Table of Contents

Foreword 04

How I Almost Got Rich Mining Bitcoin on SlushPool for a Month 06

The 8 Editions Of The First BTCTKVR Magazine 15

5 Reasons You Should Run Your Bitcoin Node on a Raspberry Pi 4 32

Elon Musk Doesn't Understand Decentralization — But You Should 38

The 3094 Bitcoin Theft Which Led To The Creation of The Trezor 46

Why Bitcoiners Should Play Final Fantasy X 51

Calling Bitcoin a NSA/CIA Project Is Disrespectful to Cypherpunks 54

Comic Strip: Bitcoin Eating Popcorn #2 60

How to Hide Your IP Address: VPN vs Tor 65

DIY Hardware Wallets, Part I 81

DIY Hardware Wallets, Part II 88

The Privacy Benefits of Taproot 96

Bitcoin NFTs On Counterparty 101

Preview: BTCTKVR Podcast Season 10 112

Foreword

The first BTCTKVR magazine was an unlikely hit: with 442 physical copies delivered all around the world, a few dozens more printed independently by open source enthusiasts, and over 1400 digital downloads in 2021, this one-man project exceeded all expectations. Furthermore, thanks to the efforts of Duck Avenger and Roberto Scott, some of the evergreen articles have been translated into French and Spanish. Later in the year, you should look forward to physical releases of their admirable work.

So how am I supposed to follow the success of the BTCTKVR magazine? In theory, it's simple: all I have to do is write longer and more in-depth articles on topics that bitcoiners find interesting (sovereignty, privacy, cypherpunk culture, collectibles, and video games), feature more practical guides and comparisons, increase the number of pages, and print it all on higher quality paper. In practice, it can become a lot more difficult due to the nature of producing magazines: not only that embarking on a grander project entails higher costs, but you must also deal with unforeseen challenges.

The writing was the easy, predictable, and straight-forward part. To produce the two beautiful volumes of this second BTCTKVR magazine, I needed the help of three graphic designers: Mihnea Niță (who brought to life the articles from the first magazine in 2021 and also did 70 pages from this one), Andrej Cibik (who completed Mihnea's work), and Bogdan Menci (who designed the second volume, "BTCTKVR: The First 109 Episodes of the Podcast").

I'm really grateful for their work, as without them you could only read these articles on the btctkvr.com website. If you ever need help with anything graphics-related, don't hesitate to contact them. This magazine is proof that they're excellent at their craft.

I must also thank this project's sponsors, who were both generous and patient. Most of them joined before they could even see a single page from the magazine, and they were all very understanding when I had to delay the release by a month. I really wanted this to be my finest work to date, and everyone had the kind of low-time preference faith that makes me feel grateful and lucky.

On a personal note, this second BTCTKVR magazine marks the end of a decade in my life. By the time you're reading this, I will have most likely celebrated my 30th birthday. Finishing this double magazine is the best way for me to end my 20s: it's basically the culmination of almost 5 years of learning about Bitcoin, so I'm happy to share with you some information that I've learned throughout my journey. It's kind of crazy to think that I've spent the second half of my 20s obsessing about Bitcoin – but at the same time, I feel sorry for not having spent 9 years doing it, as I first read about Satoshi Nakamoto's project early enough. Nonetheless, I look forward to living a long and happy life as a bitcoiner and writing many more of these magazines.

So thank you for supporting my Bitcoin Takeover project and enabling me to make a living while exploring my curiosities. As a PhD dropout who made it to the final year but didn't finalize his thesis due to writing full-time about Bitcoin, I'm always happy to discover that my work gets more traction than any academic publication would have. Likewise, I feel both amused and flattered whenever I get notifications from academia.edu to inform me that someone from a foreign university cited me – it only proves that working in Bitcoin keeps us at the avant-garde of innovation, while most traditional institutions are having a hard time keeping up and most likely are several years behind.

This second BTCTKVR magazine comes in two individual, physically separate, yet conceptually inseparable parts. You're currently holding the first one, which features articles on a wide range of Bitcoin topics. By reading it from cover to cover, you're going to learn more about protecting your privacy on the internet, understanding the nuances of decentralization, maximizing your financial sovereignty, collecting or else creating the rarest digital art pieces, as well as playing the finest video games. If the first BTCTKVR magazine was basically a collection of op-eds, this second issue comes with more guides, history pieces, and timeless

educational articles. If you read it again in 20 years, the ideas will be just as relevant – even if the hardware and software will improve.

The second part of the magazine is an in-depth breakdown of the first 109 episodes of the Bitcoin Takeover podcast. After three years of doing the show, the time has finally come to give every episode its well-deserved place in the spotlight. Many of my early recordings tend to fly under the radar, despite being very accurate representations of the Bitcoin community's finest moments through time. Due to the nature of social media, even some of the newest interviews receive very little attention even if they're really great. So now that I have an entire encyclopedia which describes every episode of the podcast, I feel like I've finally done justice to all recordings. If you find an idea or guest interesting, don't hesitate to scan the QR code included next to the writeup – it will get you to the corresponding page on bitcoin-takeover.com/audio, so you can listen to the interview with privacy and without having to register an account on some big tech platform like Spotify.

To be honest, I've written every article from this magazine with the intention of beating Bitcoin Magazine in both quantitative and qualitative terms. This is a passion project that I took to the extreme because I wanted this to be my best work to date. So I competed both with myself and the ivory tower of Bitcoin content. In rock n roll terms, this is as if Led Zeppelin released the "Physical Graffiti" double LP as their second album. I hope that it retains the same cultural relevance in time.

Just like the first BTCTKVR magazine, this one is also going to get open sourced so everyone can print their own copies. Starting February 25th 2022 (my 30th birthday), you will be able to find it for free in my GitHub repository. So print as many copies as you want and bring them to your local Bitcoin meetup, conference, or family event. You can even sell it for profit in your store, I will never ask for anything in return. The idea that my work reaches more people already makes me happy and keeps me going. But if you ever want to make me a donation, visit bitcoin-takeover.com/donate or use your phone to scan the QR code.

This is the free and open source version of the second BTCTKVR magazine, create with a very simple purpose in mind: use it for any purpose that you want.

According to the provisions of the Creative Commons Zero license, you are free to copy, distribute, print, modify, and even sell this magazine for profit. My only request is that you give credit where it's due and don't try to attribute my work to somebody else.

You can use this free and open source magazine for conferences, meet-ups, parties, birthday gifts, corporate events, and any other context or situation that you find fitting. Unlike other editions, there is no supply cap or official counting of existing copies – in other words, you can print as many as you want, on any type of paper that you prefer, and in any format you think is appropriate for your use case.

Thank you for supporting the mission of the BTCTKVR project and I hope that you enjoy this cover design by Bogdan Menci and Vlad Costea. Spread the word, Bitcoin's taking over!





How I Almost Got Rich Mining Bitcoin on SlushPool for a Month

When my friend AdventureDr offered to run an Antminer S9 for a month and let me have the rewards in exchange for supplying him with the BTCTKVR magazine, I couldn't say no to his generous offer. In preparation for this special occasion, I set up a Slush Pool account and sent AdventureDr the information required to link the S9 to my Bitcoin wallet.

So for the next 30 days, my new worker has contributed to the discovery of 200 Bitcoin blocks. During this reward era, each new block offered a reward of 6.25 BTC. Which means that in one month, the Antminer S9 has successfully helped add 1250 bitcoins to the total supply.

I should be rich, right? Well, no. You see, having joined Slush Pool means that I've opted for collaborative mining with other workers around the world. Instead of trying to get the entire reward for myself with very low odds, I've opted for more frequent but smaller mining rewards.

With a hashrate of approximately 13 terra hashes per second (that's 13 thousand billion h/s), the Antminer S9 has been one of the ~143.000 Slush Pool workers that generate an output of 7,272 exa hashes (7272 millions of billions h/s). Therefore, the device that AdventureDr ran for me only produced ~0,0000179% of the entire pool's Proof of Work.

At the time of writing, the Bitcoin network is secured by a hashrate of 161,9 Eh/s. Which means that Slush Pool only produces 4.49% of the whole Proof of Work, and my gifted Antminer S9 provides 0.000008% of Bitcoin's security. This seemingly-insignificant percentage is also reflected in the mining rewards I've received.

During my month as a remote miner, I've earned a total of 0.00237392 BTC (2373,92 bits, or 237.392 satoshis), which at the current price of $61.258 are valued at $145,82. Of Slush Pool's 30-day revenue of 1250 bitcoins, my one Antminer S9 has produced ~0,00019%.



These mining gains don't include equipment, electricity, and maintenance costs.



On average, a used Antminer S9 costs about $600 on eBay. And the ASIC miner's power draw is 1800 watts per hour, which adds up to 1296 kilowatts per month. Where I live, one kilowatt costs about 15 cents. So running the S9 for 30 days would cost me no less than $194. Which means that, if I were to sell the mined BTC to cover electricity costs, I'd lose $48,18 every month.

Luckily for me, I get to keep all the BTC and my electric energy bill will be the same as every month – AdventureDr was very fond of the BTCTKVR magazine and ran the ASIC miner for me from his dedicated facility. But if I were to purchase the Antminer S9, I'd pay $600 and subsequently cover a monthly electricity cost of $194 to keep it running.

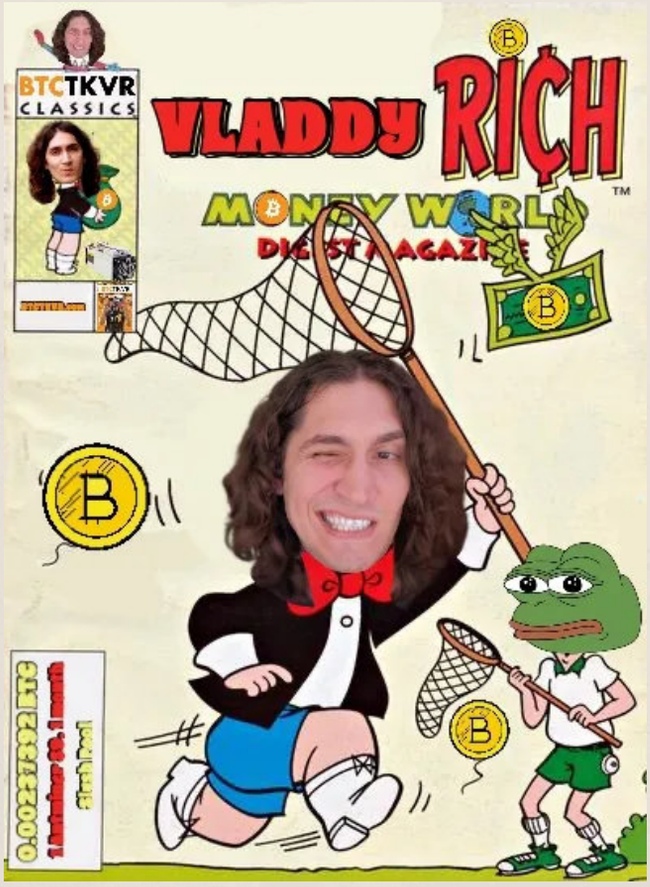
I would definitely break even and recover my initial investment if I could afford to HODL while the price of BTC goes up in the coming years. But from an economic point of view, it would make a lot more sense if I used the $600 and energy cost of $194/month to buy bitcoins. Within the same time frame, I would have a significantly greater return of investment and never have to deal with the anxieties of running an unprofitable mining operation.

Naturally, one can make two arguments:

1. that I should get a more efficient machine (more Th/s with the same energy consumption) to make a monthly profit and eventually break even with my investment;
2. that I should take the Antminer S9 to a place where the electricity cost makes mining profitable (as is the case of AdventureDr).



So if it's more profitable to buy bitcoin than to mine it, why bother?



Well, there are two very significant reasons. First and foremost, it's important to contribute to the security of the Bitcoin network. We shouldn't let it centralize in large data centers which get the cheapest electricity rates and leverage economies of scale to turn out enormous profits. Sure, they provide reliability because it's in their best financial interest to keep the operation going 24/7. But they are also easy to regulate and take down by governments.

During Satoshi's short tenure as developer, educator, and technical advisor he envisioned Bitcoin mining as something that all nodes can do with their CPUs. The competition to discover the next block was a process that all participants would pursue individually. In the whitepaper, Nakamoto even defined Proof of Work as "essentially one-CPU-one-vote".

This kind of decentralization guarantees the network's censorship resistance and reduces the chances of having one big actor who attacks the network – beyond the incentives, it's technically and computationally more difficult to have a single malevolent CPU whose hashpower exceeds the added efforts of all the honest miners.

But in November 2010, Satoshi observed the rise of Slush Pool's collaborative approach – a discovery that would forever change the economy and game theory of Bitcoin mining. Czech cypherpunk Marek "Slush" Palatinus basically asked himself "What if miners, instead of competing with each other to get the full block reward, worked together to discover blocks faster and subsequently shared the newly-minted bitcoins according to their contribution?"

Ever since, we have seen the rise of mining pools and we have observed the various dynamics involved in having an oligopoly of hash power. Miners looking to get frequent rewards would look for the pool which grants them the largest chunk of the block subsidy at the most consistent rate. Instead of doing solo mining to have the same odds as winning the lottery, they would put their hashing power together to get paid more often and be able to finance their operations more predictably.

In theory, no pool should become too big and potentially threatening to the Bitcoin blockchain immutability. But in practice, Bitmain did control more than 40% of the hash rate in 2018, and at the time there were concerns about the implications of this mining centralization issue. A similar debate took place in 2014, when GHASH.io controlled about 40% of the hash rate, while BTC Guild had a share of approximately 25%.

Sure, mining pools are not companies that control every device that works for them. Many participants are independents who switch to the pool that pays them best



for their work. But hypothetically speaking, if a few dominant pools join forces to reorganize blocks and reverse transactions, they can pull it off. And this is a scenario that we must avoid.

Independent mining from home is essential for the Bitcoin network: it contributes to the decentralization of the hash rate and increases the censorship resistance of transactions. Because yes, miners can choose not to pick up certain transactions originating from blacklisted addresses (at the expense of not collecting the transaction fees paid). Therefore, mining altruistically helps remove discrimination and therefore increase the fungibility of bitcoin as a currency. Even if it's not always profitable in fiat terms, it provides a great service.

Now let's talk about the second reason to mine Bitcoin, which is more selfish and has more to do with the state of human politics and laws: the newly-minted BTC is not KYC'd. This means that you receive coins that aren't tainted by a regulated custodian which deanonymizes transactions. Mining is a lot more private than buying from an exchange, and there are even individuals and businesses that choose to purchase their bitcoins directly from the miners to avoid any kind of documented traceability.

In countries where Bitcoin is banned or excessively surveilled, mining helps people escape Big Brother. Those living under totalitarian regimes may need to mine BTC to earn the kind of money that makes them free and sovereign. And most of the times, they need Bitcoin to bribe corrupt officials in order to be allowed to start a new life somewhere else.

The case for mining Bitcoin from home

To accomplish our decentralization goals, we need SHA-256 ASICs that are designed for home use. Not just repurposed industrial-scale mining rigs, but devices that anyone can run in their living room while making minimal profits. A remarkable product that caught my attention is the Futurebit Apollo BTC. It has an output of about 3 Th/s at an electricity consumption of 200 Watts, with an extra Eco mode which makes it draw only 125 Watts while running more quietly.





I did the math and, if I were to run the Apollo instead of the Antminer, I would make a monthly profit of $1 (at the current BTC price). Which means that I'd need about 800 months to recover my investment, granted that the electricity cost, bitcoin price, and mining difficulty remain constant.

But then again, the point of getting one of these is not to get rich, but to support the network. At 150 Watts/hour, it consumes 10 times less energy than continuously running an economical air conditioning unit. And during winter time, I can use Turbo mode to produce more heat and keep my room warm (it would actually be interesting to cut my reliance on natural gas).

This is not, by any means, an endorsement for the Futurebit Apollo BTC miner. Their device is expensive for what it does and it's being produced in such small quantities that it sells out before I get the chance to buy one (happened to me 3 times this year). I know that identical results can be achieved by downclocking an older and more affordable industrial-scale ASIC device, but the hardware's reliability is always questionable.

Conversely, I wish more companies were ideologically aligned with this movement to decentralize Bitcoin mining through individual users. We should have a small, energy-efficient, and quiet miner that we keep next to our internet router. Just like we run Raspberry Pi nodes, we ought to also have similar mining hardware and pools that support it. In the true spirit of "don't trust, verify", we should diminish our reliance on large-scale, compliant, and politically-fragile mining farms.

Yes, our full nodes can reject the blocks created by dishonest miners. But at the same time, miners can play by the Bitcoin network consensus rules and never pick up the transactions that you broadcast. There is nothing that nodes can do to push miners to write a certain transaction in a Bitcoin block. And this censorship resistance is not given to us by Satoshi, the whitepaper, or some ideological belief in the Bitcoin network's virtues – we need to claim it by running our own operations with our own hardware.

In the end, I didn't get rich mining Bitcoin. But I've learned an important lesson about profitability, economies of scale, the limitations and technical obsolesce of ASICS, and how nation states can discourage us from mining by adding extra taxes to electricity. But most importantly, I've rediscovered the significance of voluntaryist decentralization. We shouldn't expect others to honestly secure the Bitcoin network – they have the farms, but we have the numbers.

A crash course in Bitcoin mining

Bitcoin mining is the energy-intensive process which secures the Bitcoin network. Approximately every 10 minutes, a new block gets discovered – and the first miner to guess the right hash gets rewarded with the block reward and the transaction fees that users have paid to prioritize their transfer.

In exchange for providing security to the network, Bitcoin miners also become participants in this winner-takes-it-all race. There is actual energy cost involved in the production of every BTC unit, and it's always more expensive to attack the system than to honestly participate in it. Basically, the security of the Bitcoin network relies on the competitive greed and financial self-interest of the miners.

The system is based on Dr. Adam Back's Proof of Work, which was first included in hashcash in 1997. In its first iteration, "mining" was a way to prevent e-mail spam. To make sure that senders would no longer fill the inboxes of an unlimited number of recipients at no financial cost, e-mailers would have to either use their computers' processing power to mine some hashcash or else make a payment for every e-mail. This way, spamming would incur computational or financial costs.

Satoshi Nakamoto took the principles of hashcash and used them to solve the Byzantine Generals Problem (also known as the Bytzantine Fault Tolerance). Essentially, the issue of "how do we make sure that the issue of "how do we make sure that decentralized participants who don't communicate with each other will coordinate to accomplish the same goal in an honest way?" was solved with Proof of Work and incentives. This is part of what we sometimes call the "Nakamoto Consensus".

The Bitcoin blockchain is ruled by the laws of physics – and more precisely, entropy as a consequence to the first law of thermodynamics. Every event is made possible



by energy consumption, and therefore becomes provable and irreversible. This is of utmost importance for the security of transactions, as they need to be resistant against human politics.

It's generally agreed that after six new blocks have been mined, the costs of launching a blockchain reorganization attack are far too great to reverse an older transaction. Spanish mathematician Ricardo Perez-Marco and French math researcher Cyril Grunspan have even published an academic paper in which they argue that 2 network confirmations are more than enough to determine the finality of a transaction, specifically due to the multi-million dollar costs involved in undergoing an attack against it.

Bitcoin miners compete for a block reward which diminishes by 50% every 210.000 blocks (approximately 4 years). In the beginning, the subsidy was 50 bitcoins per block. In November 2012, the 210.000th Bitcoin block was mined the new reward went down to 25 BTC. Since block 420.000 (July 2016) and until block 630.000 (May 2020), successfully guessing the right hash





problem while securing the network was rewarded with 12.5 BTC. Right now, the block reward is 6.25 BTC, and it's gonna get split in half once again after block 840.000 (sometime in 2024).

This is how the entire supply of 21 million bitcoins gets issued. It will take until the year 2140 (the 34th halving epoch) to have the entire supply released. But this doesn't mean that mining will come to an end. Satoshi Nakamoto's design is to have transaction fees as a second incentive. And within a couple of decades, the sum of fees will be greater than the block discovery reward.

Every Bitcoin transaction is data which takes up space from the Bitcoin blocks. So in order to have your transaction included in a block, you need to pay a certain amount of BTC units for every byte of data you're going to occupy. As the demand increases, a game of prioritization begins in favor of the highest bidder – the Bitcoin users who pay the most for their transaction are the ones who will receive confirmations first.

So the money paid in transaction fees go to the miner (or mining pool) that discovers the block. Which means that the total block reward for the miner consists of the subsidy available during the corresponding epoch (which is constant across 210.000 blocks), plus transaction fees. For example, miners in 2021 will collect 6.25 BTC from the block reward, as well as ~0.05 BTC extra from transaction fees (at a median fee of 4 sat/byte).

But as more miners join, the difficulty of discovering a block increases exponentially, right? Which means that more energy needs to get consumed in order to produce more bitcoins over time. Well, not quite. Satoshi Nakamoto has designed the difficulty readjustment system.

After every 2016 blocks, the difficulty gets readjusted according to the existing activity: if more hash power has been added during the previous 2016 blocks cycle, then the difficulty gets increased. But if miners start giving up due to their individual economic self-interest (the cost of electricity gets higher than the reward), then the difficulty of discovering blocks will drop.

This dynamic process creates unique opportunities to seize the perfect moment to start mining, and also leads to a continuous

search for lower electricity costs. When a miner gives up and the difficulty drops, there will always be someone else on the other side of the world to take advantage of the chance to get more bitcoins with a lower effort.



Coincidentally, the most affordable kind of energy is the one that's generated from renewable sources. Bitcoin's Proof of Work mining has started a global quest for inexpensive electricity: in China, miners used water wheels (hydroelectric energy); in the United States, miners burn the natural gas that normally gets wasted during oil extraction; in El Salvador, it's the geothermal energy of volcanoes that gets used to power ASIC miners.

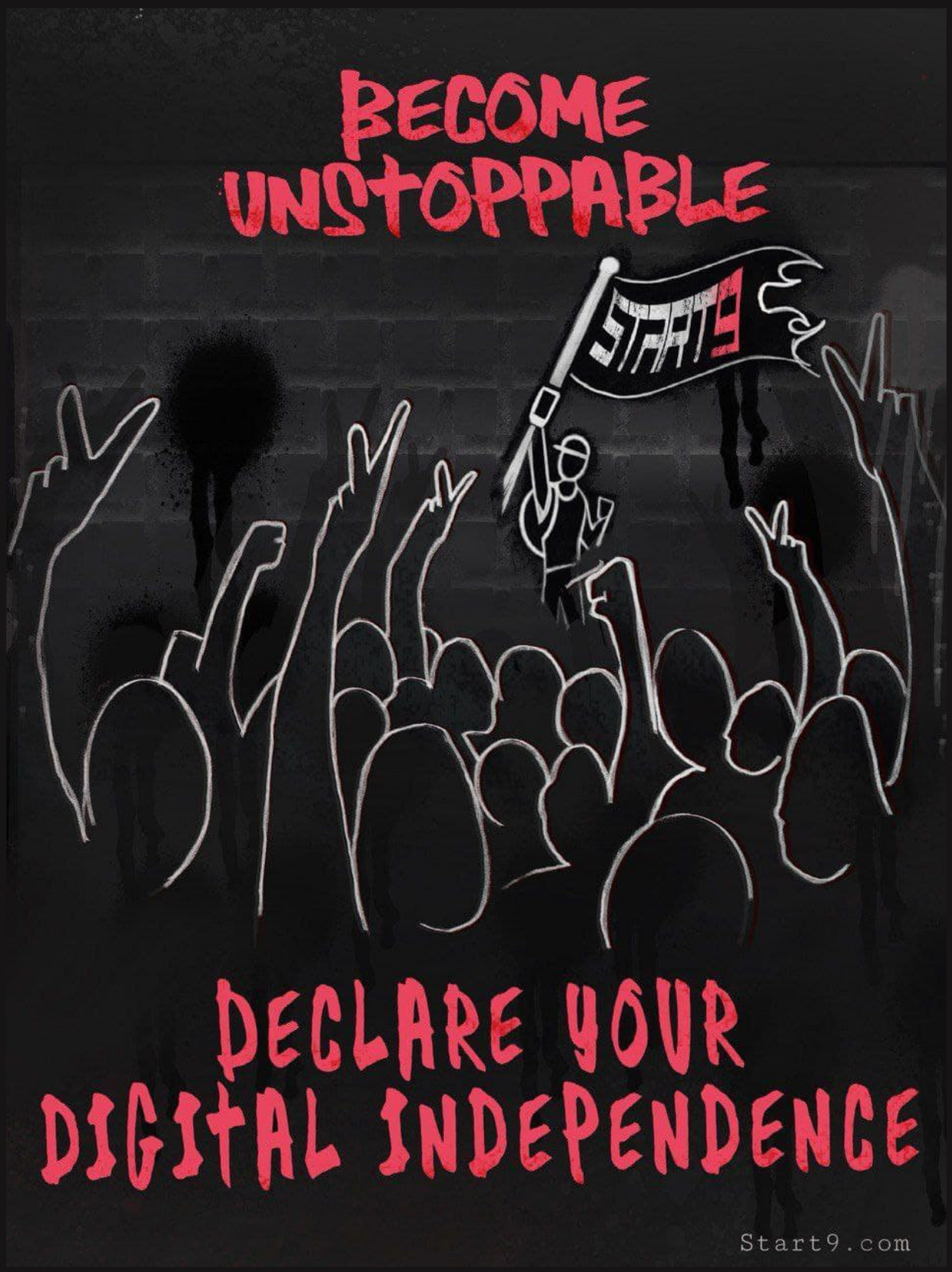
And all around the world, the surplus energy that power plants produce and power grids can't transport to consumers gets used to secure the Bitcoin network and generate some extra profits. What some describe as a wasteful process actually incentivizes the expansion and development of renewable energy.

Bitcoin mining is one of the most dynamic industries in the world. Since January 2009, it has managed to transition from the original design of "one CPU one vote" to GPU mining, and then give birth to a lucrative business of ASIC (Application-Specific Integrated Circuits, or specialized computers that can only perform one task in a very efficient way) devices.

Mining from home has quickly migrated towards industrial farms, and for a while most of this activity took place in China. But since the second half of 2021, due to China's authoritarian policies, the new leader in Bitcoin mining is the United States of America. However, my hope is that hardware companies will find creative ways to bring Bitcoin mining back into people's homes.

Crafty people around the world have already found ways to use the heat generated by Bitcoin miners to warm their homes, or boil hot water for their showers. In the end, human ingenuity is infinite and we're going to see many developments so brilliant that our minds can't even conceive right now. And as long as the Bitcoin network becomes more decentralized and reaches its goal to separate money from human politics, I'm all for it.




BECOME
UNSTOPPABLE
START9
DECLARE YOUR
DIGITAL INDEPENDENCE
Start9.com



The 8 Editions Of The First BTCTKVR Magazine

Since I first introduced it to the world via Twitter on July 19th 2021, the BTCTKVR magazine has exceeded all expectations. What started as a one-off experiment which involves printing and distributing some of my best articles has quickly turned into a part-time job. Between July and December 2021, I've sent out 442 magazines to more than 26 countries, across all 5 continents. And in spite of my best efforts, there are still people who ask me how they can get a copy.

442 might not sound like much, but we're talking about a one-man operation. For 6 of the 8 editions, I have taken care of all the logistics myself. And it can be time-consuming to manage the orders, pick up the magazines from the print shop, sign and number each copy manually, package, stamp, and then finally take goodies to the post office for delivery. But I've loved every second of it and I feel grateful that there is demand for my work.

You see, before producing the magazine I used to write a lot, record dozens of podcast episodes every year, shoot video reviews, and also do lots of other quirky Bitcoin projects like the 24/7 radio stream. But my problem was that I couldn't find an effective way to promote my work in a meaningful fashion, outside of the fragile social media echo chamber.



Sure, I'd post about my latest article on Twitter and Reddit. Then I'd do my best to start a conversation about the topic and find potential debaters. But due to the nature of

these networks, my posts would often get buried by the algorithms. Very few people would see them – let alone interact with them. It's never the signal that grabs people's attention and gets boosted, but the noise. Those who know how to juggle with drama tend to climb the ladder of success a lot faster, as proven by a few top podcasters.

And this really bothers me, as I'm not the kind of guy who enjoys playing with people's opinions and emotions for the sake of causing controversy and therefore farming engagement. I'd rather write another article or record an interesting podcast episode than argue with an internet stranger just because we disagree on one insignificant view, he happens to have more followers than me, and therefore I want to grab the attention of his audience.

Now I write articles knowing that I'll publish them in a magazine. Nothing goes to waste anymore and I have an incentive to make an extra effort to do a better job. I can focus on quality and avoid the noise. I'm also more efficient at reaching an audience, since magazines are sought-after collectibles in the Bitcoin space. Which means that I also get better at answering the annoying yet necessary question that marketing departments ask before offering any kind of sponsorship: "What is your target audience?"



Of course this doesn't mean that I'll collect data. If anyone asks me to whom I've sent the magazine, I probably wouldn't be able to tell more than 30 names out of 400+. It's because I didn't keep any kind of records and all the shipping information that I received was immediately written on the envelope that I'd later send out. At the post office, I always opted for the slower but more private delivery option which minimizes data collection.

So if you're the first recipient of this magazine, then rest assured that your data was not saved in any electronic database. It's basically the same kind of delivery that happens with normal letters: no tracking, no barcodes, no QRs, only a barebones postal service.

While I can vaguely remember to which countries I sent most of the magazines, I don't and mustn't remember everybody's name and address.



Another phenomenon that I've observed is that people pay more attention to something that they read in print. They'll even show better signs of remembrance, as some will be able to recall when they read an article and what else they were doing on that specific day. While internet articles are nice and convenient, physical media leaves a stronger impression on all of us.

Now please allow me to remind you that the BTCTKVR magazine is a free open source project: you can find all the pages and files in a public GitHub, and you are free to use the content in every way described by the Creative Commons Zero 1.0 license (read, distribute, multiply, modify, and even sell). For more information, visit github.com/VladdyC/BTCTKVR-Magazine.

