And this doesn't mean that the people from El Salvador can't or shouldn't enjoy the financial sovereignty of bitcoin – after all, we are talking about a globally-available permissionless money system which doesn't discriminate on any personal or national grounds. But the problem of declaring bitcoin legal tender is a lot more nuanced and concerns geopolitics. In a world where the US dollar is the global reserve currency and the US officials undertake every step to maintain its supremacy, a government needs to either have the proper military power to deter any foreign intervention or have strong allies who unconditionally defend its power structures.

Nation states do not enjoy the same freedom that individuals do. And even though heads of state have a certain degree of leeway and can legitimize their decisions in front of an elected constituency, they are also held accountable on an international level – either directly in organizations such as the United Nations, or indirectly via sanctions and embargoes (whose approval may involve the after-mentioned organizations, but without necessitating the participation of the sanctioned government).

While I really want to be proven wrong by real-life actions, I'm pretty pessimistic about nations states turning bitcoin into legal tender. In a world where the US dollar is becoming more competitive against the rising Chinese yuan, I don't see the government which spends the largest amounts of money on its military conceding or at least stepping back to observe how the bitcoin experiment can work. So take everything that I write in this article with a grain of salt, be doubtful, and think critically.

Though I do my best to rely on historical facts and my limited knowledge as a political science/international relations graduate, I can be wrong and I'm ready to admit it when reality contradicts my expectations. However, in this article I want to answer the question "When are nation states ready to adopt bitcoin as legal tender?".

Dr. Orangecoin or how I learned to stop worrying and love the bomb



In the post World War II global politics, the nuclear missiles guarantee nation states a seat at the table. Even if these weapons never get used, they guarantee an incredible amount of sovereignty and deterrence against foreign involvement. Nuclear weapons also open doors to negotiations and make even the mightiest of empires compromise on their agenda.

As of 2021, there are only 9 nations which have nuclear weapons: Russia, The United States of America, France, China, The United Kingdom, Pakistan, India, Israel, and North Korea. Among them, the only ones which have a weak national currency and therefore might be more incentivized to adopt bitcoin, we can distinguish Russia, Pakistan, India, Israel, and North Korea.

However, Israel is unlikely to act against the monetary domination interests of their allies. So the only real contenders remain Russia, Pakistan, India, and North Korea.

Can Russia adopt bitcoin as legal tender?

Russia has already made a series of contradictory and puzzling decisions in regards to bitcoin. As of June 2021, Russia officially recognizes BTC as property and store of value, but discourages its use as a currency. Also, government officials and their family members are legally forbidden from owning any type of foreign digital currencies (including bitcoin), as a way of preventing bribery and other forms of corruption (official source, translated source).

Also, Russia is currently undergoing a preliminary process to create a "digital ruble": a central bank digital currency (CBDC) on which it has monopoly. So it's unlikely that the Kremlin government considers making bitcoin a legal tender. On the other hand, there have been rumors about the Russian government using BTC as a reserve currency. Nothing was ever officially confirmed, but given the existing sanctions and the significant gold purchases it's likely that there might be some holdings.

It's also worth noting that in the last 10 years, the Russian ruble has lost a lot of value against the US dollar. Somebody who held US dollars since 2011 would have 3 times the purchasing power.



Unlike El Salvador, Russia is playing the geopolitical game more conservatively and seems to use deception and confusion as a way of ensuring privacy (tactics that are part of every military and statesman textbook since Machiavelli's "The Prince"). The language/alphabet barrier also plays a significant role, so the Western media's exposure to many official documents is limited.

Given the current state of affairs and Russia's position, it's unlikely to get an official announcement about bitcoin getting turned into a legal tender. But this doesn't exclude the existence of parallel economies and a potential large governmental position.

Can Pakistan adopt bitcoin as legal tender?

In January 2021, news broke about Pakistan setting up government-funded bitcoin mining farms. In a country whose fiat currency (the Pakistani rupee) is rapidly losing value against the US dollar, this makes a lot of sense. In the last 10 years, the PKR has depreciated by almost 50%.



Interestingly, bitcoin is officially banned as a currency for both citizens and businesses. There is no official exchange operating in the country, but citizens use LocalBitcoins, Paxful and other peer to peer trading platforms.

On the other hand, citizens mine from home to get an extra source of revenue, since the electricity is affordable and mostly comes from renewable sources. This proves that there is actual demand for bitcoin as a currency – and the demographics also suggest that the average age is on the younger side. For more details, read Farooq Ahmed's article.

The situation became a little more relaxed throughout the last year and is likely to shift more in favor of bitcoin. Unlike El Salvador, Pakistan is populous, is neighbored by a hostile country against which it will always want to gain an edge, and has the nuclear nukes to deter any kind of foreign intervention.

It's not a free country and has all sorts of human rights violations which are recorded by Human Rights Watch, Freedom House, and Amnesty International. But given the country's position and its adversarial approach to neighbors, as well as a lack of colonial influence from a G7 nation, I tend to believe that Pakistan finds itself in a very strong position to adopt bitcoin as legal tender – possibly one of the best in this article.

Can India adopt bitcoin as legal tender?

In March 2021, the Indian government proposed a bill that would effectively ban all activities involved in bitcoin: trading, holding, receiving, and mining. If passed, this law would make India stricter than even China in terms of punishments for bitcoiners.

At the same time, this type of approach is recurrent during hype cycles and there seems to be a lot of business development which brings prosperity into the country. From Coinbase to Coinmama, there are dozens of exchanges which offer support to Indian users.

The Indian rupee doesn't do so well either – in the last 10 years, it lost half of its purchasing power against the US dollar. This is bad news for the world's second most populous country, though the threat also opens up the door for some opportunities.



But there are two impediments that will deter India's path to accepting bitcoin as legal tender: its colonial and post-colonial ties which extend to both Russia and NATO, as well as its gold culture. These ties can be turned around the become opportunities, but India seems a lot less likely to adopt an adversarial mindset against the hegemony of the US dollar.

And yet India scores higher than Pakistan in Freedom House's evaluation of individual political rights and civil liberties. According to Amnesty International, the country has a similar record in regards to human rights and freedom of expression. But when it comes to the protection of minorities (ethnic, religious, and sexual), India doesn't do so well (according to Human Rights Watch). So why would it do better in terms of protecting the rights and property of a financial minority?

In some regards, India seems like a great place to make bitcoin legal tender. But then again, it seems less likely to break away from the financial status-quo than Pakistan and has fewer incentives to do so. It's a more traditionalistic and conservative culture which has centuries-old relations and cultural ties with some nations.

To learn more about Bitcoin in India, listen to my interview with developer Rajarshi Maitra.

Can North Korea adopt bitcoin as legal tender?

Now this is a hard question to answer. On one hand, it makes sense for a rogue government which isn't part of most international organizations and completely disregards international law to defy the global financial status-quo with a stateless and censorship-resistant currency like bitcoin. On the other hand, the Kim dynasty maintains a degree of control and Soviet-style cult of personality which isn't philosophically compatible with something like Bitcoin.

So it makes sense for the regime from Pyongyang to mine bitcoins to circumvent economic sanctions. Otherwise, the regime doesn't care much about the prosperity and well-being of its people and is much more concerned with power and control through propaganda. Allowing citizens to send and receive payments outside the borders without the government's permission is completely against the polity's interests.



And even though the North Korean won has lost more than 600% of its value against the US dollar since 2011, the declining national currency is still a way through which the dictator maintains the legitimacy of the totalitarian regime.

Maybe that some privileged elites are using bitcoins, but allowing such a revolutionary idea to exist and spread to the masses could overthrow the system – and this is against the interests of Kim Jong-Un and his family.

Yes, North Korea does have nuclear missiles and has used them to threaten other Western countries like the United States of America. They are a powerful negotiation instrument. But their purpose is not to offer freedom and sovereignty to the people.Thus, North Korea is the least likely country to adopt bitcoin as legal tender.

Wild Card: Iran

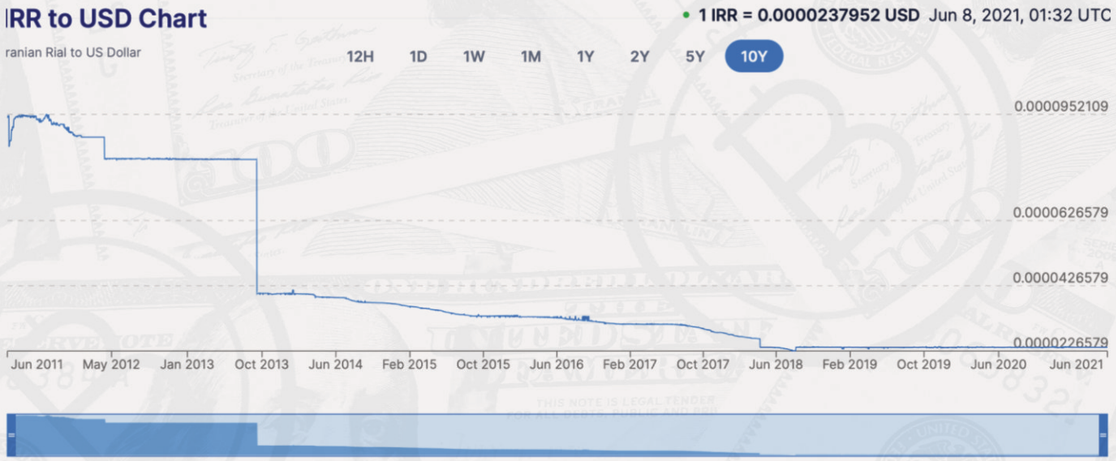
Iran is exactly the kind of country that would adopt bitcoin as legal tender. For decades, the Middle-Eastern state has undergone uranium enrichment research. Against all odds, heads of state have determined Western powers to make concessions and establish deals which prevent Iran from developing a nuclear program. But this game of threats has also manifested as a cause for economic sanctions which limited the country's ability to export oil and restricted essential imports.

Since 2011, the Iranian rial has lost more than 300% of its value against the US dollar. And most of this depreciation happened not because the country is poor on resources and cannot engage into trade, but due to various sanctions and trade embargoes.

But in relation to bitcoin, the last few years have shown us two interesting yet discouraging phenomena: on one hand, exchanges that operate in countries that are friendly with the USA have frozen the funds of all Iranian users – they didn't even get the chance to withdraw their coins within a given time frame, but instead had to wake up to the harsh reality that custodial solutions are vulnerable to geopolitical factors to which private companies tend to be compliant; on the other hand, the Iranian government has recently made significant efforts to ban mining, crack down on exchanges, and thus make it harder for citizens to become financially sovereign.

Iran might be another case of a top-down regime which wants to take full advantage of Bitcoin to avoid economic sanctions, but has no interest in allowing the people to be free. Bitcoin is merely an affair for government officials and their cronies. This doesn't mean that there can't and won't be individuals who hold BTC and mine them secretly. But it significantly lowers the chances of officially turning bitcoin into a legal tender in the country.

Yet in the midst of these struggles to avoid foreign sanctions, one can only hope that the country's leadership realizes that allowing citizens to be financially sovereign can bring a lot more prosperity and development for the country. But then again, the control may also be rooted in the religion and the political culture that Iran has had for centuries





Why Bitcoin doesn't care

Just like the internet and radio waves, Bitcoin is universal and state-agnostic. Its use doesn't make a general characterization for intentions and purpose. It's the sovereign user who decides how and for which purpose the money shall be spent.

Therefore, there will be plenty of governmental and corporate actors who will find desirable qualities in Bitcoin's features. It doesn't necessarily mean that they believe in the mission of the Bitcoin project – it only means that their incentives are aligned with the capabilities of this internet money system.

Ideally, Bitcoin should lead to more freedom and prosperity around the world. But while tyrants act as gatekeepers of money and want to control all on-ramps and off-ramps, it becomes difficult for bitcoin to be accepted for payments or else get exchanged for the local currency.

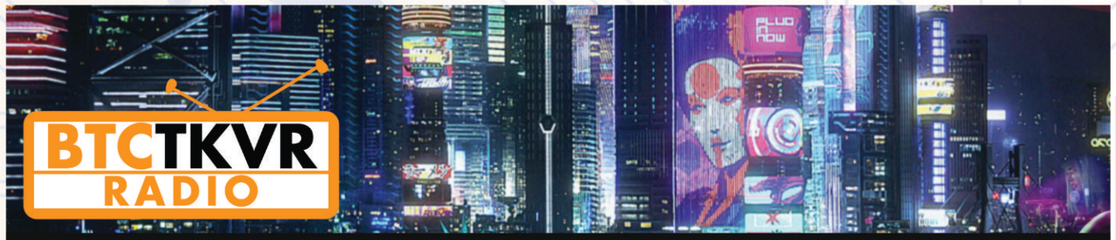
As the popularity of the Bitcoin network grows, we will see a lot of adoption on all fronts. But just because Iran surprisingly decides to declare bitcoin as legal tender, it doesn't mean that the digital currency is under the control of the government from Tehran. If North Korea mines bitcoins to escape sanctions, it doesn't mean that the project follows the domestic and international policies of the Kim dynasty. And if Russia joins the bitcoin standard, this doesn't mean that Satoshi was a spy who worked for the KGB.

Every other country or corporation might as well do the same. The permissionless nature is part of the network's beauty: anyone can use it for whichever purpose suits their needs. But this doesn't mean that there will not be consequences – the public blockchain records all transactions on every sovereign node and there are sophisticated yet undeniable ways to prove that a certain transaction took place from a certain UTXO and to a given address. Once again, what governments make of this data is outside the scope of the Bitcoin network and its purpose to help humanity achieve more freedom.

To answer the initial question once again, nation states are ready to adopt bitcoin as a legal tender as soon as they are sovereign themselves and they possess the military and diplomatic means to withstand external pressure. Once a successful example gets presented to the rest of the world, others are very likely to follow.

On the other hand, fragility at the governmental level has the potential to cause more suffering than virtues when getting exposed to a Bitcoin standard. This is why I maintain my critical position on El Salvador and consider it was the wrong place at the wrong time. One approach is to strengthen your country and become more independent from external pressures. Another one is to speculate a moment of weakness from the hegemonic powers. At this point, the USA, China and Russia are just as powerful and influential as ever – and for all of the internal crises that they face, their military spending doesn't suffer drastic negative adjustments.

I would love to be proven wrong, though. And in this unprecedented story of sovereignty and freedom, you never know what's about to happen next.



The Music on Bitcoin Takeover Radio

When I first started broadcasting the Bitcoin Takeover Radio stream on YouTube and Twitch, I have received many requests to include certain musical pieces to the playlists. It was then that I decided to integrate an hour-long musical intermission to succeed every 3-4 podcast episodes. After all, every learning session should be accompanied by a relaxing artistic expression. And yes, it rhymes.

The current music playlist includes witty, thought-provoking and soothing pieces. Some of them are strongly political in their lyrical content, while others are purely instrumental and intended to get you in certain moods. Also, the songs themselves are a mix of original compositions and Bitcoin-centric covers.

Now let's talk about the audio: to improve and slightly modulate the moody hour-long trip, I've also employed some mastering techniques that can be heard in Ocean Way recordings. Though it's time-consuming, it's always fun to play with audio plug-ins and discover how they add extra harmonics. I really hope that you're going to enjoy the end result – and if you do, please subscribe to the YouTube and Twitch channels, leave likes and comments, and collect the Lightning Network bits from Vaultoro (you'll have to listen to the stream to figure out how).

And if you'd like to make a donation to the project, check out the mainchain QR code and the Lightning address. Periodically, the artists and podcasters will receive royalties from the donations sent to the radio-specific addresses – and even though they are mostly Lightning microtransactions, they are still a demonstration of Bitcoin's ability to scale in layers and provide utility.

Without further ado, here are the songs and artists that you can hear during regular Bitcoin Takeover Radio streams:

1. Czino – Bitdrops
2. Payday
3. Richard La – Pump It Up
4. DJ J Scrilla – Faith in my Money (Money Printer Go BRRR)
5. Phil Gibson – End the Fed
6. Crypto Contagion – Bitcoin Song
7. Renegade Investor – Bankster's Paradise
8. Vlad Costea – Always Learning (About Bitcoin)
9. Zhou Tonged – B.R.E.A.M.
10. Lord Snooty of Bitcoin – BTCTKNVR Podcast
11. CryptoRaptor – The Crypto Rap
12. Pleb Music – New Technology
13. Pleb Music – Jack Mallers Stacking Sats
14. Vlad Costea – Bulls vs Bears
15. Vlad Costea – To The Moon
16. Wasabi Wallet Song
17. Guywithafork – Bullish Man

Mallorca Blockchain Days

Bitcoin & Liberty

„Nothing is true, everything is permitted"
- F. Nietzsche -

Join us at Mallorca Blockchain Days

- Juli 30 to August 02 2021 -
Palma, Mallorca, Spain

GET YOUR TICKET ONLINE

WWW.MALLORCABLOCKCHAINDAYS.COM

#MallorcaBCDays

Mallorcablockchaindays



Why Bitcoin Incentivizes Sustainability & Environmental Care

When you first buy bitcoin and learn the art of HODLing, your time preference takes a hit and your temptation to spend diminishes gradually. And when your patience pays off, you only want to spend your hard money on something that you deem valuable and of high quality. These are the two phases that irreversibly change the lives of bitcoiners and indirectly benefit the environment.

Today, bankers and governments go to great lengths to convince everyone that Bitcoin is an environmental disaster which doesn't produce anything of value. At the same time, they perpetuate an economic environment where money lose value and must be spent quickly… which is turns incentivizes the development of inexpensive, mass-produced, and low-quality goods.

In this article, I would like to argue that Bitcoin helps us return to a set of values which makes us consume less and focus on quality over quantity. And this is not something that you're ever encouraged to do as a bank customer, especially in an age when interest rates are a joke and saving gets actively discouraged. As a matter of fact, since a large number of people will have small amounts of depreciating money to spend, they will look for cheap items that they can buy after every pay check.



Bitcoin's new sustainable clothes

Consumerism is unsustainable and a lot worse for the environment than Bitcoin mining. Let's take a look at clothes: high-quality items are just as expensive as ever and may cost a significant percentage of your monthly income; but if you get something that's made from polyester instead of cotton or wool, you can afford to go to H&M, New Yorker and Zara to fill your wardrobe at a very little cost.

Are these clothes any good? Most of the times they start looking and feeling terrible after the first couple of washes. So you effectively buy future garbage that's designed to only last for one season. If you bought something of higher quality, you could have worn it and washed it for years.

But due to the incentives involved in the fiat economy, you're buying lower quality items frequently so your momentary budget doesn't take a hit. You must still pay rent, buy food, and afford to pay the rest of your bills – so instead of saving across multiple months, the financial system pushes you to either go into debt (which is pretty irrational in most cases) or else buy what you can afford at a given moment.

There is also a discussion to be had about the mass-produced low-quality items and the carbon footprint that their production leaves. Cotton and silk are more expensive, but have a lower impact on the environment. Polyester and elastane dilution reduce the production and retail costs, but significantly increase the initial and long-term environmental damage.

And I'm sure that the example applies to many fields, including food (farmer's market food is more expensive, but more natural and less reliant on plastic packaging), home appliances (a fridge which has more plastic is likely to break sooner and be less efficient), electronics (a cheap Nintendo knock-off will break sooner and receive less software support), automobiles (the $10000 car will do more environmental damage during its lifecycle and afterwards than the more expensive hybrid), and everything else that we buy at affordable prices thanks to convenience.

Bitcoin = long-term preference = sustainability and care for the environment

If you buy and hold bitcoins, you're going to get exposed to an asset whose supply is fixed and predictable. This means that if the demand also increases over time, then your purchasing power only increases against inflationary assets such as fiat currencies. But on the short term, you may also lose some of the purchasing power – so you'll be pushed to plan accordingly and wait for a longer time.

As you exercise patience and frugality, you're going to discover how much of the stuff you used to buy is not essential. And even in the case of essential items, you're going to have greater expectations. Bitcoin turns you into a responsible and conscious consumer even without you realizing it.

Instead of saying "I'm going to get a new phone this year", you will want to wait until something significantly better and potentially life-improving comes out. Instead of changing your clothes every season, you will buy something which has a higher price, but low cost-per-wear. And instead of changing your automobile to get a non-essential feature (like a better sound system or leather seats), you will save for a significant upgrade.

High-quality goods are usually more sustainable and friendlier with the environment. And Bitcoin makes us want them and have the patience until we can get them. In the process, we give up on our consumerist instincts and learn to appreciate quality over quantity. We break the cycle, improve our lives, and also live more sustainably and with greater care for the environment.

It's a little ironic, isn't it? Bitcoin, the internet currency that mainstream media often portrays as wasteful and of dubious use, can actually help us become friendlier with the environment. Thanks to the disinflationary monetary policy, we want to spend more infrequently, wait more, make more informed decisions, and get the best value for our money.

This isn't something that the Federal Reserve or European Central Bank can say about the currencies that they manage. Yet it's very similar with the kind of saving mindset our grandfathers had when they were using gold as their unit of account of choice.

So next time some low-time preference social media commentator suggests that Bitcoin is boiling the oceans, tell them that his lifestyle is a lot worse. And for every ounce of carbon dioxide that Bitcoin mining generates, you help reduce other types of pollution that's even more damaging for the environment.

Also, if you want to find out more about making your Bitcoin transactions environmentally-friendly, then read my article about onboarding the Lightning Network and ignore Elon Musk's borderline malevolent manipulation attempts.



Explaining the Lightning Network So Even A 10 Year-Old Can Understand It

As Bitcoin's second layer, the Lightning Network brings a lot of improvements. Its features instant payments that can scale to a throughput which rivals with Visa's, and most importantly it's very private. It can also do everything that altcoins like Ethereum already do (NFTs, DeFi, tokenization, advanced smart contracts), but in a more elegant and cost-efficient way.

Yet in spite of these advantages, lots of people don't onboard the Lightning Network simply because they don't understand what it is, how it works, and how they should participate. In order to facilitate everyone's understanding, I'm going to try to explain the essential terminology by using practical examples and analogies. And if you're older than 10, you're going to get it.

You Need Your Own Bitcoin & Lightning Node

First of all, in order to run the Lightning Network, you're going to have to run your own node. We live in a decentralized world, doing our best to builds products and services without trusting third parties. Ideally, you should purchase dedicated hardware for your node – and you already have pre-built solutions like:

- RaspiBlitz (about $350, there's European and US distribution);
- MyNodeBTC (about $339, you can buy it from their store);
- Nodl ($529, you can buy it from their store);
- Start9 Labs Embassy (about $289, no hard drive included, you can buy it from their store).