This may sound counter-intuitive for a project as centralized as a magazine for which one person writes all the articles. But I want the information to be available to everyone who needs it. If somebody from Burkina Faso, Tibet or Paraguay wants to print a few copies for a local meet-up or conference, then they shouldn't ask for my permission.

They might as well sell magazines and make hefty profits out of it, I'll never ask for a single bit in return. Printing, distribution, and advertising take a lot of work and I'm well aware of it. I'm happy knowing that more people read my work to get educated about Bitcoin. If anyone wants to support my work, they can make a donation.



So why did I create different editions instead of printing the exact same copy? Well, I've never intended to mass-produce BTCTKVR and sell it on every major Bitcoin-related store. I see my magazines as rare collectibles that I offer to people I like – and more than 300 of the 442 copies have been given away for free thanks to the generous sponsors that believe in my work and support it.

Another reason for creating editions concerns modifications: after the first batch of 150, I've received some feedback from David St-Onge and I had to fix a couple of issues. Then for the Raretoshi Liquid sidechain NFT edition I've added an extra article to incentivize L-BTC bidders on the platform to grab this limited print. And when I wanted to mark a special moment (like the 2021 BTC-USD all-time high) or support a conference, I've put their logo on the cover and made slight changes to the foreword.

Before printing the Counterparty NFT edition, the magazine's French translator Duck Avenger (also known as @Griptoshi on Twitter) and a Portuguese supporter known as Rafaelpac have also reported a couple of duplicate paragraphs that somehow slipped the initial scrutiny. Which means that from the first edition to the last, throughout a process which took about five months, the BTCTKVR magazine has been perfected and improved thanks to community feedback. Like a true open source project.

Of the 442 copies, I've manually signed and numbered 382 of them. I must thank Madelyn Ash and HODL Barbarian from the Atlanta Bitcoin conference team for taking care of this logistical detail with ~60 copies – otherwise I wouldn't have been able to offer the magazine to the dozens of Bitcoin developers who spoke at the event.

Likewise, I must thank Mauro Peretti, Ricardo Martinez, and Lawrence Ray from the Bitrefill team – it was them who handled the distribution of 40 out of 80 magazines from the second batch. Speaking of, Bitcoin NFT artist Crypsi has paid for the CoinFest UK edition (60 copies) and then handed them all at the event venue – and for his contribution, I'm very grateful.

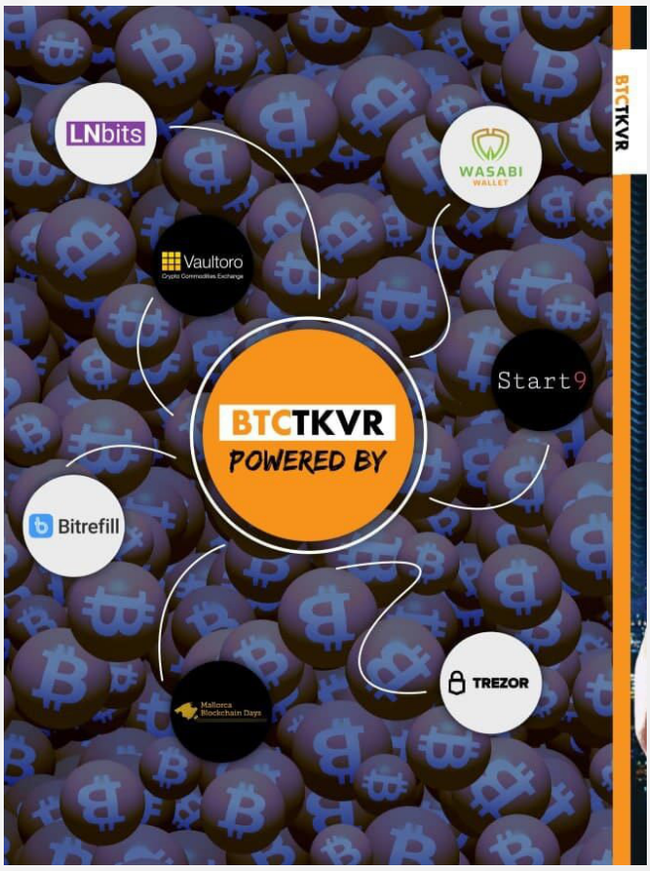


I must also thank the sponsors of the project. When I turned 29 years old in February 2021, I told myself that I would have the most productive year of my life so far. In this increasingly Orwellian world, keeping myself distracted with work helps me stay sane. And when my work aims to liberate people by teaching them how to opt out from tyranny, I truly feel like I'm doing something worthwhile.

First of all, I must thank Vaultoro CEO Joshua Scigala. Since he agreed to sponsor my podcast in November 2020, I didn't have to worry about finding a job and getting more freelancing gigs on the side. Being able to focus on what I want to create is the reason why this magazine exists and I will forever be grateful to Joshua for seeing potential in my work.

Likewise, I have to thank Rafe, Max Hillebrand, and Adam Ficsor (Nopara73) from Wasabi wallet. When I was looking for a second sponsor for my podcast, they have made key contributions which enabled a form of partnership. As I told them, I'd recommend people to use Wasabi even if I wasn't paid for it. But I feel grateful that they could work something out.

Other people who helped me print more magazines are Anthony and Kristyna from Trezor, Matt Hill from Start9 (who also produced about 5 small-sized copies for a Lightning network meet-up in Denver), Chris from Mallorca Blockchain Days, Ben Arc from LNBits, and Bitrefill's dynamic trio which consists of Mauro, Lawrence, and Ricardo. I'm equally grateful to all of them, as they supported the project before getting the chance to read a single page.



It was this incredible amount of trust that they had in my work that motivated me to exceed all expectations – which I did, as the experimental first batch of 150 copies has multiplied to 442. The fact that most of these sponsors have decided to also stick around for the second BTCTKVR magazine makes me really proud.

In 2021, the BTCTKVR magazine has been distributed at 3 conferences: Mallorca Blockchain Days (July-August), The Atlanta Bitcoin Conference (TABConf, November), and CoinFest UK (November). If we count Bitrefill's team-building event from October as a conference, then the number goes up to 4.

There was also an event in Nebraska which wanted to distribute some of my magazines, but at the time I couldn't afford to cover the printing and delivery expenses. Maybe next time!



So what's the price of a magazine which was mostly given away for free? Well, the most somebody offered for the NFT editions (on both Raretoshi and Counterparty) is 0.0021 BTC. We're talking about the third and seventh editions, which both had limited supplies of 21 copies. Now it's up to the free market to determine how much the other magazines are worth – some are older, some are scarcer, and the later editions feature some bug fixes.

Let's finally address the scarcity aspect: there are currently 8 different editions of the first BTCTKVR magazine and I don't intend to produce more – at least not in their original form. I'd probably do something like a double

feature which includes the first two magazines in one super thick binding. Don't worry though, anyone can always print more copies of the free open source version on GitHub.

Even if I do give in to pressure and decide to sell out, I'll make sure that the edition is clearly distinguishable and doesn't inflate the supply of the early editions (changing the cover and foreword are two essential procedures that you can already find in the 8 existing editions).



BTCTKVR, 1st Edition (July-August 2021)

When Nindy (European Bitcoin conference organizer) asked me if I'd like to speak at Mallorca Blockchain Days 2021, I took a quick look at the speakers list to know what to expect. As soon as I noticed that Bitcoin developers like Peter Todd (one of the most prolific Core devs and the mastermind behind RBF), Amir Taaki (creator of Libbitcoin and the BIP system), Christian Rootzoll (maintainer of RaspiBlitz) and Thomas Voegtlin (creator of Electrum wallet) were some of the headliners, I knew that a simple business card won't suffice for the purpose of introducing myself.

I needed something better that would leave a lasting impression on every speaker and participant. Furthermore, I wanted to introduce myself with an item that everyone would keep even if they disliked me as a person – with high-quality glossy paper and colorful graphics. It was then that I decided that the time was right to revisit my old idea of putting together some of my best articles to create a magazine. In mid-June, I contacted my friend Mihnea Niță and asked him to design something which resembles an old-school computer magazine.

Based on my love for classic rock, I've also wanted to include a prominent Droste effect on the front cover – just like Pink Floyd did for their 1969 album Ummagumma. Mihnea told me to snap a picture of me holding any magazine and then worked his photo editing magic to produce the iconic cover.

Ever wondered what I was actually holding? It's the Romanian video game magazine NXT LVL, which I edited in 2020. Obviously, it couldn't be BTCTKVR because it didn't exist yet. Also, the t-shirt that I'm wearing was designed by John Carvalho for his Bitcoin Intel Pro merchandise project, and he gave it to me for my 28th birthday. Allegedly, it's based on a North Korean propaganda poster.



Here's a random fact that should be useful to collectors: Mihnea designed two different versions of the cover. The first one features a futuristic Blade Runner-style metropolis in the background, while the second is filled with orange Bitcoin balls. When I couldn't make up my mind about which one we should use, we created a mixed model which takes the Tokyo-like front and adds the ballsy back cover.

The second design ended up being used for the free and open source digital version of the magazine, while the futuristic one was sent to the print shop to become the trademark of the first edition.

It's also worth noting that the design with the orange balls has been remixed for the remaining 6 out of 8 editions: by applying different effects, filters, and logos, I've accomplished to create something different. If you take a close look at the first edition prints, you're going to see that the Droste effect includes the orange ball design too – a way to foreshadow upcoming editions, just in case that the project becomes successful.

The plan was to give away the magazine for free to everyone who wanted one. And in order to accomplish this feat, I had to search for sponsors. In a matter of two weeks, I was able to convince Vaultoro, Wasabi, Start9, LNBits, Bitrefill, Trezor, and Mallorca Blockchain Days (event organizer Chris was enthusiastic about the project and really wanted me to bring a copy for every participant).

My pitch was very simple: it costs me about 10 euro to print a magazine and another 10 euro to deliver one anywhere around the world. So any amount with which you can contribute is highly appreciated. Needless to say, I feel very grateful and I would like to thank all sponsors for believing in this project's mission. All the money was spent on producing magazines – even when I had to sell BTC at a loss around $30k.

On July 19th 2021, the BTCTKVR magazine was officially announced to the world – introduced with the metropolis-themed cover which is the most distinguishable visual characteristic of this edition. Only 150 copies were printed – of which 50 ended up in the hands of Mallorca Blockchain Days participants, and the rest have been mailed to bitcoiners worldwide. Every copy is manually signed and numbered by me with a red marker pen (with the exception of number 110/150, which "Talking in Bits" co-host Marty told me that I forgot to sign).

Given that it's the first edition of the magazine, it also has all the mistakes and bugs that have been fixed in subsequent releases. But some collectors told me that mistakes usually make rare items more valuable, so I'll have to trust their expertise on the matter.

Here are the facts that every collector should know about this first edition:

Total Supply: 150 copies (manually numbered and signed with a red marker pen)

Announcement Date: July 19th 2021

Official Launch: Mallorca Blockchain Days, July 30th 2021 (50 copies were given to speakers and participants)

Distribution: Copies numbered 1 to 29 were given away to friends, family members, and people on Twitter who showed interest in receiving a free magazine. Copies numbered 30 to 80 were distributed in person during the Mallorca Blockchain Days 2021 conference. The remaining 70 copies were sent out via post delivery in August and early September 2021.

Number of Pages: 92

Printed In: Romania

Cost: Thanks to the sponsors, it was delivered/handed for free.

Final Paragraph in the Foreword: "This first issue of BTCTKVR was printed in 150 copies and will get distributed during the Mallorca Blockchain Days 2021 conference (both at the venue and outside of it). And while you can treat this magazine as a collectible, I recommend that you pass it on to a friend after you're done reading it. Every copy of BTCTKVR is a super spreader event."

Special Cover: Dark background, with a Tokyo/metropolis theme on the front cover. In the Droste effect you can see a hint about the upcoming magazines.

Famous Owners: Peter Todd (39/150), Thomas Voegtlin, Amir Taaki, Joshua Scigala (30/150), Matt Hill, John Carvalho, Nopara73, Harry Halpin, Sat Symbol, Chris DeRose, Junseth, Eppo Leemburg (92/150), JScrilla (21/150), Matthew Haywood (25/150), Hitomi Moryiama and Kenichi Kurimoto (Nayuta), Bryan and Colin Aulds, Mike in Space, David St-Onge (87/150), Marty Byrde (110/150), Ketominer, DecentralizedD1 and AdventureDr (both of them collected every issue), FartFace2000, Satoshi's Witness.

No-coiners who might sell you their copy: Search for ioana.balaur (22/150), ruthrox and georgianacomarniceanu (80ish/150) on Instagram. I tried to orange pill them, I'm not sure if it worked.



BTCTKVR, 2nd Edition (September-October 2021)

Officially launched on September 29th 2021, this second edition is also called "the Bitrefill edition" – as the gift card merchant has offered to sponsor the entire batch of 80 copies, all of which feature their logo on the front cover. Before the company's annual team-building event, I've received a special request for content: Bitrefill asked me to send 40 magazine copies for all of their employees and collaborators.

Thanks to the logistical planning provided by Mauro, Ricardo and Lawrence, each member of their team has received a little bit of love from the Bitcoin Takeover project. I was happy to once again make magazine the printer go BRRR, and I've spread the love among other bitcoiners too.

As would become the norm for each edition, I've changed the last paragraph of the foreword. Also, the front cover makes use of the template for the free open source version – thanks to a little bit of Photoshop wizardry, it looks as sweet as honey. David St-Onge's vigilant scrutiny has also played a major role: at page 39, the word "about" has been changed to "amount".

Technically speaking, this is the fourth version that I conceptualized (the second being the free open source edition which has been available since August 2021, and the third being the Raretoshi NFT which I minted on Bitcoin's Liquid sidechain later that same month). But it's the second one that I actually printed, and the longest Proof of Work chain is determined by production, not mempool transactions.



Here are the facts that every collector should know about the second edition of the BTCTKVR magazine:

Total Supply: 80 copies (manually numbered and signed with a red marker pen)

Announcement Date: September 29th 2021

Official Launch: Bitrefill's annual team-

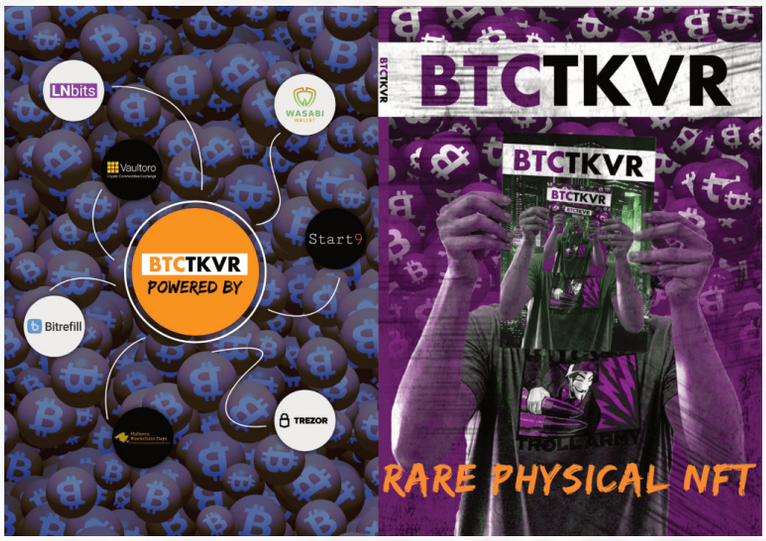
building event, which took place in early October in Spain.

Distribution: Copies numbered 1 to 40 were sent to Spain so the Bitrefill team can pick them up and handle the distribution at the event. The remaining magazines (numbers 41 to 80) were given away to bitcoiners and friends who showed a degree of interest. By mid-October, I had no more copies left.

Number of Pages: 92

Printed In: Romania

Cost: Thanks to Bitrefill, it was delivered for free.



Final Paragraph in the Foreword: "This is the Bitrefill edition of the BTCTKVR Magazine. As opposed to the Mallorca Blockchain Days edition from July 2021 (150 copies), the NFT version from August 2021 (21 copies), and the free open source version (which anyone can print), it features a unique front cover and a limited supply of 80 copies. 40 of these copies (numbered 1 to 40) will be distributed to the Bitrefill employees, while the remaining 40 (numbered 41 to 80) will be given away to various Bitcoin community members".

Special Cover: Honey-colored front cover with the Bitcoin balls background from the free open source edition. On the bottom right corner, you will find the Bitrefill logo.

Famous Owners: Giacomo Zucco, Robert Njogu (Kenya), Sergej Kotliar, Joshua Scigala, Valeriya Georgieva, AdventureDr, DecentralizedD1.

No-coiners who might sell you their copy: Search for bassosarah on Instagram. I sent her a copy, but she didn't seem to be too happy about the gift.



BTCTKVR, 3rd Edition (August–November 2021)

When I told Vaultoro CEO Joshua Scigala that I want to offer the magazines for free as rare collectibles, he told me to look into Liquid network NFTs on Raretoshi. The rationale was very simple: tokenized ownership hype was at its peak, Liquid has pretty good scalability and low transaction costs, and the user experience makes everything easy.

After returning home from Mallorca Blockchain Days in early August, I signed up to Raretoshi and submitted a slightly modified version of the BTCTKVR magazine cover. After my initiative was approved by the administrators (unlike Counterparty, which I'd discover about a month later, Raretoshi is permissioned and centralized), I've finally minted the NFTs: 21 copies for which anyone could bid amounts ranging from 0.0011 to 0.0021 L-BTC (bitcoins pegged on the Liquid sidechain).

This was the first time when I experimented with the physical NFT concept: you get the NFT from the auction website, and then also receive the physical magazine as a bonus. Furthermore, it was the first time when I actually used Liquid. Later in the month, I've documented my experiences in the article "Raretoshi: Bitcoin NFTs on the Liquid Sidechain" (a piece which was later translated to French, Spanish, and German).

The article became a bonus for this edition: which means that the Liquid NFT magazine has 6 extra pages which give collectors an incentive to also own this one. You won't find this piece of text printed in any other version of the magazine, so it's truly rare.

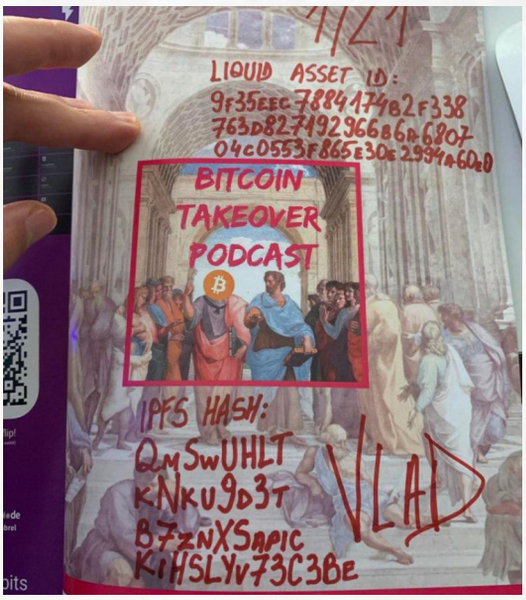


Speaking of rareness, the front cover's purple color and grungy textures is a homage to all the valuable and highly collectible trading cards. A 1999 Pikachu card, in which the popular Pokemon has red cheeks and a purple background costs anywhere between $400 and $2800. In RPGs like Diablo 2, the stats of rare and powerful swords such as Blood Edge Colossus are written in purple.

In many cultures, purple means rare and of superior quality – so I've tried to also convey this chromatic meaning to the limited-run magazine.

Aside from being rare and including an extra article, this third edition is also the only one whose entirety of owners are publicly known (at least according to their Raretoshi user names). So it's relatively easy to figure out who owns which copy.

There's also something to be said about delivery time: though this edition was first announced in mid-August 2021, it took until early November to print and send each one of the 21 copies. The whole "physical NFT" concept didn't seem too appealing in the beginning but many people were curious to



Here are the facts that every collector should know about the third edition of the BTCTKVR magazine:

Total Supply: 21 copies (manually numbered and signed with a red marker pen, with the special inclusion of the Liquid asset hash and IPFS image address)

Release Date: August 17th 2021

Official Launch: On Raretoshi, a digital art marketplace that's build on Blockstream's Liquid sidechain.

Distribution: All 21 copies were sent to the highest bidder of every Liquid NFT.

Number of Pages: 98

Printed In: Romania

Cost: Between 0.0011 and 0.0021 L-BTC

Final Paragraph in the Foreword: "This is the NFT version of the BTCTKVR magazine, of which only 21 will ever get printed. It varied from the free open source edition in three important ways: the cover is colored differently, you get a bonus article, and the Liquid asset ID will be manually written inside this magazine. Enjoy this rare collectible!"

Special Cover: A purple variation of the FOSS edition, with a gritty/grungy filter added on top. On the bottom of the front cover you'll find an orange-colored text which reads "RARE PHYSICAL NFT".

Famous Owners: Adam Soltys (1/21), DecentralizedDad (2/21), Tweetious (3/21), Crypsi (4/21), Carlo Leone Spiller (5/21), RRizzling (6/21), PippoKatz (7/21), SatsLife (8/21), Jaminunit (9/21), bteecee (10/21), Kalevmagnusson (11/21), l0n0 (12/21), Sparky (13/21), Hodlonaut (14/21), DuckAvenger (15/21), bibiki (16/21), JediBTC (17/21), KASP3R (18/21), k00b (19/21), Vizique (20/21), timz (21/21).

No-coiners who might sell you their copy: LOL

Hidden inflation: I own a defective copy that's missing two pages of content (they weren't printed for whatever reason, so they're entirely blank). I've numbered it 21/21, discovered the issue, told timz about it, and he didn't want it in this condition. So I kept it for myself and printed another one for him.



BTCTKVR, 4th Edition (November 2021)

Also known as the "CoinFest UK" edition or the "Manchester magazine", this fourth iteration of BTCTKVR was printed in early November 2021 in 60 copies. It was Bitcoin artist Crypsi who made the special order, as he wanted to make a point about physical collectibles right in the middle of the NFT mania. Not only that, but he knew that a wave a shitcoiners was going to show up at CoinFest – so Crypsi decided to offer them some proper Bitcoin education with the BTCTKVR magazine.

Initially, the financing was only supposed to cover 50 magazines. But thanks to printing price negotiations and some cheap delivery tricks, I was able to produce 10 extra copies with the same money.

At first glance, this fourth edition looks identical with the free open source version. But there are three main differences: the FOSS edition uses a slightly darker shade of orange on the front cover (#EB8931 vs #F69320, for all of you HEX geeks), while the CoinFest UK version features a stylized Union Jack in the bottom right corner of the front cover. Last but not least, the last paragraph of the foreword was changed to please the Brit receivers.

It should also be mentioned that I've never printed and signed a copy of the FOSS version of the magazine – in contrast, all the 60 copies distributed in Manchester are manually numbered and signed by me. And if you pay extra attention to the articles, you're going to notice that the fourth edition includes some tiny mistakes that I've fixed in the free open source version.

Here are the facts that every collector should know about the fourth edition of the BTCTKVR magazine:

Total Supply: 60 copies

Release Date: November 25th 2021 (but printed and sent to the UK three weeks earlier)

Official Launch: At CoinFest UK 2021

Distribution: I kept one copy (number 60/60), while the other 59 were handed by Crypsi at CoinFest 2021.

Number of Pages: 92

Printed In: Romania

Cost: Free for all CoinFest 2021 participants who asked for a copy.

Final Paragraph in the Foreword: "This special edition was created for the

CoinFest UK conference, which takes place in Manchester between the 25th and the 28th of November 2021. By virtue of Crypsi's patronage, you have received one of the 60 copies. So have fun learning more about Bitcoin and make sure you spread the knowledge to your peers!"

Special Cover: The front cover is a slightly modified take on the FOSS version, with a stylized UK flag in the bottom right corner.

Famous Owners: Crypsi, 5Ksana, Torsten Hoffmann (not confirmed).

No-coiners who might sell you their copy: Ask Crypsi, he knows best.





BTCTKVR, 5th Edition (November 2021)

When I became aware of The Atlanta Bitcoin Conference (TABConf) 2021, I immediately knew that I must do everything I can to get some of my magazines to the event. The bad news is that, by the time I figured out I want to pursue the goal of handing one magazine per speaker, it was already too late to deliver the goodies on time.

Thankfully, I've received some logistical help from the organizers (Elwood the HODL Barbarian, Madelyn Ash, and Michael Tidwell). All I had to do was cover the printing costs, and the Atlanta folks were generous enough to find a good print shop and hand a copy of the magazine to each speaker or attendant who wanted one. Thank you, guys!

Essentially, all the BTC I've earned from the Raretoshi NFT edition was spent on making this spontaneous collaboration happen. But it was worth every bitcoin fraction, as the magazine ended up in the hands of people like Pieter Wuille, Jimmy Song, Justin Wales, and Mr. SeedSigner. I haven't received confirmation from other developers, but the idea that Pieter Wuille might have read the article about Taproot makes the entire operation worthwhile.

As Michael Tidwell told me after the event, "there were a few speakers who politely declined". So I'm not sure if other developers such as Andrew Poelstra, Matt Corallo, Andrew Chow, Murch, Jeremy Rubin, and Paul Sztorc received a copy. My dream of



Nic Carter tweeting a picture of the BTCTKVR magazine next to his Tungsten cube also seems unlikely.

However, Bitcoin Magazine was in the house auctioning a few of their first issue magazines from 2012. And a few days later, I got a message from their CEO David Bailey – he informed me that he got his hands on one of my magazines and it's "very punk rock and creative/authentic". So it's probably safe to say that getting BTCTKVR to Atlanta was a good idea and I should probably do more of this.

As I was made aware, there were some attendants who picked up the magazines that speakers declined to receive. This is how Bitcoin Coder Bob (whom you can hear in S6 E2 of the Bitcoin Takeover Podcast) got his copy, and it's likely that others did the same. Mr. SeedSigner and Keith Mukai were not on the speakers list, but both took home a colorful magazine.



Now let's talk about scarcity: since this is the only edition of the magazine that I didn't print and deliver myself, I couldn't verify myself that no more than 60 copies (the number for which I paid) have been printed. Elwood the HODL Barbarian told me that "60 something mags found an owner", while Madelyn told me that "64 were printed for TAB" and one of them was sent to me. The first 60 were manually numbered by Madelyn, using a silver-colored Sharpie pen. It's very easy to distinguish thanks to the metallic texture.

While the TABConf version of the magazine was distributed two weeks before CoinFest UK, the order is determined by the first copies that were printed.

Here are the facts that every collector should know about the fifth edition of the BTCTKVR magazine:

Total Supply: 64 copies (allegedly, one is defective)

Release Date: November 5th 2021

Official Launch: At The Atlanta Bitcoin Conference 2021 (TABConf)

Distribution: All numbered copies (1 to 60) were given to speakers and conference attendants. Of the unnumbered 4, I own one.

Number of Pages: 92

Printed In: USA

Cost: Free for all TABConf 2021 participants who picked up a copy.

Final Paragraph in the Foreword: "This fifth edition of the BTCTKVR magazine was printed for the TABConf 2021 event (Atlanta, November 4-6). The fact that you've received a copy means that you must be one of the conference speakers, a member of the organizing team, or somebody really dear to those passionate bitcoiners. Take care of your mag – only 60 of these have been printed and they're all distinct from the other editions of BTCTKVR!"

Special Cover: The front cover features a left-right color contrast which resembles something you'd see in a Star Wars poster. The left side has shades of red and purple, the middle is dark, and the right side has shades of green and purple. Also, a doubling Holga effect was added to the entire surface of the image – so you can see subtle shadows all around. The composition is completed by the orange "TABConf '21" logo at the bottom.

Famous Owners: Pieter Wuille, Jimmy Song, SeedSigner, Keith Mukai, Bitcoin Coder Bob, Justin Wales, probably also David Bailey.

No-coiners who might sell you their copy: LOL



BTCTKVR, 6th Edition (November 2021)

In early November, as TABConf and CoinFest UK were getting supplied with magazines, two interesting phenomena happened: genuine demand emerged for the magazines on Twitter, with people asking me how they can get a copy if they aren't attending any of the two conferences; also, the price of bitcoin hit its new all-time high of $68444.

This was when I decided to create a collectible which marks this special moment. With a supply of only 50 copies and a price point which barely covered the printing and delivery costs ($21 via Lightning, at the ATH rate), it went out of stock before I printed the first copy.

If anything, you can refer to this as the affordable version that anyone had the chance to get in a time when the project's popularity was at its peak. It doesn't feature any major changes, but the front cover and foreword are both unique and easily distinguishable.

Some may argue that there are similarities between the ATH edition and the magazines I sent to TABConf, but you can clearly see that the colors are positioned differently, the BTCTKVR logo at the top doesn't feature the Holga effect and has orange "BTC" letters, there's a rocket emoji which covers the masked troll army soldiers, and the text on the bottom clearly reads "2021 ATH Edition".

It's also worth noting that, at the time when I decided to create this edition, some people thought I was being "bearish" in relation to the price. Well, joke's on you because I've accurately called the top. If only I applied this intuition to trading!

I took the first 10 copies of the magazine to Budapest during my visit at Wasabi wallet HQ: so 20% of the owners are developers and marketers who work on the CoinJoin wallet. The remaining 80% were distributed all around the world, in countries such as Poland, Japan, The Netherlands, Hungary, Nigeria, and the United States of America. Don't ask me to whom I sent them because I don't and shouldn't remember.

Here are the facts that every collector should know about the sixth edition of the BTCTKVR magazine:

Total Supply: 50 copies

Release Date: November 9th 2021

Official Launch: On Twitter and at Wasabi Wallet HQ

Distribution: All 50 copies have been numbered from 1 to 50. Magazines numbered 1 to 10 were given to Wasabi wallet employees and collaborators.

Number of Pages: 92

Printed In: Romania

Cost: Roughly 0.0003 BTC (300 bits/30k sats)

Final Paragraph in the Foreword: "This 6th edition of the BTCTKVR celebrates our momentarily ATH and aims to offer you a unique collectible which marks this historic moment. Only 50 copies with this cover and foreword will ever get printed – and you are the lucky HODLer of one!"