If you want to lower these expenses and undergo a nice DIY weekend project, you can buy yourself a RaspBerry Pi 4B with 4GB of RAM, a 1 TB SSD of your choice (it should be a reliable brand, though), a 32 GB SD card, a heatsink case to keep your RaspBerry Pi cool throughout summers and resource-intensive processes, and some cables. Watch this step by step tutorial by Ben Arc to better understand what you need to do in order to run RaspiBlitz.

If you don't want to buy a dedicated device, there are at least two popular ways of running a Lightning node on your computer. The more advanced one involves using Electrum wallet (full guide can be found here), and the more basic user-friendly option will take you down the Linux path with Umbrel. And if you're up for a bigger challenge, you can also run RaspBerry Pi OS on your Windows or Mac computer or turn to virtual machines.

But the recommendation to run a dedicated device concerns efficiency and security reasons: the RaspBerry Pi is very power-efficient and environmentally-friendly (it will only cost you a couple of dollars a year to keep it running 24/7), and a device which performs only one task has a lower attack surface than something that's used for opening e-mails, installing third party software, and accessing dubious web pages.

So if you can get a RaspBerry Pi to run this node, you should. It's not very affordable at this point, but it will only get better in time as the technology gets older and we get faster and more innovative hardware.

Lightning Nodes Are Islands, Channels Are Roads

One common misconception about the Lightning Network is that running a node is enough to get connected with the rest of the network. Though the node is an essential prerequisite, the next step in your journey involves opening channels with people.

To better understand the concept, think about your node as an island which just emerged in the middle of an ocean. Your goal is to build roads with everyone with whom

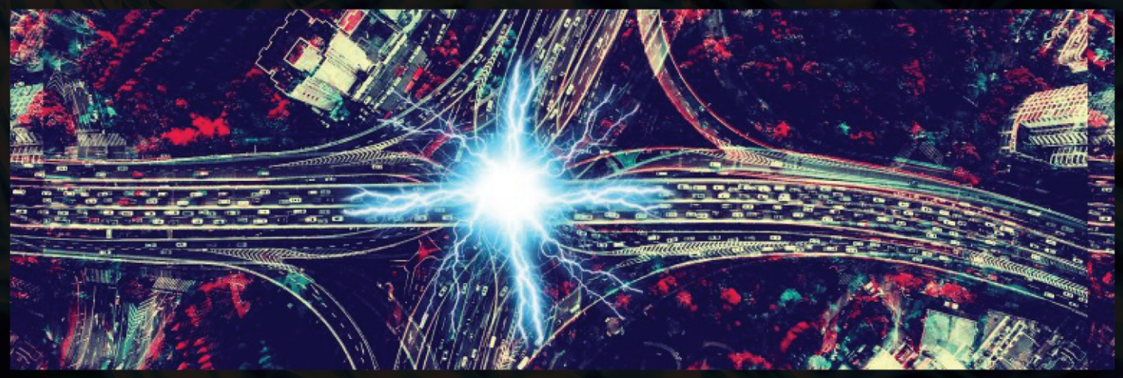


you will be transacting. More roads mean that you're going to have more connections and better shortcuts to reach certain destinations.

The size of your channels is also important, as they enable larger transactions. It's as if your bridge to another island only allows for vehicles of a certain weight to travel – the sturdier the bridge, the more weight it can support during one trip.

These roads go both ways: you can build them with other islands (and this increases your sending capacity) or other islands can build them with you (this increases your receiving capacity). A well-connected island is going to need both.

When sending money to any given island on the map, you're going to take one of the existing roads. If you have a direct road, then everything is straight-forward and you can make a transaction according to the size of your channel. But if the two of you are connected by somebody else's road, then you must pay a routing fee (basically a transit toll).



Ideally, you should open channels with every node on the network to have direct connections – but that's impractical and impossible to accomplish at scale. When millions of bitcoiners will be opening at least one channel each every day, it's going to be hard to have the funds, time, and energy to keep up with the growth of the Lightning Network. But routing is highly efficient and also has some privacy benefits: just like in the case of the Tor network, every relay node adds an extra layer of encryption and anonymity.

If you build roads, you can also collect fees from those who use your infrastructure to get to their destination. Being an intermediary for other transactions can have financial benefits, and most Lightning wallet managers allow you to choose how much you want to collect from those who use your route. Just keep in mind that it's usually the shortest, fastest, and least expensive road that gets chosen. So unless you connect some obscure islands that others ignore, you should think twice before setting a high fee. At scale, these small earnings should subsidize for the electricity costs involved in running your node.

Lightning Network managers such as RTL (Run the Lightning) will allow you to open private channels. This means that only you and the node with which you've built a bridge can see and use this piece of infrastructure. While it has some privacy benefits (nobody else will know about it), it also doesn't route other transactions so it doesn't really support the network and won't earn you routing fees.

The size of you channels (or weight resistance of your roads) is not permanent and you can resort to rebalancing in order to extend or reduce capacities. You're going to pay fees for the operation, but it's healthy to keep an eye on the ongoing operations and re-prioritize according to your observation. More popularity and use can benefit from better capacity.

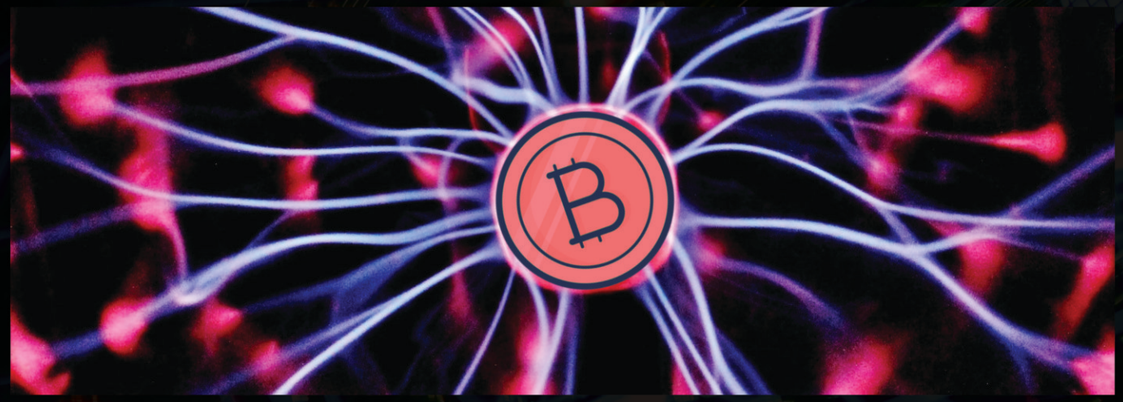
Last but not least, remember that channels are easier to take down than roads. At the click of a button, you can close the channel and take the funds back to the base layer of Bitcoin. Every time you open a channel you pay a transaction fee to BTC miners, and you do the same when you close channels. To avoid overpaying for these operations, check my guide on how to pay lower transaction fees.

The Lightning Clients: LND, c-lightning, eclair & Nayuta

Just like roads can get built from different materials which come with their pros and cons, the Lightning reference client also has four versions which have pros and cons of their own. Historically speaking, LND by Lightning Labs is the most popular implementation and it's also the one that's used by RaspBerry Pi node operating systems (with the exception of Start9 Labs' Embassy, which also comes with c-lightning). Thanks to the large spectrum of applications and network effects, it's the most friendly for inexperienced users.

Blockstream's c-lightning is more refined and better for developers, and it's built in the C programming language (hence the name). However, it has fewer applications





and is mostly used by exchanges and services which need more reliability. It's also designed to enable atomic swaps between assets on Blockstream's Liquid sidechain and BTC Lightning. This can be useful if you want to perform a peg-out without using the KYC services of a Liquid federation exchange. If LND is like Windows, then c-lightning is a robust Linux distribution that isn't very friendly with untechnical users.

ACINQ's eclair is also a popular option, as it's written in Scala and supports both Java and Java Virtual Machine plug-ins. Since many Android OS applications are written in Java, this implementation is very useful for mobile wallets. Phoenix and Eclair are two of the most popular mobile wallets, and you should definitely give them a try.

Last but not least, we have Nayuta – a Japanese company which started working on a Lightning client so lightweight that even a RaspBerry Pi Zero can operate it. More recently, they have released an alpha version of Nayuta Core and they also focus on the development of mobile wallets.

The Easiest Way to Ride the Lightning

Ideally, you should run your own node and do everything by the book. But if you only want to dip your toes into what Lightning is and how it works, you can try a mobile wallet like Blue Wallet, Breez, or Eclair.

Blue Wallet takes the cake for having the best user experience of all bitcoin wallets out there. It's also very customizable, allowing you to both connect to your own node or else rely on the company's infrastructure. And if you want to receive a Lightning payment, you install the app on your phone, generate an invoice for the amount that you want to receive, and then gasp at the speed of the transaction. Blue also has a desktop version, thus being one of the most convenient ways to start using the Lightning Network.

Breez Wallet is special because it opens a channel for you. After you deposit funds and wait for at least 3 network confirmations, you're good to go. The fact that this simple user experience happens in a non-custodial way which boosts your sovereignty is admirable. It can't compare with your full node experience, but it facilitates the advantages of Lightning with some elegant tradeoffs.

And then there's ACINQ's Eclair Mobile, which runs a light version of a Lightning node directly on your mobile phone. You can also connect to your full node by accessing the advanced settings, but even by default it's excellent for financial sovereignty. It would have been great if it was also available on iOS, but this might be due to Apple's limitations. If you have a large enough SD card, you can even run the full validating node on your phone.

If you're looking for a way to receive your first funds on the Lightning Network in an effortless way, then sign up to social media tipping and payment services such as Tippin.me and Bottle Pay. And if you have some Lightning Network funds that you need to convert to bits on the Bitcoin mainchain and you have no channels to close because you're full-custodial, then try a service such as ZigZag.



In retrospect, it was inevitable: the fiat billionaires who added bitcoin to their companies' balance sheets are not our friends and definitely not honest Bitcoin advocates. And while the likes of Elon Musk and Michael Saylor announce the creation of a Bitcoin Mining Council to effectively attack censorship resistance and attack the permissionless nature of securing the network, Kevin O'Leary essentially blackmails us into compliance:

"Right now, the institutions are interested in getting exposed to the volatility of bitcoin, but they've gotta resolve this problem. And I think there's some interesting research going on now and deep investments, and I'm part of it: to try and find a way to tag a bitcoin to prove that it has a wrapper around it to prove that it came from a sustainable miner. I know this sounds out there, but it's being worked on right now because that's what institutions want.

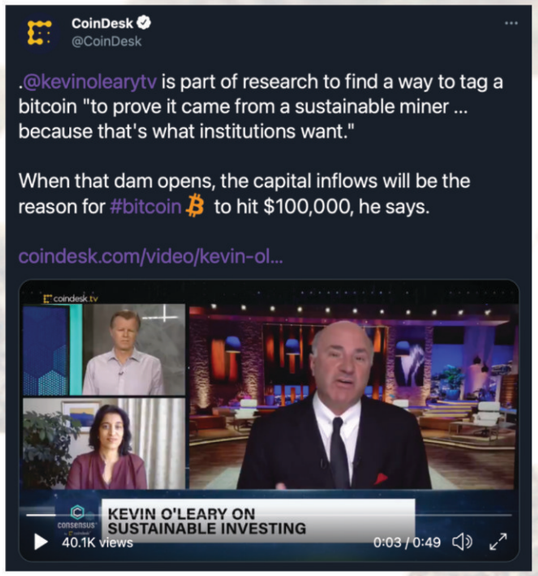
And when that dam gets released, the amount of capital that will come into bitcoin… it will be the reason why it goes to $100.000, $200.000, and all the dreaming that's been going around price appreciation. That's not going to happen until institutions start to buy it. So everyone's gotta wake up and realize that there's demand, but it's gotta be done around ESG (Environmental, Social, and Corporate Governance) concerns" (Source: Coindesk's interview)

Bitcoin Mining Council? $100k Conditioned by ESG Compliance? How did we get here?

It all seems to be happening too fast. In August 2020, Michael Saylor became a bona fide Bitcoin advocate after buying a huge position and spending the coming months in a perpetually bullish state that pleased the "cyber hornets" and their "hive mind". By May 19th 2021, Saylor announced that he and his "entities" hold about 110.000 bitcoins.

Elon Musk had a similar trajectory: he started out as a Bitcoin critic, and then gradually dipped his toes into the space in 2020 in a more playful way (he became the self-proclaimed Dogecoin CEO and then started making ridiculous statements about the potential of an otherwise highly-inflationary meme coin). After adding BTC to Tesla's balance sheet and reporting a profitable 2021 Q1 specifically thanks to this investment, Elon Musk also made a bold move when he announced that his company would sell electric cars for BTC.

But the honeymoon phase lasted for roughly 3 months: on May 12th 2021, Musk tweeted that Tesla would stop accepting BTC payments due to environmental concerns.



There are two catches involved, though: Tesla never sold any bitcoins and announced that it would once again consider accepting BTC for payments "as soon as mining transitions to more sustainable energy".

Following this tweet, the price tanked. And within a few days, the entire space was faced with more of the perpetual FUD about China banning Bitcoin mining. The declining prices and the newly-generated panic provided the perfect setting for an organization like the Bitcoin Mining Council to get established.

The tradeoff in simple: a bunch of billionaires promise to bring "institutional adoption", but in exchange they want to gain control over mining so they can vet the participants based on their arbitrary criteria for sustainable energy.

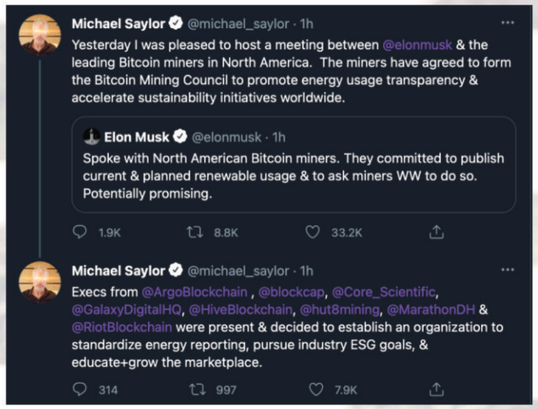
In theory, it's a win all across the board: the HODLers get the promised $100k price, the companies profit from selling carbon credits to miners, mining gets theoretically greener, and governments and trans-national NGOs get more control over Bitcoin. Everybody wins in terms of fiat money and power – but the Bitcoin project and its great ambitions get crushed by the greed and short-sightedness of a handful of self-proclaimed leaders and their ardent "number go up" fans.

Also, what do Saylor, Musk, and O'Leary have in common? They all used to be skeptics and critics of Bitcoin – but now they pose as true believers with skin in the game. They claim that their goal is to bring more institutional adoption and pump the price to the levels that everybody's dreaming of… and all they ask in return is a little bit of control which irreversibly destroys the fungibility, censorship resistance, and security model of the bitcoin cryptocurrency and of the Bitcoin network.

Why Is ESG Compliance Bad For Bitcoin?

Now hold up a minute, shouldn't we all cheer for the news that Bitcoin mining is getting greener? Aren't we supposed to be celebrating that the environmental impact diminishes and we all get to enjoy a truly





decentralized currency with a lower carbon footprint which pleases governments and institutions? Shouldn't we be happy that corporate heads are trying to bring the kind of adoption which gets us to $100k and beyond?

Make no mistake: the Bitcoin Mining Council and its ESG compliance have very little to do with environmentalism and concern top-down control over a vital component of Bitcoin's security model. Basically, a bunch of rent-seeking fiat billionaires are trying to establish themselves as the overlords of mining.

They realized that China will gradually scale down the operations, they realized that the opportunity can be geopolitically seized by the USA, and instead of allowing the free market to converge towards the least expensive forms of energy (which often times turn out to be renewables due to the low production costs) they seek to gain control.

Collectively, Michael Saylor and Elon Musk have 56.8 million followers on Twitter. Their net worths in US dollars also exceed those of bitcoin whales. And their influence in relation to the US Government is second to none: one received government subsidies and was allowed to join the narrow circle of aerospace corporations which undergo space exploration, while the other has a long history of working with governmental agencies.

Right now, Saylor and Musk are trying to become the Al Gores of mining environmentalism by selling carbon credits. Interestingly, Elon Musk tweeted about this shortly after announcing that Tesla would stop accepting BTC payments, and only a couple of weeks prior to joining the Bitcoin Mining Council conversations.

It's very likely that this is all part of a greater scheme which aims to make the US Government control more Bitcoin mining. But the fact that China (a communist country that we enjoy bashing for its infringement of human rights) has more respect for the Bitcoin miners and allows them to function without imposing a certain agenda for control says a lot. Under the guise of environmental friendliness, the United States are currently being a lot more authoritarian than the country which filters a large chunk of internet pages, bans political speech against the establishment, and coordinates a genocide against the Uyghur minority.

Also, it should be noted that Bitcoin mining is still a small endeavour in the United States of America. The higher electric energy prices, the more expensive labor costs, and the various regulations make it less profitable than in other parts of the world. The beauty of Bitcoin mining is that it leverages the best part of geopolitics: international arbitrage. If one country raises the costs and makes political decisions against it, then another one will welcome miners for the sake of acquiring a competitive advantage.

Yet the United States of America is an important battleground for Bitcoin mining, as the policies are likely to inspire NATO members and other friendly nations. And if we allow a handful of fiat billionaires to play their game without opposition, then it's likely that they will seek to gradually increase their power and influence beyond the borders of the USA.





Bitcoin Mining Should Be Permissionless, Decentralized, Efficient, and Honest

Bitcoin mining was designed to be permissionless and decentralized. This means that currently, anyone around the world can use their computing power to attempt to solve the difficult math problem – and in the process provide security for the network. Though people like Slush have created collaborative approaches (also referred to as "pools"), you can still have cases when a miner from Argentina joins a Chinese pools to maximize his chances and split the rewards with the other partners from the same team.

In and of itself, Bitcoin mining is selfish and driven by incentives: in order to make the highest profits, everyone searches for the most efficient, reliable, and affordable forms of energy. It's why most miners in China have set up their operations around water wheels in small villages, and it's also the reason why the demand for sustainable energy increases worldwide.

Also, the design of the Nakamoto consensus always makes it more profitable to mine honestly than to try to attack – if the users' validating nodes reject a block, then the miners take a significant financial loss. So if the same amount of energy gets used to mine while playing by the rules, then the rewards get bigger.

However, the nodes can't coerce miners into adding all transactions into blocks. They can only sanction dishonest work. The miners possess the power to blacklist transactions that have certain origins (for instance, the US Treasury Department has a list of 20 Bitcoin addresses). In the presence of decentralization and global mining, this is an irrational economic behavior which only makes it more costly and energy-intensive for miners to operate.



Let's say that we have two transactions: one uses "dirty" bitcoins that get sent from a blacklisted address but pays a high transaction fee, while the other is sent from Coinbase, is "clean" and it pays the smallest possible fee. A compliant miner will refuse to add the former into a block and include the latter – at the cost of refusing some precious transaction fees.

As the block rewards get halved every year, by 2028 we will find ourselves in the middle of a situation where the mining fees always offer a greater reward than the block reward itself. And this is when any type of censorship will become economically irrational.

Yet miners can still afford to play the censorship game for a few years. And maybe that nation states and trans-national corporations believe that, if they're allowed to gain more control over mining and over the narrative, they will successfully create a hard fork which increases the mining rewards to favor their thirst for censorship.

Giving them the power to decide who can mine (and who can't and must therefore pay carbon credit taxes) sets a dangerous precedent which takes away Bitcoin's censorship resistance. Sure, there will always be jurisdictions which allow free mining to take place. But standing by and watching how oligopolies and cartels get established is never a good idea.

We must stand up for the principles of Bitcoin while we still have the chance.

Principles vs Number Go Up

It's very easy for them to desensitize us and effectively make us stop caring about the fundamentals while they pump the price with the BRRRRR money. They have infinitely inflationary fiat and there are only 21 million bitcoins that will ever exist.

Instead of selling our coins to them (as legal entities, the corporations can only buy from compliant exchanges such as Coinbase), we should create parallel economies on Bisq, HodlHodl and peer to peer exchanges. If we do more meetups to do swaps in which cash or gold get traded for BTC, then it would be beneficial for the ecosystem.

Also, we should exercise our right to mine at home while we still can. It might be costly and inconvenient, but it helps decentralize the network and it takes away from the power of farms and cartels. Principled bitcoiners should also avoid joining pools such as Mara (Marathon Digital Holdings) and join forces with pools which have a long history of acting in good faith (such as Slush pool).

And whenever we get the chance, we need to give them hell and make them feel unwelcome. Bitcoin was not created to please them and their corporate plans. It was never meant to be compliant – instead, it leverages geopolitics to exist under the principles of free market capitalism.



It's time to stop idolizing Michael Saylor, Elon Musk, and other billionaires who express positive views and effectively pump our bags. We already know the nature of their game and we understand the threat model. Let's not make it worse by giving them extended control (either social or protocol-level).

Bitcoin is for people who need to escape central banking and inflation. It's for refugees and freedom fighters who need to survive in hostile political environments. It's the tool of sovereign individuals who constantly seek freedom and empowerment. And it's also the financial instrument that can effectively bank the billions of unbanked people via second layers like Lightning.

We need to teach and preach these principles, and then give no quarter to the centralizing rent-seekers. They either accept Bitcoin for what it is, or else build their own (either a fork or an entirely new protocol). Good luck getting support and benefiting from the same network effects, though.

Secure your bitcoins and boost privacy with the original hardware wallet.

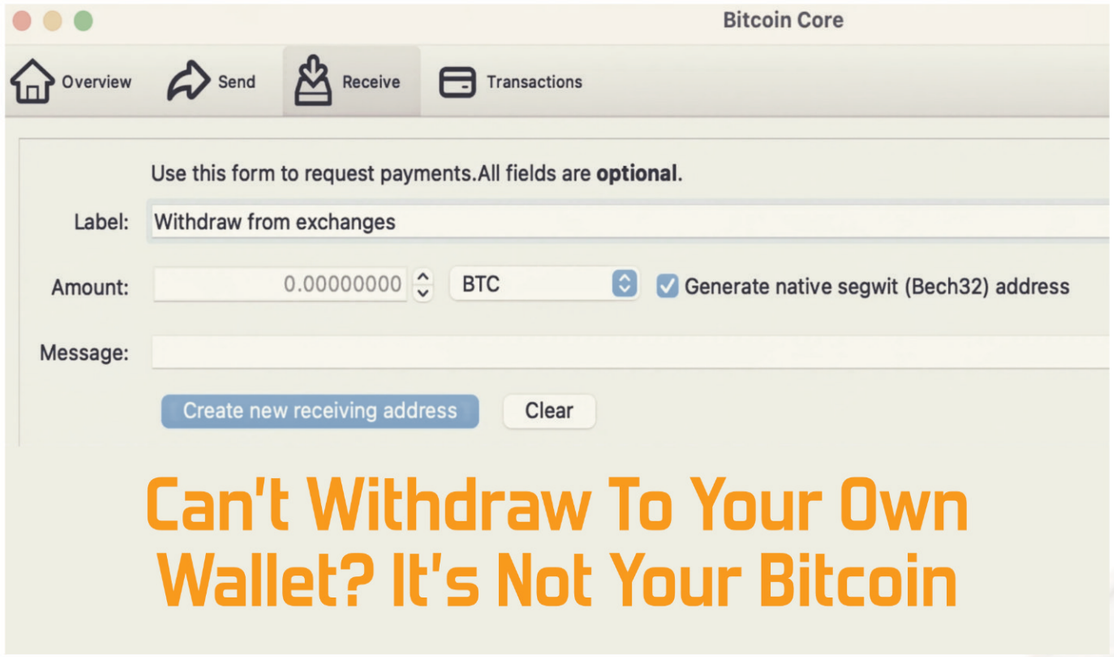


Get the Trezor Suite desktop app today at suite.trezor.io.