Special Cover: Apparently, the front cover resembles the one from the Atlanta edition. However, there are evident chromatic differences when you put them side by side. This one also lacks the "doubling" Holga

effect on the logo, features a rocket emoji on the t-shirt, and includes the text “2021 ATH Edition” at the bottom.

Famous Owners: Nopara73, David Molnar, Lucas Ontivero, Yuval Nothingmuch, Karo Zagorus.

No-coiners who might sell you their copy: LOL





BTCTKVR, 7th Edition (December 2021)

The second BTCTKVR magazine proved to be a more challenging and demanding project than I expected. With longer articles, a more in-depth approach to topics, and two other volunteers who worked on translations for each piece, the difficulty level spiked significantly. At the time, while I was coordinating with the original graphic designer Mihnea (who arranged more than half of the articles), I noticed that the development is slower, so I’ve decided to keep the fire burning by creating one last magazine edition.

Since August 18th 2021, I’ve become very interested in experimenting with Counterparty – Bitcoin’s long-forgotten protocol which makes use of the base layer to enable tokenized asset creation. And in the middle of the NFT mania, I’ve also created (and mostly given away for free) some cards.

My idea was to do exactly what I’ve done with the Raretoshi edition of the magazine – but instead of using a centralized platform which curates content, I’d pursue the permissionless and censorship-resistant path of opening a dispenser (basically a vending machine for NFTs). Everyone who purchased one of the 21 BTCTKVRMAG NFTs for 0.0021 BTC has also received a free physical magazine delivery.

At the same time, I couldn’t replicate the recipe of the third edition for two reasons: I promised that the Raretoshi review article would remain exclusive to that version, and it’s likely that the Counterparty enthusiasts aren’t very interested in a network that’s less secure than Bitcoin’s base layer.

⟷ Dispenser Details	
Transaction Hash	24c4583336acd6705f02368879be8c3dcf7933b9c6b6c9cf61271ffa984fc6f6
TX Index	1,813,804
Block #	712,796
Time	a month ago (2021-12-06T00:56:15Z GMT)
Source	1KFcTqJUUoHLhPEpYFWPv2xXmKDE4bUZRF
Asset	BTCTKVRMAG
Give Quantity	1
Escrow Quantity	21
Give Remaining	0
Satoshi Rate	0.00210000 BTC
Status	Closed

I was definitely going to write an in-depth review about Counterparty. But for rather selfish reasons, I’ve decided to keep it for the second magazine and publish this last edition in the trusty 92-page format.

So at block height 712796 (December 6th 2021), I’ve opened the dispenser. To my surprise, someone grabbed a BTCTKVRMAG NFT in the next block. Nine blocks later, another two were gone. However, the

purchases slowed down after the 9th copy and it would take another 25 days until everything sold out. Nonetheless, given the stigma/bad reputation that NFTs had among Bitcoin maximalists, the result was remarkable. In comparison, the Liquid NFT edition took almost 3 months to sell out.

In the meantime, I've also rewarded the NFT owners with some extra airdrops of cards from the Bitcoin Head series (everyone should own some VLADHEAD, JOSHUAHEAD, and/or NOPARAHEAD cards).



Just like in the case of the Liquid NFT edition, I've used the third cover (the one next to the last page) to manually write down the NFT's name, the block height at which it was dispensed, and the Bitcoin address to which the BTCTKVRMAG token got dispensed. Of course, the special number and signature are there just like in every other official BTCTKVR magazine.

Maybe that this edition doesn't bring any new content – but thanks to reports from Duck Avenger (@Griptoshi) on Twitter and Rafaelpac (who submitted an issue on GitHub), all the tiny and overlooked mistakes have been fixed. With the Counterparty version, the first BTCTKVR magazine has finally reached maturity.

Like most free open source projects, it started with good ideas and good intentions, but an execution which proved to be suboptimal in some parts. This is where enthusiastic collaborators stepped in to help with quick fixes which polished the project and made it shine. So thank you for your contributions, it's been an honor to work on this and entertain the critical minds of bitcoiners with high-quality content.

Here are the facts that every collector should know about the 7th edition of the BTCTKVR magazine:

Total Supply: 21 copies

Release Date: December 6th 2021

Official Launch: On Twitter

Distribution: Everyone bought their copy from the Counterparty dispenser which offered BTCTKVRMAG NFTs in exchange for 0.0021 BTC. Even I bought a copy for myself. But according to the Bitcoin spirit, I'll enable everyone to benefit from the pseudonymity granted by BTC addresses (so no, I won't tell you what is the number of the magazine I own, but it's neither 1, nor 21).

Number of Pages: 92

Printed In: Romania

Cost: 0.0021 BTC

Final Paragraph in the Foreword: "This is the Counterparty edition of the BTCTKVR magazine, released in December 2021. If you own this, then you bought one of the BTCTKVRMAG Bitcoin NFTs from this dispenser: 24c4583336acd6705f02368879be8c3dcf7933b9c6b6c9cf61271ffa984fc6f6

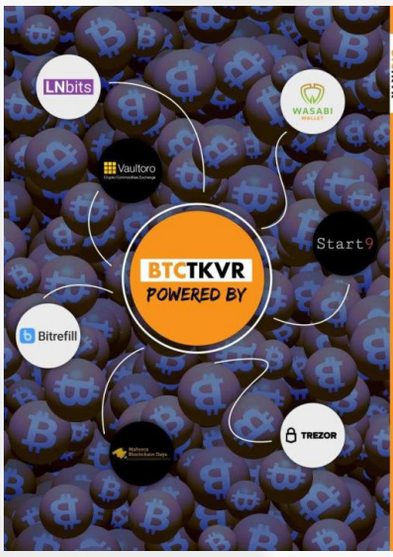
Take care of this rare collectible, only 21 of them will ever exist. For more details about your copy, check the last page. Thank you for supporting my work!"

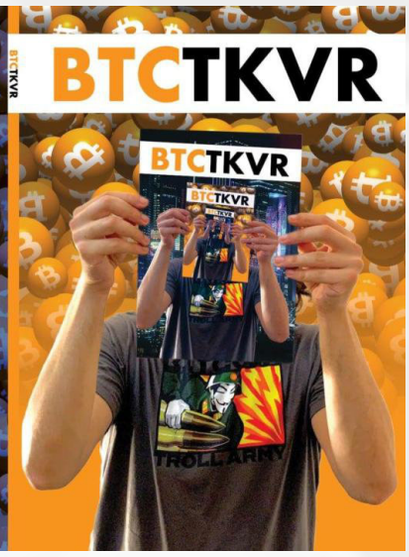
Special Cover: The front cover is as blue as the Genie from Aladdin's lamp, features a prominent glitch effect, and includes gradient samples of the Counterparty logo at the bottom.

On the third cover (next to the last page) you will find the number, my signature, the name of the NFT, the block height at which it was dispensed, and the address which received the transfer. Everything is written by hand.

Famous Owners:
bc1ql3yvqfmdpeztpt304h2rw00yl052wvllu2ldsg,
18NeUpEHzAquBcsncM5BGLR4VgaPXZhPp2,
1JTe3QnzZWAduLBRABusHziitUaYUgcm49
…well, you get the point.

No-coiners who might sell you their copy:
LOL





BTCTKVR, 8th Edition (Forever Free & Open Source)

Well, at this point you're probably asking yourself "How do I get one of these magazines without buying a copy on secondary markets?". My answer for you is simple: print your own.

Unlike every other edition, the free open source BTCTKVR magazine has no supply cap, doesn't require numbering, doesn't rely on me for any kind of service, and is therefore permissionless and decentralized. You can feel free to print as many as you want and use it for any purpose you may envision. Feel free to produce copies for your conference or meetup, create some unique birthday gifts for your friends, or even sell the copies in your store.

All the files are in the project's GitHub repository, so you can pick which pages from which articles you want to print and build your own unique copy of the BTCTKVR magazine. But if you want to create a copy which has all the 92 pages, here are the instructions:

1. Download all the magazine pages. Leave the covers for later, as they need to be printed separately on thicker paper. All the pages are jpeg files that you'll have to convert to PDF;

2. Open a conversion website like smartpdf.com (or else use similar software that you install on your computer);

3. Take all pictures in the correct order and import them in your software. If you put everything in, you should get a PDF file that's 107 MB large;

4. Download the covers from GitHub. This is a separate PDF.

5. Send both PDFs (compiled magazine pages + covers) to your favorite print shop. For an authentic BTCTKVR experience, tell them to use 300g glossy paper for the covers and 150g matte paper for the pages. The recommended format is A4, but you can feel free to experiment.

6. Based on my experience, printing a high-quality magazine costs 10 to 20 USD. The beauty of free open source projects is that you can create your own version of any quality, according to your own budget.

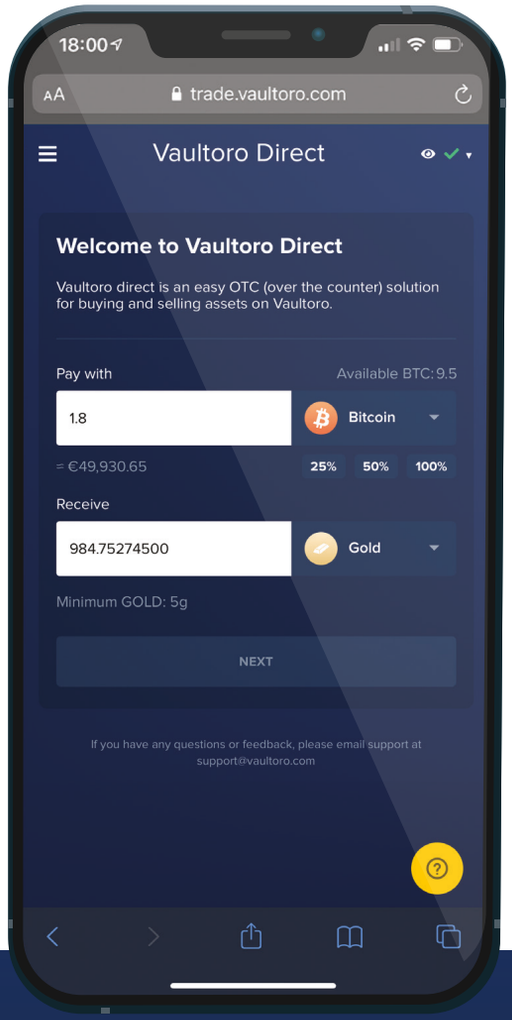
7. Enjoy reading and spreading knowledge!

For example, Matt Hill of Start9 has printed 5 copies of the FOSS magazine for a Lightning meet-up in Denver. He opted for a smaller pocket-sized format which makes this unofficial edition truly unique.

It includes a special last paragraph in the foreword, which reads: "Thanks to Matt Hill of Start9, the BTCTKVR magazine has travelled across the Atlantic Ocean to reach Mile High City. To make the event more special, we've changed the cover and this note, so your BTCTKVR is more of a rare collectible. But my suggestion for you is to pass the magazine to a friend after you finish reading it – make the Bitcoin Takeover a super spreader event".

The copies are not numbered or signed, and I didn't pay for their production or print them locally either. So I consider them an unofficial part of the collection and a great example of free open source magazine production. Everyone interested in free Bitcoin content for an event can do the same without asking for my permission or paying me anything.

But then again, if you're on the market for a truly special collectible, watch out for one of the 442 "official" copies. And if you want to become a collector, then I've offered you all the resources you need to identify any copy that you might be missing. Thank you all for supporting my work and never stop spreading the good word about Bitcoin!



VAULTORO DIRECT

SINCE 2015

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 larger variety of ERC20 tokens. Vaultoro allows you to trade with other user or use our Direct service.

INSTANT SETTLEMENT

Buy Gold and Silver in seconds.

ALLOCATED PRECIOUS METALS

Stored in your name, as your property in high security vaults 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



5 Reasons You Should Run Your Bitcoin Node on a Raspberry Pi 4

Bitcoin nodes are the network's validators: they keep miners honest and they also allow users to verify their own transactions and manage their own financial privacy. They are a tool of sovereignty which works on pretty much any computer manufactured since 2010. And yet, for many reasons, the Raspberry is among the finest choices for your validator hardware.

This article is not paid or endorsed by the Raspbery Pi Foundation and isn't meant to convince you to purchase a new device. As a matter of fact, the best computer that you can use to run a Bitcoin full node is the one you already own. However, there are some undeniable advantages that these tiny ARM-based machines have.

Sure, the earlier iterations were sluggish and unreliable. When I tested the Raspberry Pi 3-powered Casa node in February 2019, it was disappointingly slow. Most of the times I wasn't even sure if the device was stuck or if I should wait a little longer for it to load. But later in the year, the Raspberry 4 was launched and it brought faster quad-core processors, as well as 4 gigabytes of RAM – everything at the price of $55.

Thanks to this breakthrough in microprocessing and economies of scale, becoming financially sovereign became easier and more affordable. So without further ado, here are the reasons why you should run your Bitcoin node on a Raspberry Pi 4.

1. The Raspberry Pi 4 is energy-efficient and green

For all the "Bitcoin mining is boiling the oceans" narratives, it's good to have the validating side of Bitcoin run on such low-powered devices. Keeping your Raspberry Pi 4 Bitcoin node 24/7 will consume just as much energy as leaving your Max-sized iPhone to charge every day. And this is no small feat – millions of people can afford to run their own Bitcoin validators with minimal maintenance and operation costs.

At any given moment, my Raspberry Pi 4 Bitcoin and Lightning node never uses more than a third of the device's processing power.



This means that the energy consumption oscillates around the 4-watt range (a kilowatt every ~24 hours, approximately 365 kilowatts a year). At my energy provider's rate of 8.5 cents per kilowatt, it costs me $31 a year to keep the node running 24/7.

The fact that I use it to run both Bitcoin and the Lightning Network is nothing short of impressive. And given the large amount of Raspberry Pi computers that process Lightning transactions, it's safe to say that this second layer is the world's most environmentally-friendly way of sending money.



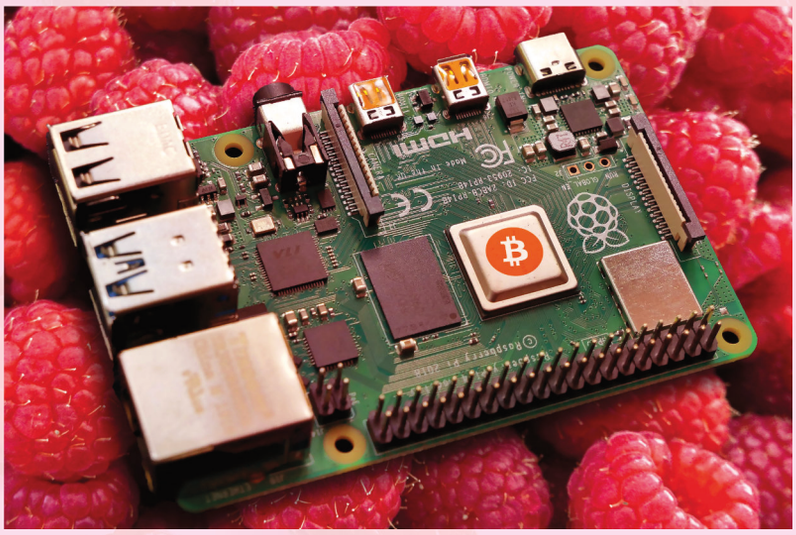
2. The Raspberry Pi 4 is inexpensive, general-purpose, and easy to source globally

If mining rigs can cost a few thousands of dollars, then buying a new Raspberry Pi 4 with a large hard drive, a cool case, a touchscreen, and cables shouldn't cost more than $200. In this setup, it's actually the 1 TB hard drive that will cost more (especially if you go for the faster, quieter, but lesser rewrite-friendly SSD).

Furthermore, the popularity of the Raspberry Pi has significantly increased its global availability and use cases. So you can walk into a local electronics store (or go to a retailer's website) and buy one of these tiny ARM machines with the maximum amount of plausible deniability. If your authoritarian government asks, you can simply claim that you want to build a video game console or an everyday desktop computer out of it – both use cases are popular and plausible, so nobody will feel suspicious about it.

In the case of Bitcoin hardware, it's important for it to not be application-specific or labelled as such. If the potential reward involves scarce pieces of digital gold, then malevolent actors will have a greater incentive to take the risk of compromising your device during the delivery process. Yet the non-Bitcoin use cases for Raspberry Pi





computers are the most common. For extra plausible deniability, you can even buy a couple of units and use one for the most common and expected use case. This way, the probability of supply chain attacks diminishes significantly (though this doesn't mean that you shouldn't do a chip verification yourself).

3. There's a lot of Bitcoin software that works on the Raspberry Pi 4

Hardware is only as valuable as the software that makes use of its capabilities. In Bitcoin's case, there are lots of robust and free open source options for Raspberry Pi nodes. Since the creation of the RaspiBolt operating system by Stadicus, we have witnessed an entire wave of user-friendly operating systems which run Bitcoin and Lightning on affordable hardware.

I usually recommend people to use RaspiBlitz, as it offers a great amount of features and extensions on top a minimalistic but well-written user interface. However, there are other great options out there such as MyNode and Start9 Labs' Embassy OS. Another popular option is Umbrel – however, its license is not specific for free open source software (at least not yet) and therefore I can't recommend it.

If I were to find desktop operating system equivalents for these solutions, RaspiBolt would be Debian Linux, RaspiBlitz would be Ubuntu, MyNode would be Mint Linux, Start9 Labs' Embassy OS would be Fedora Linux, while Umbrel would be Mac OS.

Regardless of which one you choose, you're going to find some of the same powerful software. This includes Electrum Server, Run the Lightning, BTCPay Server, Tor integration, LNBits, a mixing service like JoinMarket, and a decentralized chat application such as Sphinx (among many others).

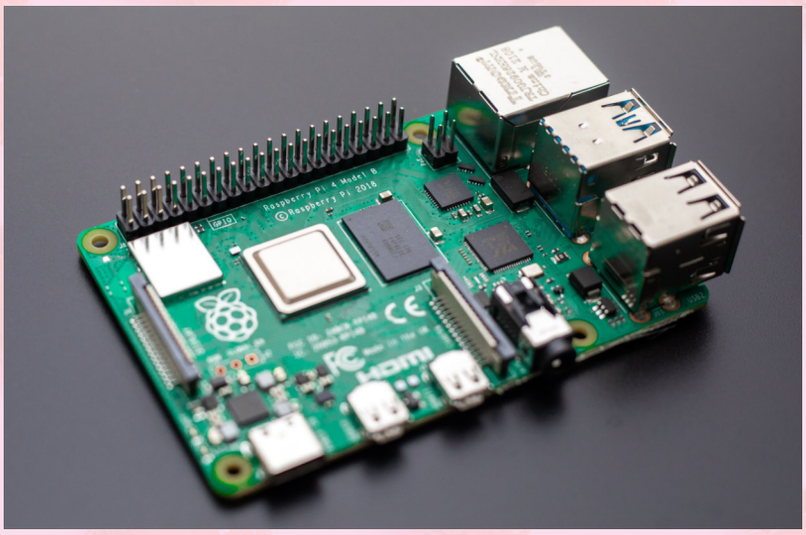
4. The Raspberry Pi 4 is tiny and quiet

There's a lot to be said about the advantages of a small computer. But mostly, especially in the case when you want to have an always-on device, it's great to be able to place it in your living room without having to worry about the noise.



If you pick a good aluminium case which dissipates heat very well, you won't even have to deal with noisy active cooling solutions. And if you run your Bitcoin and Lightning node on an SSD, there won't be any spinning to make any noises. You get the quietest, most cost-efficient, and environmentally-friendly experience.

The fact that it comes in a tiny palm-sized form factor that you can fit behind pieces of furniture also adds up to your privacy, plausible deniability, and peace of mind.



5. The Raspberry Pi 4 is pretty secure as a dedicated Bitcoin node

People use Raspberry Pi computers to run servers, relays, video game emulators, livestreaming machines, payment processors, and the killer app which rules them all: validating Bitcoin and Lightning transactions. And it's not like they couldn't do it on a more powerful computer which runs everything in virtual machines.

The issue at stake is security: if you have a device which only does one specific task and its entire hardware is optimized for it, then its attack surface is lower. On the other hand, the multi-core work computer that can run anything in virtual machines is more vulnerable to attacks due to the greater complexity of the setup.

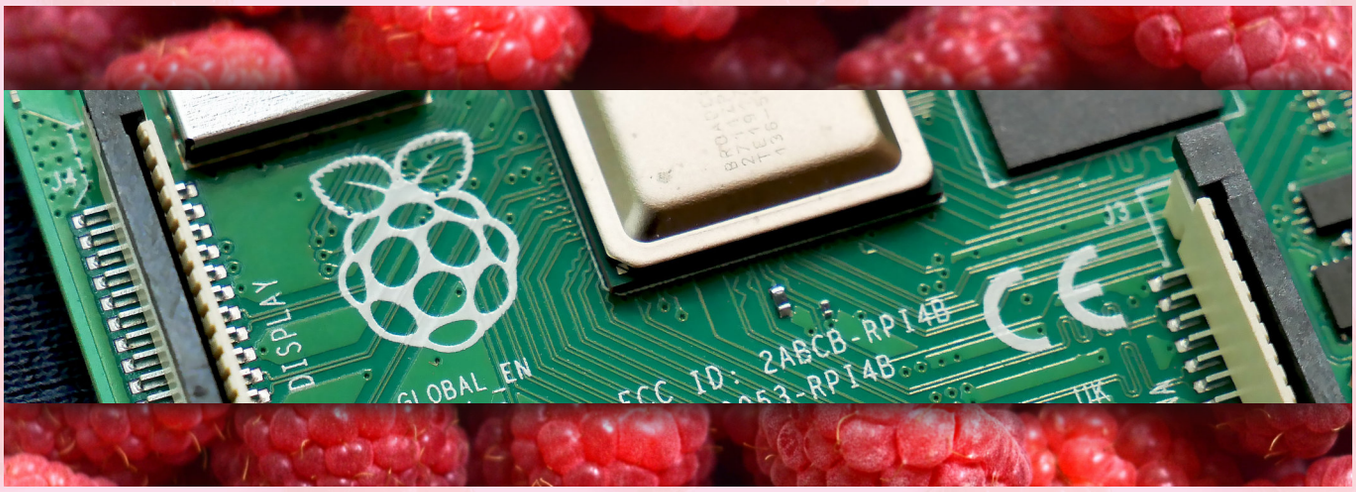
A Raspberry Pi Bitcoin node takes you back to a time when every item in your house fulfilled a single basic task: you had a turntable for music, a TV set for video entertainment, and a video game console that played cartridges. Though it's convenient to have it all on a smartphone or computer, it's also fundamentally more insecure. This is why having hardware which fulfils only one task is important, especially when you deal with sound money.

However, the Raspberry Pi 4 is NOT open source hardware



Remember the second paragraph of the article, in which I mentioned that the Raspberry Pi Foundation doesn't pay me for this and it's merely a representation of my own thoughts? Well, I was serious about it. The Raspberry Pi is great for what it does, but there are a few reasons why it's not ideal for something like Bitcoin.

Bitcoin is free open source code that anyone can read, download, verify, and potentially modify. It works on the basis of a permissionless philosophy where you don't have to appeal to any authority in the world in order to access the network. Free open



source software also needs free open source hardware. However, there isn't enough of it right now.

So if you want to build your own Raspberry Pi because you find yourself in a country that won't let you import one, you're gonna have a hard time. And if you need to replace or upgrade parts of the board, it's also unlikely to find replacements (unless you purchase a new Raspberry Pi altogether). This is part of the tradeoff involved in the ARM architecture: you get systems on chips (SoCs) and systems on modules (SoMs) that are hard to replicate by using general-purpose parts that you find on the market.

There's also a debate to be had about chips with NSA backdoors: as consumer-grade computers, the Raspberry Pies are most likely surveilled and hackable by government agencies.

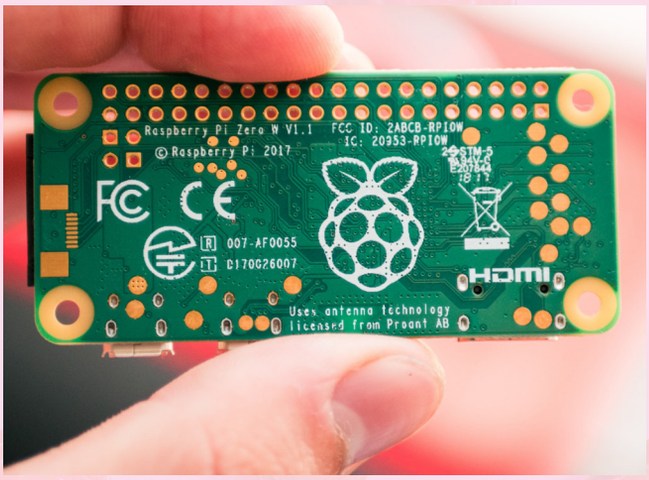
If you want a truly open source hardware experience, then look into RISC-V computers. By manufacturing or purchasing (and subsequently verifying) one of these, you know that you're using an open standard that nobody can compromise without leaving a visible trace. There is a price to pay for your extra privacy, though: a computer that can barely surf the web will cost you about $4000 and there isn't as much Bitcoin software that you can run on it.

Though Bitcoin Core has been running on RISC-V since the release of version 0.18.0 in May 2019, I couldn't find any Lightning clients that work with these open source CPUs. And if LND or c-lightning don't work, then you won't benefit from the other applications either (RTL, LNBits, BTCPay, and Sphinx Relay).

Part of the reason why the RISC-V standard doesn't get too much support is the cost of the hardware – very few people can afford it, which is the exact opposite of the reason why the Raspberry Pi is so popular. But given the recent resurgence of open source hardware thanks to Trezor's Tropic Square and bunnie's Precursor project, we can hope that in the future they will also turn their attention to processing units, RAM memory, and mother boards that are verifiably open source and don't cost more than the average gaming PC.

It has only been 13 years since Bitcoin got launched and 9 years since Edward Snowden revealed to us the magnitude of NSA's surveillance operations. Also, it wasn't until 2018-2019 that the RISC-V really became popular and open source chip manufacturers started to raise money.

Maybe that for now, low-powered computers such as the Raspberry Pi and the Arduino are the kings of the game. But in the future, we might have completely open source hardware to run all the great Bitcoin free open source software.



motorina0



Elon Musk Doesn't Understand Decentralization – But You Should

Decentralization is hard and Elon Musk clearly doesn't understand it. Not only that he has a childish view on blockchain scaling and chooses to disregard the existing research on the topic, but he is also blatantly ignorant when it comes to wealth concentration (yet another factor which makes a project decentralized) and doesn't seem to get incentives in a Proof of Work system. In a nutshell, he is the epitome of the "I just heard about Bitcoin, I'm here to fix it" meme.

Maybe that we shouldn't expect much from a company CEO who excels at receiving government subsidies while criticizing them and has also been involved in the creation of PayPal – a centralized internet payment system which uses infinitely inflationary government money and relies on a revenue system that can make profits even if it stops charging transaction fees (the fact that it's rigging conversion rates and collects user data is already enough).

But just because the world's richest man doesn't understand Bitcoin (or his meme-able fork of choice, Dogecoin), it doesn't mean that you also shouldn't. As a matter of fact, I will make sure that by the time you will have finished reading this article, you will understand decentralization and Bitcoin a lot better than Elon Musk.



Decentralization means that anyone should be able to participate in the network

On May 16th 2021, Elon Musk tweeted: “Ideally, Doge speeds up block time 10X, increases block size 10X & drops fee 100X. Then it wins hands down.”



Before we begin analyzing the intricate implications of this tweet, I must start by saying that Bitcoin and Dogecoin have a fairly similar architecture. After all, Dogecoin is a more inflationary copy of Litecoin (which in turns is a slightly modified Bitcoin fork). So even though some parameters such as block size, block time, and supply are different from one coin to another, the underlying principles are the exact same – especially when we focus on decentralization.

Now let’s get back to Elon Musk’s tweet, which mentions 3 parameters of cryptocurrencies: block time, block size, and transaction fee. The first two are extremely important for defining decentralization, while the third criterion is essential for security and long-term sustainability (and therefore, also indirectly consequential for decentralization).

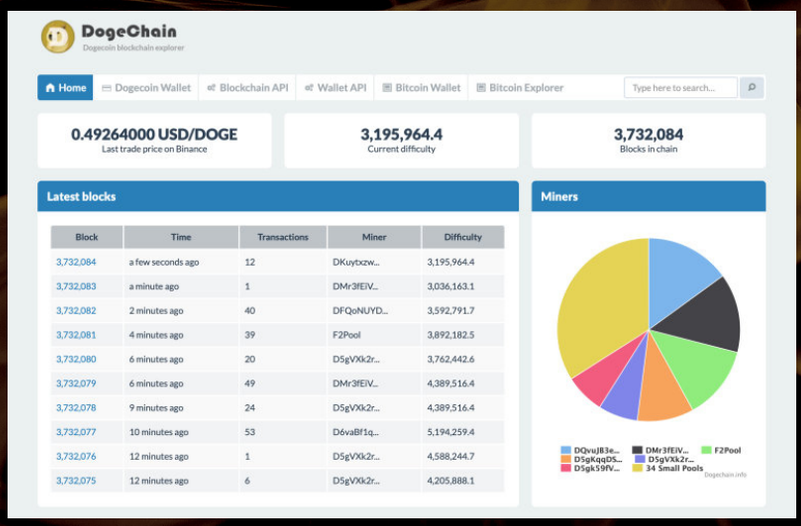
The block time is the factor which decides who can validate the blockchain on the basis of internet speed. Most famously, the Bitcoin network mines a new block at an approximated rate of one every 10 minutes.

This means that nodes from all around the world can get in sync if they are able to download 1-2 megabytes every 10 minutes. And this is especially great in cases when users come from authoritarian countries where the access to internet is limited or restricted. It’s also great for people living in the rural areas of lesser developed countries, who may not have access to high-speed connections. Anyone around the world can validate the blocks that get generated in the Bitcoin network. And theoretically, miners could even undergo their operations in the middle of nowhere while accessing the signal



from Blockstream's satellites. I've explained this in greater detail in my article "Bitcoin Is Not Slow – It's Highly Secure".

Dogecoin already has a block time of 1 minute – and this design favors internet users with broadband connections and faster access speeds. Billions of people get denied the chance to sync their nodes, as only city dwellers are able to get all the data in real time. The situation is also bad for interplanetary transmission (one of Musk's ambitions), as sending a radio signal from Earth to Mars can take anywhere from 4.2 to 21 minutes (depending on the momentary distance). In most cases, Bitcoin would be better suited for this use case.



And yet Dogecoin's block time is fairly reasonable given the amazingly-low demand for block space. As a matter of fact, this $63 billion project only processes a handful of transactions per block – which is indicative of centralized ownership and excessive retail trading on the exchanges' balance sheets. The amount of Dogecoin empty blocks in the middle of a bull market (and clear bubble) is staggering – keep in mind that 1 transaction means that only the block reward was sent to the successful miner.

This leads us to the part about increasing Dogecoin's block size 10X times. Though it seems unnecessary given empirical data, let's assume that somehow the users start using the blockchain. If DOGE transactions were to fill 10 megabyte blocks every 6 seconds, then the public ledger would grow by 100 megabytes per minute, 6 gigabytes per hour, 144 gigabytes per day, and 4.32 terrabytes per month. Almost as bad as Chia, Bram Cohen's terrible yet overhyped Proof of Work Frankenstein.

Sure, this scenario is unlikely, as even in the case of Bitcoin there are times when the blocks don't get entirely filled. But even if an average of a quarter of block space gets filled, then the Dogecoin blockchain expands by 252 gigabytes per week. To put this into perspective, it took the Bitcoin blockchain 12 years to reach 350 gigabytes in size.

For most people around the world, a 1 TB hard drive is fairly expensive. But if Dogecoin issued 10 megabyte blocks every minute, then the capacity of the terrabyte SSD would get filled in a week. In comparison, the Bitcoin blockchain adds about 51.32 gigabytes of data every year, so the same 1 TB hard drive should cover 19 more years of running a full archival node.



When designing a decentralized system, you must make sure that you don't price out anyone with discriminatory network upgrades. If you can't validate your own transactions and check the state of the entire network with your own node, then the system is centralized.

The internet definitely doesn't ask you to get a high-end computer to access webpages – and as a money system, Bitcoin aims to be as inclusive and open to the greatest number of people around the world. Elon Musk clearly doesn't understand this and aims to

centralize an abandoned yet meme-able project under his own unpredictable dictatorship which seeks to turn something universal and open into a pet project.

To recap: if you can't join the network as a validating node, then the project is not decentralized. Decreasing the time interval between blocks excludes the people running slow internet connections, while increasing the block size will boost the storage and computation costs of all participants (therefore phasing out those who don't upgrade regularly). This is why second layers like the Lightning Network exist. But it seems like Elon Musk wants to build another PayPal.



Decentralization requires incentives (including mining fees)

Though Dogecoin is momentarily extremely inflationary, its halving schedule should reduce mining rewards significantly over the next few years. The same happens with Bitcoin, which raises the stakes of the disinflationary game of scarcity every 210,000 blocks (approximately every 4 years).

As the reward for discovering a block gets lower, miners should become incentivized to keep on securing the network. On the fourth page of his seminal whitepaper, Satoshi Nakamoto described a system which eventually becomes inflation-free and whose miners get incentivized to keep going by virtue of transaction fees.

Without these fees, the incentives get broken and it's likely that many miners will stop supporting the network. But the 100X fee reduction that Elon Musk described might be ideal for him to take over the network and keep on mining blocks at a financial loss while retaining control.

Arbitrarily lowering the fees will result in reducing the amount of miners. And fewer miners means less decentralization and greater odds at controlling the network. While this might be what Elon Musk is after, it's a terrible idea. There's nothing revolutionary or disruptive in a system that the world's wealthiest man can censor – after all, it's the dynamics of geopolitics that make Bitcoin and Dogecoin more fungible and resistant to blacklisting transactions.

Paying 100 times fewer fees sounds great in practice, but in the long term it will only erode the system and lead to more control/centralization or more inflation. Also, fees are great for preventing spam transactions – if there's a cost involved, then people are less likely to clog the network



with lots of small transactions because they must pay for each one of them. Musk's vision for Dogecoin is technically flawed.

Decentralization and wealth distribution

On May 17th 2021, Elon Musk responded to Pranay Pathole's concerns about the wealth concentraPon of Dogecoin. According to BiPnfocharts, there are 107 Dogecoin addresses that own more than 66.7% of the supply. Also, there is one address which owns 28.34% of the enPre supply – a disproporPonate amount, given the supposed ambiPons of the project. Elon Musk chooses not to look into the issue with nuance, by offering a generic response about Robin Hood potenPally being the biggest whale. While it might be true, it's not confirmed.



But let's compare this situation to Bitcoin's. The top 3 addresses are clearly identified as the cold storage funds of Huobi, Binance, and Bitfinex. And cumulatively, they own 2.68% of the users' funds – that's right, the biggest entities are actually custodians which store the funds of hundreds of thousands of customers.

In Bitcoin, there are currently about 16,000 addresses which own 62.95% of the supply. Not ideal, but still better than Dogecoin's situation where 107 addresses hold over one third of the currency units. Ethereum also looks worse, with large individual wallets holding too many coins (most likely a consequence of their 70% premine and early investors or cofounders who didn't sell).

So why does wealth distribution matter for decentralization? It's also about incentives and inclusiveness. Nobody would want to take part in a project where a small number of elites control most of the money. The investors wouldn't want to become subjected to such a risk, the developers wouldn't want to be under the control of a few actors, and miners would also find the centralization displeasing and unsustainable on the long-term.

These large holders are single points of failure that rig the game for everyone else around them. Holding a bigger stash might also imply a greater influence on development and some political power in the network. Which is definitely a threat for an unmaintained network like Dogecoin.

Bitcoin distribution

Balance, BTC	Addresses	% Addresses (Total)	Coins	$USD	% Coins (Total)
(0 - 0.001)	19622119	51.64% (100%)	4,060 BTC	187,107,133 USD	0.02% (100%)
[0.001 - 0.01)	9421945	24.8% (48.36%)	35,992 BTC	1,658,595,444 USD	0.19% (99.98%)
[0.01 - 0.1)	5740398	15.11% (23.56%)	185,966 BTC	8,569,804,347 USD	0.99% (99.79%)
[0.1 - 1)	2400783	6.32% (8.46%)	752,247 BTC	34,665,493,898 USD	4.02% (98.79%)
[1 - 10)	665522	1.75% (2.14%)	1,697,758 BTC	78,237,101,339 USD	9.07% (94.77%)
[10 - 100)	130726	0.34% (0.39%)	4,255,733 BTC	196,115,278,881 USD	22.75% (85.7%)
[100 - 1,000)	13970	0.04% (0.04%)	3,947,599 BTC	181,915,645,208 USD	21.1% (62.95%)
[1,000 - 10,000)	2073	0.01% (0.01%)	5,092,326 BTC	234,667,670,041 USD	27.22% (41.85%)
[10,000 - 100,000)	84	0% (0%)	2,236,025 BTC	103,041,850,124 USD	11.95% (14.63%)
[100,000 - 1,000,000)	3	0% (0%)	501,390 BTC	23,105,341,964 USD	2.68% (2.68%)

Addresses richer than

1 USD	100 USD	1,000 USD	10,000 USD	100,000 USD	1,000,000 USD	10,000,000 USD
33,006,829	14,871,813	6,221,037	2,033,219	394,735	90,020	7,984

Don't tell Elon: Dogecoin is a minority hashrate chain which gets merge mined with Litecoin

Dogecoin's continued existence as a network is due to pure benevolence on behalf of some actors. Most importantly, the Litecoin miners have decided to save Dogecoin in 2014 by allowing it to get merge mined. So instead of becoming vulnerable to malevolent attackers, it's protected by some of the same Scrypt miners who secure the majority hashrate chain.



Litecoin's mining is nearly as energy-intensive as Bitcoin's, but differs in some regards which concern technical specifications (Bitcoin's SHA 256 is processing-intensive, while Litecoin's and Dogecoin's Scrypt is rather memory-intensive).

But if Elon Musk decides to criticize Bitcoin mining while turning a blind eye to the way in which Dogecoin gets produced, then he's a textbook hypocrite who virtue signals with cherry-picked data to appeal to an angry and woke mob while covering his Dogecoin dealings under a veil of ignorance.

To say the least, Elon Musk is intelectually-dishonest, inconsistent, and strongly biased. If left alone, Dogecoin would fall prey to attackers who can afford to rent some mining gears for a few hours. And if the project gets co-opted by Tesla or SpaceX, then it loses its value proposition.

The changes proposed by Elon Musk require a centralizing hard fork

Hard forks are network changes which require all participants to join a new blockchain. They create an incompatibility between the old blockchain and the new one, and therefore rely on the consensus that everyone should migrate.

The easier it is to pull off a hard fork, the more centralized the project is. Ideally, sovereign node operators and miners should be wary of new changes, reject leadership, and choose to verify every line of code individually and selfishly. But when the world's richest man shows up and says he wants to take on a leadership role, it's already a bad sign that will only lead to more centralization. And yes, I am also a critic of Michael Saylor's involvement.

Will the exchanges support a hard fork just because Elon Musk is involved? That's questionable, since lots of them are



principled and really try to analyze the long-term fundamentals (as opposed to Binance, which seems to support anything that generates trading volume).

Will the users migrate to Dogecoin Elon's Vision? Well, there aren't so many users in the Bitcoin sense (sovereign nodes). So it's up to exchanges and the entities that do have an incentive to run a node to decide. There's too much centralization involved, though.



For reference, the Bitcoin developers are doing their best to avoid hard forks. The recent Taproot trial only proves that the network is mature enough to decide in a decentralized way on a soft fork (an upgrade which doesn't change the consensus rules and is optional for the entire network).

There's a reason why Bitcoin development is so conservative: the decentralization works

Decentralization is hard. And if you're new in the space and you're accustomed to a world where phone application updates get deployed and installed within minutes, you're going to have a hard time understanding a system like Bitcoin which relies on lengthy deliberation and tends to get ossified over time.

If improving blockchains was so easy, wouldn't Bitcoin already have bigger blocks, faster block times, and lower fees? It's a little naive to assume that these proposals are new and nobody has ever thought about putting them into practice. And a Silicon Valley "move fast and break things" mentality certainly doesn't help a money system that's supposed to make everyone's savings secure rather than fast and easy to transfer.

Dogecoin was never supposed to get such a high valuation and wasn't created for the purpose of increasing the wealth and influence of the world's richest man. But here we are talking about this topic and trying to define what decentralization should look like – as opposed to Elon Musk's poorly-informed musings.

Decentralization is hard – and I hope that this lengthy article of mine has helped you understand it better than Elon Musk. If you're looking for a shorter version, then search for the "decentralization is hard" thread that I posted on Twitter.



Mallorca Blockchain Days

Bitcoin & Liberty

„Nothing is true, everything is permitted“

- F. Nietzsche -

Join us at Mallorca Blockchain Days

July 14 - 17 2022

Palma, Mallorca, Spain

GET YOUR TICKET ONLINE

WWW.MALLORCABLOCKCHAINDAYS.COM

#MallorcaBCDays

Mallorcablockchaindays



The 3094 Bitcoin Theft Which Led To The Creation of The Trezor

Back in 2012, the times were a lot simpler for bitcoin HODLers. As a matter of fact, it would take another year and a half until they were even called HODLers – as the term "HODL" was later coined by the whiskey-drinking Bitcoin-Talk user GameKyuubi.

We're talking about the early days, when the price of 1 BTC ranged from 4 to 13 dollars throughout an entire year. Today's volatility margin for a few seconds used to be the entire market cap of bitcoin – and most of the users were cypherpunks, computer nerds, and libertarians.

Consequently, people were a lot more relaxed about security and didn't consider all of the threat models that make all of us feel so suspicious today. Losing coins was a lot more common, as even some of the more technical users were reckless about using hot wallets.

To their credit, the wallets at the time required users to either recover wallet.dat files (in Bitcoin qt), scan QR codes of private keys (for mobile wallets), or type in the keys manually (that's right, people used to make payments by entering addresses by hand). It would take another year and a half until the BIP39 standard was invented, so users can convert their private keys into mnemonic words from a dictionary.



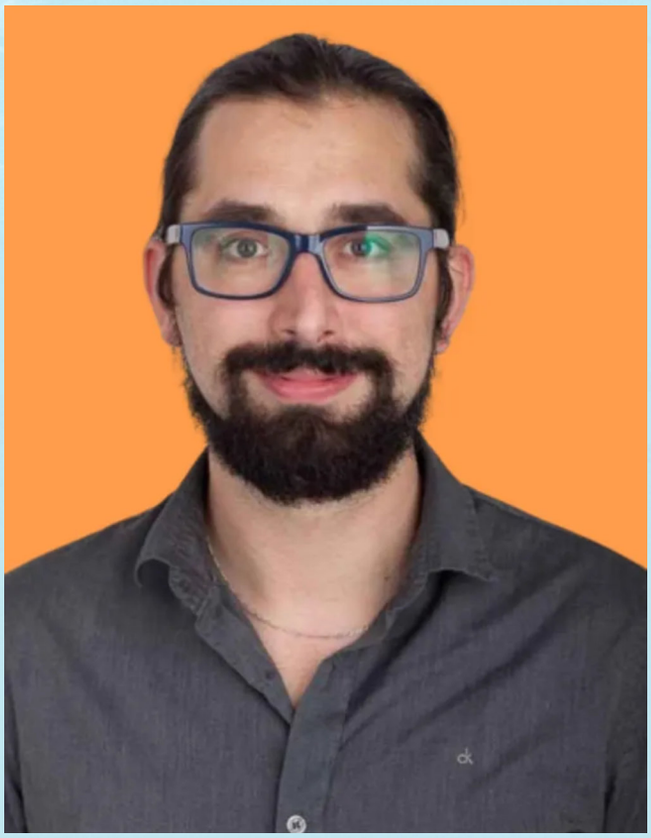
March 1st 2012 – Slush Pool's Linode Backup Servers Get Hacked, 3094 BTC Get Lost

In Early 2012, Marek "Slush" Palatinus was running his operations at Slush Pool (the world's first mining pool, as acknowledged by Satoshi himself) with a little help from cloud hosting company Linode. Everything seemed to be fine until March 1st 2012, when Slush received an unexpected text message from his pool monitoring service – apparently, his bitcoin reserve had been unexpectedly depleted.

After undergoing some investigations, the Czech cypherpunk discovered that two of the Linode servers he was running as backups for the mining pool data were compromised – somebody had restarted them and had their administrator passwords changed.

The issue concerned a vulnerability in the Linode manager software – it had nothing to do with the security of the Bitcoin software or the mining pool's protocols. It's likely that Bitcoin was becoming a hot topic among computer hackers, as many other Linode instances running bitcoind have been targeted around the same time.

In total, 50000 BTC were stolen from Linode servers on March 1st 2012 – thus marking the biggest theft of bitcoins yet. And all of this happened due to one security update that was succesfully exploited by hackers. Even Gavin Andresen's bitcoin faucet, which was giving away free BTC, was affected by this unfortunate event.

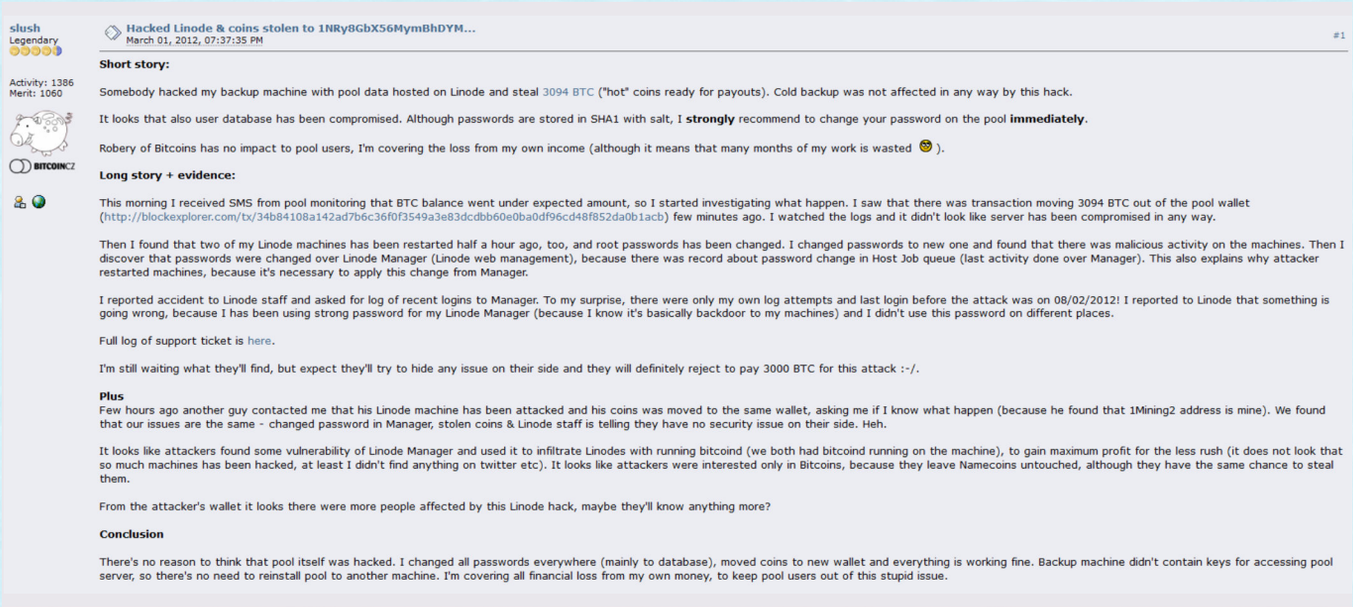


internally screams

And yes, there was a time in history when people were giving away bitcoins for free just to grow the community and create a healthy economy.

But let's get back to the exploit: of the 50000 bitcoins lost that day, "only" 3094 belonged to Slush Pool – about $15.312,





slush
Legendary

Activity: 1386
Merit: 1060

BITCOINCZ

Hacked Linode & coins stolen to 1NRy8GbX56MymBhDYM...
March 01, 2012, 07:37:35 PM #1

Short story:

Somebody hacked my backup machine with pool data hosted on Linode and steal 3094 BTC ("hot" coins ready for payouts). Cold backup was not affected in any way by this hack.

It looks that also user database has been compromised. Although passwords are stored in SHA1 with salt, I **strongly** recommend to change your password on the pool **immediately**.

Robery of Bitcoins has no impact to pool users, I'm covering the loss from my own income (although it means that many months of my work is wasted).

Long story + evidence:

This morning I received SMS from pool monitoring that BTC balance went under expected amount, so I started investigating what happen. I saw that there was transaction moving 3094 BTC out of the pool wallet (http://blockexplorer.com/tx/34b84108a142ad7b6c36f0f3549a3e83dcdbb60e0ba0df96cd48f852da0b1acb) few minutes ago. I watched the logs and it didn't look like server has been compromised in any way.

Then I found that two of my Linode machines has been restarted half a hour ago, too, and root passwords has been changed. I changed passwords to new one and found that there was malicious activity on the machines. Then I discover that passwords were changed over Linode Manager (Linode web management), because there was record about password change in Host Job queue (last activity done over Manager). This also explains why attacker restarted machines, because it's necessary to apply this change from Manager.

I reported accident to Linode staff and asked for log of recent logins to Manager. To my surprise, there were only my own log attempts and last login before the attack was on 08/02/2012! I reported to Linode that something is going wrong, because I has been using strong password for my Linode Manager (because I know it's basically backdoor to my machines) and I didn't use this password on different places.

Full log of support ticket is here.

I'm still waiting what they'll find, but expect they'll try to hide any issue on their side and they will definitely reject to pay 3000 BTC for this attack :-/.

Plus
Few hours ago another guy contacted me that his Linode machine has been attacked and his coins was moved to the same wallet, asking me if I know what happen (because he found that 1Mining2 address is mine). We found that our issues are the same - changed password in Manager, stolen coins & Linode staff is telling they have no security issue on their side. Heh.

It looks like attackers found some vulnerability of Linode Manager and used it to infiltrate Linodes with running bitcoind (we both had bitcoind running on the machine), to gain maximum profit for the less rush (it does not look that so much machines has been hacked, at least I didn't find anything on twitter etc). It looks like attackers were interested only in Bitcoins, because they leave Namecoins untouched, although they have the same chance to steal them.

From the attacker's wallet it looks there were more people affected by this Linode hack, maybe they'll know anything more?

Conclusion

There's no reason to think that pool itself was hacked. I changed all passwords everywhere (mainly to database), moved coins to new wallet and everything is working fine. Backup machine didn't contain keys for accessing pool server, so there's no need to reinstall pool to another machine. I'm covering all financial loss from my own money, to keep pool users out of this stupid issue.

since the bitcoin price was slightly below the $5 mark. As of March 27th 2021, this loss amounts to almost $169 million.

Slush decided to cover the loss from his own pocket, so no pool participant would be affected by this unfortunate event. However, he took it all as a lesson – since he'd effectively lost the money he earned in months of doing work for Slush Pool, he decided to never allow this to happen again.

The Czech cypherpunk figured out that the issue wasn't just Linode: it could have happened to any service which is constantly connected to the internet, and can therefore get attacked. And as the interest for Bitcoin was on the rise, a better solution for private key management had to be invented.



The World Meets Trezor: The First Bitcoin Hardware Wallet

After the 3094 BTC hack, it would take another 2 and a half years until Bitcoin security enthusiasts could get their hands on the Trezor. And the price of admission would baffle today's coiners: 1 BTC ($500 around launch date) for the standard plastic case version, and 3 BTC ($1500 in May 2014) for the metallic case version.

But in their defence, the price of bitcoin spiked from $118 in May 2013 to $500 in May 2014, and it hovered above the $1000 mark in late November. So it wasn't the best time to use BTC as a unit of account – though the price remained within the $400 range for most of 2014.

The road to releasing the world's first hardware wallet was also bumpy and somewhat of an odyssey in and of itself – Slush co-opted two friends to create SatoshiLabs (Slush Pool collaborator and CoinMap creator Pavol "Stick" Rusnak, as well as business developer Alena Vranova).

Though they faced issues with the manufacturing and distribution, what they brought into the world was truly majestic: a device which manages your private keys in a secure environment, is as open source and verifiable as the Bitcoin code



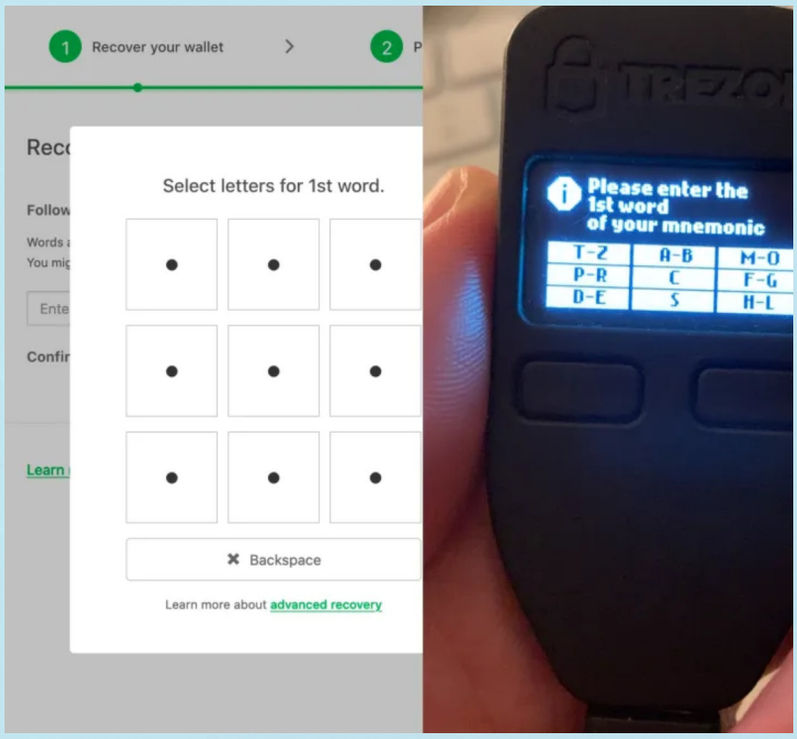
itself, and only makes transactions if you press a physical button to make the confirmation.

The Trezor is responsible for popularizing the BIP 39 and BIP 44 standards – after it got released, lots of wallets have co-opted the 12/24 word mnemonic words encryption format and added support for the Bitcoin Testnet. Also, due to the open source nature of the Trezor, many other hardware wallets emerged to provide extra features with various tradeoffs: the KeepKey, the Coldcard, the BitBox, the Jade, and the Passport owe their existence to the Trezor design and codebase.

And it's not like SatoshiLabs stopped innovating after releasing the Trezor. The company is responsible for creating over 50 open-source standards and contributing to lots of other open source repositories (NixOS, Bitcoin Core, MicroPython, and more). More recently, they also decided to pursue the creation of truly transparent secure element chips with the Tropic Square venture (which might produce a new Trezor hardware wallet in late 2022).

It "only" took one Linode backup server hack and the loss of 3094 bitcoins, and now everyone's coins are safer. So it's definitely interesting to observe how far we've come in terms of Bitcoin security and how our storage methods have become more sophisticated in the last 10 years.

And the best part about it is that it's all free and open source: millions of people around the world can work towards improving and hardening the existing security, so no HODLer will ever have to deal with the pain of losing bitcoins in a hack. Now all we have to do is figure out how to convince our friends and loved ones to withdraw their coins from exchanges and embrace financial sovereignty.





AnyCOLO.Net

CHEAP & RELIABLE VPS

PAY WITH BITCOIN
(ON-CHAIN & LIGHTNING)

HOST ANYTHING YOU WANT
FROM $4/MONTH



Why Bitcoiners Should Play Final Fantasy X

After spending almost 80 hours playing the remastered version of Square Enix's 2001 epic adventure RPG Final Fantasy X, I've come to the conclusion that the leading characters have a lot in common with bitcoiners. I know that this sounds a little crazy and my thesis can be easily dismissed by claiming that everyone who spends too much time in a fictional world will end up projecting some personal ideas on the action.

But I swear, Final Fantasy X does have something special and bitcoiners are going to have a huge mindblower at the end of the third act. Mostly because it's a story about disillusionment and discovery, where five teenagers and their more experienced mentor embark on a journey that's supposed to follow a centuries-long tradition.

I don't want to spoil the pleasure of discovering how the events unfold, but let's just say that along the way there are unexpected twists. Just like in every Final Fantasy game, for that matter. But at one point, the protagonists basically say "Screw your stupid tradition, we have found a better way and we refuse to perpetuate your vicious cycle". In my mind, this was a huge "eureka" moment which truly resonated with the general attitude of bitcoiners: we tend to defy the establishment and work towards figuring out our own path to go forward.

Yet there's another interesting resemblance between Final Fantasy X and Bitcoin: there is a strong sense of responsibility and honor which keeps the idealistic protagonists on their track. Even after they discover that they were serving a bogus religion whose point was not to promote truths, but to control and nurture ignorance, they carry on by themselves and through their own means.

Tidus, Yuna, Wakka, Lulu, Rikku, Kimahri, and Auron don't give up on the mission just because they discover that everything around them is a lie which covers up an uglier truth. Instead, they work together to fix the world in a way which prevents the same cycle from repeating itself.



Sounds familiar? It's because the plot twist from the end of the third act (which I won't reveal because I still hope that you'll be playing Final Fantasy X) is very similar with the experience bitcoiners have. We don't want to sacrifice our lives for their crooked system – instead, we're trying to build something better.



We live most of our lives believing in a system that's supposed to work in our best interest and is said to be the best that could exist. And then one day we find out that our leaders feed us comfort and hope in exchange for our obedience. Almost everything is rigged against us, but the money system is the one that feels most enraging – since we spend a third of our lifetimes (even more if we work for our own project) working and our time gets rewarded with a devaluing monetary unit that can be politically-debased, this truly hurts.

And then we discover Bitcoin and have our Plato's cave moment – we see reality for what it is and try to figure out what we should do with our lives next. The pessimistic way is to feel bitter about the whole situation and keep ourselves busy while observing the ignorance of others. The optimistic way is to try to educate everyone around us in hope of a fairer world. And this is exactly what the Final Fantasy X protagonists do.

Sure, the story can have religious, political, financial, and even parental interpretations. Maybe this is why the game is regularly praised as a masterpiece of the PlayStation 2 generation and one of the best entries in the Final Fantasy franchise. And though some of this information may seem banal or self-evident, we do need perpetual reminders about our roles in this grand scheme.



I tend to think that bitcoiners are just as pure at heart as Final Fantasy protagonists – they may hide behind "toxic" and unapproachable personas, but at heart they are truth-seekers and truth-tellers. This obnoxiousness can sometimes be the result of true conviction – something that no altcoin will really ever have, since most of their communities are driven by greed and dreams of enrichment.

After having finished Final Fantasy X, the best I can do is recommend bitcoiners to play it. Yes, the game can be grindy and has those J-RPG mechanics. But the story is incredibly great and will help you remember what kind of person you are and what you should be doing with your knowledge and conviction.

Final Fantasy X is currently available on PC (via Steam), PlayStation 4/5, Xbox One, Nintendo Switch, and obviously the OG PlayStation 2. It costs about $25 and comes bundled with X-2, a cornier direct sequel which I will probably be playing next to search for some hyberbitoinization hints. If you don't want to play the game and just want to watch the cutscenes that tell you the story, you have 11 hours of content that's available for free on YouTube.