TREZOR

Brought to you by SATOSHILABS

www.trezor.io
www.satoshilabs.com



Can't Withdraw To Your Own Wallet? It's Not Your Bitcoin

Nowadays, bitcoin has turned into a fashionable asset that traditional financial institutions make available to their clients. As of May 5th 2021, block height 682078, we have companies like Robinhood, PayPal, Revolut, and even regular banks which allow their customers to purchase bitcoin amounts. And according to recent news, "hundreds of US banks" are about to add bitcoin custody services.

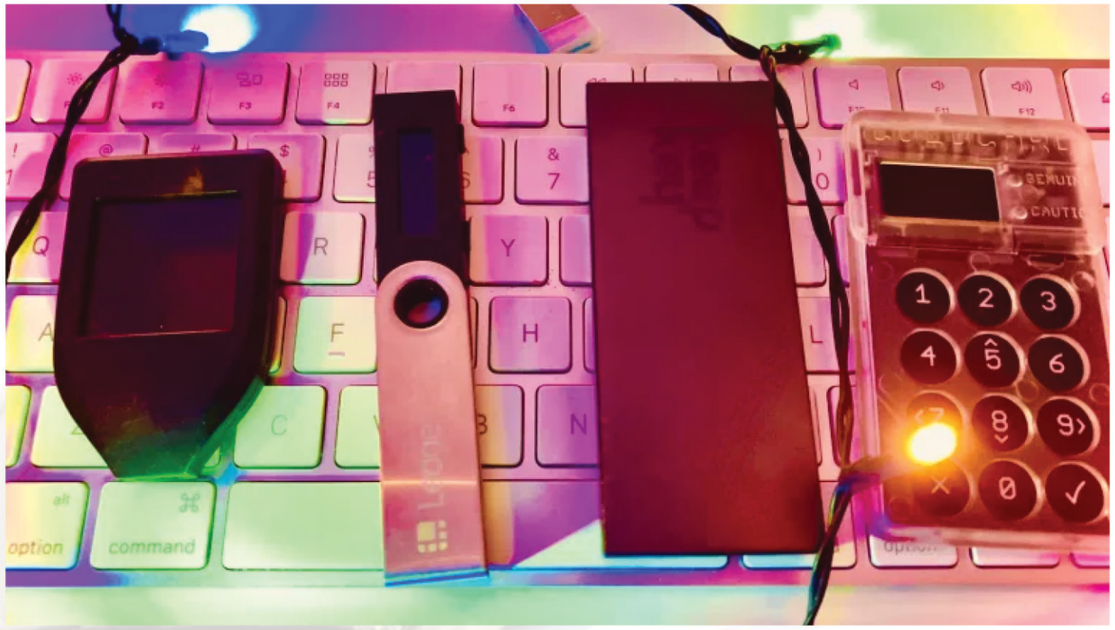
Lots of people might argue that this is great for BTC adoption, since financial services that people have been using for years are now enabling the purchase and sale of sound money. But the argument which I'm going to present in this article is that, beyond the "not your keys, not your bitcoin" mantra, there is no way to prove that the financial institution actually owns the bitcoins that you buy.

In the case of fiat, you can always withdraw the money from your account. You go to an ATM, you insert your card and type your PIN, and then select the amount that you want to take out. But even in this scenario in which you can withdraw your money, it doesn't mean that everyone else can. All of today's banks use fractional reserves – so at any given time, there is only enough money available to support the bank run of a certain number of customers. If you deposit a lot of money, it's likely that the withdrawal will get slow and burdensome.

But regardless of your financial situation, you are legally eligible to take your money out and use it for whichever purpose you deem worthy.

Theoretically, Bitcoin should fix all of these issues by offering a more transparent system. You know that the money is yours because you verify it with your full node. And when you want to spend your UTXOs, you don't need anyone's permission to proceed. You are your own bank and this is meant to be an integral part of your financial soverignty.

Unfortunately, it gets nasty when third parties from traditional finance get involved. Not only that they are accustomed to fractional reserve banking, but there is no authority to impose that they hold bitcoin reserves for all the units they are selling. We can end up with the artificial inflation paradox that I previously described in my article about ETFs: people buy and sell bitcoins that can't be verified on the public blockchain, and for which there is no proof that they even exists. What prevents these companies from effectively inflating the bitcoin supply though a legal and institutional sale of unbacked assets?



It's unlikely that there will ever be an audit of bitcoin reserves and verification of users' accounts. And even if there is, these companies can operate without actually buying a corresponding about of BTC whenever a customer trades fiat currency for bitcoin on their platform.

So if you own bitcoins on PayPal, Revolut, Robinhood, or any other financial service that doesn't let you withdraw, for the sake of your financial sovereignty, you should sell the coins for fiat and then transfer the money to an exchange that lets you withdraw the verifiably-real BTC. As long as you pay the same price as everyone else, you don't want to get the shorter end of the stick and effectively get deemed a second class user.

Which exchange should you use? Well, I'd personally recommend you P2P ones like Bisq and HodlHodl. But if you want to take the centralized route, Kraken and Bitfinex are some of the oldest and most bitcoin-friendly choices on the market (I'm not getting paid to promote either and have no ref links).

After you've made the purchase of verifiably real and scarce BTC, take a look at the network fees, determine your time preference, and withdraw the coins to your own wallet. For extra privacy, you can CoinJoin with Wasabi and break the link between the exchange and your new wallet.

And if you're looking for better ways to secure your coins, get an open source hardware wallet like the Trezor, the BitBox02, or the Coldcard.

Just stop gambling money on companies that won't even prove that your bitcoins were mined and exist in one of their wallets. It's anti-BTC and against the principles of individual financial sovereignty.





Why Bitcoin Free Open Source Software Matters

Why are bitcoiners so obsessed with free open source software? And what's wrong with open source licenses which restrict commercial use? After all, the developers should find a way to monetize their work and the entire tech sector is filled with patents which secure intellectual property.

In other words, why does Bitcoin software have to be free and open source, in a way which allows anyone to use it for any purposes (including commercial use)?

Well, this is about the nature of verification and incentives. Let's say that I write the best wallet code ever. I publish the source code, but expect royalty payments from other companies and individuals that want to use it. This can help me signal to VCs that I have a product which can be sold, so that I can also raise some funding and grow my business.

Sounds like a solid plan, right? Well, it would work quite well if this wasn't about Bitcoin. You see, the Bitcoin standards for code are very high in terms of honesty and transparency. Something that manages the ownership and transmission of provably-scarce and in-demand digital money should not be taken as lightly as "just another app".

Naturally, people are always skeptical when they deal with BTC software. This is why the "Don't trust, verify" slogan emerged and it's also the reason why developers get paid to check the code before it starts managing a significant amount of bitcoins.

But wait, isn't it enough that developers publicly publish the code to their work? Why does the software also have to be free? Well, there's a catch which concerns incentives: if people can't use your code in a commercial way, then fewer people will care enough to scrutinize everything. Ideally, open source code should get vetted by multiple developers, across an extended period of time.

The most tested something is, the sturdier and safer it becomes – so this is why modifying and repurposing code even for commercial purposes matters. Next up, I'm going to present to you two case studies from the Bitcoin space.

Case Study: Trezor

Let's take the example of Trezor, the world's first Bitcoin hardware wallet. The two masterminds behind the project, Slush and Stick, were stubbornly in favor of using general-purpose parts that run on free open-source software. Even if it meant that anyone could fork their work to create a competing product like the KeepKey, the Coldcard, and the BitBox02.

By offering this free open source license, they've increased the incentives to verify and harden the code. If KeepKey sells a product which uses the Trezor codebase, then it's likely that the company will find some issues that they will report back to Trezor. If the situation is worse and a customer has a problem, then the seller will have to figure out a solution. And this solution will also get back to the creators of the original product, so they can also fix it.

Therefore, we can say that the existence of the KeepKey, the Coldcard, and the BitBox02 has only improved the security of Trezor. And even in cases when they found no major issues, they proved that the code is safe.

Open source is a collaborative effort which takes the original work and expends it to serve different purposes and fulfil the needs of more users and developers. And if the software enables something as delicate as bitcoin ownership and management, then it must be uncompromising in its transparency and incentives.

Unless enough people verify the code and test it, you probably shouldn't touch it. And if a product makes use of commercial licenses, then it's actively discouraging the most critical of reviewers from contributing – the competitors who want to build by using your work as a starting point.

Case Study: Bitcoin Full Nodes

My main inspiration for writing this article is rooted in the debate surrounding full node dashboard software. Essentially, RaspiBlitz is the only uncompromising actor in this field – but their user interface is not nearly as friendly as the one used by myNodeBTC (which only recently switched to a free open source license) and Umbrel (which uses a commercial open source license to prevent unauthorized forks).

It's only normal for bitcoiners to want their software to benefit from the greatest amount of scrutiny. At the same time, the developers shouldn't have to work for free.

MyNodeBTC is objectively great and might be responsible for popularizing the user friendly-dashboard which is free to



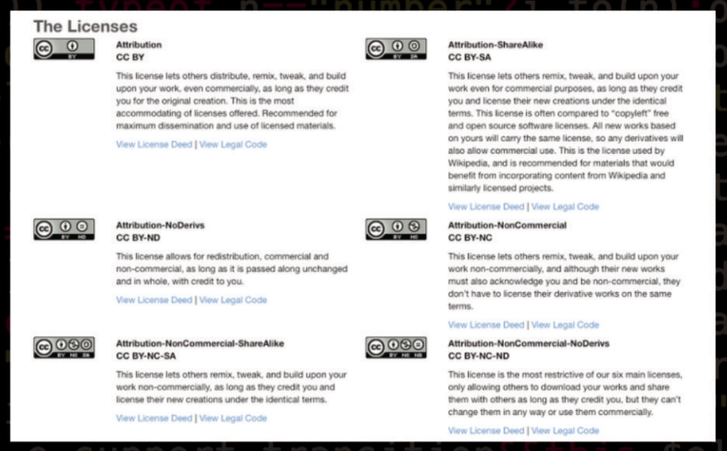
download, but costs extra for the integration of extra services such as BTCPay Server. The company is also selling "node in a box" devices to those who don't want to build their own node from a Raspberry Pi. This may be a profitable business model, but does it not guarantee that the software has been scrutinized by independent developers unless other individuals and companies can also use it for commercial purposes.

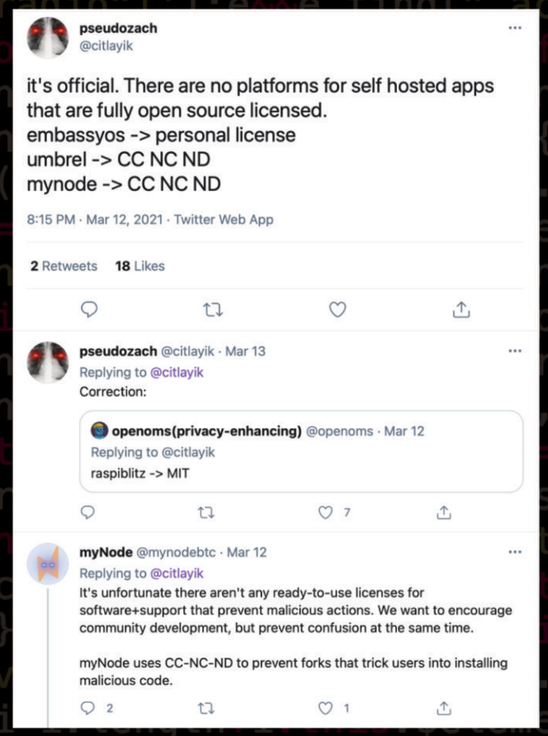
Likewise, Umbrel is today's most intuitive dashboard for running a full Bitcoin node. It looks sleek, nice, and elegant. It has all the features. But its open source license makes it a commercial product that cannot be used by competitors. It's all been outlined in their legal letter and, while the development team acknowledges that the situation is not optimal, their plan is to monetize the software.

Another rising actor which offers a nice dashboard under a restrictive open source license is Start9 Labs. Their Embassy OS looks promising, will add lots of features, but will definitely need to switch to an MIT license if they want all the benefits of free independent scrutiny.

Again, this would have been perfectly fine anywhere outside of the Bitcoin space. It's fine for Linux distributions like Red Hat and SUSE, it's optimal for video game engines like Epic's Unreal, but it won't work for Bitcoin software.

The Creative Commons Non Commercial Non Derivatives (CC-NC-ND) license type works on the "you can look, but you cannot touch" principle. It's great for artists, but it discourages crucial security





experimentation. By being allowed to fork the code, play with it, and even sell it, you get a lot of useful feedback and enable others to discover issues that you wouldn't have thought about.

While you can pay for audits and reviews, they only go as far as publishing a report which relies on the expertise and reputation of a team of experts. There's still trust involved, even if you're dealing with renown professionals.

On the other hand, making your software free and open source (FOSS) will actively encourage anyone on the internet to use your code – so every fork is a dedicated audit which extends the purpose, functionality, and security of the original design. And if major breakthroughs are made with your code, then nobody stops you from using them. It's likely that you, as the original developer, will retain the first mover advantage and network effects (as it happened in the case of Trezor).

How Is Free Open Source Software Supposed to Make Money?

If you've read the article up to this point, then you will probably call me an entitled communist who expects others to work according to his expectations. And you're free to call me any names you want, but my goal here is to seek the best tool for individual sovereignty with Bitcoin. If the best of these tools are objectively free and open source, then I'm going to use these conditions for analyses.

And I'm very much aware that I wrote a Bitcoin full node review last year and it treated the free open source criterion pretty shallowly. But even though I feel ashamed of some of my previous work, I am happy that I'm constantly learning and getting better at what I do.

Now let's talk about the two ways in which free open source software can make money. The most obvious one is donations: people who use something free that they find useful will send some money in exchange. Now, I know that this idea is very ideology-driven and in practice most users will not make a single donation if they can get something for free.

But there are lots of individuals who possess disposable income – and when they come across free open source software which does the job of a paid product, they will send donations. Sometimes companies that create free open source software also create foundations to allow donors to deduct the money they send from their tax amounts.

However, these criteria don't really apply to Bitcoin software – as the programs don't replace paid alternatives and we don't really have foundations. This doesn't mean that people should stop sending donations, though – they're the best way of showing someone that you appreciate the work.

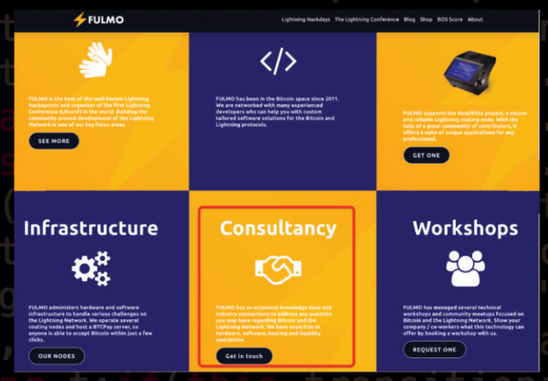
This leads us to the second way of making money from free open source software: consultancy work. And it goes like this: if you built something useful and free, it still doesn't mean that most people will understand how it works or will afford to pay computer scientists to reverse engineer it. So they'd rather pay the makers to make custom installations, provide tech support, and add new essential features.

RaspiBlitz and MyNodeBTC are already offering this kind of consultancy – the former in a custom way, and the latter through a $99 premium service. But the only ones doing it right (at least in the Bitcoin spirit sense) are Fulmo (RaspiBlitz).

As someone who provides free Bitcoin education and relies on donations and sometimes sponsorships, I can really understand why it's important to find good monetization means. I'm all for funding developers who work on Bitcoin projects and I'm often times upset that Bitcoin development is underfunded due to greater shitcoin interests (this may become the subject for another article).

But my advocacy is for finding ways to monetize through means that are compatible with the demands of Bitcoin. This is very hard in a HODL culture where people sending donations may feel like Laszlo Hanyecz when he bought his two pizzas.

But we really need to establish a healthier donation culture and also get consultancy when we need it (though this is more of a feature for companies that make a lot of money and don't want to take risks). Anyway, my point is that we like to talk a lot about building a parallel economy with Bitcoin, but the incentives rarely make us take steps towards it. Free open source software is important and we should only impose the highest security standards on those who produce it – while also supporting their work.





How & Why Michael Saylor & MicroStrategy Can Become Bitcoin Villains

MicroStrategy has purchased an additional X bitcoins for Y amount of cash at an average price of Z per #bitcoin. As of 2/30/2021, we #hodl a lot of irreversibly KYC'd bitcoins acquired for BRRRR billion dollars at an average price of said BRRRR divided by the number of irreversibly KYC'd bitcoins per bitcoin. $MSTR

Sounds familiar? This is the tune that mesmerized the Bitcoin community and the price of bitcoin alike. And since August 2020, a new verse gets added to the already-familiar chorus almost every month.

This tune, along with a flawless apprehension of Bitcoin memes and culture, has made fellow bitcoiners write hymns and praises about Michael Saylor's mightiness, leadership, and strong hands. Now he is everyone's favorite Giga Chad, he gets quoted for telling Laura Shin that the price is going up forever, and almost everyone seems to be happy about his new leadership position among Bitcoin-investing CEOs.

Some say that Michael Saylor "gets it", others already assume that he wants to be remembered as the greatest corporate CEO of all time and the man who accelerated hyperbitcoinization. There are even hive mind individuals (see the paradox there?) and cyber hornets who cheerfully propagate his message across all channels, while expressing hope that MicroStrategy would buy more bitcoins to pump the price beyond a certain resistance point.

People who otherwise would have never been interested in the work that MicroStrategy does are now buying stocks. And as of April 7th 2021, the price is five times higher than it was before Michael Saylor has announced the purchase of the first bitcoins. It looks like a win-win all across the board and it's likely that more companies are noticing the rejuvenation in stock interest.

Yet I can't help but feel skeptical. And I'm not only worried about the fungibility of bitcoin as a currency, but I also feel concerned about the damage that Michael Saylor can cause if he ever becomes evil (either through his own will or by virtue of a psy-op).

After all, we're not dealing with a regular business man: Michael Saylor is the co-founder and CEO of MicroStrategy. And MicroStrategy is an intelligence company which operates within the legal boundaries



of the United States of America, regularly works with the US Federal Government, and makes all of its money helping contractors gather data and process it. In a situation like this, assuming good faith and work in the best interests of Bitcoin is naive at best.

But now let's break down the two entities and identify how and why they can become Bitcoin villains. I'm not only doing it for the sake of my own critical spirit, but to also help others understand the magnitude of this potential threat. I haven't worked in intelligence, but in Hollywood films intel guys usually quote Sun Tzu's hundred battles probability game before proceeding to tap their keyboards frantically. So please allow me to do the same.

How & Why MicroStrategy Can Become A Bitcoin Villain

Just so you don't think that this whole piece is the mark of a vendetta against Michael Saylor the man, I'm going to talk about MicroStrategy first. After all, it's the corporation that owns the nearly 100.000 BTC (I lost count, but I'm pretty sure they're getting close) and the CEO can get replaced by the board of directors. You know, when the Pepsi guy shows up and steadily replaces the co-founder by virtue of his Cola Wars tactics. Oh wait, that wasn't Micro… never mind.

I'm not going to say that MicroStrategy can sell the bitcoins to dump the price, because that's the lowest hanging fruit and I'm usually dissatisfied with cheap attacks. It's not the fact that MicroStrategy can sell the bitcoins that worries me, but how it's going to HODL/sell them.

You see, bitcoin as a currency is not very fungible. Not only that you can use blockchain analysis to track the origins of BTC amounts, but you can also trace the origins of coins to the block when they were first minted. Yes, it's true that CoinJoins can help add an extra layer of bamboozling and plausible deniability – and I'm a big fan of Wasabi Wallet's research in privacy advocacy and mixing research. And yes, the coins get divided in subunits shortly after being sent as coinbase rewards, so tracing every UTXO to its origins can be a lot of work.

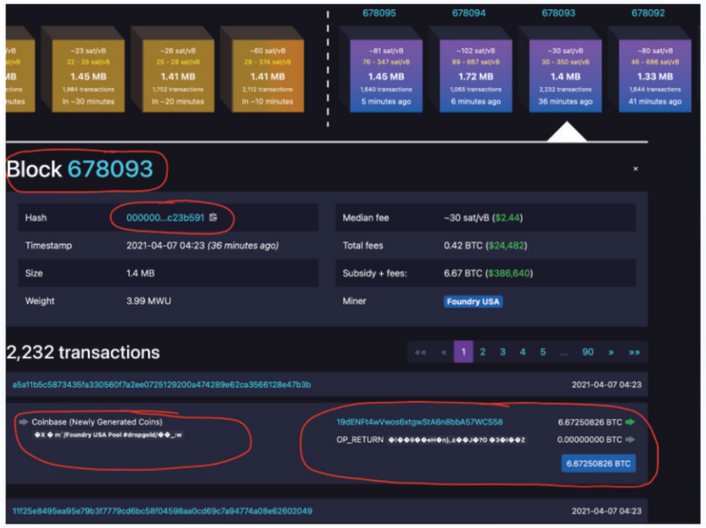
But let's get back on track: every bitcoin that MicroStrategy acquires in its portfolio gets added to their balance sheet. It gets acquired via contracts and it can only be sold through legal means which involve contracts. As a publicly-traded company which operates under the laws of the United States of America, MicroStrategy must be absolutely transparent about the bitcoins that it owns. And it's not like they can engage in blockchain-obfuscation and other privacy developments that may come along the way.

So the bitcoins that MicroStrategy (and every publicly-traded company, for that matter) owns are forever tainted. The more they buy, the less fungible bitcoin becomes as a currency. As the number of "wild" and "untainted" BTC lowers, it's going to become a lot easier to track and identify the



transactions that happen on what the US Federal Reserve calls "hosted wallets". This way, bitcoin will truly become digital gold – in the sense that gold bars will get registered with a stamp which, unlike its metallic counterpart, cannot be physically-melted, obfuscated, or concealed.