Bitcoiners who are into video games should definitely play Final Fantasy X. And gamers who beat Final Fantasy X will definitely have an "eureka" moment when they start reading more about Bitcoin, as it will feel like the disillusionment which gives them some answers about the world.


PANTIES FOR BITCOIN
ANTIFRAGILE
PANTIIES FOR THE
SOVEREIGN WOMAN
PANTIES FOR BITCOIN
Made in Italy



Calling Bitcoin a NSA/CIA Project Is Disrespectful to Cypherpunks

I've recently asked my Twitter followers to mention their favorite Bitcoin conspiracy theory. Surprisingly, most respondents have mentioned the CIA, the NSA, or another "three-letter agency" as the potential creators of the cryptocurrency.

Deater Bob suggested that Satoshi Nakamoto might have leaked the Bitcoin project from sources within the US government. Gilroy pointed out to a master plan that would eventually use Satoshi's coins as the foundation for a new US treasury. The likes of Juan Galt and Jack have also suggested that the NSA might have been involved.

And in spite of some creative replies (such as Wladimir Van Der Laan's theory about Bitcoin being a fungus and Bmo Masari's suggestion that the internet itself might have attained consciousness in order to create Bitcoin), I couldn't stop thinking about the popular associations between the creation of Bitcoin and governmental agencies.

Therefore, I will explain why the association is wrongful – and even if Satoshi Nakamoto was the CIA or the NSA, Bitcoin no longer belongs to him, and it isn't even as innovative as most people think.

Bitcoin didn't come out of nowhere and borrows multiple breakthroughs that cypherpunks have previously made. To Satoshi Nakamoto's credit, he has created the best solution for the Byzantine Generals Problem, and is/are responsible for releasing a form of decentralized electronic money that actually became a success. The difficulty adjustment every 2016 blocks is also a fine touch, and one which has been crucial for the survival of the network.

However, there is a cypherpunk tradition that precedes Satoshi's emergence by 20+ years. This article will present only a few of the inventions that have taught Satoshi how to design Bitcoin and which proven flaws to avoid.



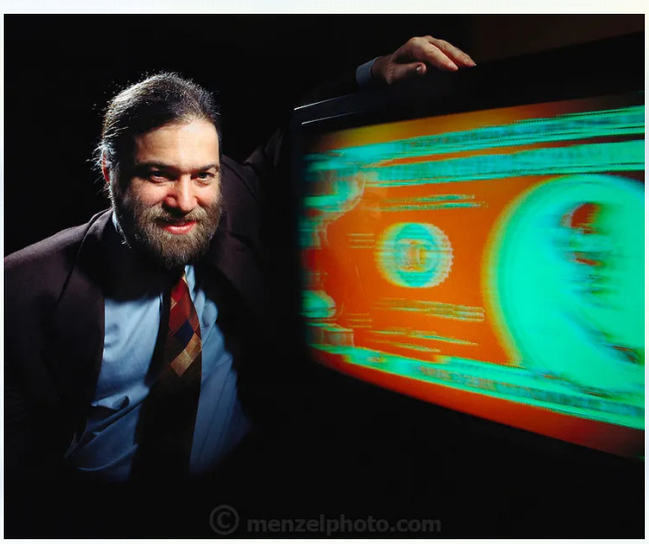
Satoshi Nakamoto might be the CIA/NSA, but Bitcoin is rooted in the cypherpunk tradition.

Lots of nocoiners, precoiners, and poorly informed bitcoiners think that Satoshi Nakamoto invented the blockchain and deserves all the credits for the accounting system which spawned an entire industry.

Like many other cryptographic inventions, the blockchain was first conceptualized by David Chaum during his PhD at Berkeley University. His 1979 Vault system even includes checks and balances that very much resemble Bitcoin's: watchers (block explorers), doers (nodes), executives (miners), czars (developers).

Chaum also created the first form of digital money (ecash) with the DigiCash corporation. It was designed to fix the trust issues of online credit card payments with a form of money that is private enough to conceal the personal data which is irrelevant to the transaction. However, its centralization ultimately led to a disappointing demise in the late 1990s. Interestingly, Satoshi doesn't mention Chaum in the Bitcoin whitepaper.

Let's get back to the blockchain: the idea of an hash chain that is used for linked timestamping is also presented in a 1991 research paper by Stuart Haber & W. Scott Stornetta. Unlike David Chaum's work, Satoshi does reference this breakthrough in the Bitcoin whitepaper. Also, popular bitcoiner Jameson Lopp has cited the research as a precursor to Bitcoin's blockchain.



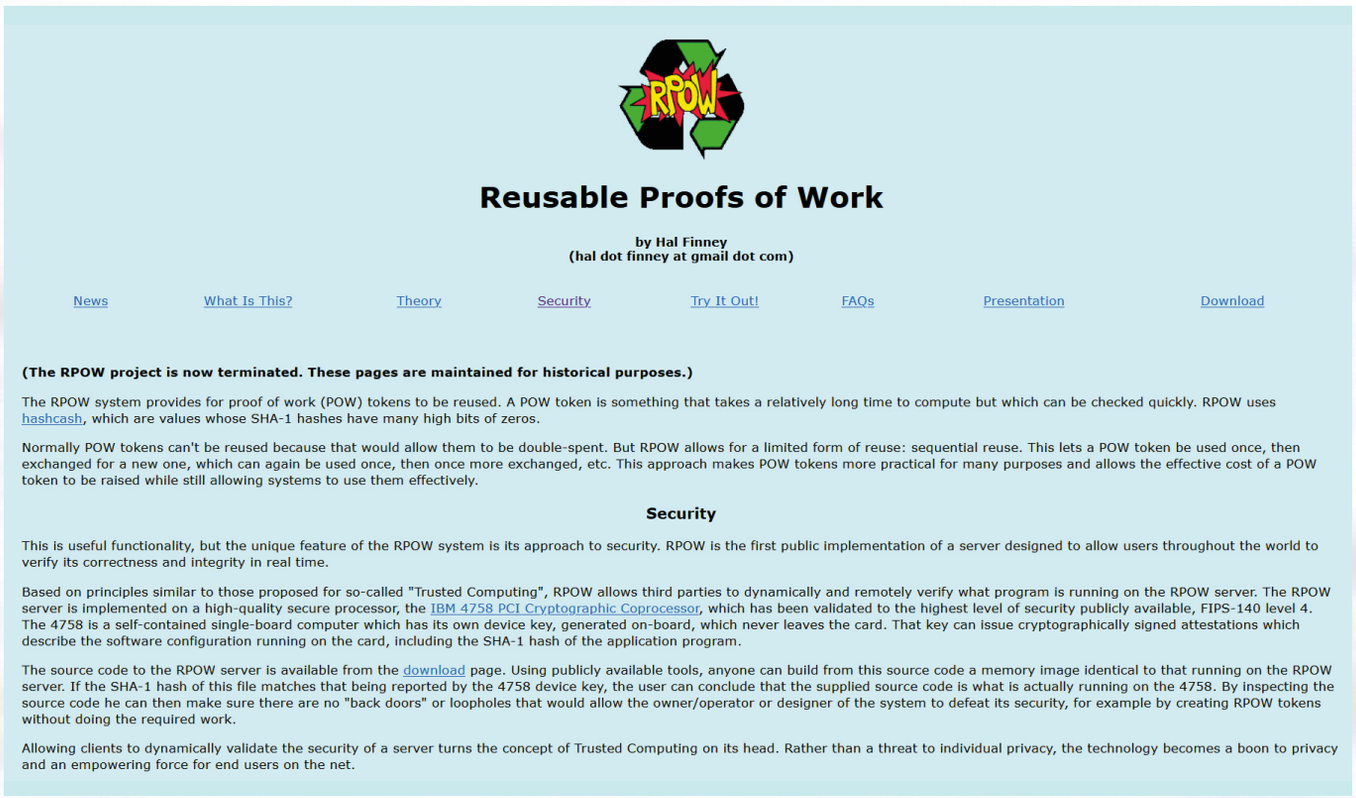


Then there's the choice of Elliptic Curve Digital Signature Algorithm (ECDSA), published in 1998 by Canadian computer science researchers Don Johnson, Alfred Menezes, and Scott Vanstone. With ECDSA, public keys, private keys, and signatures get generated in order to guarantee that the bitcoins can only be spent by the rightful owners.

A popular theory says that Satoshi Nakamoto picked ECDSA over Schnorr signatures out of convenience, as more libraries were available to suit his/their specific needs when designing Bitcoin. Yet there are lots of privacy concerns (that do involve the NSA's tendency to implant backdoors) that will eventually replace ECDSA with Schnorr signatures (thanks, Pieter Wuille!).

The idea of cryptography that uses public keys is also not proprietary to Satoshi Nakamoto: Ralph Merkle was researching the topic in 1980 (as acknowledged by the Bitcoin creator in the whitepaper), and Phil Zimmermann's private e-mailing tool PGP (on which Hal Finney has worked for many years) has been available on the internet for free since 1991.

Speaking of Hal Finney, he almost discovered Bitcoin with his Reusable Proof of Work (RPOW). However, it's Adam Back who gets cited in the whitepaper for inventing the hashcash system in 1997 and perfecting it to prevent e-mail spam. Without these



Reusable Proofs of Work

by Hal Finney
(hal dot finney at gmail dot com)

News | What Is This? | Theory | Security | Try It Out! | FAQs | Presentation | Download

(The RPOW project is now terminated. These pages are maintained for historical purposes.)

The RPOW system provides for proof of work (POW) tokens to be reused. A POW token is something that takes a relatively long time to compute but which can be checked quickly. RPOW uses hashcash, which are values whose SHA-1 hashes have many high bits of zeros.

Normally POW tokens can't be reused because that would allow them to be double-spent. But RPOW allows for a limited form of reuse: sequential reuse. This lets a POW token be used once, then exchanged for a new one, which can again be used once, then once more exchanged, etc. This approach makes POW tokens more practical for many purposes and allows the effective cost of a POW token to be raised while still allowing systems to use them effectively.

Security

This is useful functionality, but the unique feature of the RPOW system is its approach to security. RPOW is the first public implementation of a server designed to allow users throughout the world to verify its correctness and integrity in real time.

Based on principles similar to those proposed for so-called "Trusted Computing", RPOW allows third parties to dynamically and remotely verify what program is running on the RPOW server. The RPOW server is implemented on a high-quality secure processor, the IBM 4758 PCI Cryptographic Coprocessor, which has been validated to the highest level of security publicly available, FIPS-140 level 4. The 4758 is a self-contained single-board computer which has its own device key, generated on-board, which never leaves the card. That key can issue cryptographically signed attestations which describe the software configuration running on the card, including the SHA-1 hash of the application program.

The source code to the RPOW server is available from the download page. Using publicly available tools, anyone can build from this source code a memory image identical to that running on the RPOW server. If the SHA-1 hash of this file matches that being reported by the 4758 device key, the user can conclude that the supplied source code is what is actually running on the 4758. By inspecting the source code he can then make sure there are no "back doors" or loopholes that would allow the owner/operator or designer of the system to defeat its security, for example by creating RPOW tokens without doing the required work.

Allowing clients to dynamically validate the security of a server turns the concept of Trusted Computing on its head. Rather than a threat to individual privacy, the technology becomes a boon to privacy and an empowering force for end users on the net.

cryptographic breakthroughs, Bitcoin could have never reached the same degree of security – and the brilliant mining incentives most likely wouldn't have existed.

Yet another great cypherpunk who doesn't get cited in the whitepaper but has figured out 90% of Bitcoin is Nick Szabo. His Bit gold system successfully connects many puzzle pieces from amongst the most brilliant cryptographic discoveries, and also creates the "digital gold" principles that are rooted in Austrian economics (scarcity, fixed issuance rate which avoids the pitfalls of hyperinflation, easy verification).

Unfortunately, the Bit gold design relied on a majority of network participants and could easily become subjected to 51% attacks. Also, it had an issuance rate (inflation) that the market would decide – which means that there would be times when more blocks would get mined, and other times when there wouldn't be any kind of activity and the system's security would most likely lower. What Satoshi Nakamoto did was to replace the rule of CPUs with the rule of hash power, as well as figure out how to design a disinflationary financial system (start with a high issuance rate, reduce it in half every 4 years).

These cypherpunks were all about privacy and resisting the NSA

The "punk" in "cypherpunk" should successfully delineate the movement from government servitude. According to Tim May's 1994 opus "The Cyphernomicon", the cypherpunks were very much against surveillance and sought to keep their privacy on the internet while inventing tools to also help others.

Compliance in itself was synonymous with an ideological capitulation. David Chaum wrote "Blind Signatures for Untraceable Payments" in 1983, and "Security Without Identification: Card Computers to Make Big Brother Obsolete" in 1985.

In an October 1995 report by the NSA (which was declassified in 2008), some concerns were expressed in regards to the ways in which DigiCash can be used for criminal activities. The existence of this particular document proves that Chaum's intentions were real and he truly was concerned with privacy.

It's very unlikely that cypherpunks like Finney, Szabo, Back, Haber, and Stornetta worked for the NSA, CIA, or any other governmental agency. Otherwise their work would have been classified and restricted to only be used by authorized personnel.



And even if we assume that the open source work was released as such for the purpose of getting further improved by other voluntary cryptographers on the internet, the fact that these tools work against the monopolistic interests of the NSA/CIA also makes the cypherpunks look pure at heart.

If the NSA decides to use RPOW or the ideas behind Bit gold to build a system of their own (which most likely happened already, to some extent), it doesn't mean that the inventors of these systems were their employees.

Bitcoin was invented by Satoshi, but it never belonged to him

At most, a returning Satoshi Nakamoto can move his coins and spend them. There is no backdoor key, there is no reserved lead developer position, and there is no active developer who awaits the return of the creator.

Like it or not, Bitcoin is not the same network it was in 2009. It has undergone numerous improvements and will continue to leave Satoshi Nakamoto's legacy behind as more parts get replaced.

After all, the point of Bitcoin is not to remain unchanged over time, but to keep its monetary policy, guarantee that Satoshi can return at any time and move the coins, and preserve decentralization.

There is a lot that Satoshi Nakamoto got right, but also plenty of code that was removed or replaced by developers. Hal Finney has spent a lot of time fixing design flaws in Bitcoin (and even added extra zeroes to define the system's smallest monetary unit as 1/100.000.000 BTC) and he set a precedent for future devs to seek more elegant and efficient fixes for an otherwise rigid project.

DOCID: 3839357 ~~TOP SECRET~~

Approved for Release by NSA on 04-07-2008, FOIA Case # 10369

Vol III, No. 43 — Communicator — NSA's Employee Publication — 30 October 1995

THE FUTURE OF MONEY: PROTECTING DIGITAL "CASH" (U)

(U) Some of you may be aware that one of the big stumbling blocks in using the INTERNET for buying and selling goods and services is the lack of a secure and reliable system to pay for them. Several entrepreneurs have been attempting to develop reliable solutions to this problem. Mark Twain Bankshares of St. Louis recently announced that it would soon offer its customers electronic cash or "E-Cash" services developed by DIGICASH, an Amsterdam company run by cryptography-savvy David Chaum. Initially these services are intended to overcome many of the disadvantages of using credit cards for small dollar transactions, but these same technologies could offer new opportunities to those bent on counterfeiting, money laundering, or electronic theft.

Bitcoin as a monetary system is set in stone with a fixed supply, a predictable inflation until 2140, clear mining rewards, and convenient difficulty adjustments every 2016 blocks. But Bitcoin as a network is bound to receive lots of upgrades that make it faster, more private, and more efficient.

Improvement proposals like Schnorr signatures, Taproot, MAST, and Grafroot are designed to bring greater privacy and block efficiency (transactions will get smaller and more affordable).

Then there are lots of privacy improvements that are being explored on altcoin networks and sidechains (it's only a matter of time until Confidential Transactions or MimbleWimble get added to the base layer to some degree). In the future, it's likely for transaction privacy to become more popular, and smart tricks that still guarantee supply auditability and inflation resistance will be implemented.





If Satoshi returned, he probably wouldn't recognize his own invention. But that's for the better, as the network is growing and becoming much more efficient for its purpose. Bitcoin is like a muscle car which receives upgrades without ever changing the body frame – it will always retain the main design qualities, but with a better engine and bulletproof windows.

If Satoshi Nakamoto is the NSA/CIA, then Bitcoin does not belong to them

Is Bitcoin designed by a three-letter agency? It's definitely possible. Could the CIA and NSA use Bitcoin for transactions? That's even more likely. But neither of these two probabilities lead to a conclusion that puts a governmental agency in control.

Right now, Bitcoin may possibly be the most decentralized computer network on the planet. It has functioned since January 2009 with only two instances of downtime (due to an inflation bug in 2010 and due to poor network synchronization in 2013) and has ~10000 nodes operating worldwide (not counting the ones running on Tor and the

ones that didn't open the 8333 port).



Some argue that backdoors may exist: and the most damage they can do is break the signatures (which can lead to funds being stolen) or break the cryptography behind SHA256. In either case, it's possible for the community to hard fork to a new chain, replace both ECDSA and SHA256 with existing alternatives that have already been developed, and restore previous coin ownership on the basis of cryptographic proof. The solution seems unpopular now, but may prove to be the last resort in the event of a serious attack of the kind which Bitcoin never really faced.

The battle against Big Brother is relentless, and it's clear that government officials understand the trade-offs involved in launching attacks or momentarily lack the means to engage. It's also probable that the CIA and the NSA find the existence of Bitcoin convenient, as they use it themselves and have their own ways to track transactions on the blockchain by looking at communications between participants and other network-level clues.

But even if we assume that Satoshi Nakamoto was the father of all CIA agents, the experiment has escaped his hands and he is no longer in control – and nor will he ever be again, unless the network becomes more centralized (as it happened with BCH and BSV).

And even if half of the Bitcoin community is under CIA's paycheck, then the other half can still resist attacks by moving to another chain which retains the rules but changes the security mechanisms. It's all open-source software and the means to protect one's property should be enforced.

Yet thanks to the brilliant network incentives, it's better for everyone (CIA agents or not) to stick together and protect the same network. For as long as greed works, Bitcoin will remain secure and adversarial in terms of whom it onboards and for what reasons.

The "don't trust, verify" motto mostly refers to other people's personal validation and implies having your own node as a way of proving that the funds exist and are rightfully yours. Therefore, it's an assumption that everyone else is out there to rob you – because you know, everyone's a scammer.





Comic Strip: Bitcoin Eating Popcorn #2

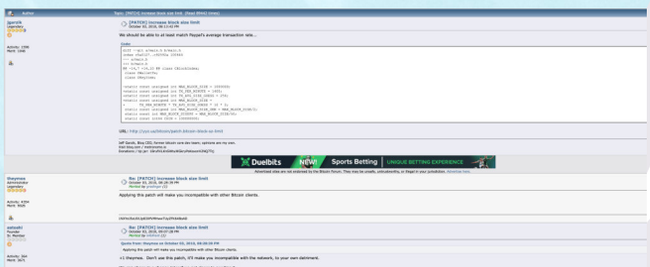
Over the years, Bitcoin has undergone numerous centralizing attacks. The idea of increasing the block size to enable more transactions at lower costs has been around since the project's infancy.

In October 2010, Core developer Jeff Garzik wrote a "patch" which aimed to "match PayPal's average transaction rate". He published it on the Bitcoin Talk forum, where moderator Theymos and Satoshi quickly warned everyone that the code is incompatible with the existing consensus rules of the network – running it would cause users to operate on a parallel chain which is no longer Bitcoin.

However, Satoshi did make a statement which led some into thinking that increasing the block size for scalability purposes is only a matter of time: "We can phase in a change later if we get closer to needing it". But in the context of requiring this upgrade, he said "if" instead of "when".

In practice, Satoshi created a consensus rule which fixed Bitcoin's maximum block size at 1 MB. This limitation became an inconvenience to some business owners who wanted to build their infrastructure or at least settle some of their transactions on the Bitcoin blockchain.

By virtue of the liquidity they were bringing, some business owners considered



jgarzik — **[PATCH] Increasing block size limit**
October 03 2010, 13:42 PM

We should be able to at least match PayPal's average transaction rate…

theymos — **RE: [PATCH] Increasing block size limit**

Applying this patch will make you incompatible with other Bitcoin clients.

satoshi — **RE: [PATCH] Increasing block size limit**

+ theymos. Don't use this patch, it'll make you incompatible with the network, to your own detriment. We can phase in a change later if we get closer to needing it.

that the Bitcoin network should upgrade to accommodate their needs – regardless of the centralization concerns which most likely were also convenient to them despite being against the purpose of the Bitcoin project. So instead of figuring out how to make Bitcoin work for their particular use cases with optimizations (such as internal ledgers, transaction batching, and sidechains), they wanted the network itself to change according to their needs.

In the coming years, a pretty dramatic scaling debate took place. Between 2014 and 2017, four major proposals have been made:

1. Bitcoin XT (later integrated in BIP 101, which sought to double the block size every 2 years until the year 2036, when the maximum block size would have been 8 gigabytes);
2. Bitcoin Classic, which aimed for a more conservative one-time block size doubling to 2 megabytes;
3. Bitcoin Unlimited, which allowed the miners to decide the block size;
4. SegWit2X, which increases the block size to 2 megabytes and also activates SegWit (the scaling proposal that Bitcoin Core developers introduced as an upgrade which mainly fixes the transaction malleability issue);



These proposals sound really good, except that they effectively make the network more centralized due to the increasing requirements for storage, internet speed, and processing power. Broadcasting one megabyte across the network at an average rate of 10 minutes, while having sovereign nodes store a few hundred megabytes worth of mempool data is feasible even on a Raspberry Pi that gets paired with a poor internet connection.

Arbitrarily increasing this number comes with greater hardware requirements – and according to what we've learned from other projects, eventually Amazon Web Services (AWS), Google and Microsoft Azure ultimately become the optimal solutions for handling all on-chain operations. The switch from sovereign self-validation to trust in industrial-level computers is against the spirit of the Bitcoin project and effectively exposes the network to government attacks.

Then there's also the fee market argument: as the block reward gets reduced in half every 210.000 blocks (approximately four years), the transaction fees must pay the miners enough money to cover their equipment and electricity costs. So to maintain the security of Bitcoin, block space needs to become expensive. Deciding that it should be cheap threatens to compromise network incentives.



Some argued that by increasing the block size, the amount of transactions in a block would also increase. Therefore, Bitcoin's security budget should get covered. But this is not a certainty – with smaller blocks, there is constant demand regardless of market phases which keeps the miners going; if the blocks are big and there isn't much activity, then the miners take a financial loss and will switch off.

The block size debate wasn't only technical, as it also acquired a political dimension. As Chris DeRose argued during season 10 of the Bitcoin Takeover podcast, it's likely that some people were angry at the Core development and wanted to put themselves in a higher position of power.

Regardless of the intentions, a hard fork (changing the consensus rules in a way which pushes everyone to update their client) was problematic because it would effectively divide the community. No proposal got enough traction – so after three years of debates and Scaling Bitcoin conferences, no solution received enough support.

Some thought that the change was irreversible and premature. Others were concerned about a political takeover that would centralize Bitcoin. Meanwhile, the big blockers camp started implying that not changing Bitcoin is financially beneficial to companies like Blockstream (which develops the Liquid sidechain and the c-lightning client for Lightning network) and encourages short-term use of altcoins.

Unfortunately, a hard fork did happen on August 1st 2017. The big block crowd (consisting of XT, Classic, and Unlimited developers and supporters) has embraced the new Bitcoin Cash chain, whereas the



users backing the real and decentralized Bitcoin have activated SegWit via UASF (user-activated soft fork).

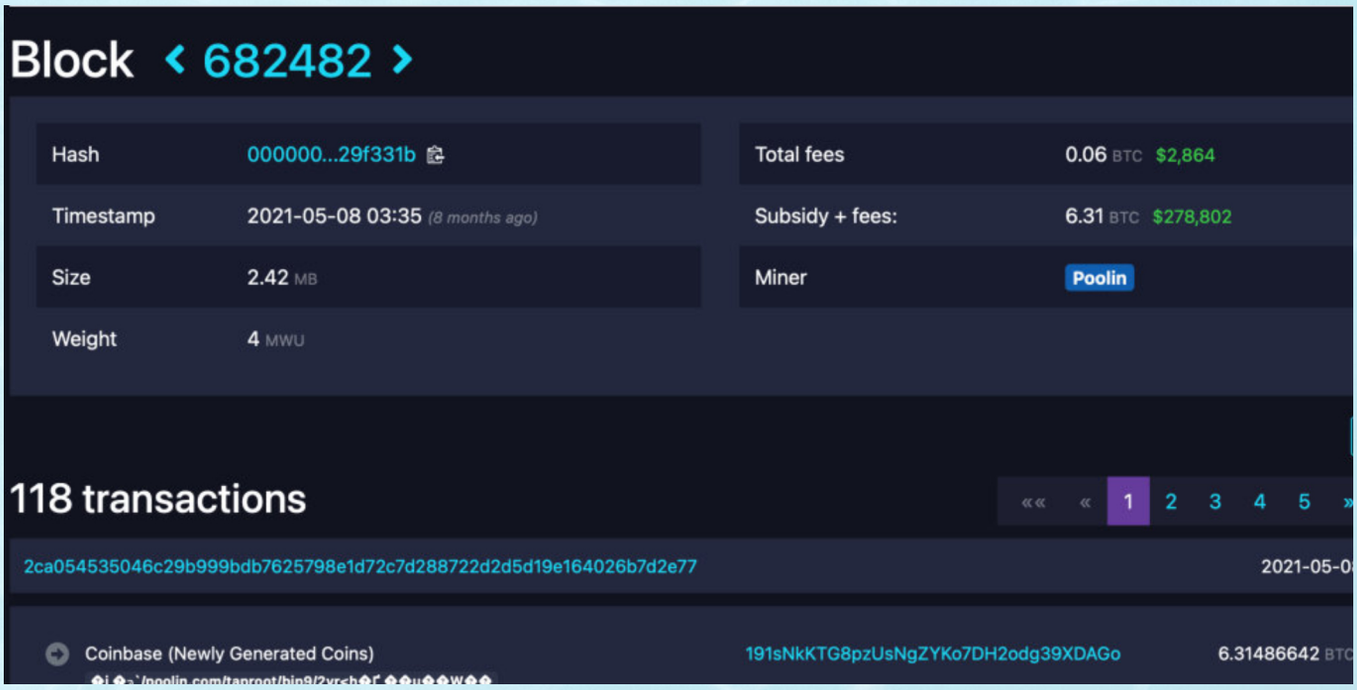
A soft fork is a network upgrade which doesn't break consensus. Activating it is completely optional, but at some point in the future it's expected to become the norm. At scale, it accomplishes the same goals of a hard fork – as all users eventually update their node software to include the changes. But those who don't want to run the new code are free to opt out while remaining on the same network as everyone else.

From a technical point of view, SegWit is a masterpiece of elegant design. It's exactly the kind of code that should be expected from the people who spend the entirety of their day working with Bitcoin code. Theoretically, it can make blocks extend up to 4 megabytes during times of high demand. But practically speaking, 2 megabytes is more common.

To date, the biggest Bitcoin block ever mined is number 682482, which Poolin discovered on the 8th of May 2021. It has a size of 2.42 megabytes and still exceeds the average size of a BCH block (as the Bitcoin Cash network, despite enabling big blocks, didn't get traction and has very little demand for block space). This situation led to the rather funny question "Which Bitcoin has the big blocks, after all?".

Bitcoin didn't really eat popcorn during this dramatic phase of its existence. But it did remain decentralized and accessible to anyone around the world. Second layers like the Lightning network and sidechains like Liquid, RSK, Statechains and Drivechains play the scalability role just fine. They settle transactions faster and at lower costs, but lack the security of the base layer – which is a tradeoff that everyone must consider depending on the amount that they're sending.

But for Bitcoin's resistance against centralizing hard forks, we must thank the conservative and stubborn Core developers (especially Greg Maxwell, Pieter Wuille, Johnson Lau, Eric Lombrozo, and Luke Dashjr), as well as every user who supported SegWit, Lightning, Liquid, RSK, Counterparty, Omni, Statechains, Drivechains, and every other proposal which helps Bitcoin scale and/or acquire more functionalities. This comic is for all of you.




I'll make you scale
2014-2015
Bitcoin XT
2 MB FTW
2016-2017
Bitcoin Classic
Miners decide block size
2016-2017
Bitcoin Unlimited
2 MB blocks & SegWit
2017
SegWit2X
SEGWIT
2022
Liquid
by Blockstream
Drivechains
rsk
SHIT COINER TEARS
Bitcoin eating popcorn, BTCTKVR.com

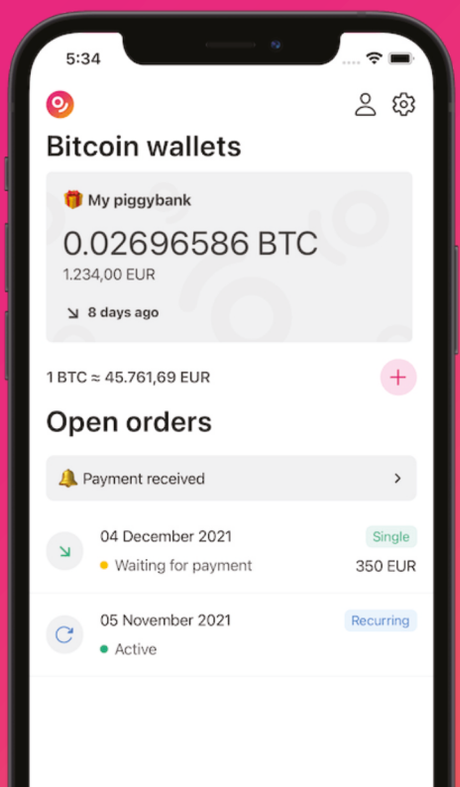
Bitkipi

Easy Bitcoin stacking with Bitkipi. The KYC-lite DCA App for your painless Bitcoin only saving experience.

bitkipi.com

Download Bitkipi, start stacking!

External Wallet purchase available soon!