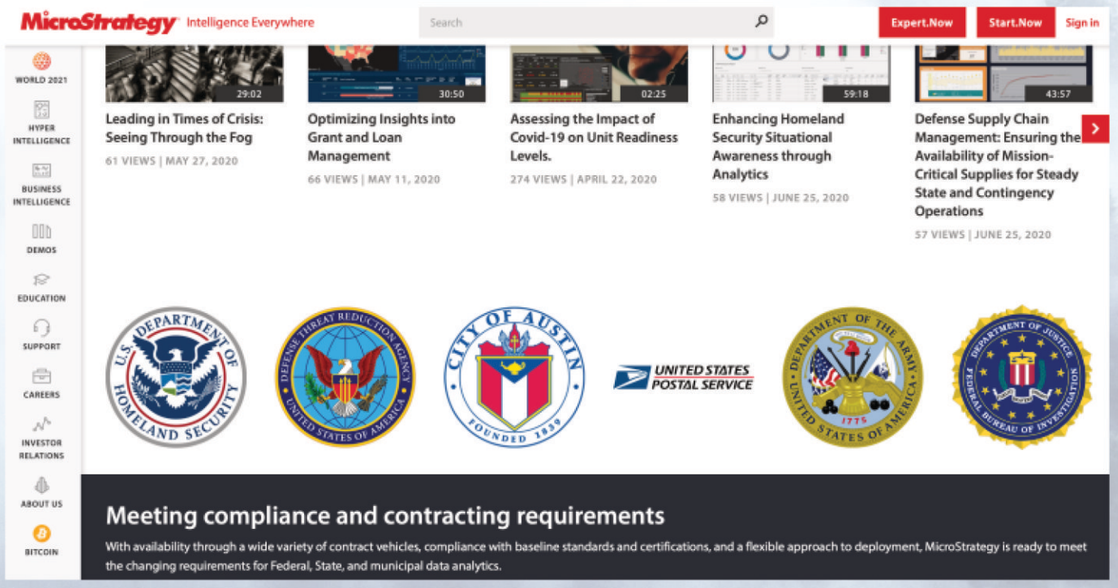
MicroStrategy doesn't have to sell to crash the price of bitcoin to become a villain. All the company has to do is keep on doing what it already does and irreversibly destroy the fungibility of BTC. It's not like these coins will ever get in the hands of plebs, they will always get transacted via contracts and institutional settlements which clearly identify the public blockchain UTXOs.



If more publicly-traded companies follow the example of MicroStrategy and add lots of bitcoins to their portfolio, then they're essentially fulfilling the regulatory desires of the US Government. I've previously written about it in this article and I'm going to say it for as long as I'm still allowed to express my opinions without third party constraints.

MicroStrategy can also work directly with the Federal Government and provide blockchain analysis tools. They won't be as detailed as the ones that exchanges like Coinbase provide (they hired the former Hacking Team to track all the incoming and outgoing transactions, for Satoshi's sake!), but their analysis tools might come in handy for some specific tasks. It's not like MicroStrategy is a stranger to contracted work for the Department of State and the Department of the Army.

TLDR: MicroStrategy is helping the US Government regulate bitcoin as a currency. And it's not that I have something against the US Government (I'm an avid reader of James Madison's and Thomas Jefferson's works, I love capitalism and free markets, I come from a country which used to be communist until 1989 and I dislike the rise of Russia and China). But I want my currency of choice to be as fungible as cash (I'm also an avid reader of George Orwell's books).



But before that, here's a word from our sponsor: FUNGIBILITY SAYS DON'T SELL YOUR BITCOINS TO BIG EXCHANGES THAT WILL AFTERWARDS SELL TO MICROSTRATEGY. DON'T KEEP THEM ON LENDING SERVICES EITHER, AS YOU'RE HELPING SHORT SELLERS SUPRESS THE PRICE FOR A MEASLY RETURN. BE SOVEREIGN FFS.

How & Why Michael Saylor Can Become A Bitcoin Villain

For a moment, let's forget that we're talking about Michael Saylor and bitcoin. Let's say that you're in high school, sophomore year. You've spent many years training to join the basketball team and become the shooting guard which leads it to state championship. Then a new kid arrives to your school, pays for gym renovations, buys the entire team some new cool jerseys, and never misses a chance to show off how cool he is.

He effectively bought his seat at the table and he's going to be in the team – and it's not like he's terrible or isn't talented enough to have earned it in time. Heck, this guy has even learned your friends' jargon and uses the exact same memes to express teenage angst. It's very hard to hate him, as he's objectively helped everyone, he brings more visibility to the highlights of your high school basketball team, and makes the state championship goal seem a lot more tangible.

This is a metaphor about how I feel about Michael Saylor – while I appreciate his efforts, I'm not convinced about his genuine intentions. He's gained a huge social media following over the months, he has definitely learned how to use the community's language and memes to effectively appeal to both mainstream and hardcore Bitcoin audiences, and I'm afraid that this can all be used to launch social attacks.



There are two scenarios through which Michael Saylor can become evil: one which he influences the "hive mind" directly, and one which is a lot more sophisticated and only requires his participation via proxies. For a man of his intellect, I reckon that the first scenario is highly unlikely – unless he, as a US citizen and CEO of an American publicly-traded company, gets coerced to act in bad faith.

Michael Saylor doesn't have to try to launch a 51% attack on the Bitcoin network or try to change the consensus rules to become a villain. All he must do is launch social attacks against certain developments and make use of his influence to convince both community members who run sovereign nodes and developers to boycott various proposals.

So what he can do is advocate for the preservation of the current state of Bitcoin, discourage people from using privacy tools, and buy himself and his corporate friends enough time to load up on BTC until privacy efforts become more or less futile. After all, these companies need bitcoins to escape inflation and taxation for multiple years – while the average pleb only wants a nicer house and the kind of car which turns heads.

Bitcoin has a long story of "slaying" heroes and it includes A-listers like Gavin Andresen, Mike Hearn, Jeff Garzik, Roger Ver, and Trace Mayer. It's likely that Michael Saylor has learned from their mistakes and won't conduct himself in a way which raises similar suspicions. Which I why I suspect that he may use proxies (other CEOs who buy large amounts of bitcoin and don't care about their reputation within the community, sockpuppet accounts, and/or developers who act in bad faith).

On one hand, it's like you've been waiting for him all along. On the other hand, you feel skeptical due to the means through which he has earned his spot in the team and you know that his influence far exceeds yours and he can easily manipulate other people's opinions and attitudes.

My reading of Saylor is that he doesn't like privacy – but then again, as the CEO of a publicly-traded American corporation, he can't directly express his love for Wasabi, JoinMarket, and Pay to End-Point. Still, as the CEO of the same publicly-traded American corporation, he will pursue the best interests of his investment plan, project his understanding of bitcoin, and conduct himself according to the will of his shareholders. So acting against BTC privacy is not far-fetched, since more fungibility is not necessarily compatible with the views that Saylor expresses during interviews.

The ultimate test of character and conviction for a bitcoiner is the bear market. That's when we can truly tell the LARPers and selfish marketers apart from the ones who truly care about the project. In the case of Mr. Saylor, I'd love to see the way he acts when the winds are blowing hard in the opposite direction and his ship is no longer reaching the planned destination on time.

Part of me wishes that the "hive mind" was more concerned with the qualities of bitcoin as a currency than with the opinions of a CEO who speaks in popular memes. But then again, who am I to judge? I chucked during the "it's going up forever, Laura" moments and had some of my own moments when I thought he was one of us. Yet I remain vigilant and skeptical – I didn't join this space because I enjoy feeling the warm comfort of conformity and like-mindedness, but because I'm a critical person who likes to ask questions.

So I'll keep an eye out and use this article as a reference point which tracks Michael Saylor's and MicroStrategy's evolution over time. And yes, I've avoided the other low-hanging fruit about price manipulation (as in, Michael Saylor posts tweet about buying more BTC, and the price pumps with incredible precision). I'm more concerned about bitcoin as a currency than about the price. And part of me was feeling happier when we were trying hard to break $9k with Vegeta memes.

But to quote another meme, "this is gentlemen" – we've wanted more bitcoin adoption and we're getting it in ways that we wished would happen last. Sadly, it wasn't the regular people who got in first. After being scared by mainstream media, they have waited for the legitimation of "trusted" institutions. MicroStrategy is just the beginning or the institutionalization of bitcoin, whether we like it or not.



Bitrefill
Live on Crypto
twitch
Domino's
DOORDASH
Bitrefill
GIFT CODE
X4TY-31M5
Uber Eats
Download on the App Store
GET IT ON Google Play
Bitrefill.com



Bitcoin Public Key, Receiving Address, UTXO: What's the Difference?

Public keys, receiving addresses, and UTXOs are three concepts with which even some of the most seasoned bitcoiners sometimes struggle to juggle. They are very similar in meaning and, in usual language, they can even become interchangeable. Even Satoshi Nakamoto referred to the "public key" with the meaning that we give today to receiving addresses. And it's not uncommon to hear "I own bitcoins in an address" instead of "I own bitcoins in an UTXO" (the latter is more correct).

This confusion happens because all of these terms can be used to describe the coins one received. However, you should use "address" to refer to coins that you expect to receive, "UTXO" to talk about the coins that you already received, and "public key" as an umbrella term which contains all of the your public addresses and UTXOs.

As you can already see, there are temporal and consequential differences between public key, receiving address, and UTXO. But the good news is that I'm going to take the time and explain them in this article.

Bitcoin Public Key and Receiving Address

If you're looking for the short explanation, here it is: all Bitcoin wallets have a private key (which you should never reveal to anyone) and a public key (in the modern BIP 32 Hierarchical Deterministic wallets, it's called an xpub or the Extended Public Key). As acknowledged by Satoshi in the whitepaper, he took inspiration from Ralph Merkle's 1980 research paper "Protocols for Public Key Cryptosystems".

This public key is like an umbrella which covers both receiving addresses and UTXOs. From it, you can generate a virtually unlimited amount of unique receiving addresses. Most of the QR codes you find online when you make payment services are receiving addresses that are derived from Extended Public Key.

Most importantly, you can share one of these addresses publicly without revealing the rest of the addresses generated from the same xpub, or the funds you received in them. So you can share an address, receive a payment in it, but everyone checking that address on a blockchain explorer will not see how much you own in other addresses in your wallet (i.e. derived from the same xpub). It's an important privacy feature which Satoshi Nakamoto described in title 10 of the whitepaper, and was later extended by Pieter Wuille with HD wallets.

Bitcoin Receiving Address and UTXO

How about the UTXO? Well, it stands for Unspent Transaction Output and refers to the bitcoins that were not spent in an address. As defined by the Bitcoin Wiki, it's the smallest individual unit of your wallet's balance – as the sum of UTXOs determines the amount of bitcoins you control with your wallet's private keys.

In simpler terms, it's like a pocket in your jeans, that you use to store money. So when you make a payment, the seller and the witnesses around you will only see the amount of money that you take out of that specific pocket.

The UTXO (or pocket) concept is great, as it preserves your privacy. You can walk around with millions of monetary units, but when you make a payment you only reveal to the world watching that you have a reasonable amount which covers the expense of the goods or services that you're buying.

Let's say that you're buying a carton of milk, which is worth $3 and you have one pocket where you're holding $100000 in $100 bills and another pocket where you have $5. If you were to reach for the pocket where you have more money and take your money out, everyone around you would observe that you're rich. And it's likely that there would be some bad actors who will start thinking of ways to steal your money.

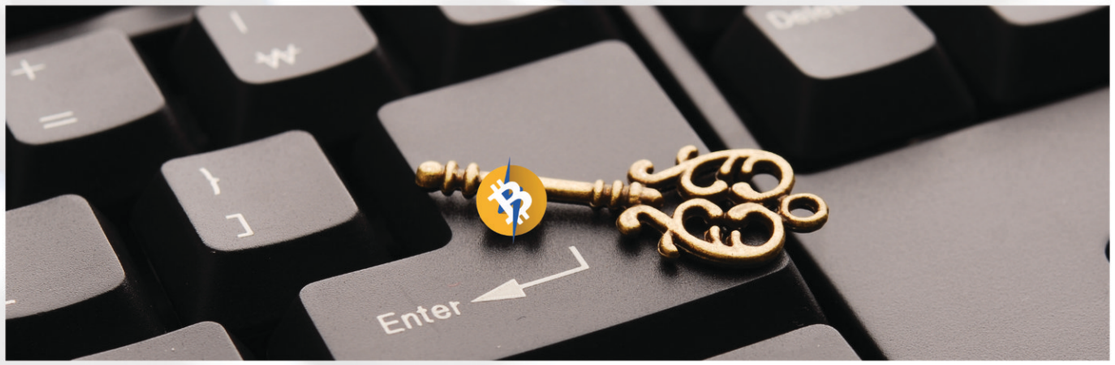
On the other hand, if you only draw the $5 bill for your $3 expense, then your privacy is excellent and no bad actor will waste time and energy trying to mug you. The risk/reward ratio certainly discourages any kind of attack.

It's all the same with UTXOs – the Bitcoin network keeps track of all the coins you did not spend (and therefore are in your possession). And the sum of these UTXOs make up the possessions in your wallet, which you can only spend if you can sign a transaction with the private key.

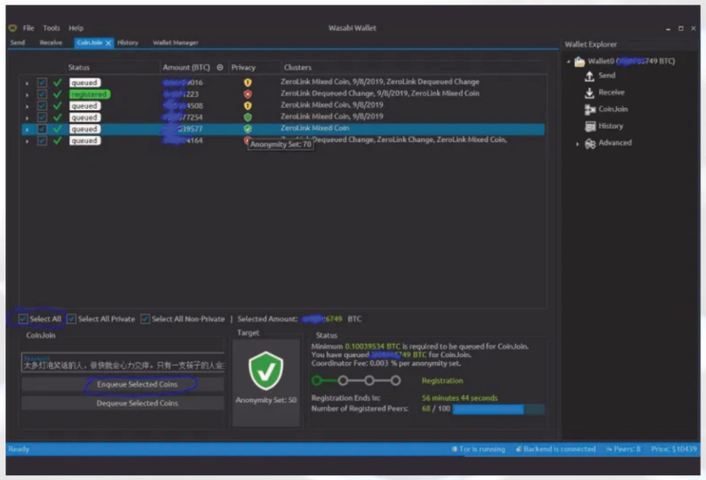
Which Wallet Allows Me To Generate Unlimited Addresses and Also Manage UTXOs?

These concepts are mostly confusing because wallet developers label them as "advanced features" that are for power users. This gives them an excuse to sometimes mix your UTXOs under the same wallet balance (so you don't get to choose which coins you spend, the selection gets made automatically) and also limit the amount of addresses that you generate (we even have wallets that only give you one receiving address per account).

It also means that these wallets are in control of your xpub, and therefore know how many coins you own, with whom you are transacting, and if/how many receive addresses you're generating.



Here's the good news, though: there are wallets that help you protect your receiving privacy and also add an extra layer of plausible deniability. And they're completely free and open source, so you don't have to pay anything.



On desktop, you have Wasabi Wallet and Bitcoin Core. For beginners, Wasabi is probably better – it routes your internet connection through the Tor network by default, it prevents address reuse, and it also makes UTXO management as simple as managing folders.

Bitcoin Core is also great, as instead of only downloading a few block filters via Tor, you run your own full node and become completely sovereign. However, to enable UTXO control you're going to have to open the Options menu, choose the Wallet tab, and tick the "Enable Coin Control Features" box before saving the new setting.

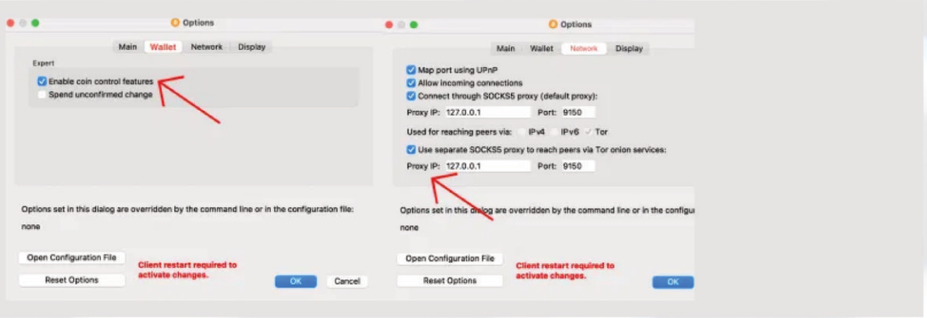
Also, for better privacy, go to the Network tab (still in the Options menu), and tick the Tor-related boxes, as well as set proxy IP 127.0.0.1, in port 9150 (a typical Tor setting). After you change these settings, you're going to have to restart Bitcoin Core. It's a little bit more advanced, but still not very complicated.

But the best part about Wasabi and Bitcoin Core is that you can use them in a complimentary way: while running Core in the background, it automatically connects as a full node to Wasabi. This gives you the best mix of privacy and security, so you maximize your sovereignty.

You can also use your hardware wallets with Wasabi (Trezor, Ledger, Coldcard, and BitBox02 will definitely work). This means that you extend their features beyond the standard capabilities of the official software, while also maximizing your sovereignty and control. You no longer connect to their servers, you no longer share your xpub (with the sum of addresses and UTXOs included) with any company, and you embrace your freedom with all the benefits of extra privacy.

If you're looking for a mobile wallet which allows you to control your own xpub by connecting to your own full node while enabling UTXO control, look no further than Blue Wallet. It's available on both Android and iOS, and it has all the advanced features under a friendly user interface. Just keep in mind that, unless you tick all the sovereignty boxes (full node, Tor routing, UTXO control), you will be using an SPV wallet and somebody else will have your public key.

No matter which one of these options you will choose, you will get more control over your public key (including generated addresses and UTXOs). This is great for financial privacy, connection-level privacy, as well as overall sovereignty.





Why Bitcoin Is Bullish Even When The Price Dumps

Consider this: how long does it take you to liquidate your bank account? Well, you'd have to submit a request, wait for some manager's permission, and then wait a few days until you can finally get your money. You pay middlemen fees, the government will take its share, and it's likely that the bank will also come up with an extra tax to make you lose some more money – they'd do anything to make you regret exiting their system.

In the case of Bitcoin, cashing out is seamless and nearly instant. When you decide you want to sell your coins, you simply transfer them to the buyer's address and wait until you receive your dirty fiat. Yes, you pay for a transaction fee and you do have to wait for block confirmations. But this will most likely cost less and take a smaller amount of time than receiving a fiat wire transfer – if speed is what you're looking for, then you're most likely better off using a stablecoin like Tether or else demanding for a cash payment.

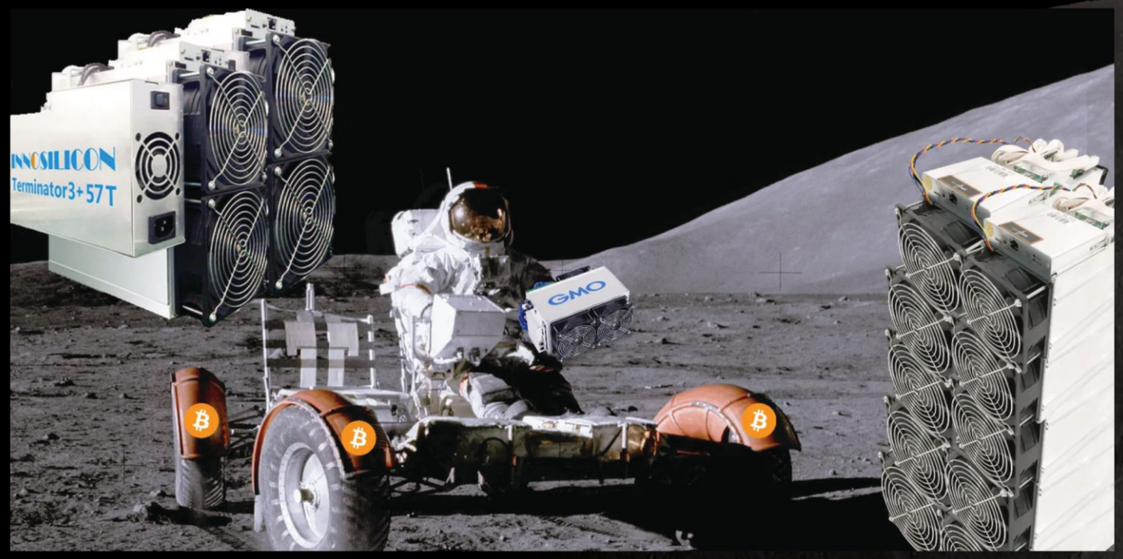
So while you might be worried that the price is going down too fast, it's specifically because Bitcoin is permissionless and a lot faster than the traditional financial system. And if you enjoy celebrating the monumental price pumps, then you should also have sympathy for the corrections and dumps. The principle is the same – investors get in and out whenever they want, without waiting for a third party to vet their decision.

Now let's consider how empowering this is and what it entails for human rights. Is your wealth more protected if you must wait entire days until a bureaucrat decides that you deserve to withdraw your own money? I could argue that if you're not in charge of making decisions in regards to your own savings, then they're not really yours and you have effectively delegated control over the product of your time and labor.

Bitcoin belongs to whoever is able to sign the unforgeable cryptographic keys. And in order for the money to be truly yours, then you should be able to use it whenever you want, for whatever purpose you deem worthy of the expenditure. So when we see the price of BTC dumping really fast, it only means that the network protects private property rights very well and passes them on to other owners in a free and permissionless way.

Of course, 1 bitcoin will always be 1 bitcoin and denominating in fiat money is only a short-term game. But instead of panicking, casting blame on others, and feeling entitled to only see big pumps, we should appreciate that the system works like it should. Free markets are naturally wild – but Bitcoin always provides incentives for somebody else to step in and become the new owner via decentralized, immutable, peer to peer, and permissionless transfers.

So yes, bitcoin is bullish even when the price dumps. If this is your first cycle, then have some patience. Price discovery, even if it eventually leads to millions of dollars, happens in phases which adjust to human greed. The bull will be back as soon as more people understand why they need Bitcoin. Also, you shouldn't be investing your rent money or mortgaging your house anyway (regardless of what Twitter influencers will do and say).



On Taking Bitcoin Mining to the Moon. . . Literally

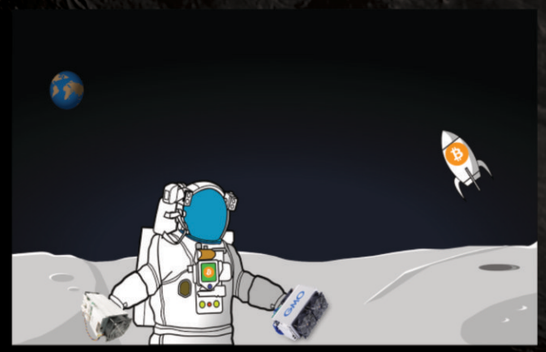
As humankind becomes an inter-planetary species which embraces the Bitcoin standard, we should seriously consider extending the mining operations beyond Earth. The reasons behind the expansion take into consideration both single point of failure scenarios (Bitcoin would be destroyed if our home planet remained the only place where the currency gets secured, while some catastrophic Death Star-like event happened) and the distribution of mining to relay transactions a lot easier across our galaxy.

Furthermore, moving mining operations to celestial bodies that we don't inhabit (such as Earth's natural satellite) would bring environmental benefits while lowering the delay between transmissions to other around the Solar System. If we factor in the 2-week lunar days and the amount of energy we can capture and use for mining, we get a pretty sustainable extension for the already-existing Earth operations.

The Moon is not the end goal, but only the first step towards making Bitcoin the inter-planetary network which helps us make payments. After we successfully establish mining operations on the Moon, we can undergo easier expansions to Mars and other planets.

There is already an ongoing project in which NASA and Nokia are putting 4G technology on Earth's natural satellite, so following it up with Bitcoin mining would be really useful expansion. In time, if we manage to make mining equipment to withstand extreme temperatures, we can also get closer to the Sun by setting up operations on Venus and Mercury (which would be ideal, given the amount of solar energy that we can capture and use).

This article is inspired by Blockstream's project to deliver Bitcoin blockchain synchronization via commercial satellites, as well as Peter Todd's 2017 hard sci-fi on Bitcoin mining in space. And while some political and physical challenges may exist, the idea is not as far-fetched as it first sounds.



Bitcoin Mining on The Moon: The Delay Times

When it comes to Bitcoin mining, one of the biggest concerns is always the lag (or delay time) which reduces the miners' competitive advantage in discovering blocks. A faster and more stable internet connection is always preferable – yet thanks to the satellite synchronization and the development of high-speed mobile networks across areas which have no broadband infrastructure, the situation is gradually changing.

Now let's do the math. The average distance between the Earth and the Moon is 385.000 kilometres (240.000 miles). Conversely, the speed of light, which radio waves reach when they propagate in vacuum, is exactly 299.792.458 m/s. This means that sending a message with the speed of light to the Moon and back will take an average of 1.28 seconds.

But we should also take into consideration the shape of the Moon, the smoothness of the surface, and the antenna polarization of these transmissions. According to existing research, there is a delay of this mathematically ideal time which bumps the average EME (Earth-Moon-Earth) radio signal propagation time to an average of 2.56 seconds.

Given Bitcoin's block-issuing time of approximately 10 minutes, this kind of delay time is more than acceptable. Therefore, we already possess the technology to make this space expansion of Bitcoin mining work.





Bitcoin Mining on The Moon: The Solar Energy and Temperature

Beyond the single point of failure and environmental criteria, we should also consider the amount of solar energy that we can use for Lunar Bitcoin mining. And as you might remember from school, the Moon rotates around its axis throughout 27 Earth days – which means that it has a 13 1/2 daytime, and a 13 1/2 night time. This almost fits the 2 weeks Bitcoin meme.

In theory, this sounds ideal for capturing and using solar power. There is an extended amount of time during which the energy can be stored, so if we developed efficient batteries we could sustain the activity throughout the entire night cycle.

According to 2019 NASA research, building solar panels in space might be as easy as clicking "Print". In theory, the Moon surface should get a similar amount of sunlight as Earth during daytime. So we can assume that the solar constant (aka solar irradiance) of 1.36 kW per square meter also applies to the Moon.

But due to the lack of an atmosphere and the absence of clouds to stand in the way of sunlight, the solar energy production should be slightly higher on the Moon surface. It all sounds feasible, but the main challenge is still storing the energy for almost two weeks with negligible waste.

At this point in our research, we should factor in the Lunar temperature swings. Given the Moon's lack of an atmosphere, the heat doesn't get preserved and we go from extremely hot to extremely cold. The extremes are 127 degrees Celsius (260 Fahrenheit, 400.15 Kelvin) for daytime and minus 173 degrees Celsius (343.4 Fahrenheit, 446.15 Kelvin) during nights.

For reference, a Bitmain Antminer mining ASIC operates within a range of 65 to 135 degrees Celsius (149 to 275 Fahrenheit, 338.15 to 408.15 Fahrenheit). With proper ventilation and heating, the device is very likely to withstand the extreme temperatures of the Moon's daytime.

However, the issue comes at night. Not only that it's hard to store the electricity for two weeks, but we must also ensure a proper temperature to make the Bitcoin mining devices function. Ideally, the heat generated from mining should get preserved throughout the 13-day sunlight cycle so it can be used to sustain the operation during the night.

So in order to make Bitcoin mining on the Moon work, we need to find better materials to store both electricity and heat. If we solve these two problems, there is no other obstacle – and further research can be put into expanding towards Mars and Mercury.

Bitcoin Mining on the Moon: The Governments and Space Exploration Monopolies

Even if we fix all of the technological and physical issues which concern Bitcoin mining on the Moon, we must still fix space travel, exploration, and research – fields which are currently in an unfair situation of government monopoly.

Sure, we do have private companies which seek to offer space travel and colonization services. But in order for them to operate, they still needed to get permission from governmental authorities and they worked with governmental agencies for their early testing.

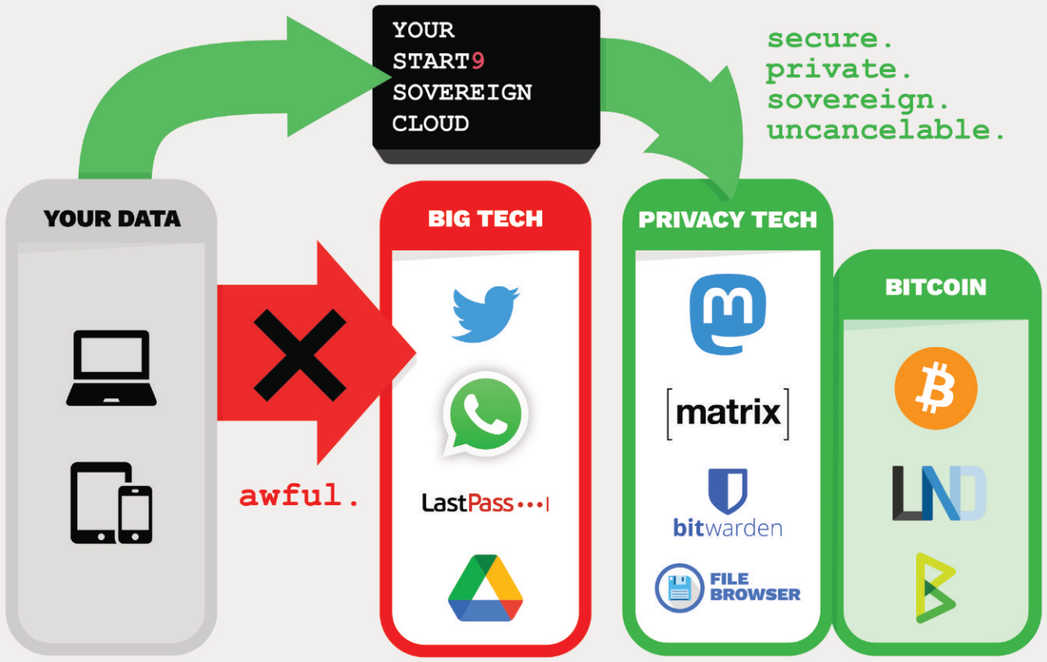
Hopefully, the situation will change in time and space travelling will be as simple as getting a bus ticket, while interplanetary law will allow for some innovation without restricting exploration and scientific development on the grounds of private property enforcement. In other words, we should make sure that our future legislators don't treat uninhabited places as if they entirely belong to them or to monopolistic private entities.



But if the price of expanding Bitcoin mining in space is that of entrusting a handful of governments with control over the mining operations, then the effort is probably not worth it.

DUMP BIG TECH

BE YOUR OWN CLOUD



Start9.com

@start9labs
@start9_labs



How to Make Bitcoin Transactions Environmentally-Friendly

So you've read the news about Bitcoin mining consuming a lot of energy. And while the numbers are difficult to verify and the methodologies seem to vary according to the institution behind the study (and its financial interests), some rough estimates suggest that miners across the world use a lot more electricity than entire countries (popular examples include Argentina, Ireland, and Switzerland).

Critics of Bitcoin mining suggest that all of this computationally-intensive activity is wasteful and unnecessary in a context where nation states and individuals pledge to reduce their carbon footprint. They also point out to the fact that Visa and Mastercard transactions are still greener in terms of energy consumption, so the switch from traditional finance makes a lot less sense in their ecology-centric view.

It's very likely that these same critics live in first-world countries that are governed by rather stable democracies that don't limit their economic or private property rights, but that's besides the point. Personally, I can argue that energy production is infinite and not some kind of zero-sum game where we decide what use case is worthwhile and which one should disappear – and instead of ranking our civilization's priorities, we should think of ways to reduce the environmental impact of existing energy consumption trends. Planting trees and working towards the preservation of ecosystems might be a good start.

But what do I know? As a bitcoiner, I might be biased towards supporting my preferred form of money. Just like mainstream media journalists and environmental scientists defend their own favorite form of money and suggest that nothing else should exist. As humans, we are subjective according to our own limited knowledge and narrow understanding of the world.

So where does this lead us? Are we going to let the oceans boil as we become sovereign from oppressive nation states? Are we going to replace the proven Proof of Work with something experimental that consumes less electricity? Is it really worth it to drain the entire energy of the Sun to fuel our libertarian pipe dream as we sip the financial sovereignty Kool-Aid?

In this article I'm going to try to debunk some common myths about Bitcoin mining and energy consumption. At the end, I'll also suggest ways to make your transactions more environmentally-friendly (spoiler alert: it involves the Lightning Network and/or sidechains like Liquid or DriveChain).

What Is Bitcoin Mining and How Is It Tied With Transactions?

In a nutshell, Bitcoin mining is the process through which transactions get confirmed in new blocks that add up to the blockchain. As miners solve a complex mathematical problem to compete for the discovery of blocks, the successful ones get two rewards: a block reward subsidy (the reward is called a coinbase and gets halved every 4 years) and the sum of fees from the newly-confirmed transactions.

These rewards act as an incentive to keep the operations going and make sure that they stay honest in relation to the consensus rules – if miners try to cheat, then full nodes will automatically invalidate their work and make it wasteful.

The term "mining" originates from the Bitcoin whitepaper, where Satoshi has written an analogy between the Proof of Work block discovery process and the more traditional gold mining. This comparison is useful because it simplifies the understanding of the phenomena involved and also introduces us to the resource exchange: to get the mining rewards, electricity and CPU time get expended.

But the comparison between Bitcoin mining and gold mining is not very relevant from two points of view:

– we know the total supply of bitcoins and where to find them (unlike gold, which can exist in larger quantities than we think and may also be found on other planets or asteroids);

– if we spend more resources on Bitcoin mining equipment and consume more energy, we won't be getting more bitcoins (unlike gold, where enough resource allocation can lead to a greater discovery of mines and quicker extraction). Thanks to the dynamics of the Nakamoto econsensus, the mining difficulty increases when the activity gets more intense (more participants join the competition) and decreases when the activity gets lower. This adjustment takes place every 2016 blocks (approximately 2 weeks) and makes sure that the addition of new coins follows the schedule.

To put it in a different perspective, mining is Bitcoin's equivalent of having the banks settle a transaction – the entities involved check the validity of the money, transfer it from one party to the other, and then exchange fees according to the nature of the service.

The main difference is that Bitcoin accomplishes this feat without trusted third parties or centralized institutions. Everything is decentralized and autonomous from the political decisions of governments and central banks.

So Bitcoin mining is an integral part of having a decentralized, trustless, and censorship-resistant network. The only drawback is that miners and nodes require a lot of energy to verify/confirm each transaction and function according to the consensus rules. In the next section I'm going to explain how we shouldn't minimize this cost and how we can actually reduce it without a security tradeoff.

6. Incentive

By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.

The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.





Bitcoin's Proof of Work vs Proof of Stake

Usually, this narrative of Bitcoin being wasteful is also promoted by altcoin investors and developers who promote their own Proof of Stake systems. But as any competent security expert will tell you, pursuing an ideological path will not always help a system withstand attacks. For all of its heavily-marketed greenness, Proof of Stake is oligarchic in nature and leads to a rather irreversible decentralization which consolidates the status of an elite few. Not only this, but it's also very experimental and has yet to prove its efficiency on the long term.

Ethereum developers might brag about their Casper PoS implementation and its friendliness to the environment, but there's a reason why its release has been delayed for years. Do you really think that Bitcoin, a trillion dollar asset which benefits from the best and most experienced developers in the space, wouldn't have already made the switch to a better technology if it was provably-superior?

Not even the second cryptocurrency by market capitalization wants to take the extra risk without proper testing – but at least it does a better job in the marketing/PR department, as it conveniently deflects from the fact that gamers use their video cards to

Features	Proof of Work	Proof of Stake
Fault Tolerance	50%	33%
Fork Choice	Objective	Subjective
Unforgeable Costliness	Yes	No
Proxy for Value	Yes	No
Accumulated Work	Yes	No
Block Creator Location	External	Internal
Division of Power	Yes	No
Sunk Investment	Yes	No
Full Replication	Yes	No
Fallback to Bitgold	Yes	No
Socially Scalable	Yes	No
Computationally Scalable	No	Yes

mine it. After all, Ethereum does use some of its centralizing premine to finance development and get good publicity.

It's also worth noting that there are Ethereum proponents who agree that Proof of Stake is inferior from a security and wealth distribution standpoint – and to better understand this view, I recommend Donald McIntyre's excellent analysis on the topic (whose summary you can find in the table below).

The argument isn't only about Ethereum's planned transition to Proof of Stake. For instance, EOS' system of Delegated Proof of Stake (DPoS) has generated situations of dishonesty – the community-elected block producers have found ways to buy votes that keep them in power and thus establish cartels that ultimately centralize the network. Not only that this goes against the intentions of creating trustless and decentralized systems that scale, but ends up becoming pointless – it's less efficient than a fully centralized setup like Amazon's Web Servers, yet just as easy to control.

Furthermore, Proof of Work is very dynamic and allows for participants to invest external capital into securing the network. This means that you can acquire coins and participate in the network's security without buying the bitcoins of current holders. You don't influence the price or perpetuate a scheme, you merely provide a service and receive rewards.

In Proof of Stake, you secure the network by locking your coins and you receive rewards according to the amount of coins you've locked. This means that newcomers who want to participate in staking will have to buy the coins from old timers. And this sounds a lot like a Ponzi scheme, where established hierarchies get overturned only if early adopters sell their coins to newcomers. Once the stream of newcomers stalls and the current stakers see returns of diminishing value, the network might be in serious trouble.

In comparison, Proof of Work allows for some very dramatic changes. Miners will cease to operate if their profitability diminishes. Mining farms and hardware manufacturers such as Bitmain can make terrible management decisions and lose the throne in a matter of months. Nothing is set in stone, and new players can enter the mining game without requiring the permission of a foundation, federation, or human-governed political structure.

Bitcoin will probably never switch to Proof of Stake and mining will go on for the foreseeable future. But what about governments? They can ban Bitcoin mining, can't they?

Bitcoin Mining, Pools, and Government Bans

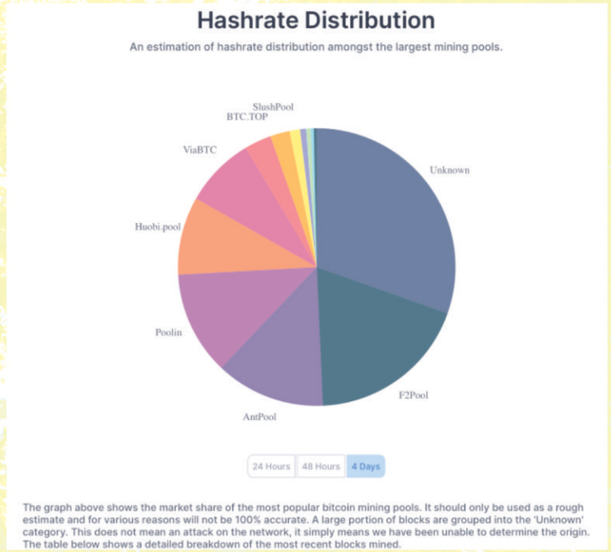
Wait, so Bitcoin has mining pools? As in miners that get together and centralize their hashrate to maximize their chances to get rewards? How are they any different from federation members, block producers, major stakers, delegates, and other entities which operate in Proof of Stake systems?

If you look at a graph which ranks mining pools by hashrate, you will find that a large percentage of Bitcoin mining takes place in China. This doesn't look much like decentralization, does it?

F2Pool, Huobi, Poolin, Antpool, Via.BTC, and BTC.TOP are all located in China, so what if the government decides to shut them down? Can Bitcoin withstand a 40% hashrate drop? Well, it's not that simple. And in order to explain the arguments, we will have to define mining pools.

So let's say that I decide to mine bitcoins from home. I bought myself a fairly powerful machine, I benefit from low-cost electricity, and therefore I should be able to make a nice profit from the operation. There are two approaches to it: I can either mine as a solo operator and compete for the entire reward with very low chances in relation to the rest of the network, or I can join a pool to increase my chances while sharing all rewards with the other participants of the mining pool.

Slush (whom you can hear in S4 E8 of the Bitcoin Takeover Podcast) is the inventor of the world's first mining pool. Back in November 2010, Satoshi Nakamoto himself reacted to this game-changing element which was introduced to the Bitcoin security dynamics.





If I were to play the devil's advocate for the concept of mining pools, I'd say that concentrating and professionalizing hashrate objectively offers more efficiency and predictability. On the other hand, it's important for individual mobility and autonomy to exist, so miners can switch to solo mode or join another pool which better represents their interests. This also circumvents potential government bans on mining.

Yes, governments can physically-seize mining equipment and shut down mining rigs. But this will not stop mining from happening. You see, Bitcoin leverages geopolitics and keeps nation states at the edge of financial accountability and at the risk of losing the innovation race. To some extent, Bitcoin is inevitable: are you going to ban mining and convince your allies to do the same? Then another nation will gladly welcome the operations and thus acquire a competitive advantage in what might just turn out to be the reserve currency of the future.

Yes, it's nice to think in global terms and assume cooperation between nations. But at the same time, the UN Security Council (which seats the USA, Russia, China, the United Kingdom, and France) rarely reaches the required unanimity to vote on issues. The dynamics between Russia, China, and the USA guarantee that we won't ever have a world government or a dominant ideology. The economic stakes are way too high and there are many cases when the debasement of one's currency affects the prosperity of the other.

And if you're not convinced by this argument, then look at how cooperation went on during the covid19 pandemic and how poorly everybody coordinated towards a seemingly-common goal. For every country that instated lockdowns, there was another one which allowed freedom lovers to come in. For every mandatory mask mandate, there was a place which rejected the norm. And for every attempt to create a vaccine passport, there has been a counteraction to enable travelling without such a document.

It's not like small nation states are entirely accountable to the bigger military powers. Also, it's not like international waters or the international space don't exist as alternatives to become the new home of Bitcoin mining. As long as there is an incentive and a clear use case, people will find ways. Governments couldn't take down Pirate's Bay (an objectively more centralized enterprise) and they're going to have a harder time with Bitcoin. And if everything else fails, there's nothing that stops Bitcoin users from running mining operations under the Tor network from their home computers.

Mining pools currently exist for reasons which concern efficiency. It's more professional and stable for the network's hashrate to remain consistent, and it's also more profitable for individuals to join pools since the rewards are more consistent (but significantly smaller) than in the case of solo mining. Also, there are developer proposals which seek to increase the autonomy of mining pool participants – just because they put together their hash power doesn't mean that they always agree.



Matt Corallo's Betterhash is just one example of removing the centralization risks involved in pool mining. Slush Pool (the world's first mining pool) already offers Stratum V2, which is developed in collaboration with Corallo. But we should never forget that Proof of Work is dynamic and we're still at an early stage of Bitcoin mining.

In the future, we might find better and more efficient ways to mine. As computation and integrated circuits improve, we shouldn't be surprised if a few years from now we can encompass a lot of hashing power in today's Raspberry Pi equivalents. Home mining might become more common thanks to an increased Bitcoin adoption, and it's likely that retail hardware manufacturers will catch up by offering dedicated consumer electronics.

The current trend of mining professionalization may become a lot more amateurish on a global scale – and in the best way possible. If the miners keep the hardware in their own homes, then the risks associated with physical confiscation and shutdowns get increasingly lower.

Also, we should not forget about the role of Bitcoin in power grid efficiency research. In many cases, Bitcoin mining uses energy that doesn't get used for any other purposes and would otherwise get wasted. We are still terrible at storing electric energy and our power infrastructure doesn't always scale up to sustain our ambitions for development (and this isn't just a Bitcoin issue).

To be able to have more electric cars and other electricity-powered appliances, we need to improve our energy production and distribution. And whether we like it or not, Bitcoin helps in this regard. Though it's hard to prove, some even argue that Bitcoin accelerates green energy production because sustainable and environmentally-friendly sources are also the most cost-effective for mining. There's definitely a lot to say and a lot to research in this regard – but it would be foolish to downplay Bitcoin's role in this scheme.

How To Save Energy and Become Environmentally-Friendly Using Bitcoin

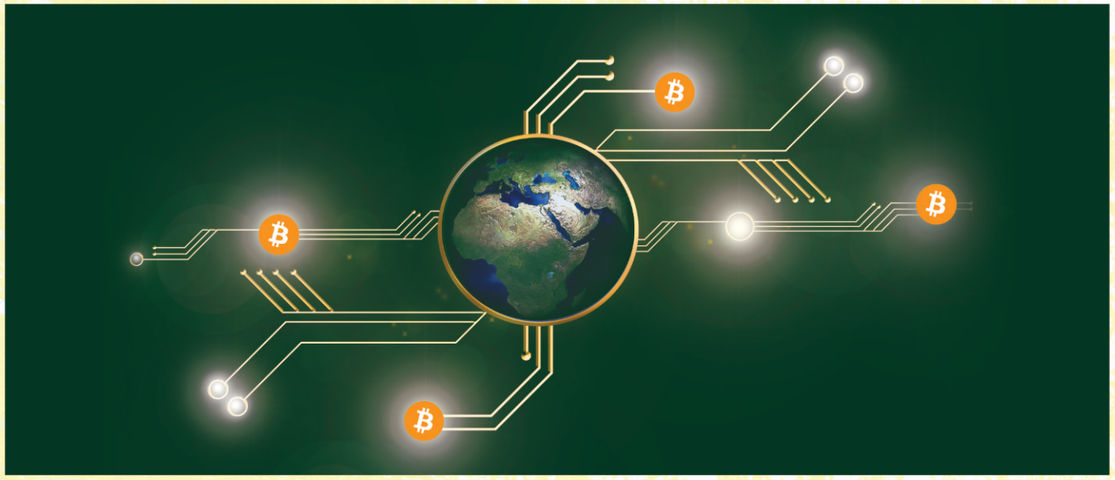
Bitcoin mainchain transactions are essential for the network's security. But if you want to reduce the energy consumption by making your own Bitcoin transactions environmentally-friendly, you must start using the Lightning Network or sidechains like Liquid and Drivechain.