Available on the Google Play

Download on the App Store



How to Hide Your IP Address: VPN vs Tor

(From the PrivacyPros.io Blog)

Note: this article is an extended revision of the piece which was first published on the PrivacyPros blog in March 2020. This crossover event could take place thanks to the goodwill Bryan and Colin Aulds, who are the owners of Billfodl/PrivacyPros and have always been supportive of my work.

Compared to the original article, you will see three significant changes: first of all, the information has been updated to present the latest stats; secondly, since this magazine doesn't care much about SEO optimization, the phrases are longer and some explanations go more in-depth; thirdly, Mullvad VPN is now part of the comparison. For now, this is the most complete version of this article. And if you want to support PrivacyPros, buy their Billfodl metal plates or use their referral links to purchase your VPN subscription.

In its early years, the internet functioned as a global, neutral, and universal network. It didn't matter where the user was located or what internet service provider (ISP) he employed. For a while, everyone could access the same web pages without any kind of arbitrary restrictions.

However, governments and transnational corporations have eroded the internet's neutrality and freedom.

Today, the way you experience the network depends on your ISP and jurisdiction. Sometimes the content is regionalized and incomplete in comparison with the original, but in an increasing number of cases it's restricted or banned. Not only that, but your browsing history might just be tracked, stored, and sold to the highest bidder by your internet service provider. And if you take into account all the more or less sophisticated bad actors who can use your public footprint against you, then you'll come to the conclusion that you need better protection. Bitcoiners should know very well that they need a reasonable amount of privacy and plausible deniability to avoid attracting the attention of online hackers and to not get assaulted in meat space.

You can boost your privacy and regain your right to obtain free information by obfuscating your IP address. What is your IP (internet protocol)? Well, it's the unique identifier which ties your internet identity to your ISP (internet service provider). It's assigned to your home router, so all devices around the house that connect either via cable or wirelessly shall bear this identifier. If someone has your IP address, then they can easily figure out the approximate location due to the ISP being a public entity. Thankfully, there are services that can become your "mask" so that you surf the web with an identity that you either choose (VPN) or generate randomly (Tor).

This article will teach you how to choose the right tool for the job of protecting your fundamental human rights.



Why Hide Your IP Address?

Since the USA repealed net neutrality, certain websites load slower or get filtered. It all depends on the policy and interests of your internet service provider.

Much of what you see on the internet is a result of your geographical location.

Here are some examples of surfing experiences that vary according to where you are in the world:

- If you're in China, you are behind the Great Firewall. The only way to get unfiltered news from Western media is to get a proxy to trick websites into thinking that you're from a free country.
- In Cuba, you only have access to web pages curated by the government.
- In Venezuela, the government regularly bans social media content.
- Journalists in Russia self censor their content to avoid imprisonment.

All these are bad news for access to free information and free speech. Therefore, hiding your IP address is necessary to protect your fundamental human rights.

There are other reasons to hide your IP address, though.

Sometimes your adversary is an internet company which arbitrarily curates what you can and cannot see.

Netflix has exclusive series and films that are only available in certain countries. Subtitles or dubs in your native language also have limited availability. But if Netflix believes you are in another location, they will unlock the region-specific content.

There's also the matter of privacy.

ISPs in many countries store your browsing history and have the right to sell it to the highest bidder. Many of the online retailers you shop at are collecting your information as well.

If you don't want your data sold, it's up to you to prevent your ISP from getting your data in the first place.

At the end of the day, we want to hide our identity and activity AND gain access to restricted content. To achieve that, we must use a VPN and/or a Tor connection.

How to Hide Your IP Address on Mac, Windows & Linux



There are two popular ways to hide your IP address on MacOS, Windows, and Linux. The first is to use a Virtual Private Network (VPN), while the second is to use The Onion Router (Tor). As you'll find out later in the article, they are not mutually exclusive.

VPNs allow you to access the internet through a third party general purpose server. For increased privacy, this server encrypts your data and mixes it with packets coming from other users.

Because it's hard to tell which user transferred what data, any participant has a

degree of plausible deniability. However, keep in mind that metadata (information about file sizes and time of access) can reveal a lot.



Tor is a peer to peer network, just like Napster and BitTorrent. When you access the Tor network, you connect to a minimum of three random network peers (known as “nodes”).

These nodes then encrypt your data packets and route them to the destination. This endows your internet access with military-grade privacy and security.

Thankfully, both VPN services and Tor browsers are widely available across all devices and operating systems. In the next section, I’m going to present some criteria for choosing the best VPN, as well as popular products that you can purchase.



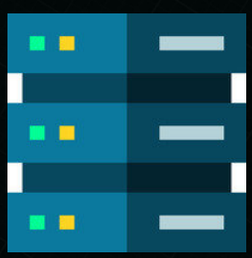
Hide Your IP Address Using a VPN

There are many VPNs to choose from. Hundreds, actually. Some are better than others, and good marketing campaigns don't necessarily translate in great quality or good privacy. Much like every other product and service, with VPNs you usually get what you pay for. That means free VPNs are rarely worth using and they won't be recommended in this article – they’re most likely spyware.

So what makes a VPN service great? Below you will find the features and criteria you should use in a good analysis. Then, to help you decide which VPN is best for your use case, you will find top picks for all budgets.

What to Look For In a VPN

Number of Servers and Countries



How many servers does the VPN allow you to access? This is important because you are sharing these servers with other users. If too many users simultaneously connect to the same server, your speed could be affected. On the other hand, if there are only a few users on the server then it becomes easier to identify your traffic. The key is to find the perfect balance between speed and the ability to hide in a crowd.

Apart from the total number of servers, their global spread is equally important. The more countries and jurisdictions you get, the better. You never know when your favorite Netflix film is only available in France – and it’s important to find a French server with quick load times. And when an internet service costs more in some countries and less in others (a decision that makes no sense on a global computer network), it’s good to have the choice to minimize your expenses.



Speed



How fast are upload and download speeds? In some cases, using a VPN will make your browsing experience slower. This is true even when using the best services around.

That's because when you use a VPN, the content that you consume gets accessed through a shielding third party. And if you are trying to stream or torrent video while using the VPN, download speeds will be very important.

As mentioned in the previous section, speed should not come at the expense of losing privacy. Otherwise, the whole purpose of using a VPN gets defeated. So for the sake of boosting your plausible deniability, you should search for servers which have a considerable number of simultaneous users but aren't running full.

Privacy Record



Does the VPN have a history of leaking data or making false claims about the privacy it offers? If a VPN is not transparent about past breaches or how it protects your privacy, how can you be sure it is working? It's important to know that the service does what it promises to offer.

The bad news is that most services, despite running on open source standards, don't also open source their code for public auditing purposes. And even if they do (as is the case with Mullvad and ExpressVPN), there is still a degree of trust involved when it comes to their servers. You can't also verify the hardware that runs the code.

There are also audits that VPN services regularly do to reassure their customers that all the promises from the terms of service are fulfilled. Yet they only mean that on the days of the audit (which was previously known), the VPN services had everything in check. While they're not being audited, they act in opposition to their claims and get away with it.

But ultimately, it's the track record that matters the most. Just like Bitcoin has the Lindy effect (the longer it exists and runs properly, the more longevive it's likely to be), VPN services rely on their reputation of doing what they're claiming to do. Mullvad, ExpressVPN, and Surfshark are the ones that rank high in this regard. NordVPN, for example, has fallen out of grace and will have to prove itself in the future to remain competitive.

Payment Options



All VPN services let you purchase the service with your credit card. In some cases, you can even send wire transfers or cash via post. However, to remain truly anonymous during your purchase you should use bitcoin payment.

The bad news is that not all VPN services let you pay with BTC – and if they do, they'll ask for an e-mail address or another way to identify you. The good news is that the best VPNs get it right.

Value



The price is always a criterion when choosing your VPN. But it's not precisely the amount of money that you pay that matters, but the quality of the product that you get in exchange.

On one side of the spectrum, you have free or very affordable VPNs that most likely collect some data about your internet access. You should avoid them at all costs.

On the other hand, you have the more expensive premium services. And price isn't always the best indicator of great privacy. For instance, ExpressVPN costs almost twice as much as Mullvad but has slightly weaker privacy primitives. What Express offers is better compatibility across devices (routers, video game consoles, televisions) and more extensive tech support.

Five VPN Picks, Featuring Different Tradeoffs

The following VPN services are all available for both Mac and Windows. Some of them even support Linux distributions, mobile phones, and gaming consoles.

PureVPN: Affordable, compatible with lots of devices, pretty fast, but questionably private



PureVPN is fast and very affordable. With special discounts, it costs as low as $2.05/month for a two-year plan and offers other options as well.

It comes with the promise of decent speed, over 6500 servers spread across 78 countries, and outstanding compatibility. This means that you can switch between 300,000 different IP addresses whenever you wish.

And if you want to extend the privacy and security to your iPhone or PlayStation gaming console, PureVPN offers a dedicated version of the app for each device.

There are some documented downsides, though.

For instance, several servers don't perform as quickly as advertised. Also, there are some minimal network logs that the service keeps, which might be a deal-breaker for those who value privacy the most. So the "Zero Logging" policy is questionable. Though the company claims that it does't store any logging data, PureVPN has been instrumental in helping the FBI catch a stalker in 2017.

Sensitive and potentially life-threatening operations are not recommended to be executed through PureVPN. But if you're looking for a service which unlocks Netflix content at a low price and provides lots of options for speed and reliability, then this might be one of your best choices.

Furthermore, it's interesting to see that you can pay for the service with bitcoin. Paying online without a credit card makes a difference for your privacy.

PureVPN was created by a development team from Hong Kong, but has its headquarters in the British Virgin Islands. Though the jurisdiction is great for enabling the exchange of sensitive data, the service's tainted track record should make you think twice before you do anything that can get you arrested (such as bypassing the Chinese firewall or expressing anti-governmental views in authoritarian countries).

Where PureVPN shines is streaming and everyday use. Its strongest point is the extended cross-device compatibility, as well as the wide range of available servers across multiple jurisdictions. But if you want greater privacy and security, you should look at alternatives that deliver them with fewer compromises.

NordVPN: Best VPN for Multiple Connections



When choosing a VPN, Nord is a worthy contender.

Of all the services reviewed in this article, Nord offers the most attractive ratio of speed, number of servers, and price. During times of special offers, you can purchase a subscription for as low as $3.29/month.

Nord is also the VPN service which received the most celebrity endorsements.

On their website, they highlight PewDiePie's one-sentence review to suggest that the product "helps access epicness". It's also very likely that you've heard of NordVPN, as the company is involved in many influencer sponsorships.

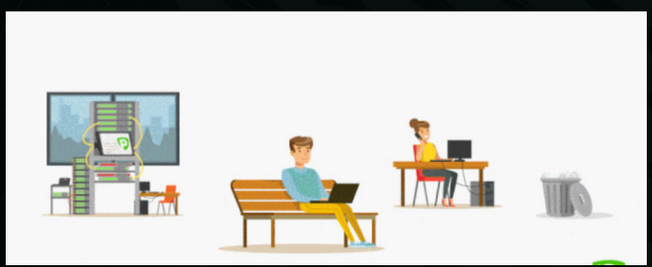
And yes, it's a pretty good VPN which also enables bitcoin payment to boost your privacy against the company. All you need is an e-mail address to confirm your registration and payment, then you're good to go.

Unlike PureVPN, Nord offers fewer servers and requires extra configuration steps to work with video game consoles and televisions. You only get applications for all the major operating systems (both mobile and desktop) and browsers. But as opposed to Pure, Nord is an overall better VPN service which offers two interesting features: double VPN (you connect to 2 different servers while one works like an onion layer for protection) and Tor over VPN (you basically turn on onion routing on top of your VPN connection).

However, Nord's track record is not immaculate and the company is still trying to recover from a serious issue. In March 2018, some private keys belonging to a NordVPN server in Finland were leaked. But this information didn't become public until the fall of 2019. It is estimated that this breach affected only 50 to 200 NordVPN users, but this was enough to harm the service's reputation.

Outside of this unfortunate mishap, Nord is a fine choice. It still offers one of the fastest and most user-friendly VPN services on the market. And it's decently priced for what it does.

NordVPN can bypass the Chinese firewall, doesn't store user logs, and unblocks Netflix. It also enables quick torrent downloads for those who need to transfer data fast. And its Panama jurisdiction allows for fewer cases of collaboration with nosy governments.



Surfshark VPN: The Bang for the Buck

Surfshark is slightly more expensive than Pure and just a wee bit cheaper than Nord. Yet it has an immaculate track record and offers more than 3200 servers in 65 countries that you can access through an intuitive dashboard.

To protect your identity, you can buy your subscription using Bitcoin. But just like in the cases of Nord and Pure, the transaction is handled by a payments processor like Coingate or CoinPayments. This isn't a big deal for your privacy, but it proves that the company won't touch your bitcoins and receive the fiat money equivalent. If you want a VPN that really accepts your BTC, you should take a look at Mullvad (more on that later).

Surfshark's Achilles heel is its more limited connectivity. In comparison with Pure and Nord, you can use fewer IP addresses. Yet it also offers a double VPN feature with pairs from different jurisdictions (for example, France and Sweden – two of the countries that are rather good at protecting internet access).

Also, it doesn't offer a supplementary Tor connection like Nord or dedicated apps for video game consoles like Pure. To get these, you will have to do the configurations manually. As for the jurisdiction, the company is based in the Netherlands and therefore must comply with present and future EU regulations – which is not as great as Nord's Panama operation. But the good news is that Surfshark offers good support and documentation to help you make the service work on all devices. As for Tor, you can get the browser yourself (as well as

Orbot on Android).

Surfshark VPN's good speed, decent price and excellent privacy record qualify it as a serious contender for a top spot. It's a decent in-betweener which offers most of the features without any major compromises. It's great for both bypassing the Chinese firewall and unlocking Netflix. But if you need more serious privacy against governments and corporations, you should pay extra for Mullvad.

ExpressVPN: The Gold Standard



Of all the services presented in this article, ExpressVPN is the most robust and time-tested. It's the VPN that actually innovates and publishes the open source code on GitHub.

Express has been in the VPN business since 2009, and has maintained a clean record. In a world where hacks and breaches get revealed every day, it's quite remarkable that ExpressVPN has never had major issues. If you're searching for a solid internet privacy experience, this is the best you can get. It's only topped by Mullvad, but that one is a different animal with a different target audience.

But here's more praise for ExpressVPN: the service also has an exemplary policy to not store user data, which was proven under pressure. After the assassination of Russian ambassador to Turkey Andrei Karlov, one of ExpressVPN's servers was seized. As it turns out, the killer was using the privacy service.

Turkish officials thought they would find data from the assassin's social media and email accounts. Yet in spite of law enforcement's expectations, the server contained no records. This sounds like bad news for law enforcement on this particular case, but it's good news for privacy. The police will have to negotiate or extort the withdrawal of data by dealing directly with the criminal. And thus, ExpressVPN's promise to include no back doors and keep no logs proved to be true.

Furthermore, the Chinese government considered ExpressVPN to be a threat to their firewall. Officials from Beijing have pressured Apple to remove the app from the App Store. How did ExpressVPN react? They published a blog post to reaffirm the company's commitment to free and open internet.

These events have only strengthened ExpressVPN's reputation in the field. They also positioned the service in a spot where it leads by example. But the excellent record and proven history of good practice come with a price: the monthly subscription is $8.32 for a 12-month commitment. And if you opt to pay for only one month, then the price is $12.95. In comparison with Nord, Surfshark and Pure, you pay a premium. But if you care for quality, it's well worth it.

As of December 2021, ExpressVPN allows you to access servers in 160 locations that are spread across 94 countries. The quantity is comparatively not too impressive, but the geographic distribution is more generous. More jurisdictions will grant you better tools to gain privacy in various situations. They allow you to unlock a greater amount of Netflix content and circumvent governmental censorship. In comparison, hundreds of servers in one country are easier to block or shut down.

Yet ExpressVPN lacks a native Tor integration like Nord and an option to connect to two different servers (double VPN) like Surfshark. On the surface, it seems to be marketed more towards streaming and unlocking content. But the excellent track record and generous documentation suggest that it can do much more.

There are two more reasons to like ExpressVPN: the open-source Lightway protocol (which greatly increases reliability and access speeds), as well as the company's apparent bitcoin maximalism (though the payments processor of choice is BitPay, which diminishes the power of the BTC-only focus).

Mullvad VPN: The Choice of Cypherpunks (Peter Todd, Carl Dong)

The most private data is the one that provably doesn't get stored in the first place. And Mullvad takes these privacy and security precautions to a whole new level by generating random account numbers instead of asking for pre-existing credentials (e-mail, phone number, or Bitcoin node address). All VPNs in this article brag about a "no logs policy", but Mullvad provably respects the principle by keeping the experience private by default.

Also, the service is open source and every line of code can be verified on GitHub. Under the GNU General Public License v3.0, you can even fork the code and sell a competing product – it's not like it's that simple to acquire a global network of servers, though.

Mullvad costs 5 euro (approximately $5.5) per month regardless of subscription time, accepts bitcoin payments, and even offers a 10% discount for using the world's hardest and most liquid money. If you're extra paranoid about your privacy, you can access the page using Tor and set up a new randomly-generated account every month (this way, your accounts become disposable and so does the data that they generated). Also, Bitcoin Core developer Carl Dong offers a service which enables instant and more private Lightning Mullvad renewals – just go to vpn.sovereign.engineering.

It's pretty safe to say that Mullvad is in a league of its own and is designed for people who can't afford to compromise on privacy. Sure, you can use it for streaming on Netflix but ExpressVPN and Surfshark will always be faster.

Mullvad has applications for all major operating systems and browsers. If you can't access any of these, you can go for the general-purpose and open source WireGuard and OpenVPN, which you'll have to point to the Mullvad servers. Speaking of servers, you get 759 of them in 38 countries and 64 cities. About a quarter of them belong to Mullvad, while the others are rented – a distinction that will help you assess the amount of privacy that you want to get.

Interestingly, Mullvad is based in Sweden. This means that the company must comply with EU data regulations. However, they can't give away the data that they don't collect in the first place. Compared to NordVPN and Surfshark, the access speed is slower, you get fewer servers, and you can't connect to two servers simultaneously. But Mullvad doesn't even know your e-mail address and offers you a service that's very honest about what it is and what it does.

And yes, during S4 E7 of the Bitcoin Takeover Podcast, Peter Todd mentioned that he uses Mullvad specifically because he understands how the service operates and perceives it as being honest about not collecting and making money from logging information.



Compare Top VPNs

	PureVPN	NordVPN	SurfShark VPN	ExpressVPN	Mullvad VPN
Open Source	No	No	No	Yes	Yes
JurisdicPon	BriPsh Virgin Islands	Panama	The Netherlands	BriPsh Virgin Islands	Sweden
Promises No Logs Policy	Yes	Yes	Yes	Yes	Yes
Immaculate Track Record	No (helped the FBI in 2017)	No (got hacked in 2018)	Yes	Yes	Yes
Speed RaPng	8/10	9/10	9/10	10/10	7/10
Data required to register	Only e-mail if you pay with BTC	Only e-mail if you pay with BTC	Only e-mail if you pay with BTC	Only e-mail if you pay with BTC	None
Double VPN	No	Yes	Yes (MulPHop)	No	No
Tor integraPon in the app	No	Yes	No	No	No
Pay with Lightning	No	No	No	No	Yes, on vpn.sovereign.engineering
Who handles BTC payment?	Coingate	CoinPayments	CoinGate or CoinPayments	BitPay	Proprietary node
Servers (Dec. 2021)	6500+ servers in 78 countries	5175 in 60 countries	3200+ in 65 countries	160 locaPons in 94 countries	759 (162 owned & 597 rented)
Protocols	PPTP, SSTP, OpenVPN, L2TP	NordLynx (WireGuard), IKEv2/IPsec, OpenVPN	Wireguard, IKEv2/IPsec, OpenVPN	Lightway, L2TP IPsec, OpenVPN	Wireguard, OpenVPN
Price for 1 month (no discount)	$10.95	$11.95	$12.95	$12.95	$5.6
Monthly price with longest-term subscripPon	$2.05	$3.71	$2.21	$8.32	$5.6

Hide Your IP Address Using Tor

What is Tor?

The Onion Router (Tor) is a free and open source software protocol which enables anonymous communicaPon between internet users.

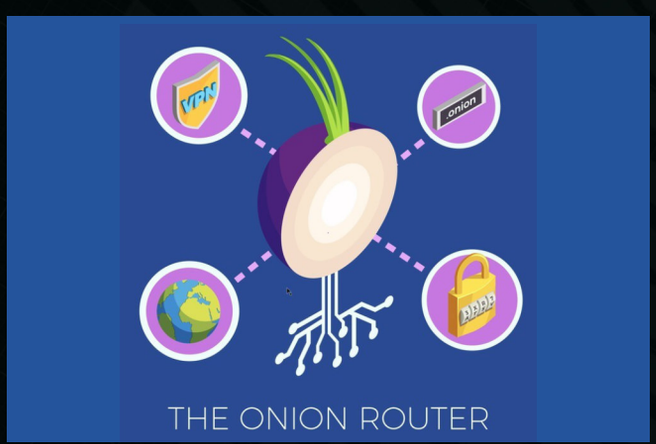
By using a privacy technique that's called onion routing, Tor operates on a worldwide network of over 6,000 relay nodes. It's called an "onion" because it comes in many layers that cover and protect the core.

The nodes involved will randomly route data packets in equally random combinations. A relay can only know where to send the data for the next step, but has no knowledge about the original sender and the final receiver.

For example, let's say that Alice wants to visit Amazon without revealing her IP address. To increase her privacy, she will run the Tor browser. This way, her connection gets relayed through multiple random routing nodes.

The Tor network encrypts the data and transforms it into a packet wrapper. This enables a relaying privacy which places unknown intermediaries between Alice and Amazon. When nodes encrypt and forward Alice's data, they don't know much. All a relaying node can see is what the previous peer sent and the next destination of the data.

Also, the path of choice is completely random. This means that any of the 6000+ relay nodes can receive the access data, encrypt it, and pass it along. There is an un-





encrypted part of the Tor setup, though. It's found in the communication between the last relaying node and the data receiver.

In our example, Amazon will be able to see information about the exit node. This means that identifying Alice involves route path backtracking and step-by-step data decryption. The Tor de-anonymization process is not impossible, but definitely challenging and resource-intensive.

Nonetheless, the most private Tor communications take place between Tor users, with information that never leaves through an exit node and gets relayed back and fourth. If someone who doesn't use encryption interacts with a Tor user, then part of the anonimity is gone. Hackers will just have to extract or social engineer data from the unprotected party.

Also, Tor's privacy and anonymity are not perfect. For example, Europol has been able to take down dark market websites in 2014.

This was part of their initiative to crack down on illicit online activities.

Yet only because some criminals use Tor doesn't mean that the network only exists for them. Investigation journalists, diplomats, law enforcement officials, and generally vulnerable people all need this kind of privacy. Tor enables safer communication across the internet. Which means that it can also strengthen law enforcement and enforce human rights protection.

Likewise, the Tor browser is an excellent way of repelling trackers, ads, and malware. It protects your rights on the internet in a practical way. Just like you pull the drapes and close doors when you need more privacy, you should also use Tor.

Now here's the tricky question: how does Tor, a centralized free open source software, get its money? Non-profits and open source software projects usually struggle with raising funds.

Interestingly, a big chunk of the money for Tor comes from the US Government. Three main institutions are involved: the US State Department, the Broadcasting Board of Governors, and the National Science Foundation.

The US government's involvement is no surprise, though. The concept of onion routing dates back to a 1990's US Naval Research Laboratory project. In the beginning, Tor enabled a private communication channel for governmental agencies.





As time went by, the tools were open sourced to promote human rights worldwide. This may seem like an irrational expense by the US Government. But it actually serves their agenda of universal democratization and human rights.

Most authoritarian and totalitarian governments are hostile to the USA's foreign policy. Sometimes they also happen to threaten journalists, diplomats, and local freedom fighters. So for protection purposes, useful privacy tools are a must. In their situation, privacy is a matter of life and death. Thus, an interesting utilitarian argument emerges: it is better to protect those who need it, even if some criminality blossoms in this environment. It's not like criminals can't



be targeted through other means (mostly metadata analysis of data packets getting exchanged and social engineering).

You should always be aware that the NSA might be able to intercept Tor communications. They run exit nodes, they do metadata analysis, and also have other means to track and surveil beyond your computer. So if you want to hide from the US intelligence agencies, you're better off not using Tor (or the internet) at all. But if you only want privacy against private entities or governments with weak surveillance systems, then you're probably fine.

Is Tor a VPN?

Now this is the kind of question that sounds stupid at first, but gets more complex as you think about it. In hindsight, both VPN services and Tor conceal your IP address. They encrypt your data, and then forward it to another party that won't know who you are. This makes them useful privacy tools.

But the main differentiator between Tor and a VPN is randomness. A VPN service will only allow you to connect to a limited number of known servers. With some logging information, they will know how, when, and where you connect. This is why it's important to choose your VPN with precaution.

In contrast, Tor is completely random. Every new tab in your browser will generate a new relaying path. Each time you want to get a new identity, you get it by pressing a single button. And whenever you connect, it's very difficult to backtrack on the routing path.

With three random relaying nodes between you and the destination, you have a lot more privacy. While you can set up your VPN service to route through many nodes like Tor, it will still lack the randomness.

This is also an issue of anonymity: VPN users register with email address and payment info. In the case of Tor, you download a free software and run it without signing up to anything.

The distinction exists even in the name of the anonymity services. Tor is open source and a collective effort of freedom lovers who run relaying nodes. Like in the case of Bitcoin, anyone can volunteer to run a node.

But the "P" in VPN stands for private. The



network to which you connect belongs to somebody and follows a set of rules. Even if the software is open source (as in the cases of ExpressVPN and Mullvad), you must still trust that the hardware specifications are honest.

You can't join the Virtual Private Network with your own server. This would require registration, which leads to a loss of anonymity by default.

In conclusion, Tor is not a VPN because it's a public network. Much like Bitcoin, Tor is open source and permissionless. Unlike Bitcoin, it’s a centralized project.

To some extent, the anonymity protocol can also be censorship-resistant. Tor grants you the liberty to run your own node, randomly access other people's routing hardware, and encrypt the data at every step.

You don't have to trust in a company, but in an open source protocol that you can verify. And most importantly, Tor has no monetary cost. But it would be great if you ran a relay to support the network.

Advantages of Using Tor

First of all, Tor is an excellent privacy tool. Through it, the data you send gets encrypted and routed by random anonymous nodes. In this sense, Tor is one of the most private ways of experiencing the public and open web.





Another advantage of the Tor protocol is the ability to browse the deep web. This is the hidden part of the internet, that only those who know the exact address can access.

The deep web isn't exactly the mythical place which enables free markets for guns and drugs. Often times, the media distorts reality for sensationalism. Most use cases are either governmental or human rights-related. On the deep web, government officials can communicate with other departments or embassies.

Tor is also for oppressed individuals: people living under authoritarian regimes can message other freedom fighters with greater privacy. This helps them organize movements and teach each other how to resist the oppression. They can also get access to information from abroad that their government censors. And in the process, investigation journalists from the free world get access to information that they can report.

For the average internet user from the free world, Tor provides anti-corporate privacy. If you hate how Google, Amazon, Facebook, and Microsoft track you across websites, then Tor is an off switch. The open privacy protocol helps you opt out from surveillance capitalism.

There is a lot of value in individual privacy. Let's say that a close friend has cancer and you search for books on treatments. If you browse without privacy on Amazon and you're logged into your account, your data gets stored. In exchange, Amazon may sell your search data to interested third parties.

Who might want data about people looking at books on cancer? Insurance companies! In the future, your insurance premium might get increased because of your suspicious searches. There is nothing illegal or shameful in searching certain items on the internet. But some third parties might interpret your browsing history in a different context.

This context can damage your reputation, your finances, and even your professional life. And thus, it is better to run Tor and stop worrying about corporate surveillance. Browse anonymously, and then buy the items that you want in person, with cash.



Disadvantages of Using Tor

There are three disadvantages of using Tor – and if you're not chased by the CIA, then there are only two.

The biggest of issues is about internet connection speed. Having your data encrypted and relayed will decrease your upload and download speed. Tor increases page loading times.

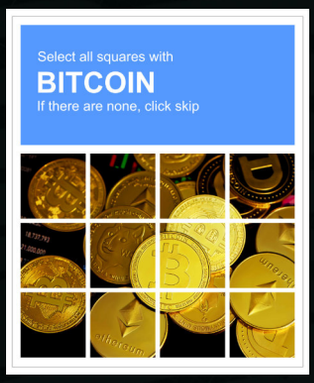
In some situations, it may even limit displayed content (such as ads and JavaScript).

This is why you should adjust the Tor settings according to your privacy needs. At the highest setting, you won't be able to see any Javascript, while images and fonts change their look.

This is the greatest amount of privacy and security against tracking that you can get.

But if you lower the threshold, you can experience the same web visuals as with any other browser. There is a trade-off involved, but your connection is still encrypted and relayed via onion routing.

The biggest disadvantage of using Tor is political. Exit nodes, which carry the message to the destination, are Tor's main attack vector. Your government might just run one of these exit nodes for data surveillance. Also, the US Government offers most of the financing of the Tor project.



This can mean that Uncle Sam has a special interest in the network and might watch it. But if the goal is to protect yourself from surveillance capitalism, Tor is great.

The last disadvantage is about how third party websites react to Tor. Some web pages will make you run extra security checks to prove you're not a bot.

This isn't a big issue per se, but you still have to waste time doing CAPTCHAs: clicking on vehicles, streetlights, and finding crosswalks. When you have to do it on most pages you open, it's very inconvenient and annoying.

Google already adds an extra step for their search engine. They will most likely argue that they protect the service against bots. Yet other search engines like DuckDuckGo are friendly with your use of Tor. This means that Google's issue might also be with privacy and their ability to track.

How Do I Get Started With Tor?

There are three simple and accessible ways of getting started with Tor.