Lightning is ideal because it can run on a low-powered device like the Raspberry Pi. This means that sending and receiving transactions relies on a computer network in which every device consumes lightbulb levels of energy. For reference, a Raspberry Pi 3B+ costs as little as $6 to run 24/7 for an entire year – this is a lot less than most of your electric appliances. The Raspberry Pi 4 is more powerful and also a little bit more energy-hungry, but it should not raise operation costs to more than $10 per year.

Onboarding the Lightning Network requires at least one transaction on the Bitcoin blockchain to open a channel with somebody else. But as soon as you're in, you can make an unlimited (well, depending on how many coins you own) number of transactions with high speed, great privacy, Visa-level scalability, negligible fees, and insignificant energy consumption. If you're looking to minimize your carbon footprint while using Bitcoin, then Lightning is the way to go.



Think of Lightning like it's a night club tab – you pay an admission fee (the initial base layer transaction) and then you're free to transact with everybody



nside while keeping a private ledger with them. When you leave the bar, someone at the exit will do the accounting for you so that all transactions get charged to determine your final balance.

Or better yet, Lightning is like trading gold certificates: the base layer involves actually moving the gold around (a costly and resource-intensive activity), so you trade ownership certificates with people. When you're done transacting and want to get your digital gold, you only need to do one transaction which gets your funds unlocked on the Bitcoin blockchain. Entering and exiting the Lightning Network require the base layer. But what happens on the actual second layer is instant, private, and a lot more affordable.

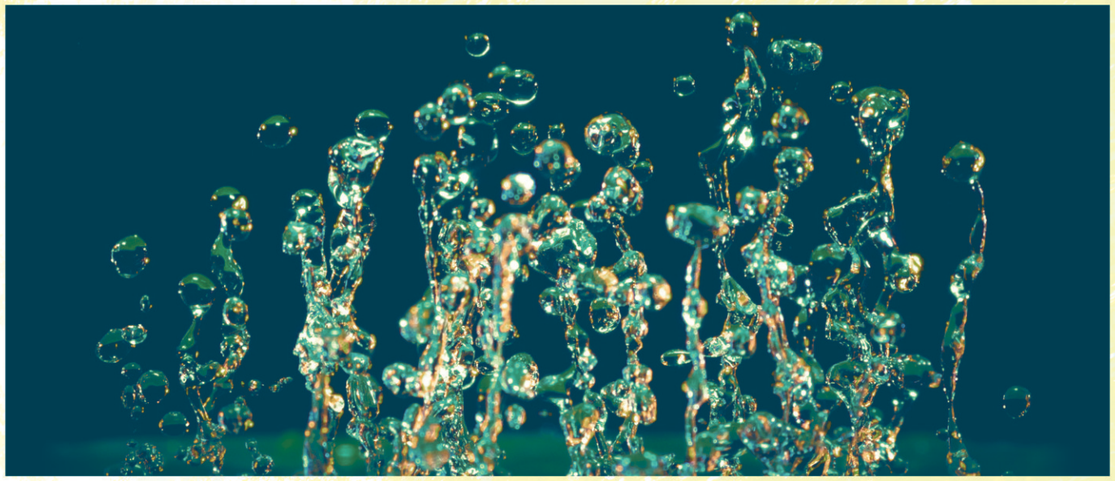
As a Lightning Network node, you can also choose to route other people's transactions. This means that your channels will allow others to make payments, and your participation as a trustless third party earns you small fractions of the paid transaction fee. Once again, this kind of activity consumes a lot less energy than an iPhone that's running video games. The cost of operating and maintaining a Raspberry Pi-based operation is low, efficient, and friendly with the environment.

If you're interested, here's a guide on how you can set up your own Lightning node with a Raspberry Pi and a general-purpose hard drive. It's a nice DIY project that can be quite educational and empowering in terms of sovereignty. And the RaspiBlitz code is entirely open source and has been vetted by users for longer than 2 years. If you'd rather buy a pre-built node as a product, check out the Fulmo shop (or LightningInABox in the USA).

The Liquid sidechain is also a lot more energy-efficient than the Bitcoin base layer. But as opposed to the Lightning Network, it's not as decentralized and not permissionless at all. Also, every operation requires the validation of federation members that run validating servers. This activity is still friendly with the environment, as compared to most traditional ways of processing and routing payments.



In terms of greenness (pun intended, since Blockstream has a mobile wallet called "Green"), Liquid is just as friendly with the environment as Proof of Stake



validation systems. It exists for the purpose of helping Bitcoin exchanges move large amount of coins with greater speed and more privacy. And in this process, it helps the Bitcoin network scale in a way which is efficient on all fronts.

The same can be said about other sidechains such as RSK (which helps move Ethereum smart contracts to Bitcoin), Paul Sztorc's Drivechain (which brings scalability and privacy) and Ruben Somesen's Softchain, Statechain, and Statechain. With some well-known trade-offs, they provide extra services and conveniences that the Bitcoin base layer doesn't have.

This way, Bitcoin users who think about their carbon footprint and want to minimize electricity consumption can choose to trade the superiority security and decentralization of the main chain for the peace of mind of reducing environmental impact. There are lots of choices out there, and most of them fulfil the criteria for saving energy. This doesn't mean that Bitcoin mining will eventually stop – it just means that you as an individual can choose to reduce the amount of energy-intensive base layer transactions that you do. You can voluntarily limit your use of the best means for decentralization just like you can voluntarily become vegan.

But for the rest of the world, there will always be a choice. And just because you know what's best for yourself and what satisfies your expectations doesn't mean that something else should not exist. There's great demand for decentralized non-governmental money, there are billions of people worldwide who need Bitcoin to escape from tyranny, and we can all agree that offering financial freedom to those who need it the most will always outweigh the energy costs.

So if you want to use Bitcoin in a way that's environmentally-friendly, then use the Lightning Network or one of the sidechains. You're going to enjoy great speed and privacy, while also reducing your energy use and carbon footprint.





The Significance of Satoshi Nakamoto's Coins

Satoshi Nakamoto's bitcoin holdings have long been a subject of speculation. How can the creator of Bitcoin never actually spend any of his coins? Why is it that no single unit has been moved in longer than 12 years? Could it be that Satoshi Nakamoto is dead? Or could he be the strongest HODLer of all times, as he understands the value proposition a lot better than everybody else?

In this article I will present three significant perspectives on Satoshi Nakamoto's bitcoins. In a sense, they are complimentary. But for the sake of clarity, I am going to take each one of them and expand the arguments:

– it's Satoshi's private property so we should no longer care, as the project has moved on and he is free to do whatever he wants with his money;

– Satoshi's coins are a huge honeypot for hackers, and every moment when they're still untouched proves that the Bitcoin network securely stores value;

– Satoshi's coins are a constant reminder for Bitcoin Core developers, which tells them that they should be conservative and never make changes which would compromise Satoshi's private property;

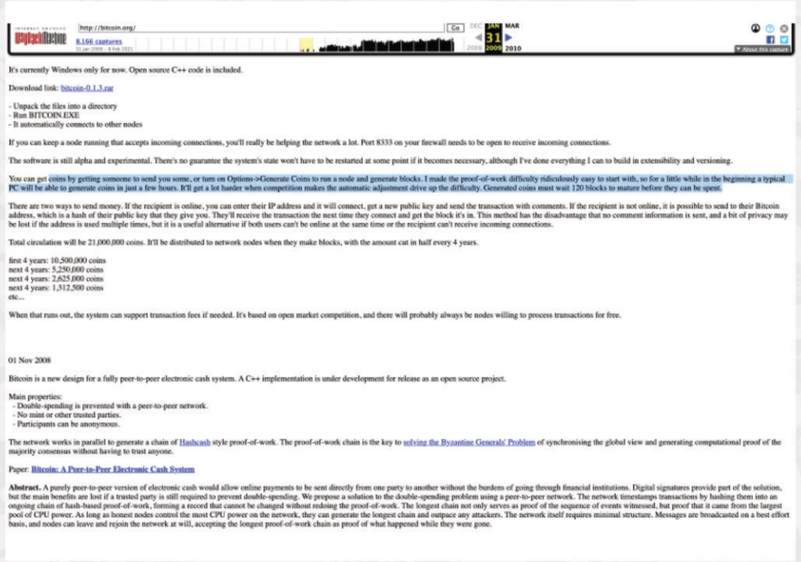
1. Satoshi's coins are his property, so we shouldn't care

Satoshi Nakamoto has mined his coins after the network got launched, in a time when bitcoins had no value on any market. We're talking about 2009, when there were no BTC exchanges, there were very few miners, and one could easily mine some coins with the computer CPU.

The members of the cryptography mailing list already knew about Bitcoin's launch, and people such as James A. Donald, Ray Dillinger, and Hal Finney have provided technical feedback to improve Bitcoin's security. All of this happened in November 2008, when "crypto" stood for cryptography, there was no cryptocurrency market, and there definitely wasn't a "blockchain industry".

After this early introduction, Satoshi launched version 0.1 of the Bitcoin software on January 8th 2009. He was the network's first miner, and kept the network alive during a time when nobody else seemed interested in collecting the 50 BTC as a reward for block discovery.

This is what the bitcoin.org website looked like in January 2009



For the pre-mine apologists out there, who enjoy justifying their unfair pre-market token distribution by highlighting how Satoshi Nakamoto was the only miner for months and in a way "pre-mined" his bitcoins, it should be mentioned that Satoshi obtained his BTC fairly after the network launched. He played by the network's rules and kept it alive while there was nobody in the world who would trade goods or services in exchange for bitcoins.

The network was still in its early days, there were still bugs to fix. As a matter of fact, somebody exploited a massive inflation bug in August 2010, when two addresses received 92.2 billion BTC each. At the time, the most significant transaction happened two months prior and involved a certain GPU miner named Laszlo. He famously sold 10.000 bitcoins for two pizzas.

So yes, Satoshi did earn his coins fairly and his mining cannot be labelled as a pre-mine since everybody on the cryptography mailing list knew about Bitcoin's whitepaper and launch. Furthermore, lots of fans of Chaumian ecash, egold, liberty dollar, and other similar projects jumped on board during the early days. Maybe that their effort to acquire bitcoins (in fiat money and labor terms) was lower in those early days, but they also took a greater risk by accepting that an experimental computer project can be real money.

Now that we took ownership and fairness out of the way, we need to make it clear that Satoshi's coins belong to him and we must respect his decision to do whatever he wants. 12 years after the network launched, the market demand is great enough to buy his coins if he decides to sell. The Bitcoin project has grown beyond Satoshi's influence, he has no control over the network or market, and there are plenty of enthusiasts who would gladly buy Satoshi's bitcoins.



2. Satoshi's coins are a huge honeypot for hackers

This about it: the Bitcoin network is an open ledger which allows you to see how many coins are stored in every address. While we don't know for certain which addresses belong to Satoshi, we can find the blocks that he mined and associate the reward addresses with his identity. Analysts estimate that Satoshi owns about 1.125.150 BTC, and he's spent the coins from 19 of the blocks he mined (the first one being block no. 9, whose reward he used to make the first ever transaction to Hal Finney).

So there are more than 22.500 blocks whose rewards Satoshi Nakamoto has collected, but never spent. You can see them on the public ledger, you can verify that they were never moved, and then realize that nobody was able to break Bitcoin's cryptography to steal any of the BTC.

The reality is that Satoshi's coins are a honeypot for hackers. Who wouldn't want to gain access to at least 50 BTC (about 2 million USD at today's rate) for finding a vulnerability in the Bitcoin code? It's a no-brainer, really.

As long as Satoshi Nakamoto's coins don't move, we know that the network is secure and you can't break the cryptography of a wallet by exploiting some bug. It's a guarantee that it's safe to store wealth on the Bitcoin network and no unwanted third party can break the wallet's encryption. However, this doesn't mean that you should be reckless and it's recommended that you assess your threat model to know how to respond to other types of attacks (to your computer, to your phone, or to your physical integrity).

How can we know that the coins move due to Satoshi's direct action and not because his wallets were hacked? Well, that's a pretty tough question. If Satoshi ever decides to sell any of his coins, we should expect him to leave a message on one of his known accounts. There is no reason for him to act quietly, as the spending would leave the suspicion that his wallet got hacked and Bitcoin may not be as secure as we thought.



The Satoshi we know is fair and transparent about his actions in relation with the Bitcoin network. So to avoid any kind of negative speculation about the network's security, he would sign a message from his PGP, access his Bitcoin-Talk account, or send an e-mail from his known addresses (vistomail and gmx).

3. Satoshi's coins push for conservative Bitcoin development

Bitcoin is built on the basis that private property matters, and the network will cryptographically guarantee your ownership as long as you can sign a transaction with the right private key.

If the Bitcoin network was to undergo some kind of hard fork that would change the addresses or even redistribute the "lost" coins, it would infringe the property rights of the creator. And if not even the creator can safely store value on the Bitcoin blockchain for a long time, then nobody's wealth is really safe and the floodgates for arbitrary confiscation are open by a terrible precedent.

Satoshi's coins have the role of keeping Bitcoin developers in check while making them responsible for protecting the wealth of the person (or group of people) who created the system. As long as they are there, developers must guarantee software compatibility with old address formats and systems that Satoshi used in 2009 and 2010. It's a huge responsibility that every Bitcoin developer inherits and must take very seriously to insure the fairness and functioning of the system.



Sure, the developers can't change anything by themselves and network participants have learned to become conservative in relation to every proposal for new software. New optimizations and refinements are made with every version of the Core client, but it's up to the sovereign node operators to decide whether or not they run the code. In this truly decentralized system, the developers only make proposals with open source software – and community members choose whether or not they accept them.

So the community must also learn to understand the sanctity of private property and never get greedy in regards to Satoshi's coins, by pushing the developers to write code which redistributes them. This is also a slippery slope that can lead to a dystopian version of Bitcoin that we really don't want to materialize.

The existence of Satoshi's coins makes us all responsible for keeping the system fair and respecting everyone else's private property. And the longer they remain unmoved, the stronger this culture of respecting property becomes.



Comic Strip: Bitcoin Eating Popcorn #1

I've read the news today, oh boy. As it turns out, a bunch of ETH shills have taken over the r/ethereumfraud subreddit. It seems like they want to silence the truth from being told – and as true scammers, they do their best to hide their history and make themselves look good and fair.

Of course, this coverup doesn't change the facts. Ethereum had a huge premine (somewhere around 60%) and seeks to become an unfair oligarchy via Proof of Stake. The project set a dangerous precedent when it broke immutability during the 2016 DAO fork (aka blockchain rollback which saved the investors' money) and subjected itself to so-called "governance". Also, Ethereum Classic is the original project.

And for every good idea, there's a benevolent dictator who can approve it or shun it. Who would seriously want a money system in which five people in a conference call can make significant changes to the monetary policy?

Also, today it's hilariously difficult to run a full node. The ETH leaders themselves had to redefine what it means to run a node to make it seem like anyone can still do it. In reality, not even the Ethereum Foundation is running its own node and the project relies on companies like Infura, Geth and Amazon to store every transaction, application, and smart contract.

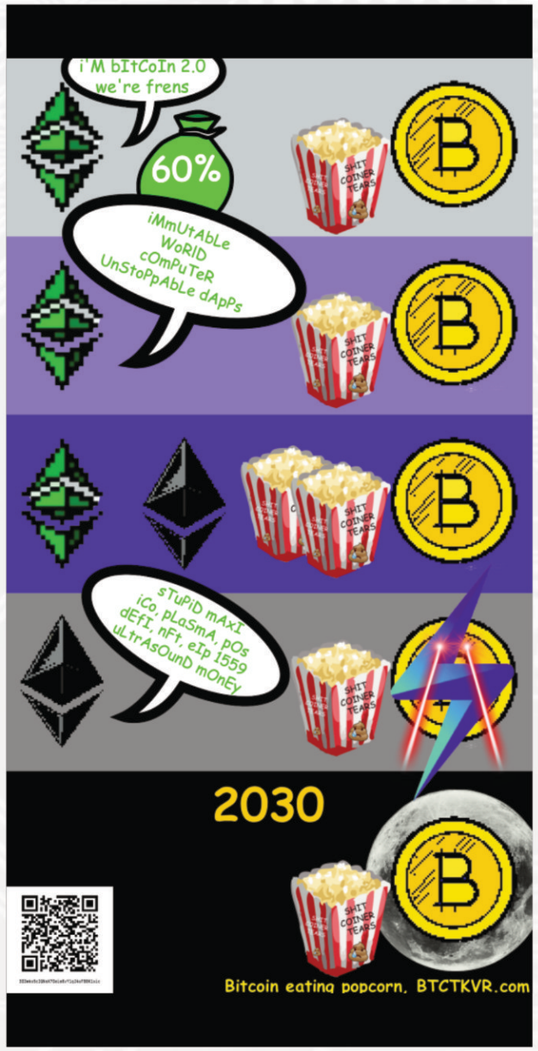
Yes, I'm a big Ethereum critic and I think its fundamentals are flawed beyond any kind of fixing. I also hate censorship.

But there's a silver lining to this story. I've decided to express my angsty feelings in a more creative way. So thanks to the silencing of r/ethereumfraud, I've decided to take a shot at creating a comic strip which reveals some of the ugly truths about the Ethereum project. Basically everything they don't want you to know, but in a small and easily-comprehensive shape.

While taking a shower, I came up with the "Bitcoin eating popcorn" concept – basically a stoic approach to all the temporary and ephemeral scams going on in the space. I'm also thinking about something related to the dogecoin and Elon Musk situation, and I'm pretty sure that it's gonna involve popcorn.

I'd like to dedicate this to Blockstream's Grubles and Leon, the fact checker (I think he was suspended from Twitter, but we miss him). Also, here's the stuff that the new mods of r/ethereumfraud are trying to destroy.

Hope you're going to like the 8bit style and historical approach to presenting facts. Bitcoin will always be eating popcorn as scams come and go. Also, it would be really terrible if this comic strip of mine ended up getting posted on r/ethereumfraud like a hundred times until the new mods get mad and ban everyone, wouldn't it?

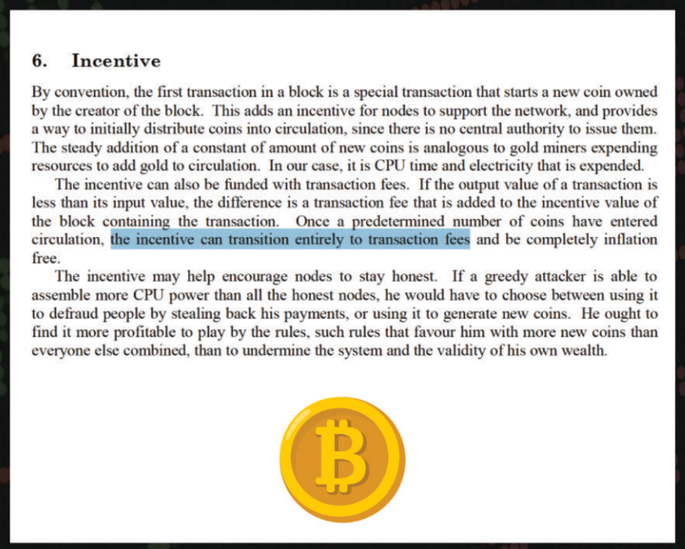


WASABI WALLET
BITCOIN WALLET WITH COINJOIN
NO DATA JUST PRIVACY
Open source, non custodial, privacy focused
Bitcoin Wallet for desktop.
New software coming soon:
WASABI 2.0
No minimum denomination
New CoinJoin protocol: WabiSabi
Completely revamped easy to use UI
so simple, your grandma can use it!
www.wasabiwallet.io



How to Pay Lower Bitcoin Transaction Fees (Full Guide)

Fees are an essential part of the Bitcoin economy. They help prioritize transactions and support miners with an extra incentive. And as the mining rewards get halved every 4 years, transaction fees are going to play an increasingly significant role in the security of the Bitcoin network. As Satoshi Nakamoto himself said in his 2008 whitepaper:



6. Incentive

By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.

The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.

The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

In other words, in order for Bitcoin to succeed as a project, the mining fees need to keep mining profitable. Furthermore, fees are also needed to keep the network censorship-resistant – as an irrefutable financial incentive, they eliminate political, geographical, and other types of criteria that may discriminate between transactions. As long as there is a fee to collect, miners will not have to undergo a selection or arbitrary prioritization of which transaction gets added to the next block and which one gets stalled.

But this doesn't mean that you should pay a lot or that you must always bid the amount required to have your transaction included in the next block. You have means to leverage this fee market according to your own time preference – so if you're not in a hurry, you can pay less and wait more for the first confirmation.

This article is meant to guide you towards confidently using a wallet which allows you to manually set fees, and also help you discover how Bitcoin can be used with minimal costs. Do your own research and you can save some precious bits by lowering your time preference and leveraging the mempool system in your own advantage.

If you're feeling like you can take the extra challenge, you can onboard the Lightning Network to always have smaller fees with instant confirmation times. At the end of the article I will provide a short guide on how you can get started.



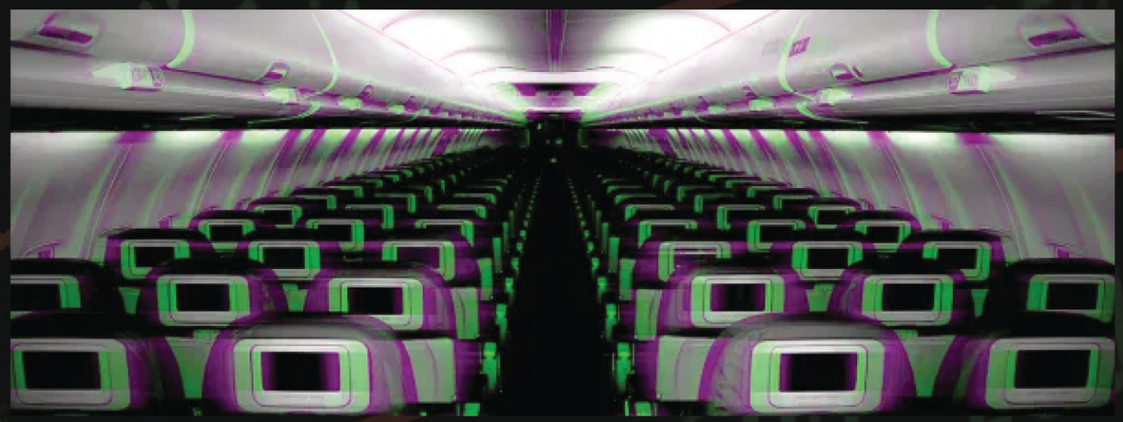
How do Bitcoin fees work and why are they sometimes high?

The answer is simple: Bitcoin transactions get stored in a public ledger that's divided into blocks. These blocks get discovered by miners that run complex computations, and validating nodes verify the miners' activity to make sure that their work is honest. But the available block space is limited and can only fit about 3000 transactions (though not all transactions are equal in complexity and size, so the number can vary). Under this framework of scarcity, we get a free market in which all participants bid to have their transactions included in a future block.

When will your transaction confirm? Well, that depends on how much you're willing to pay and how long you're willing to wait. So it's a matter of time preference. You can pay a very low fee if you're willing to wait for a few weeks, or you can pay the bitcoin equivalent of $10 to make sure that miners prioritize your transaction. Of course, the $10 example is only relevant as of March 2021 – as Bitcoin's valuation in USD increases, the same amount of bits will have a greater monetary value (hence the paid fees will also be "higher").

If this explanation is a little bit too difficult for you to understand, then think about airplane seats: each plane has a limited number of seats, so if you want to catch the next one you must always pay more than you normally would. When the seats for the next flight get scarce, you should expect to pay 2-3 times more to get on board. But if time is not a problem and you can afford to plan ahead, you're always going to pay less.

In the case of both Bitcoin and plane tickets, it all comes down to supply and demand. If the supply of block space is limited, then you should expect to pay more. If you're in a hurry to have your transaction confirmed, then you should also provide a greater incentive for miners to pick it up and write it in a block as fast as possible – hence a higher fee.





MINER PRIORITIZING BITCOIN TRANSACTIONS ACCORDING TO FEES

As a rule of thumb, you should never pay for the transaction fee more than 10% of the amount you're moving. And you probably shouldn't make a transaction on the base layer if the amount you're sending is lower than the fee you must pay (for example, send $1 when the fee is going to cost just as much). The same applies to centralized wire transfer services such as Western Union and Money Gram: if the amount is very low, you're going to get charged a fixed rate nonetheless; this disincentivizes small transfers.

So before you make your Bitcoin transaction, you should think about how much you're sending and how much you're willing to pay for the transaction to make it to the recipient. Then you should also check the state of the mempool.

Wait, what is the Bitcoin Mempool?

The mempool is the place where all unconfirmed Bitcoin transactions wait for confirmation. Depending on the fees they're set to pay, these transactions can wait in the mempool until the next block or for a longer amount of time.

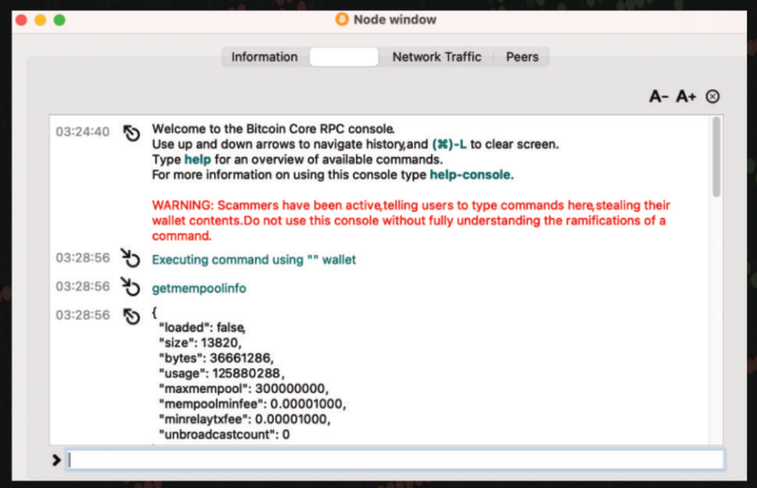
It's Bitcoin nodes that verify, store and broadcast these transactions across the network. When miners discover a new block, they take the ones that pay the highest fee and include them. And after the first block containing a transaction gets mined, every other block that gets added serves as another confirmation which ossifies existing transactions.

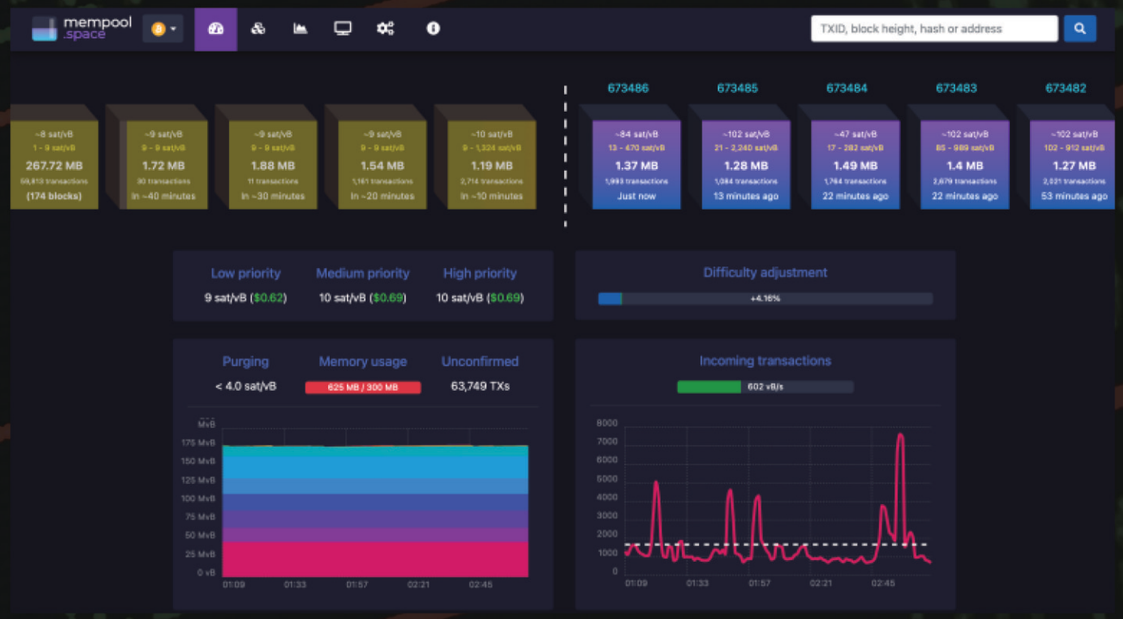
In other words, the Bitcoin mempool is like a purgatory for unconfirmed transactions. These transactions won't cross River Styx to get to the other side unless they pay a toll to the rower.

The ones paying a lower fee will stay on the boat (mempool) for a longer time.

Usually, nodes keep transactions in the mempool for a few weeks. But more recently, the infrastructure has improved significantly and various optimization has been made to increase the memory bandwidth of nodes. Libbitcoin developer Eric Voskuil explains a little bit how these optimizations work in this episode of the Bitcoin Takeover Podcast.

So even if it takes months, transactions won't get dropped (though, historically speaking, it's very unlikely for this to happen). Bitcoin developers have created two ways to mitigate very low fees: RBF (replace by fee, which allows participants to bump the fee of a transaction), and Child Pays for Parent. You can find out more about this situation from Andreas Antonopoulos' recent video on the topic.





Where and how do I watch the Bitcoin Mempool?

A Bitcoin transaction mempool exists on every node. Depending on the decisions of each sovereign node, transactions get stored or dropped according to a threshold for maximum storage and minimum relay amount. Essentially, there is a very high chance for nodes to have identical mempool – especially if the settings in the Core/qt client are default.

So if you're running a full node, then you can easily check what's going on with a few simple console commands. After opening the console, type in getmempoolinfo and you will see details about the size of the mempool in bytes, as well as the minimum fee you must pay to get your transaction confirmed in the next block.

For more specific verifications, you can type in getmempoolentry, followed by your transaction's ID. For example, if Satoshi Nakamoto wanted to see his historic transaction to Hal Finney in the mempool, he would have had to type getmempoolentry f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16.

But let's assume that you're not running a full Bitcoin node or that you're too lazy to use it for such information. It may be that you also need more information about the median fee in previous blocks and you are better at processing visual data. Well, you're in luck: mempool.space is the perfect resource that will help you determine how much you want to pay for the Bitcoin fee.

The graphic interface on mempool.space doesn't just tell you the recommended fee. It simultaneously displays information for which you would have had to type in lots of console commands. You get to see the fees that users paid to have their transactions included in previously-mined blocks, and you also receive an estimation that's based on existing mempool entries. Furthermore, you get an estimation for priority which helps you determine how much you're willing to pay according to your time preference.

Yet one of the major drawbacks of this kind of estimation is that unforeseen events can happen. Sometimes blocks get mined faster or slower, depending on the current hashrate. If the blocks get mined fast, then the transaction fees will temporarily lower. Conversely, if it takes a longer time to mine a block, then you will also see more high-fee transaction appearing and therefore slowing down the confirmation of all the others that pay less.

In spite of these variables, you should still be able to make accurate estimations to help you save money on Bitcoin transactions. Also,

mempool.space is not the only resource: you also have mempool.observer and the good old Johoe's Bitcoin mempool size statistics (which bitcoiners have been using for years before friendlier options came along).

Keep in mind that mempool.space also works as a blockchain explorer. So if you paste your transaction ID in the search box that you find in the top right corner, you will see the state of your transaction and an estimation on when you get the first confirmation.

How To Set Bitcoin Transaction Fees Manually (in Bitcoin Core, Wasabi, Blockstream Green & Blue Wallet)

Unfortunately, many Bitcoin wallets will not allow you to set the fees yourself. On the grounds of it being "too hard" and "for power users", they will make the judgment themselves. This means that lots of popular wallets (most of them belonging to exchanges) will try to include your transaction in the next Bitcoin block.

Sometimes it's good, as you withdraw without having to worry for longer than 10 minutes. But if you understand that Bitcoin is a global internet network and you know that all transactions get stored in the mempool until miners pick them up, you will never worry that your coins got "lost".

It may be that the newbie-friendly wallets are keeping users under a veil of ignorance instead of providing education on how they should use their bitcoins to maximize sovereignty. But then again, lots of these services are custodians of your coins and they may even engage in some fractional reserve practices (meaning that not all customers can withdraw at the same time, as the company has used the coins to diversify in other assets).

Let's not open that can of worms and get back on track. Setting your Bitcoin transaction fees manually should be available in all wallets. But in this article I will present 4 wallets: two for desktop and two for mobile phones.

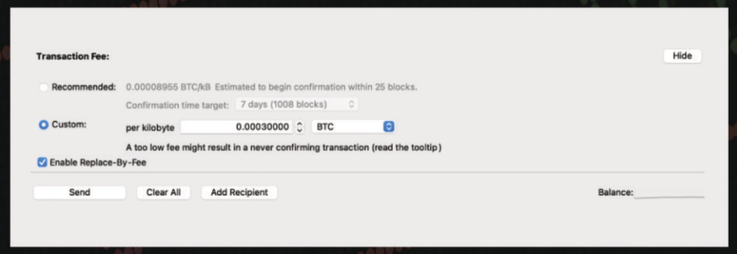


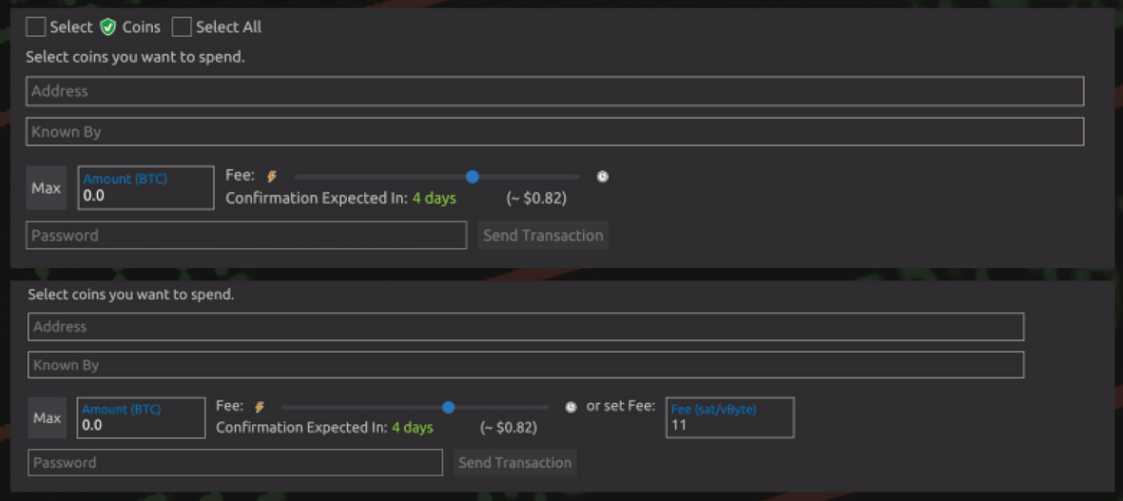
A. Setting Custom Transaction Fees in Bitcoin Core

In Bitcoin Core (the full node wallet you should be using on your computer), the "Send" tab has an entire section that's dedicated to transaction fees. Since fees are essential for maintaining the security of the Bitcoin network, they get the royal treatment they deserve. So you can either use the built-in estimation or use the research you've done yourself on mempool.space. But since the automatic estimation is only based on your nodes' own observation, it's a lot safer to set the transaction fee yourself.

Notice that the unit measurement is BTC, bits, or satoshis per kilobyte. So if you're used to a measurement such as sats/byte, then you're going to have to multiply by 100 to get to the kilobyte level. Therefore, if you were going to type in 3 sats (or 0.03 bits) per byte, then you should write 300 sats/kb or 3 bits/kb. To better understand denominations, read this article.

Also, take into account the measurements on mempool.space. Your safest bet to save on fees is to use the "Low Priority" recommendation. You can also go lower, but during bull markets you shouldn't go lower than 2 sats/byte.





B. Setting Custom Bitcoin Transaction Fees in Wasabi Wallet

Another desktop wallet that makes it easy to set transaction fees manually is Wasabi. By default, Wasabi uses time preference as the fundamental unit of measurement and also does the automatic conversion to US dollars. So instead of measuring confirmation time in Bitcoin network blocks, you get actual estimations in hours, days, and weeks.

But if you go to the "Settings" menu and enable the "Manual fee entry" option, you will also be able to type in a fee according to your own observation on a service such as mempool.space. The added complexity only consists of an extra box which allows you to type the fee amount.

Notice that unlike Bitcoin Core, the unit of measurement is per byte, as opposed to the kilobyte. It's a major difference, as in the latter case you must multiply your amount by 100. In this regard, Wasabi keeps it simple: if you want to pay 5 sats/byte for your transaction (which in this market would probably confirm in about a week), then you can definitely do it.

Find out more about how Wasabi works from this interview with the wallet's creator, Nopara73.

C. Setting Custom Transaction Fees in Blockstream Green and Blue Wallet

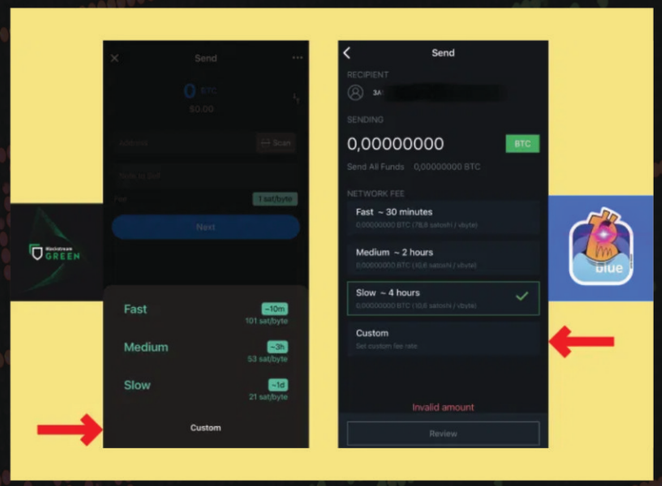
It's fascinating how Bitcoin wallets get named after colors, isn't it? I've chosen these two because they are some of the most scrutinized and popular mobile wallet options. They are both available on Android and iOS, and they feature lots of interesting power user features which range from multisig setups to connecting your own full node or hardware wallet.

But if you want to set a custom transaction fee in Blockstream Green and/or Blue Wallet, then you're only one touch away. In the "Send" menu, after you set the amount, you will see an interface which recommends you to use three different types of fees according to time preference (notice how this approach is very popular). But at the bottom you can also opt to have your transaction sent with a fee that you set yourself, based on your own research on a website such as mempool.space.

In Blockstream Green, you must first type, paste, or scan the recipient's Bitcoin address. In Blue wallet, everything is on the same screen. Also notice that, despite the fact that I've taken the screenshots just a couple of minutes apart, the estimations are different. And there are two reasons for it: firstly, it's likely that a Bitcoin block got mined in the meantime and the estimation for fees has adjusted accordingly; secondly,

we should remember that these estimations are based on the observation of the node which provides blockchain information, so there is room for a slight relativity.

Usually, these wallets recommend higher Bitcoin fees by default to avoid unpleasant situations where they deal with angry users who contact support. But if you know what you're doing and have analyzed the mempool in advance, you can definitely save some precious bits – especially if you're not in a hurry and you don't mind if the transaction receives its first confirmation a little later.



Switching to the Lightning Network

If you constantly want to pay less than a cent for your transaction fee and have it confirmed instantly, then you should consider switching to the Lightning Network. For microtransactions, it's very hard to beat and it also have better privacy than the Bitcoin base layer.

Sure, using Lightning requires opening channels and for these you have to pay on-chain transactions. But for the price of one on-chain transaction you can perform thousands of low-cost Lightning transactions (as long as your channels remain open and there is a route to get you to the destination). And when you want to take your bitcoins to the main chain, you close all the channels (a series of actions that will also get charged as base layer transactions with higher fees).

If you make transactions frequently and need instant confirmations, then you should definitely get on Lightning. But if you're a HODLer who makes only a few transactions every month, then it's probably better to stay on the main chain and pay higher fees – it's also the more secure method.

Using the Lightning Network requires a Lightning node. And you can either set up your own or use somebody else's (trust a custodial service). Ideally, you should get a low-powered computer like a Raspberry Pi and set it up to be your 24/7 Lightning node (since it doesn't consume a lot of energy and it's quiet, you won't notice the difference on the electricity bill or while you sleep). Here's a guide to get you started with an investment of about $250.





You can also buy a Lightning node from companies such as Fulmo, Lightning in a Box, myNode, and Nodl. But for the purpose of understanding how Bitcoin works, it's better to do it yourself by following a simple guide. You're also likely to get support from the community if you get stuck, and this journey will feel rewarding as soon as you realize what you've built on your own. But then again, feel free to buy "node in a box" solutions if you don't have the time or willingness to experiment yourself.

If you'd rather trust someone else with your Lightning channels and funds, you have services such as Tippin.me, Bottle Pay, Blue Wallet, and Wallet of Satoshi. Tallyco.in and Blue Wallet also let you connect your node to the service, while Bitrefill allows you to rent Lightning channels to send and receive payments (they're called Thor).

Jack Mallers, lead developer of Strike, has also found a way to send Lightning transactions around the world by charging his bank account. So you should definitely check out his work if you want to see what the future of Bitcoin and Lightning may look like. This is only part of the reason why Mallers was included in Bitcoin Takeover's "Top 7 Bitcoin Wallet Developers of 2020" article.

Also, Breez offers a service which opens Lightning channels for free (at least for the time being, until they build a customer base). Under an intuitive user interface, the affairs concerning inbound capacity for your channels happens behind the scenes. This means that you don't have to worry about the technical aspects involved in using the Lightning Network. If you'd like to try Breeze, it's available on both the iOS AppStore and the Android Google Play.

Lightning is definitely a great option that will get more traction when the number of Bitcoin users increases, the price becomes less volatile, and there is more merchant adoption to accept payments. So we shouldn't be surprised if every store in the shopping mall runs its own Lightning node on a Raspberry Pi. If the fees really matter to you and you transact frequently, then you should try Lightning.

Acknowledgments: special thanks to Matthew Haywood for suggesting improvements to the article. He identified a few typos, provided further technical assistance to remove some ambiguities, and helped make this article truly evergreen. You can also thank him by following him on Twitter and listening to his interview on the Bitcoin Takeover Podcast (S5 E9).

THE BITCOIN TAKEOVER PODCAST



Listen to the Bitcoin Takeover Podcast on Sphinx, Breez & More

For longer than two years, the Bitcoin Takeover Podcast has been available on all the traditional platforms: Apple Podcasts, Spotify, Google Podcasts, Breaker, and every other aggregator which took the RSS feed and made use of it on a proprietary player.

But now the transition to podcasting 2.0 is complete: after successfully setting up my Lightning node and receiving some advice from Blockstream product manager Matthew Haywood (whom you can hear in S5 E9), I've finally managed to get Bitcoin Takeover listed on Podcastindex.

All it took was registering with the node, submitting the show's RSS feed, and confirming an e-mail address – no KYC, no passport scanning, no face ID, no fingerprint authentication. This is part of the new internet, where submitting personal data is mutually undesirable and gets avoided as often as possible.

So why is Podcastindex such a big deal? In the Bitcoin space, it's the gateway to getting added to the Sphinx chat application, as well as the Breez Lightning wallet. The people who are interested in listening to podcasts can do it from the interface of an app which facilitates the access and also makes it easy to send payments. Essentially, the monetization scheme which involves the Lightning node involves making podcast listeners pay for the time they spend listening: for each minute, they drop a few bitcoin fractions.

But there's more to the picture than meets the eye: every podcast added on Podcastindex also gets listed on a plethora of mobile apps. From the podStation Chrome browser extension to the Podcast Guru Android app, there are over 31 new places where Bitcoin Takeover can get discovered.

Sphinx and Breez are also rising in popularity among bitcoiners, so they should not be neglected. As a matter of fact, if you would like to join the Bitcoin Takeover tribe on Sphinx, you can follow this link or else scan the QR code below. Thank you for continued support and I hope that you will keep on enjoying the content that I create during this new era of podcasting.



VAULTORO
DIRECT

TRADE BETWEEN CRYPTO
AND PRECIOUS METALS

Secure your crypto gains without having to rely on fiat or banks, with physical Gold and Silver.
Be ready to buy the dip, trading back to Bitcoin, Ethereum and a variety of ERC20 tokens.
Vaultoro allows you to trade with other user or use our Direct service.
Since 2015.

INSTANT SETTLEMENT
Buy Gold and Silver in seconds.