By far the most popular involves downloading the web browser. It's free, it's lightweight, and its interface very much resembles Firefox. The software is available for Windows, Mac, Linux, and Android. So unless you're an iPhone user, you can use it.

If you own an Android phone or tablet, you can download and install Orbot. This free and open source tool can be set to route all applications and data communications through Tor. This means that even Google Play and Facebook can get tricked to believe you have a different IP address.



With Orbot, you can make sure that the data you send and receive is much more private. Advanced users can even connect to specific bridges or relays. And in Google's panopticon, this can be a useful tool.

If you're on a computer, you can install a free Linux distribution called Tails. It's an operating system whose internet connection forces the use of Tor by default. Tails works on PCs as old as 10 years old and champions privacy. Once installed, you will also find useful cryptographic tools and a suite of office applications.

If the Tor browser has its limitations in scope, Tails offers holistic privacy. The only drawback of Tails is the reduced amount of available applications. If you need specific professional tools, you're better off using Windows or MacOS. But if your main focus is internet privacy, then Tails is the way to go.

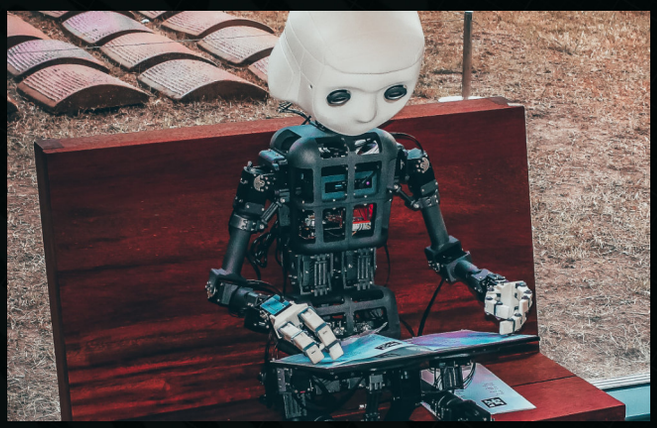
How Do I Use Google With Tor?



In most cases, Google will discourage the use of proxies (including VPN and Tor) with annoying CAPTCHAs. The rationale is simple: to see the search engine results, you will have to do a Turing test which proves you're a human user. This is a way for Google to keep bots away from spamming the search engine to influence content rankings.

Due to the CAPTCHA system, you will have to click on pictures according to instructions. Google will ask you to find all cars, bridges, cross walks, and street lights in random images. The process shouldn't take longer than 30 seconds, and after you submit a correct answer you're all set. That is, unless you've made a mistake and need to start over.

If you dislike doing this Turing test, switch to DuckDuckGo. DDG won't track you, won't collect data, and won't penalize your for using Tor.



Should You Use Tor With a VPN?

Combining Tor and VPN is the best way to protect your privacy on the internet.

Through this method, no routing node on the Tor network is able to see your real IP address. This means that the exit node backtracking attack becomes more difficult to perform because it adds an extra layer of inconvenience for the surveilling side. Also, should the Tor routing somehow fail, you're still protected by the VPN.

In a blog post, even VPN heavyweight ExpressVPN recommends stacking the two privacy tools. NordVPN enables it from the app, while Surfshark offers a free step by step tutorial.

At the same time, you should know that only the VPN through Tor setup offers real benefits. Putting a VPN service on top of Tor is more difficult, has no privacy gains, and slows down the connection.

The VPN + Tor combo is the best an average internet user can get to maximize privacy and security. To breach this setup, you need to use very expensive and sophisticated tools. Most data surveillance systems are powerless and inefficient against Tor over VPN.

Yet if you're interesting enough, nation states own the means to surveil your metadata and draw conclusions from your behavior. They can also track you in non-electronic ways via social engineering. So even if you have the best internet privacy you can get, determine your threat model with precaution and don't act like H.G. Wells' depiction of the invisible man.

PRIVACYPROS.IO

Billfodl



BITCOIN IS AN ESCAPE HATCH.

DON'T LOSE YOUR KEY.

BACKUP WITH BILLFODL.

USE CODE 'BTCTKVR' FOR 15% OFF.



DIY Hardware Wallets, Part I: Building Your Own Trezor One, Model T and BitBox02

We are living in the golden age of DIY hardware. Thanks to advancements in microprocessing and production/distribution, today we can purchase tiny yet powerful computers at surprisingly affordable prices – and then use them to perform unexpectedly-complex tasks.

The Bitcoin community certainly took notice and turned some of these general-purpose chips into financial sovereignty machines. From the popular ARM Cortex STM32 chips to the amazingly-inexpensive Raspberry Pi Zero, there are lots of options that you can use to build your own hardware wallet. But before we talk about the options that you have in order to build your own hardware wallet, it's important to mention the reasons why you should pursue this path.



Why is DIY better?

First of all, if you live in a country where there is no distribution of Trezor, Ledger or BitBox02, then building your own device is certainly the more affordable option. Secondly, if your government is hostile to Bitcoin and everything concerning it, then it's strongly recommended to use some of the



same parts that can also build a portable Tetris machine to secure your precious digital gold.

Even if you live in a country where commercial hardware wallet distribution is possible, pursuing the DIY route is still worth your consideration. If you're concerned about privacy (and you should be), then you shouldn't give your name and address to a vendor and a delivery company that will store your data in their records for multiple years – the case of the Ledger database hack is a very good example of why privacy and DIY hardware are important.

Furthermore, supply chain attacks are real: you don't know who's going to handle your hardware wallet from the moment it leaves the factory and until it finally gets delivered to you. If somebody knows what a Trezor is, they might compromise its hardware or its packaging (a very popular attack involves the insertion of already-generated BIP 39 seed phrases, in hopes that newbies would deposit their coins to addresses controlled by the malevolent actor). Sure, these companies make great efforts to prevent such attacks by layering their packaging and introducing cryptographic tricks to verify the integrity of the hardware and software. But if you know what you're doing, then DIY is definitely safer: using general-purpose off the shelf hardware and free open source software that you can personally verify is definitely the power user approach.



Hardware wallets you can build yourself:

Now let's talk about the hardware wallets you can build yourself. Essentially, there are two categories: the commercial devices whose circuitry and schematics have been open sourced (Trezor, BitBox02) and the non-profit community projects that were created specifically for DIY work. The Trezors and the BitBox02s come with the advantage of a more tested and scrutinized codebase and architecture since they are sold commercially. The teams behind the projects could afford to pay for bounties and security audits, but there's also a greater incentive for hackers to break them.

On the other hand, DIY projects like SeedSigner, Specter DIY and Bowser offer an extra layer of convenience, as they can be built from very common parts and require almost no soldering or experience with electronics. They aren't as tried and tested as their commercial counterparts and you shouldn't expect to get much support in the process. Yet they have advantages of their own and give everyone the opportunity to become financially sovereign.

In this first article, we're going to analyze what it takes to build your own Trezor and/or BitBox02. Naturally, the follow-up will focus on the Seedsigner, the Specter DIY, and the Bowser wallet.



Building your own Trezor One:

During the 2014 Kickstarter campaign which led to the launch of Bitcoin's first hardware wallet, Trezor co-founders Marek "Slush" Palatinus and Pavol "Stick" Rusnak presented their intention to create a device that could even satisfy the demands of Bitcoin creator, Satoshi Nakamoto. This meant that the software and the circuitry are transparent and 100% open source, so that anyone can see what the device is doing at any moment.

The Czech company's GitHub repository offers the complete board, schematics, and bill of materials (BOM). According to these



documents, you need 24 moving parts, the most important being the OLED display, the STM32F10XRXT6 microcontroller, the buttons, the case, the tactile switch, and the micro-USB port. The cost of everything should not exceed $20, though you also need a soldering gun and the dexterity to put it all together by yourself.

So even though the cost of producing a Trezor One hardware wallet is low, the assembly part can be difficult and intimidating for a newbie. But if you need to build yourself the most tried and tested hardware wallet, you're going to need to develop some practical skills. After all, it's no surprise that the Trezor One is the most copied device in the world and there are hundreds of companies that sell it under different brands all around the globe. As a matter of fact, newer devices such as BitBox02, Coldcard, and Foundation Devices Passport use significant parts of the Trezor code and to some extent can be labelled as "clones".

As soon as you're done putting together your custom-made Trezor One, you can flash the firmware according to the instructions from the GitHub repository. Once you're done, your new DIY hardware wallet will work perfectly with Wasabi wallet – and choosing Wasabi instead of Trezor Suite will bring you some privacy benefits concerning full node connectivity and the trustlessness of the onboarding process.

For more information about Trezor's open source ethos and commitment, listen to my interview with CEO Marek "Slush" Palatinus on the Bitcoin Takeover Podcast.

Building your own Trezor Model T:

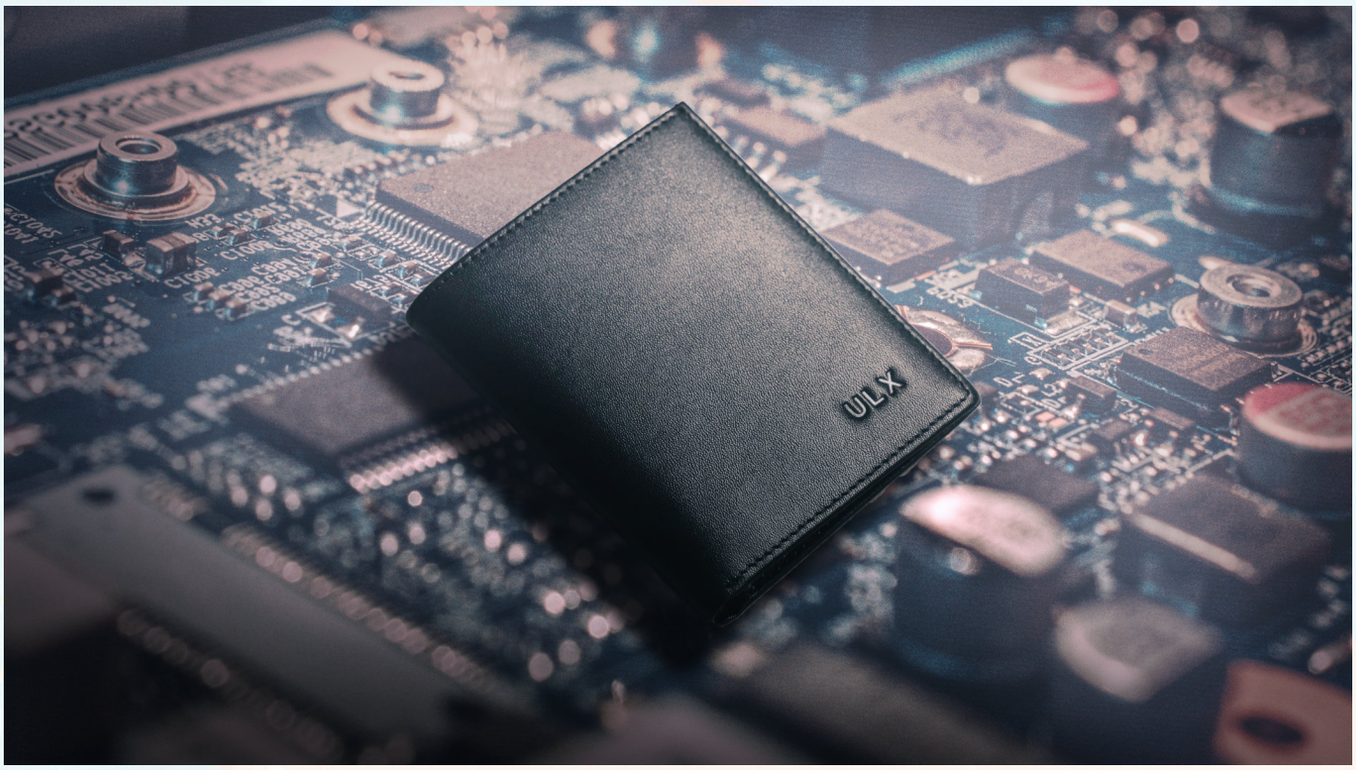
Launched in the fall of 2017, the second generation Trezor hardware wallet features some much-needed improvements. It replaces the two-button scheme with a color touch screen that's easier to use, and also comes with a faster processor which allows for more complex backups such as Shamir Secret Sharing to be made. The device is also more reliable at handling intricate multisig setups (such as 8 out of 8), as demonstrated by Jameson Lopp's comparative review.

However, the Trezor Model T also comes with greater electronic complexity: the bill of materials lists 109 parts, while the schematics are more elaborate and sophisticated. This means that the Trezor Model T is a more difficult and demanding DIY project than its predecessor. To make up for it, the build instructions are also more detailed and feature more pictures to guide you along every step.



In terms of security, the Model T comes with the advantage of allowing you to type the passphrase directly from your device – which is a great feature to have, especially when you think that your computer keyboard might be compromised/ logged. So even if you don't care much about multisig reliability or Shamir backups, it's still worth considering the Model T for its input upgrade.

The chip that drives the Trezor Model T is the STM32F427VIT6 microcontroller – an ARM Cortex M4 unit which features 2 megabytes of flash memory and is clocked at



168 Mhz. You can find it for about $20, but you'll definitely get better deals for bulk purchases. The display also costs about $5, and the remaining electronics should add another $20 (from case to the USB-C and micro-SD ports, and all the way to the various connectors). But before we judge Trezor for selling the device at a price which greatly exceeds production costs, we shouldn't forget that the device requires significant soldering skills to build (greater than the ones needed for the Trezor One), the company is mostly focused on improving software security standards (so you pay for the research and development of the SLIPs) and there's also a cost involved in offering customer support.

For a skilled DIY hobbyist, the Trezor Model T can be a fun weekend project. The fact that the parts are general-purpose and easy to find online should provide a great amount of plausible deniability in authoritarian states, and the extra features will make the supplementary effort worthwhile (as compared to the more simple Trezor One).

Just like the Trezor One, you can use your newly-built Model T with Wasabi Wallet. Keep in mind, however, that Wasabi won't work with multisig setups and Shamir Secret Sharing. Only BIP39 setups will do.

Building your own BitBox02:

Launched in the fall of 2019, the BitBox02 is a spin on the original Trezor design which brings some notable hardware and software modifications. Though it started from the same codebase, it's different enough to deserve the spotlight. Philosophically speaking, the device aims to offer the compromise between open source auditability and physical security which makes it the middle ground between Trezor (100% open source) and Ledger (about 40% open source, with an opaque secure element chip).



The part that makes the BitBox02 less open source than the Trezor but more physically secure is the inclusion of the ATECC608B general-purpose security chip. This means that you can protect your device from a malevolent actor's physical access without resorting to a software passphrase (that you may forget or lose if you're not careful enough). So if you want to take your physical security to the next level, you should consider building a BitBox02.

Besides the secure chip, ShiftCrypto's second generation hardware wallet features some interesting choices: the device uses a male USB-C connector which makes it easy to also plug into your mobile phone (no cable is required as long as you have the right port in your computer or phone), and the touch screen is replaced by touch sensors on the top and bottom of the hardware wallet.

In terms of software, the BitBox02 makes use of Schnorr signatures to verify the integrity of the software and prevent supply chain attacks. The system is called anti-klepto and, even though it may not seem very relevant for someone who builds their own hardware wallet, it is still a great self-verification tool which prevents outside meddling with the code. Learn more about this security mechanism from my interview with ShiftCrypto software developer and researcher Benma.

To help you build your own BitBox02, ShiftCrypto has published a bill of materials (which should be updated to include the ATECC608B chip which has replaced the 608A in 2021), an extensive datasheet, the circuit board schematics, and even an X-ray picture that should help you figure out how to connect every part to the board. The guide is not as detailed as in the case of the Trezor hardware wallets, but any experienced hobbyist should be able to figure it out.

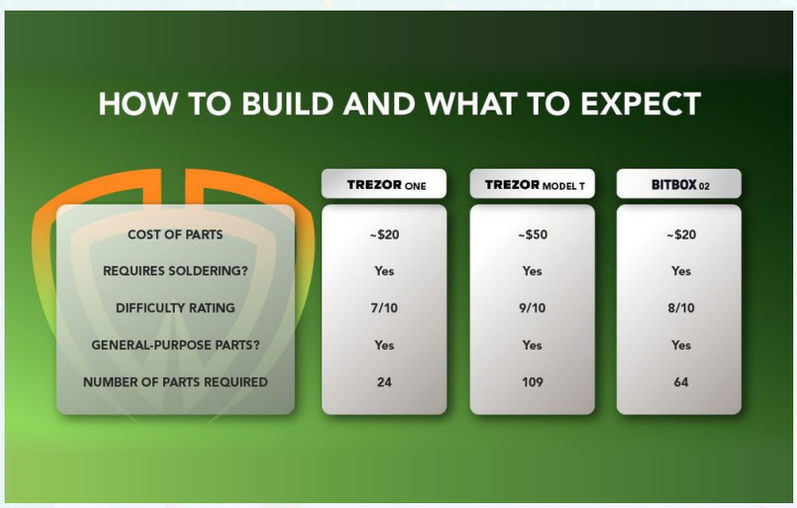
Now let's talk about the costs: in bulk, the ATECC608B secure chip can be bought for about $1. But due to supply chain issues in the microchip industry, it currently seems to be out of stock on some of the most popular retail websites (and will most likely sell at a premium due to scarcity). On the other hand, the 32-bit ARM Cortex M4F ATSAMD51J20A microcontroller chip costs approximately $6 and also appears to be hard to find. The PRTR5V0U2F suppression diodes and every other small part also adds up about $3 to the production cost. In total, purchasing the parts required to build your own BitBox02 should cost about $20 (including USB-C port, micro-SD card slot, touch sensors, and the OLED screen).

The BitBox02 has more parts than the Trezor One, but fewer than the Trezor Model T. It also features more affordable parts than Trezor's flagship model and offers some physical security. So if you find these qualities desirable, then you should grab your soldering gun and start ordering the parts while they're still in stock.

And yes, your BitBox02 will work with Wasabi wallet. But just like the Trezor devices, you will have to connect to the native software (in this case, BitBoxApp) in order to perform firmware updates.

Does building your own hardware wallet have to be so hard?

Well, no. Today we have the SeedSigner, Specter DIY, and Bowser devices and they are a lot more accessible to hobbyists who don't want to solder diodes to a PCB while consulting complex schematics. However, they aren't as tested! Find out more about how you can build these hardware wallets and the costs involved in the next part of this article!



WASABI.WALLET 2.0

A Bitcoin Wallet that provides privacy by default



- Coinjoin any amount
- No coordination fee under 0.01 BTC
- No coordination fee for remixing directly from a coinjoin and when 1 transaction away from a mix.

Wasabi is the standard for Bitcoin privacy

wasabiwallet.io



DIY Hardware Wallets, Part II:
Building Your Own PiTrezor, Specter DIY, SeedSigner and Bowser Wallet

There are two important categories of DIY hardware wallets that you can build from general-purpose electronic devices: the ones that run a ported firmware (a group of coders make a well-tested software available on more common hardware), and the ones that run original code.

Both of them are fairly easy to build and have very few moving parts that you need to put together. But from the get-go, you should understand the tradeoffs: a project like PiTrezor might be a convenient port which allows you to run the most tested hardware wallet software on a Raspberry Pi, but it doesn't mean that the port itself is vetted by security professionals or maintained to include the latest updates from Trezor. Conversely, a project like SeedSigner or Specter DIY might be original and open source, but this doesn't mean that many experts have verified the code either.

This is why the recommendation regarding these devices that you can build yourself is to check the code or pay a professional to do it for you. If you're going to use DIY hardware wallets to protect large amounts of bitcoin, then it's better to take the multisig path. If each device is nothing but a key to your coins and there is no single point of failure that can make you lose your funds, then it's generally safer to use something with a higher risk profile.

At this point, we should ask two very important questions: first of all, why build a DIY hardware wallet at all if the security is questionable? Well, some of the two best arguments include your ability to survive political authoritarianism, and the avoidance of supply chain attacks. Something that you build yourself from common parts is going to help you maintain your privacy and plausible deniability in relation to your government – and the delivery company won't know what you're up to either.

The other important question that we should ask at this point is: will your DIY hardware wallet work with Wasabi? Well, the answer depends on the hardware wallet model. Something like PiTrezor should work

as it's essentially the Trezor firmware on a different and more accessible system. Specter DIY and Bowser ought to also work since they use standards included in the HWI and PSBT specifications. In the case of the SeedSigner, single sig setups are still on the roadmap for development; therefore, Wasabi compatibility will have to wait for a little while.

Once again, these open source DIY hardware wallets are still in an early phase of development and mostly recommended in multisig setups. Don't take reckless risks with your bitcoins. If you're a hardware wallet hobbyist or an individual who's trying to gain financial sovereignty in an authoritarian environment, consider creating more elaborate setups which don't rely too much on a single device – even if this means that you're going to do a Shamir backup or multisig setup that isn't compatible with the Wasabi software.

After having presented the warnings, let's take a look at the four DIY hardware wallets in order to determine the costs, the difficulty, and the complexity of the task.

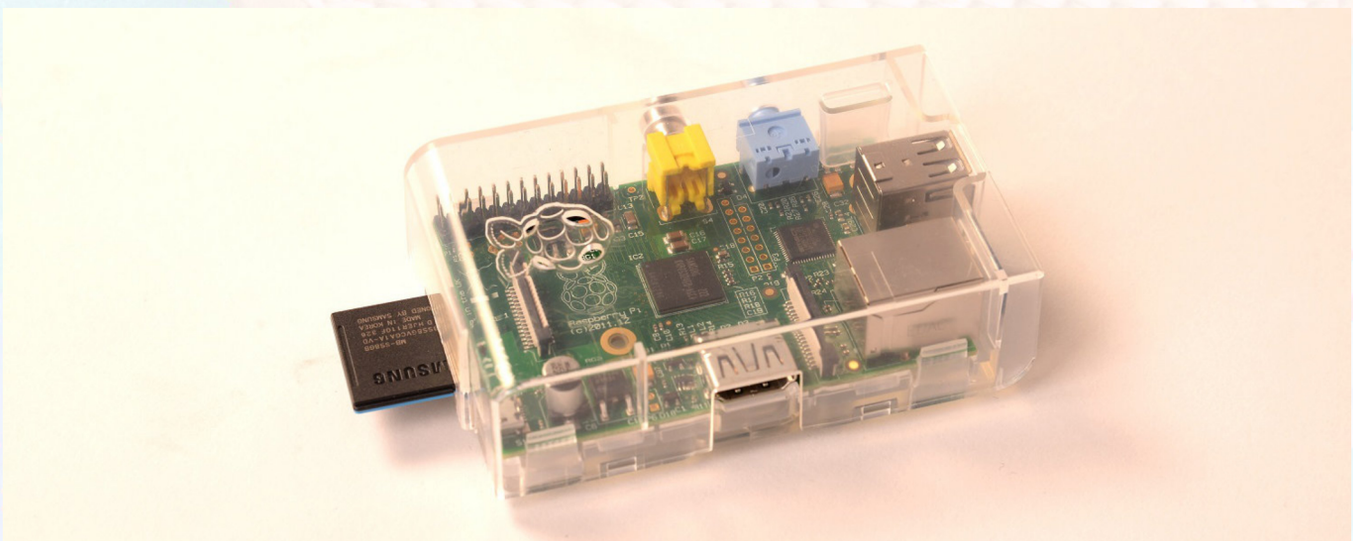
Building your own PiTrezor

A rule of thumb in security is to follow the most tested path. This way, you know more about the experiences of others and have a better understanding of all the tradeoffs involved. And since Trezor has been around since 2014 and the code has been under constant scrutiny since its inception, it's pretty safe to assume that the firmware works well and has been constantly hardened by disclosures.

PiTrezor is a port of the original code, which makes the STM32F10XRXT6-optimized firmware run on the more common and popular Raspberry Pi Zero. You can buy a Pi for virtually everything, from video game emulation to IoT experimentation, robotics and Tor relays. Also, the Raspberry Pi Zero only costs $5 and is among the most accessible mini-computers in terms of both price and the ability to find one in every corner of the world. Compared to the default Trezor microcontroller, the Pi Zero is a lot more popular and it's also easier to source compatible accessories.

Furthermore, the PiTrezor port also works on the Raspberry Pi 4 – the more powerful device which is mostly used by individual Bitcoin node operators. One major advantage of these devices is that they come with full USB ports which allow you to connect your keyboard to use as input. This means that you don't need to worry about finding buttons that fit to some kind of enclosure, as you have the option to operate the PiTrezor with a peripheral you already have.

Therefore, the process is a lot easier and requires no soldering or parts assembly if you run PiTrezor on a Raspberry Pi 4. However, the costs are higher by about $30.



Now let's talk about the parts and costs. There are two versions of the Raspberry Pi Zero, and you should get the more affordable one which has no bluetooth and WiFi. Not only because these ports are useless, but



also due to the fact that they can represent extra attack vectors to break the device or extract information. Although the PiTrezor maintainer suggests that the Zero W is just as secure because the firmware has no drivers loaded for the communication ports, a competent hacker can still exploit them if he gains physical access. Hence, for security and money-saving purposes, it's better to purchase the basic $5 Pi Zero.

Other parts include an SD card larger than 100 MB (basically any that you'll find nowadays for a couple dollars), a micro-USB to USB cable (about 1 dollar), a mini HDMI cable which connects to a monitor, TV or dedicated screen (costs about $3 assuming that you already have a monitor or TV), two push buttons that are compatible with the Raspberry Pi (about 2 dollars and you only need them for the Pi Zero configuration, as the Pi 4 can make use of your USB keyboard) and some wires to solder the buttons to the board (roughly 1 dollar). Optional parts include a dedicated screen which is useful for portability reasons, and an enclosure which protects the board and circuits from dust, physical damage and other factors.

Assuming that you pay 5 dollars for the Raspberry Pi Zero and 9-10 dollars for the remaining parts, we'll conclude that building the most basic yet electronically-demanding version of the PiTrezor will cost you about $15. Keep in mind that the screen, the enclosure, the soldering iron and the shipping of all these parts are not taken into account and can easily double the costs.

If you take the Raspberry Pi 4 route, you're going to only need the $35 device (go for the entry-level 2 GB model, you're not going to need that much memory for a Trezor), the 2 dollar SD card and the micro-USB to USB and mini-HDMI male to HDMI female cables. These should cost about 6 dollars. And while the approximated total of 41 dollars might sound like it's pretty expensive, at least you don't need to do any wire soldering and it doesn't require any special equipment for this task. You flash the firmware on the SD card, plug the Raspberry Pi to a power outlet, connect the external video port to your HDMI-compatible monitor or TV screen (anything newer than 10 years has it), and use your USB keyboard as input. It's pretty geeky, but somebody living in a place where Trezor



hardware wallets have no official distribution is going to really enjoy the power of DIY sovereignty.

Before we move on to the next part, here's another reminder that while the PiTrezor code is open source and basically a port of the official Trezor release, you should be cautious and avoid putting too many coins into this device without properly verifying the code. The safest way to use a PiTrezor is to make it one of your multisig devices, so there is no single point of failure. But you should always be cautious. As Trezor CEO Marek "Slush" Palatinus said in S4 E8 of the Bitcoin Takeover Podcast, there are around 40 Trezor clones worldwide and their modified code doesn't always get the scrutiny that it should.

Building your own Specter DIY

Specter creator Stepan Snigirev has started an entire DIY revolution in the Bitcoin hardware wallet space. Thanks to his micro-bitcoin and micro-arduino projects, low-powered devices are now able to run a lightweight version of the Bitcoin client. Most remarkably, he has created a hardware wallet which can be built using off the shelf parts, which runs non-Trezor code. While every commercial secure key management electronic device, from KeepKey to Coldcard and Foundation Devices Passport makes use of Trezor's open-source firmware in some capacity, the Specter DIY dares to be different.

To build your own Specter DIY, you only need an STM32F469I-DISCO developer board that you can buy for about $62, as well as a 1 dollar mini USB and a 1 dollar micro USB cable (both of which you most likely already have from phones or other hardware wallets). The device itself has everything you need, from touchscreen input to flash memory that you use to install the Specter firmware. So it's an all-in-one solution, which at best, only requires an enclosure to keep dust away.

Today, lots of Bitcoin power users build their own Specter DIY hardware wallet to avoid supply chain attacks. But since the code is not as vetted as Trezor's and may have vulnerabilities that weren't discovered thus far due to a lack of incentives (the Specter DIY is still a niche product that is



hard to find and the reward for cracking the code doesn't match Trezor's bounty program), it's best to keep the device for multisig. This is exactly what the developers of Specter recommend: they see their DIY project as something that's complimentary to other hardware wallets. You can still use it as a single-sig device, but the use case where it shines is multisig.



One recommendation for the Specter DIY is that you also purchase an additional barcode scanner module which costs $40. It will make the device more usable in an air gapped way, as you can scan QR codes and confirm transactions without connecting the hardware wallet to a computer. Additionally, you can make the Specter DIY self-contained with a battery. The complete assembly instructions are available in the project's GitHub repository. Furthermore, you will also find a video tutorial on YouTube.

In total, the Specter DIY should cost anywhere from 64 to 120 dollars to build. And if you also want an enclosure, you can either 3D print it according to specifications or else purchase it from a professional like Richard from the Czech Republic (not a direct endorsement, but I did buy my cases from him). This may sound like the Specter is an expensive device, but if you buy it pre-built then it's going to cost you 350 euros (414 dollars) for a full-featured enclosure + 60 euros (71 dollars) to also have the STM32F-469I-DISCO board attached. So it's definitely better to pay 150 dollars for a full-featured device that you build yourself from parts which you can source from different vendors than to spend $485 on the Specter Shield.

To better understand the scope and purpose of the Specter DIY project, listen to Stepan Snigirev offer all the explanations in S8 E11 of the Bitcoin Takeover podcast.

Building your own SeedSigner

The SeedSigner is a simplified fork of the Specter DIY, which replaces the development board touch screen experience with the powerful affordability of the Raspberry Pi Zero. Its main goal is to offer a powerful device that anyone can build for approximately $50.