ALLOCATED PRECIOUS METALS
Stored in your name, as your property in a high security vault in Switzerland.

AVAILABLE 24/7
Buy and sell physical gold and silver after the traditional markets are closed.

Vaultoro™
The European Alternative Asset Exchange

VAULTORO.COM



We need to start denominating bitcoin in bits

Most of us will never own a whole bitcoin – and it's perfectly fine. It's not like all gold investors can or should buy an entire bar or bullion. But when you're running away from arbitrary inflation which severely damages your purchasing power, every quantity counts. The name of this game is steady accumulation, and each one of us should do it at their own pace.

Today's high bitcoin price is the result of programmed scarcity and 12 years of increasing demand. But the best part about it is that we're just getting started, as millions of realize that their money can beat hedge funds, investment firms, and even banks.

Bitcoin is very divisible and right now anyone can buy a few fractions and steadily accumulate amounts that will eventually lead to their financial sovereignty. For the last few years, the standard has been the satoshi (1 bitcoin = 100 million satoshis). But dividing to 100 million is far from being the most intuitive approach, and the cost of 1 satoshi in US dollars is too insignificant to feel tangible.

This is why I argue that we should use bits – where 1 bitcoin = 1 million bits.

As I write this article, 1 bit can be bought on bitcoin exchanges for approximately 3.7 US cents. Yes, that's $0.03, with a chance to hit $0.04 later in the day if the Elon Musk effect persists.

The quantity might seem insignificant, but then again so did 1 bitcoin in 2009. At the same time, it's tangible enough to get acquired with physical money. You can find 3 coins of one cent each and trade them for 1 bit (or 100 satoshis) on the Lightning Network. That's not something you can do with a satoshi (the 100th part of a bit).



Right now, 3 cents is cheaper than dogecoin and pretty much on par with XRP. If people thought about bits instead of bitcoins, chasing price goals would be easier. The idea of pumping 1 bit to $1 sounds a lot more feasible than taking bitcoin to $1 million.

Yes, it implies the same effort. But it no longer seems like only institutions or financial firms can do it – the average folk can chip in and purchase an amount which counts and makes a difference. Wasn't "vires in numeris" (power in numbers) one of the most popular bitcoin slogans?

The reason why bits were abandoned as a denomination in favor of sats is that the metric system was added on top. Who cares about milli, centi, deci, and deca bitcoins? It sounds confusing to most of the English speaking world which uses the Imperial system, and it's an overall terrible way of communicating value.

Table of all units

This table is intended to include all well-defined units of bitcoin value, including less common and niche units.

Unit	Abbreviation	Decimal (BTC)	Alternate names	Info
Algorithmic maximum		20,999,999.9769		Calculations#
tam-bitcoin		2,814,749.76710656		1,0000,0000 tonal
mega-bitcoin	MBTC	1,000,000		Rare in context
kilo-bitcoin	kBTC	1,000		Rare in context
hecto-bitcoin	hBTC	100		Rare
Initial block subsidy		50		Until block 210000[1]
bong-bitcoin	ᵇTBC	42.94967296		1,0000 tonal
Current block subsidy		6.25	block	As of halving day 2020, block 630000
deca-bitcoin	daBTC	10		Rare
mill-bitcoin	ᵐTBC	2.68435456		1000 tonal
bitcoin	BTC	1	coin	SI base unit
san-bitcoin	ˢTBC	0.16777216		100 tonal
deci-bitcoin	dBTC	0.1		Rare
ton-bitcoin	ᵀTBC	0.01048576		10 tonal
centi-bitcoin	cBTC	0.01	bitcent	Formerly frequent[2]
milli-bitcoin	mBTC	0.001	millibit, millie	Occasional
bitcoin	TBC	0.00065536		Tonal base unit
bitcoin-ton	TBCᵀ	0.00004096		0.1 tonal
bitcoin-san	TBCˢ	0.00000256		0.01 tonal
micro-bitcoin	µBTC	0.000001	bit	Frequent
bitcoin-mill	TBCᵐ	0.00000016		0.001 tonal
		0.0000001	finney[3]	
bitcoin-bong	TBCᵇ	0.00000001		0.0001 tonal
	sat	0.00000001	satoshi	Blockchain value
	msat	0.00000000001	millisatoshi[4]	Payment channel value

In everyday language, we use hundreds, thousands, and millions to express quantity and significance. Telling someone that you own a deci-bitcoin sounds less impressive than telling them about your hundred thousand bits or ten million satoshis. We need to get rid of this overcomplicated system and make it as elegant and comprehensive as we can.

Why bits are better than satoshis

Here's my argument: bits are the best unit of account for the base layer (where even a 1 sat/byte transaction costs about 140 sats, or 1.4 bits), while sats are best suited for the Lightning Network (the place where microtransactions take place).

A bit is less of a dust amount than a satoshi. If you own about 2 bits on an exchange, you will most likely be able to pay for a transaction fee (which takes a long time to validate) and move the remaining amount to your own wallet.



We should also consider the branding: it's easier for a Bitcoin newbie to understand that 1 BTC has 1 million bits. Tell them about "satoshis" and they will most likely feel confused about the whole situation. Then ask them to multiply or divide by 100 million and it's even harder.

Yes, satoshis are part of the Bitcoin code and they are inevitable. But before we see bitcoin hit $1 per satoshi (which seems to be the goal of many people), we're gonna have to get to $1 per bit first. And the latter is more attainable and can train our HODLing muscles a lot better than something which appears to be impossible at this point.

At today's rate, getting 1 bit to $1 implies a 27x price increase. This sounds attainable for the everyday person who puts $100 of their savings to buy some bitcoin. On the other hand, getting to $1/sat implies a 2700x increase. To a lot of people, this sounds unreasonable – even if we believe that it will eventually happen.

It's all about psychology, and I would argue that contributing to a mission whose goal is to get 1 bit to $1 is a lot more social and involving than telling people to become "satoshi millionaires". The former is about team work and working towards a common goal, while the latter entails the same consumerism that a lot of people resent. I'd argue that we need to keep it competitive and set realistic goals that we can actually achieve.

And as I previously mentioned, in most fiat currencies you have physical money that can be used to buy bits. You can buy a bit with the fiat in your pocket: US dollar cents, Canadian dollar cents, British pound pennies, and euro cents, Turkish liras, Chinese yuans, Japanese yens, Romanian lei, Zimbabwean dollars, Algerian dinars, and so on.

Can you do the same with satoshis? Not with lots of national currencies. So it's better to tell people about something that they can buy with money they hold in their physical fiat wallets. It gives them a sense of conversion, as opposed to 0.00037 USD (the current price of 1 satoshi, for which we have no way to express in our common financial language.

We also need to consider volatility: with bits, the swings appear to be a lot less wild than with bitcoin. So if the price goes down from $50.000 to $40.000 and you hold 100 bits, your relative purchasing power went down by only $1 at today's rate. You could have done a lot worse if you invested in some "backed" national currencies.

If my arguments haven't convinced you, then you should also look into Adam Back's pitch from December 2020. While I have taken inspiration from his tweets, I've adapted the information to some empirical observations that I've made. And I think that bits are a better unit of account for the next few years – at least when we refer to the Bitcoin base layer.



Okay, so you want to use bits as the unit of account for bitcoin. What's next?

Now that I've identified a way to make bitcoins more attractive to the average retail investor, it's time to spread the education and lobby to exchanges. We need to convince them to list "bits" as an option, so more people can chip in.

It makes a lot of sense for "bits" to be the preferred way of expressing smaller bitcoin units, but this time around we need to make sure that we keep the metric system prefixes away. 100 bits sound more appealing than 10.000 sats, and the fact that they can be bought for the equivalent of $3.7 at today's rate makes the trade sound a lot more intriguing.



You're not just purchasing fractions from a bitcoin, but you're also partaking in a community plan to increase the value of that bit to $1 or more. And if you buy $100 worth of bits and the price of Bitcoin goes up or down by 20%, your position only gets affected by $20 – a lot less wild than buying GME stocks or some Wall Street asset which is a lot more volatile. It's easier to think in bits, as the gains and losses are tangible and have corresponding physical representations of fiat money.

1 bitcoin = 1 million bits = 100 million satoshis. We'll use bits until we get to the dollar parity (1 bit = $1), and then switch to satoshis if it gets more convenient. But until then, we have work to do. There will only exist 21 quadrillion bits and we need to help everyone grab some before it's too late!

Jimmy Song's BIP 0176

In the midst of the phenomenal December 2017 price increase, Bitcoin Core developer Jimmy Song wrote BIP0176 to standardize bits as the preferred unit of account. This way, users would send small amounts with greater ease and also make instantaneous conversions to fiat money.

Song suggested that the term "bit" already has a monetary meaning which precedes the computer science unit of measurement for data, where 1 bit is the eighth part of a dollar. But contrary to the suggestions presented in this article, he accepted the metric system by acknowledging that the bit and the micro bitcoin (μBTC) can remain synonymous in the Bitcoin lexicon.

It's definitely an interesting proposal which reflects an early concern of the five-digit bitcoin prices in USD. And today, the wallet section of Bitcoin Core optionally allows users to send amounts and pay transaction fees while accounting in bits.





It's Time to Replace BTC-USD with BTC-Gold

As we watch the price of bitcoin hit new all-time highs against the US dollar, it's hard not to feel like this pairing has lost all meaning. Yes, the demand for BTC is growing among companies and hedge funds, and we can say that the project is finally well-understood by mainstream finance. And yes, it's nice to watch Bitcoin surpass the market cap of companies such as Facebook, Samsung, Alibaba, Berkshire Hathaway (rat poison squared, anyone?), and Tencent.

But lately, the USD has lost value against most fiat currencies. The Japanese yen? It seems like every month brings a new USD-JPY low. The euro also looks a lot better than the dollar, as the USD-EUR chart is abysmal for the American economy. And if you look at the Chinese yuan, the situation is even worse.

Economists can blame the situation on the covid19 pandemic, but the truth is that other fiat currencies have performed better than the US dollar under similar circumstances. The fact that the Biden administration is going to print more money for stimulus checks (and the amount estimated is 3 trillion dollars, so each citizen can get about $2000) definitely doesn't help with preserving the value of the gold-decoupled Bretton-Woods reserve currency.

Every sign available, from the financial behavior of investment funds to the projected political decisions, suggests that the dollar is going down hard. With the exception of patriotism or blind trust in the soft or military power of the US government, I can't think of any arguments to feel bullish about the USD.



When I wrote the article "Bitcoin Will Soon Reach New All-Time Highs – But USD Valuation Becomes Irrelevant", I honestly did not expect the events to unfold so quickly. But here we are, watching how a 12 year-old decentralized digital currency makes Uncle Sam look weak and incompetent.

It's time to start comparing Bitcoin with Gold.

Just because a fiat currency has a poor performance and shows very few signs of recovery doesn't mean that we should look for another fiat currency to better understand the price of 1 bitcoin. At this point it's clear that the fiat experiment is collapsing. It seemed like a terrible idea in 1971 when the Nixon administration started it, and now we can observe why it failed.

Rank		Name	Ticker	Market Cap	Price	Today	7d	Price (30 days)
1		Gold	GOLD	$11.707 T	$1,843	-3.69%	-3.08%	
2		Apple	AAPL	$2.219 T	$131.92	0.76%	-0.58%	
3		Saudi Aramco	2222.SR	$2.046 T	$9.31	0.29%	-0.29%	
4		Microsoft	MSFT	$1.652 T	$218.56	0.12%	-1.74%	
5		Amazon	AMZN	$1.59 T	$3,169	0.22%	-2.69%	
6		Silver	SILVER	$1.372 T	$25.11	-7.89%	-5.33%	
7		Alphabet (Google)	GOOG	$1.203 T	$1,785	-0.12%	1.90%	
^1	8	Tesla	TSLA	$835.89 B	$881.84	8.06%	24.96%	
^1	9	Bitcoin	BTC	$767.75 B	$41,289	4.92%	40.74%	
v2	10	Facebook	FB	$759.09 B	$266.51	-0.83%	-2.43%	



Historically speaking, gold is the most stable currency. Not only that, but it has the largest market cap in the world (you know, measured in US dollars). To better strengthen Bitcoin's role as digital gold, we should act accordingly and point out when major swings occur.

Sure, bitcoin is bound to have more volatility while the number of people trading it every day across mainstream financial markets is still lower. But we need to get there.

The time has come to finally leave the US dollar in the dust and show the world how the inconveniences of the gold standard can get fixed under a bitcoin standard.

And if you're interested in trading bitcoins for gold bars and vice versa, check out Vaultoro. If we're ditching fiat, we should only focus our attention on hard money. And with Vaultoro, you can even have the gold amounts shipped to your house, or benefit from the insurance and Swiss security. They've been around since 2015, and their CEO Joshua Scigala is an OG bitcoiner who has participated in two Bitcoin Takeover Podcast episodes.

Use the URL vaultoro.com/bitcointakeover and start trading today! While I don't benefit directly from your sign-up via referral link, it helps me get sponsored with the podcast and the content that I create. Just keep in mind that trading involves risks, this is not financial advice, and you are responsible for your own decisions.





Companies Can't Wait to Buy Your Bitcoins To Opt-out from Inflation & Taxation

Bitcoin has finally gotten to the point where companies truly understand its value proposition and the political context provides all the incentives to dump fiat. It has taken the project almost 12 years to finally find its place in mainstream markets, and this time around it really seems like the situation is going to be different.

Maybe that the community infighting during the scaling debates didn't help, and the fact that early bitcoiners were trying to replace Visa with on-chain transactions was unrealistic in regards to what Bitcoin is. But these failed experiments and the bear markets that followed them have only made Bitcoin more resilient and have helped everyone truly understand its nature and purpose.

In 2020, hedge funds have made a historic step in accepting BTC as a reserve asset. Legendary investor Paul Tudor Jones has also contributed to the legitimation of Bitcoin across mainstream markets. Then came companies such as Square and Microstrategy. And after this, a valuable realization came around: Bitcoin is the perfect asset to store value for multiple years.

By holding Bitcoin, companies can opt out from inflation & taxation, then borrow fiat against it

In the United States and most jurisdiction, there is no tax involved in buying bitcoins and holding them – you only pay capital gain taxes when you decide to sell for fiat. But in a time when fiat currencies lose value to inflation, holding cash reserves is a terrible idea – or as Microstrategy CEO Michael Saylor put it, "like sitting on a melting ice cube".

So when a company purchases BTC, it's a long-term move that's meant to protect the assets against the unpredictability of politics and financial markets. Sure, Bitcoin can go down in market valuation and is highly volatile. But it's the only "bubble" in history which keeps on re-inflating every few years due to the diminishing supply of new coins and the increasing demand for BTC. Bitcoin is disinflationary thanks to its mining issuance program, and will become completely deflationary in 2140 when the last mining reward gets collected.

In a world where the fiat experiment shows signs of failure, it makes very little sense to hold reserves in infinitely inflationary currencies. If you want to maintain your purchasing power, you must turn to scarce assets that are also in high demand.

Historically, precious metals such as gold and silver fulfil the role of allowing people and companies to hedge against fiscal policy and preserve wealth. But Bitcoin is more portable, easier and quicker to trade, cheaper to verify, and is also provably scarce. By running a node, you have information about everything that takes place on the Bitcoin blockchain – you know all about transactions, you can verify the validity of incoming coins, and you can permanently check the existing supply of BTC to make sure that the network functions the way it was designed.

Now here's yet another interesting fact: you can keep your scarce digital money by lending fiat against your BTC. There are many services which allow you to do it (Celsius, BlockFi and Nexo are only three of them), and it's a great way to survive in the fiat economy without having to sell your bitcoins. Furthermore, you don't pay any taxes if you lend money. So this is extra convenient for companies that hoard Bitcoin reserves and sit on them for multiple years.

Regular people need Bitcoin for censorship resistance and wealth protection. Companies need Bitcoin for world domination.

If you accumulate 1 BTC, it's likely that you dream of buying a nice house and a car. Anything to improve your living standard and help you enjoy your life a little more.

But if you're a company holding bitcoins, then your goals should be a lot more ambitious and transcend the fiat status-quo. In a Bitcoin standard, a company which owns large reserves is going to dominate markets and play a major role in political decisions.

So if your goal is to exchange your bitcoin for a Tesla, then you should probably think twice. There are only so many bitcoins, they are in high demand during these troubled times, and you may get a better deal in the near future when more companies wake up and decide to put their reserves into Bitcoin.

The more people HODL and the stronger their conviction is, the more significant their role is going to be in the post-fiat economy. But in the end, it all comes down to your expectations and your time preference. Some people play the long game, others just want to enjoy the moment. There is no wrong approach, just different goals. Nonetheless, you've been warned: they're coming for your bitcoins!





At 12 Years Old, Bitcoin Is Turning Into a Rebellious Teenager

Bitcoin came into the world with a very quiet and humble whisper that very few people heard and even fewer understood. Its birthmark is a political statement against bank bailouts and their arbitrary nature, and its goal is even more ambitious: to separate money and State.

On its 12th anniversary, Bitcoin is roaring – and it reveals the tendencies of a rebellious teenager. Given all the insults that it had to take over the years, it's only normal to strive to prove all critics wrong. Mainstream economists called it a Ponzi, a pyramid scheme, and a bubble. As a reaction to these claims, Bitcoin only became more decentralized and saw an increasing demand across global markets.

At the same time, Bitcoin has a long history of being misunderstood or feeling pressured to change to fit someone's agenda. Even some of its so-called "friends" said it was too slow and tried to undergo drastic interventions to modify its properties. But those who did understand Bitcoin have found ways to allow it to flourish without compromising its qualities. Real friends don't try to change you, but help you improve.

Today, hedge funds and investment firms consider Bitcoin to be their new "golden" asset – and they find this partnership mutually-convenient, as Bitcoin can help them run away from inflation and taxation.

```
00000000  f9 be b4 d9 1d 01 00 00  01 00 00 00 00 00 00 00  |................|
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000020  00 00 00 00 00 00 00 00  00 00 00 00 3b a3 ed fd  |............;...|
00000030  7a 7b 12 b2 7a c7 2c 3e  67 76 8f 61 7f c8 1b c3  |z{..z.,>gv.a....|
00000040  88 8a 51 32 3a 9f b8 aa  4b 1e 5e 4a 29 ab 5f 49  |..Q2:...K.^J)._I|
00000050  ff ff 00 1d 1d ac 2b 7c  01 01 00 00 00 01 00 00  |......+|........|
00000060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 ff ff  |................|
00000080  ff ff 4d 04 ff ff 00 1d  01 04 45 54 68 65 20 54  |..M.......EThe T|
00000090  69 6d 65 73 20 30 33 2f  4a 61 6e 2f 32 30 30 39  |imes 03/Jan/2009|
000000a0  20 43 68 61 6e 63 65 6c  6c 6f 72 20 6f 6e 20 62  | Chancellor on b|
000000b0  72 69 6e 6b 20 6f 66 20  73 65 63 6f 6e 64 20 62  |rink of second b|
000000c0  61 69 6c 6f 75 74 20 66  6f 72 20 62 61 6e 6b 73  |ailout for banks|
000000d0  ff ff ff ff 01 00 f2 05  2a 01 00 00 00 43 41 04  |........*....CA.|
000000e0  67 8a fd b0 fe 55 48 27  19 67 f1 a6 71 30 b7 10  |g....UH'.g..q0..|
000000f0  5c d6 a8 28 e0 39 09 a6  79 62 e0 ea 1f 61 de     |\..(.9..yb...a.|
000000ff
```

Even regular folks have understood that Bitcoin protects their wealth a lot better than any government, thanks to the high network security and due to the arbitrary nature of private property protection and confiscation.

So we shouldn't be surprised if 12 year-old Bitcoin rebels against everyone around. The line between allies and foes is still thin. Some critics some turned into believers, while some supporters have turned into annoying foes. Even though it's clear what

Bitcoin is and what it's trying to accomplish, there are still people who disagree with the mission or think it should play out differently.

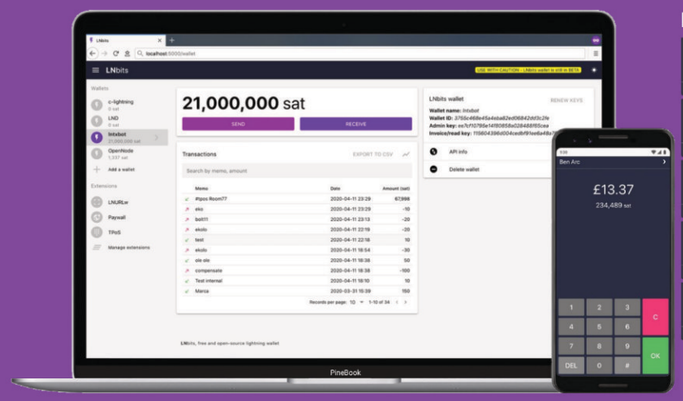
What we know for certain is that everything is set in place for Bitcoin to rise. Against all odds, in spite of all critics, and without any mercy or concern for non-believers. On January 3rd 2009, Satoshi Nakamoto has released Bitcoin to the world with a very clear mission. And at this point, Bitcoin the teenager seems a lot more likely to succeed than to fail. Fiat money and central banking, your days are numbered. Happy 12th birthday, Bitcoin!

If you enjoyed this article, check out the piece that I wrote on Bitcoin's 10th anniversary in 2018: "At 10 years old, Bitcoin is a wunderkind who's fighting for our freedom".

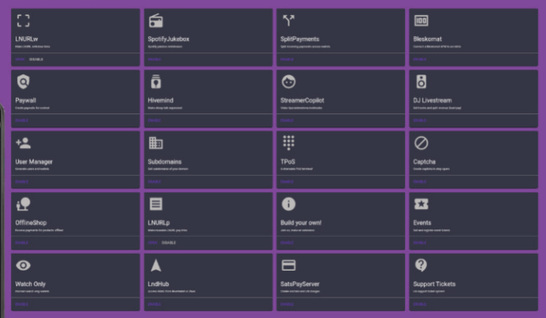


LNbits

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



LNbits extensions:



Free sats!
(Scan with a bitcoin lightning wallet)

Coinflip!
(Scan with a bitcoin lightning wallet)

LNbits can be used as:

- Community banking/custodial solution
- Accounts system, each wallet with their own API keys
- Extendable platform using LNbits simple extension framework
- Part of a development stack for a bitcoin service
- Your own branded lightning wallet
- An insta-wallet system

LNbits can run on:

RASPIBLITZ Clightning LND
LNPay.co LNTXbot myNode
opennode spark Umbrel

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



LISTEN ON

BITCOIN-TAKEOVER.COM/AUDIO Breez YouTube


LNbits
WASABI WALLET
Vaultoro
Crypto Commodities Exchange
Start9
BTCTKVR
POWERED BY
Bitrefill
Mallorca Blockchain Days
TREZOR