Unlike the Specter DIY, the SeedSigner is currently only optimized for multisig xpub generation and makes use of a more traditional layout with physical buttons. The main drawback of this design is that some soldering is required to put together the device. But since it relies on the popular Raspberry Pi architecture, one can easily buy GPIO hammer headers (which cost $7) to avoid all the hassle.





To assemble a SeedSigner, you need a Raspberry Pi Zero computer (once again, the 5 dollar basic version without the WiFi and bluetooth is recommended), a 1.3 inch square LCD screen with a resolution of 240x240 pixels (which costs about $14) and a camera that's compatible with the Pi Zero system (the recommended model is the AuviPal 5MP 1080p, which is currently out of stock but should cost around 20 dollars).

The SeedSigner lead developer has also open sourced the specifications for the enclosure, so that anyone with a 3D printer can create their own. This is bad news for people who don't have access to 3D printing, especially due to the fact that the input requires physical buttons that come with the case. However, there are vendors and hobbyists (again, like Richard from the Czech Republic) who will 3D print cases for about $20.

So while the electronics required to build a SeedSigner cost around $39 (below the 50 dollar goal), you're going to spend slightly more to have the full experience. Nevertheless, putting together a SeedSigner is more affordable than the Specter DIY from which it borrows the code.

Speaking of the code, once you assemble the hardware you're going to need an SD card and you must also type in a few commands on an external keyboard. The complete guide makes it simple to follow, so even if you don't understand what you're doing you will successfully set up the SeedSigner.

You should also keep in mind that the SeedSigner is an air gapped device which is optimized to work with multisig-friendly wallets such as Specter Desktop, Sparrow, and BlueWallet. So you won't be able to access it from Wasabi Wallet until single sig support gets added for PSBT setups. At the moment, it is still a geeky DIY project that casual users won't find too friendly or accessible. But thanks to community contributions, it's quickly improving.

To better understand the philosophy behind SeedSigner, listen to S8 E10 of the Bitcoin Takeover podcast. If you need help along the way, search for the full assembly guide on YouTube.

Building your own Bowser wallet

Created by Ben Arc, the Bowser wallet is an even more simplified fork of the Specter DIY. All you have to do in order to build this hardware wallet is to buy a $40 M5Stack ESP32 Basic Core and install the firmware with a micro-SD card.

This means that the Bowser wallet is by far the most inexpensive and simple to configure DIY hardware wallet. You even get a full step



BOWSER WALLET



by step YouTube guide which helps you along the way. However, there are a couple of geeky quirks that you should consider: first of all, the hardware wallet also works as a video game system which runs a stylized version of Tetris. This is great for plausible deniability, as nobody will guess that the generic-looking device in your hands is also a Bitcoin device – which is very useful for people who seek to maximize their privacy in places that may be hostile to the idea of financial sovereignty.

Secondly, the Bowser wallet makes use of Morse code for input. This is by far the geekiest feature in any hardware wallet, as you must either carry a sheet of paper which tells you how to type every letter of the alphabet or memorize the code. Once again, since most people have no idea how Morse code works (and may even mistake it for Braille) this is excellent for privacy. But the feature effectively makes the device harder to use even by the hardware wallet owners, so depending on your threat model you should assess to which extent you need this extra complexity.

The Bowser hardware wallet is a pretty cypherpunk device as it mixes the privacy of video games and Morse code with the convenience of using a compact general-purpose computer. You can dispose of the unit at any moment and get a new one – just make sure that you have your backup in a safe place.

Currently, Bowser is designed to work with Electrum wallet and makes use of the PSBT standard to sign transactions. This means that it should also work with Wasabi Wallet, so long as you use the options associated with the Coldcard Wallet.

For more information and in order to better understand what the Bowser wallet is, listen to Ben Arc on S8 E9 of the Bitcoin Takeover podcast.

HOW TO BUILD AND WHAT TO EXPECT

	PI TREZOR	SPECTER	SEED SIGNER	BOWSER
COST OF PARTS	$15-$30 RPi Zero / $41-$60 RPi 4	$65-$150	~$60	~$40
REQUIRES SOLDERING?	Yes RPi ZERO / No RPi 4	No	Depends on setup	No
DIFFICULTY RATING	5/10 for RPi Zero 3/10 for RPi 4	2/10	4/10	1/10
GENERAL-PURPOSE PARTS?	Yes	Yes	Yes	Yes
NUMBER OF PARTS REQUIRED	6-8 for RPi Zero 4 for RPi 4	For the most basic build, but you can add a battery, QR scanner, smart card reader and a case.	4	1 (plus SD card)

Don‘t let other people hold your Bitcoin.



Get your **BitBox**02 hardware wallet at
shiftcrypto.ch & 5% off with **BTCTKVR**

Swiss made open source



The Privacy Benefits of Taproot

The Taproot soft fork is an essential step towards improving Bitcoin's on-chain privacy. After the upgrade got activated on November 14th 2021 at block height 709632, blockchain analysis companies are going to have a harder time determining what's happening on the public ledger. Inconveniently for those seeking to deanonymize all bitcoin transactions, Taproot makes most on-chain contracts and conditional transfers look identical to regular transfers. Indirectly, this also benefits scalability (multisig setups no longer take more block space) and fees (smaller transaction outputs translate in lower costs for the users).

This article, however, focuses on the privacy aspect of Bitcon's soft fork. It seeks to explain how Taproot increases every user's plausible deniability and potentially poses a threat to the blockchain analysis business. To make this improvement easily comprehensible, the benefits will be divided by use cases.

How Taproot Increases Lightning Network Privacy

The Lightning Network is Bitcoin's layer for instant, private and inexpensive transactions. Unlike a blockchain, it's extremely scalable, fast and doesn't require the entire network to store and validate every operation. The more elegant design also enables greater privacy: only the parties involved in a money transfer and the routing nodes can get information about an ongoing transaction. Outsiders are completely left in the dark and unable to tell anything about the actors involved and the amount of bitcoin that they moved around.

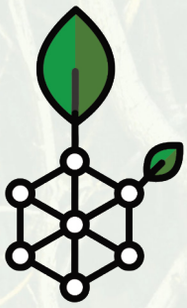


But since Taproot is a base layer upgrade, does it really affect Lightning? Without this Schnorr-friendly upgrade, channel openings and closings get revealed on the public blockchain exactly as what they are: 2 of 2 multi sigs with hashed time locked contracts (HTLCs). After the Taproot activation, everyone opening or closing a Lightning channel collaboratively will appear to be doing a regular transaction which is indistinguishable from the others.

Previously, blockchain analysts were able to tell when certain transactions would close Lightning channels. But after Taproot, they will only be able to see that the coins have moved. They won't know how they moved, they'll only observe that the amount has been spent in an indistinguishable way.

However, the privacy level still isn't perfect. As pointed out by Wasabi Wallet creator Adam Ficsor, non-private Lightning channels broadcast a channel point which corresponds to the opening output. Therefore, this bit of information, which can be observed on the Lightning network, gives away information about the output that is engaged in the channel opening. Taproot does make Lightning network channel opening private, but only if the channels are also private. Similarly, even though CoinJoin transaction before and after opening a Lightning channel can obfuscate the previous and future, the Lightning gossip would still reveal the precise UTXO controlled by the node operator. There is promising research to mitigate the problem with ring-signature proofs for DoS protection.

How Taproot Increases Sidechain Privacy



Like Lightning channel openings, sidechain peg-ins also rely on a multisig contract. On RSK (Rootstock, a Bitcoin sidechain which seeks to port Ethereum smart contracts), there's a two-way peg (2WP) which ensures that the BTC gets transferred safely. But after Taproot, this transaction is going to be indistinguishable from all the others and will also occupy less block space.



The same happens for Blockstream's federated sidechain Liquid, as well as Drivechains. Regular transactions, Liquid peg-ins, Lightning channels and user multisig will look exactly the same.

How Taproot Increases Multisig Privacy

In recent years, multisig setups have become extremely popular among bitcoiners. As the user experience has improved with wallets such as Electrum, Sparrow and Specter, many community members have chosen to make their coins harder to steal, hack or spend. The idea behind it is that you don't need to trust a single wallet or entity with the randomness and security of your private key. You use different devices with different processing units to generate your keys, and afterwards you can go as far as distributing your private key backups to different parts of the world.

Depending on your setup (most users do 2 of 3, but you can go as far as 15 of 15 if you prefer complexity), you can get a lot of extra security at the expense of losing accessibility – and if you make it too hard even for yourself to recover the coins, you might just lose them.

Taproot has two essential benefits for multisig setups: it makes them more accessible (the transaction cost of signing a 19 of 20 transaction will be the same as taking care of a single one) and also adds an extra layer of privacy. All the unnecessary information will no longer appear on the public blockchain. This preserves the secrecy of all the signers by only displaying the main input and its corresponding output. Before Taproot, blockchain analysis could determine which keys from the setup have signed the transaction. After Taproot, this information will become unavailable to the public.

How Taproot Increases the Privacy of Bitcoin Smart Contracts

Since day one, Bitcoin has enabled smart contract functionality. Basically, users have been able to broadcast conditional transactions which would instruct the rest of the network when the funds become available for spending. Multisig setups, Lightning channel openings and sidechain peg-ins are all variations which make use of different types of conditions.

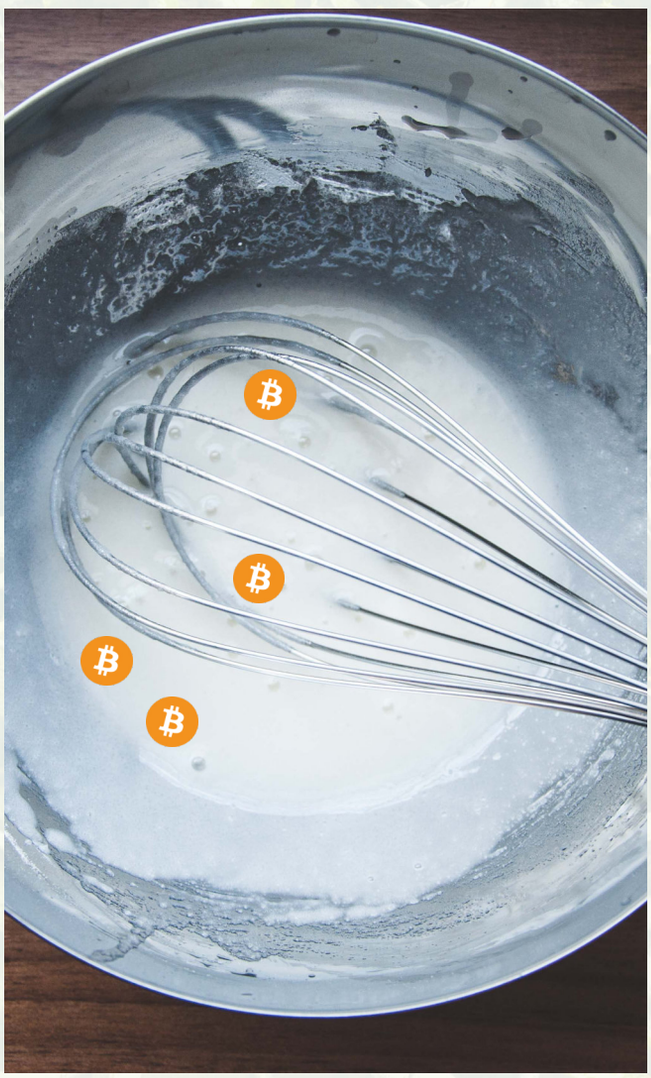
So let's consider a basic contract in which Alice locks her bitcoins until a certain block height when she thinks her infant child Bob will be a grown adult, or else allows for Bob to unlock the amounts as soon as he becomes technically capable of signing a multisig transaction. Under the current framework, both conditions get revealed to the entire network and become part of the immutable ledger. But with Taproot, only the one that gets executed will actually become public. It's an efficiency upgrade which saves precious block space but also a great privacy trick that's going to enable lots of creative ways to preserve wealth across time.

Taproot Simplifies Invisible Coin Swaps

Mercury Wallet by CommerceBlock has become increasingly popular in recent months. This is because of a special feature which performs a change of output ownership on the Lightning network and effectively enables users to trade their coins' transaction history in an elegant and scalable way. If bitcoiners open Lightning channels and trade UTXOs with one another, they can obfuscate a lot of the previous activities involving their money and return to the BTC blockchain with a different set of coins. Mercury Wallet makes use of Ruben Somsen's statechains concept to lock funds for a predetermined amount of time and conduct mixes between equal outputs.

In a sense, Coinswaps are CoinJoins that make use of Lightning's scalability and low fees. Thanks to Taproot, they too are indistinguishable from the other transactions.

However, with Coinswaps, you always face the risk of receiving a more problematic UTXO which may have a criminal history. Instead of combining multiple transaction histories (as in the case with CoinJoins), it enables an anonymous market for swapping transaction histories. As Wasabi wallet creator Adam Ficsor pointed out in a recent interview, the two privacy solutions can become complimentary tools: “The combination seems to be more interesting though: CoinSwaps to and from CoinJoins, which could make low anonymity set CoinJoins get as much privacy as a CoinSwapper would.”

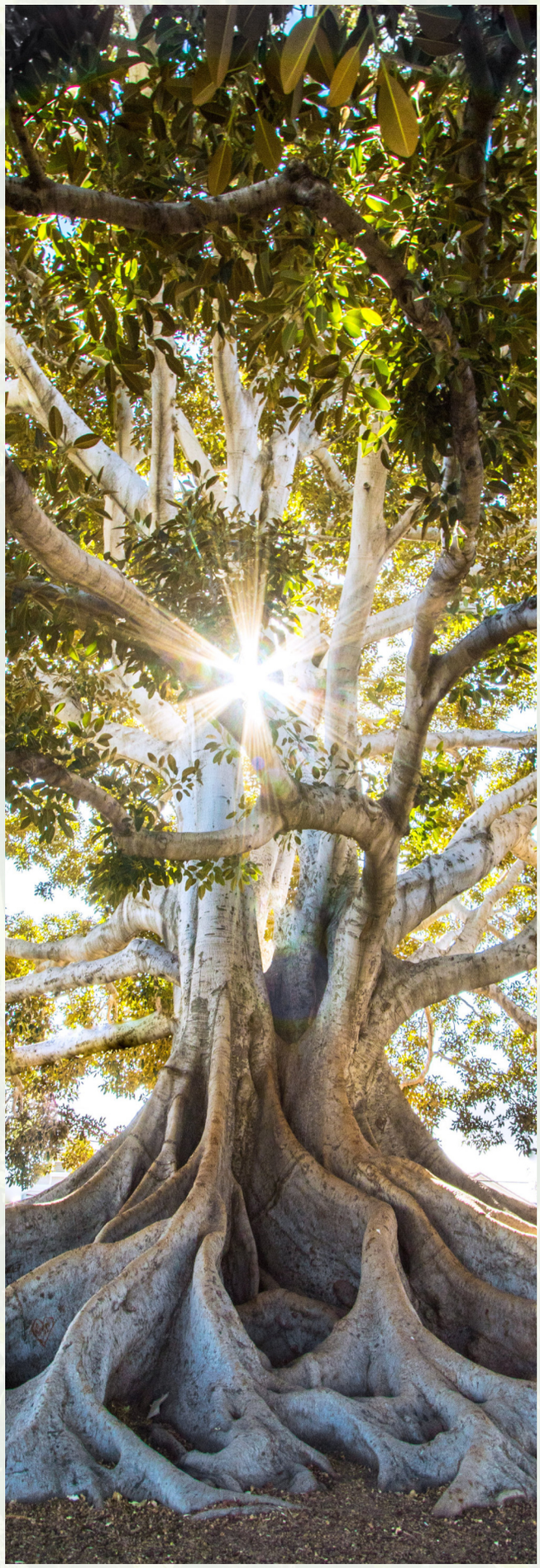


Bitcoin Privacy After Taproot

With Taproot, Bitcoin has undergone a long-desired upgrade to the more efficient Schnorr signatures, while also taking a few steps towards winning the battle against financial surveillance. This doesn't mean that blockchain analysis becomes obsolete after this upgrade, though. First of all, it will take time for users to update their nodes to the latest Taproot-friendly client (so the benefits will not be enjoyed by everyone). Secondly, developers have to release wallets and applications that make use of Taproot's full potential. For now, not much has changed since block 709632, when the soft fork was activated. But the numerous benefits of Taproot give hope for swift adoption.

Furthermore, the Bitcoin protocol can be optimized even further for scalability and privacy. One of them may be Jeremy Rubin's OP_CHECKTEMPLATEVERIFY (BIP-119, formerly known as OP_SECURETHEBAG), which batches transactions to reduce the amount of inputs and cut down on fees during moments of high demand and congestion. With it, CoinJoins and Coinswaps can get even more plausible deniability since the same technique becomes a natural component of the Bitcoin transaction routine.

Other solutions include Drivechains (Paul Sztorc has managed to create a Zcash-like chain which serves the purpose of increasing the fungibility of processed bitcoins), Mimble Wimble extension blocks (an ongoing experiment on Litecoin, which may be useful if it proves to work), and the hope that Core developers will figure out a way to integrate zero-knowledge proofs or Confidential Transactions without the need for a hard fork. However, the Schnorr signature-powered Taproot is still a great start and the way in which it was activated gives us hope that one day bitcoins will acquire nearly-absolute fungibility.



WASABI WALLET



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



Bitcoin NFTs On Counterparty

(And How To Get Or Create Your First One)

Omnipresent all across media channels and yet largely misunderstood, NFTs are this cycle's subject of fascination and (mostly) irrational speculation. Due to the excessive hype associated with the "looks rare" movement, some commentators even went as far as comparing NFTs to the ICOs of 2017 and 2018 – and rightfully so, the exuberance for scarce assets and the ease of "minting" NFTs has led to a situation where everybody seems to issue and sell whatever they may perceive as a collectible. Just fiat inflation issues.

But unlike ICOs, with NFTs what you see is what you get. Nobody buys these tokens expecting anything else other than receiving a unique digital asset which is associated with a piece of art. While ICOs come with roadmaps and promises about the future of the project, NFTs are cryptographic hashes written on the blockchain. Basically baseball cards for nerds.

It's also worth mentioning that not all NFTs are created equal: while the most widely-known and commercialized are ERC-721 tokens on Ethereum, there are also Liquid sidechain tokens that get traded on Raretoshi. However, the truly special ones get minted on the Bitcoin blockchain via Counterparty, benefit from the most secure network of them all, get stored on pretty much every sovereign node, and receive unique names that act just like internet domains that can't be replicated. If the token is the art, then it's the most resilient and provably one-of-a-kind of them that matters the most and is most likely to stand the test of time.



And yes, there's also the associated art. Presented under the form of a jpeg, gif, YouTube link, or even audio file, it's basically the mutable and changeable visual representation of the token. But the art file itself does not get stored on the blockchain: most of these only exist on Imgur, IPFS, or some other centralized website which specializes in allowing users to upload and share images. This means that one shouldn't regard the jpeg as anything more than the nice wrapping which offers visual details about the token's significance.

Though some users start lawsuits and get offended when the same image gets used to mint another NFT, they should remember that they actually paid for a unique token that provably can't be replicated. It's "non-fungible" (you can't replace one with another, as there is no identical hash) and it's essentially what Hal Finney described in 1993 while suggesting how cypherpunks can have "hours of fun".

Crypto trading cards.

- **To: CYPHERPUNKS <CYPHERPUNKS@TOAD.COM>**
- **Subject: Crypto trading cards.**
- **From: Hal <740761041@CompuServe.COM>**
- **Date: 17 Jan 93 13:48:02 EST**

Giving a little more thought to the idea of buying and selling digital cash, I thought of a way to present it. Were buying and selling "cryptographic trading cards". Fans of cryptography will love these fascinating examples of the cryptographic arts. Notice the fine way the bit patterns fit together - a mix of one-way functions and digital signatures, along with random blinding. What a perfect conversation piece to be treasured and shown to your friends and family.

Plus, your friends will undoubtedly love these cryptographic trading cards just as much. They'll be eager to trade for them. Collect a whole set! They come in all kinds of varieties, from the common l's, to the rarer 50's, all the way up to the seldom-seen 1000's. Hours of fun can be had for all.

Your friendly cryptographic trading card dealer wants to join the fun, too. He'll be as interested in buying your trading cards back as in selling them.

Try this fascinating and timely new hobby today!

Hal

As previously established, the images are mere visual representations that help you understand what the token is about. However, it's this totally fungible and replicable art that initially draws your attention and makes you want to support a certain artist's work. Some of these files (most commonly jpegs and gifs) are meritoriously artsy, others come with an amateurish dankness, but most of them seem lazy, half-baked, uninspired, and most likely only exist to make a quick buck on the hype train.

Which is why I'm bearish on Ethereum and Solana NFTs, but bullish on Bitcoin Counterparty creations: the art isn't only better, but also timeless enough to stand the test of time and make a comeback even after the investment bubble bursts. Bitcoiners build protocols and layers that last and find a purpose years after they were declared dead and abandoned. The Ethereum side is all about finding new sources of hype and conveniently burying the past failures. In 2021, the Omni layer was revived through John Calvalho's Synonym project, while Counterparty once again rose to prominence thanks to its rich history of art. Don't expect to read similar news about Raiden or Plasma.



Where do NFTs come from?

There's definitely more to the jpeg than meets the eye. And much like everything else that Ethereum turned into a soulless VC-funded yet unscalable snake pit, NFTs were first popularized on Bitcoin's Counterparty protocol between 2014 and 2016.

Mind you, it was Namecoin (formerly known as BitDNS, a hard fork of Bitcoin which Satoshi Nakamoto himself endorsed) that gets credited for issuing the first NFTs in history: Quantum, Blockheads, Comicons and Cryptoeggs were basically avatar projects which sought to provide every new user a unique digital identity. They weren't meant to become collectibles, but people started trading them and they accrued market value. Several years later, Ethereum would copy this approach with CryptoPunks and other similar computer-generated profile pictures that you can see in Twitter avatars today.

But after the Counterparty protocol launched in January 2014, bitcoiners started to create their own form of tokenized art. From this point onwards, you can identify two significant schools of thought: the video game asset innovation side (Shaban Shaame's "Spells of Genesis" and Christian

Moss' "SaruTobi Island" cards being two of the finest examples) and the meme side (Rare Pepes, Fake Rares, Leftist Tears, Bitcoin Heads). Of course, not all of these NFTs emerged in 2014. The Rare Pepe directory was first created in September 2016, Spells of Genesis cards first appeared in September 2015, while Fake Rares and Bitcoin Heads were issued in the second half of 2021.



Yet the element that makes them stand out is the fact that they're user-generated via graphic design software or even hand drawing. Bitcoiners love proof of work – so unlike their Namecoin and Ethereum counterparts (no pun intended), they don't issue art that a computer generated automatically. You can find a charming human element in all of these Bitcoin NFTs.

To find out more about the history of NFTs, read WhiteRabbit1111's excellent article "The origin assets of the digital antiquities market (NFTs)". It's a deep dive into all sorts of projects, some of which are lesser known but deserve praise for pioneering what would later turn into a thousand-bitcoin industry (most notably, OLGA is really endearing).

What is Counterparty?

Counterparty is a Bitcoin protocol that history books rarely mention. Even "Mastering Bitcoin", arguably the most extensive and exhaustive of all publications on the topic, only describes Counterparty in one paragraph before moving on to altcoins (which get more coverage).

One could argue that Counterparty is a relic from a long-forgotten past, a ghost town which serves as a reminder of the early intentions and aspirations of bitcoiners. Essentially, it's a protocol which enables anyone to permissionlessly issue tokens and set up contracts which pay dividends to holders. Counterparty is a bona fide prototype of what would eventually get turned into the Ethereum project – except that it had a fair launch, it has no blockchain of its own, and all of its transactions (from issuance to transfers) get settled on the Bitcoin blockchain and pay transaction fees.



In 2014, bitcoiners dreamt of tokenizing stocks and commodities on their beloved network. Trade Apple stocks, cocoa bean futures and gold tokens on Bitcoin? Sure, why not! Build decentralized companies whose assets exist natively on the Bitcoin network? That's also possible on Counterparty. Tokens that do fundraisers and pay dividends to their owners? Yes sir!

This was before the scaling debate and before deciding that blocks should remain small to preserve decentralization and censorship resistance. Most people behind the project would later jump ship to the new and shiny Ethereum, which could technically do more and theoretically scale better for these use cases.

Because for a while, Counterparty transactions were unfairly regarded as "spam" which doesn't serve the best interests of the Bitcoin project. One could argue that someone's money doesn't get confirmed faster due to the intensive trade of Counterparty tokens, since the former pays higher fees than the latter. Also, the OP_RETURN transactions that Counterparty uses to insert arbitrary data in Bitcoin blocks takes more block space than a regular transaction.

But then again, this means that a higher fee gets paid. Also, to keep the Bitcoin project's incentives sustainable, we must build a competitive fee market. There's also another small bit about the Bitcoin network being permissionless and enabling users to be sovereign (i.e. use their own money however they want). So how can it be spam if it pays its fair fee to the miners?

Counterparty has been on the "wrong"



side of Bitcoin history and many chose to not talk about it at all. It has a native token (XCP) which is used to give arbitrary names to assets: if you pay 0.5 XCP, then you can call your new NFT "BTCTKVRMAG" instead of allowing the protocol to automatically name it "A11113761191968729490" (where "A" stands for "asset"). You can also sell your new tokens and give dividends to holders by using the XCP token.

But there's a catch: Counterparty was created by bitcoiners who witnessed the Mastercoin ICO (which later turned into the Omni layer) and hated it. The creators of the protocol didn't want to do a fundraiser and offer investors a token. That's not Bitcoin enough.

So instead, they asked participants to "burn" their BTC and receive XCP in exchange. What this means is that in January 2014, almost 2131 bitcoins were irreversibly sent to the address 1Counterparty XXXXXXXXXXXXXXXUWLpVr. They purposely made up an address that's hard to generate, and to which nobody has access. So in order for the entire supply of 2,648,755 XCP tokens to get created, real BTC had to get burnt.

According to the March 23rd 2014 article "Why Proof-of-Burn", the bitcoiners who created Counterparty didn't want the developers to gain an unfair advantage and they didn't want big investors to get any control over the network either. Everyone had an equal chance to burn BTC and receive XCP in exchange. Also, nobody got a first mover advantage so there would be no centralized entity to coordinate a pump and dump scheme. Everyone is just as interested in the project's success and faces the same risks.



However, this doesn't mean that the value of the XCP token is pegged to the price of BTC, or that the market cap should be equivalent with the 2131 BTC. As of December 28th 2021, 2131 BTC are worth $105 million while the entire XCP supply is only worth $32.8 million. This comparison was not even necessary to prove a point about XCP being a utility token that doesn't compete with bitcoin. It's not supposed to be a store of value, you only buy it to issue your named asset and use it for its intended purpose. Holding XCP speculatively would be foolish, as the token is not even listed on popular exchanges and the only way to acquire it is through dispensers.

Speaking of dispensers, Counterparty is a bona fide decentralized exchange. Anyone can sell assets without anyone's permission and have the BTC (or some other Counterparty token) get automatically sent to a personal wallet after each transaction is settled on the main chain.

If you want to buy 0.5 XCP with your BTC to name your brand new NFT or issue dividends to your existing NFT holders, then you go to a dispenser and search for the user offering the most advantageous deal. FreeWallet.io, possibly the best Counterparty interface available right now, lets you navigate between exchanges (open markets for various token pairs) and dispensers (vending machines where you buy/sell Counterparty tokens and NFTs for BTC).

The vanity aspect in issuing named tokens is pretty unique to Counterparty. If you look

at Raretoshi NFTs on Liquid, you're going to observe that they're named after the random cryptographic hash (for example, e9f53c1fd6f71eccbe2f3bf5523ef29d1de9fbb9a155c7682808ffcd17299728). On Ethereum, they bear the name of the contract (for example, JScrilla's PEPEGOAT spinoff Rare Pepe Wallet ReDux is called 0xb932a70A57673d89f4acfFBE830E8ed7f75Fb9e0). The major difference is that on Counterparty you buy appropriately-named assets and you can use the token name to search for any kind of transaction information on the xchain explorer.



Counterparty is basically an early version of Ethereum which got built on top of the Bitcoin blockchain as a protocol whose transactions get settled with BTC while paying fees to the Bitcoin miners. It was most likely abandoned because it scales really poorly. But in the summer of 2021, when the NFT mania was at its peak and Ethereum was dealing with ridiculously high fees, bitcoiners remembered about Counterparty and seized the low demand for Bitcoin block space to bring some old art back to life.

While some will discourage the use of Counterparty and recommend Raretoshi on Liquid or RGB Spectrum on the Lightning Network, the reality is that none of these are as secure or as decentralized as the Bitcoin blockchain. Also, none of them is guaranteed to live for as long as the base layer itself. And since there are lots of collections which exist on Bitcoin, there will be collectors to acquire an interest in them. The goal is clearly not to "scale", but to grant the highest security and longevity to assets.

Counterparty has been pronounced "dead" many times before, but it made a couple of comebacks specifically because it's built on Bitcoin and requires minimal maintenance – the assets will always exist and they're secured by a global network of miners and full nodes, so it's only the user interfaces (wallets) that need improvement from time to time. Your NFTs may cost more to create and transfer (as compared to centralized platforms like Liquid and Ethereum), but they are also safer because shutting the network is virtually impossible. Also, is it really shitcoining if you build it on top of Bitcoin and contribute to the network's security budget by paying fees with every transaction?



How to create your first Bitcoin NFT on Counterparty with Freeport

Depending on how much you care about the name of your asset, there are two ways of issuing Bitcoin NFTs on Counterparty and they have different difficulty levels. By far, the simplest way is to get the FreePort wallet by Joe Looney (available as a Chrome and Firefox browser extension), transfer a couple of transactions worth of BTC, and then follow the simple user interface to upload your jpg/gif and issue your NFT.

If you use FreePort, you'll never have to touch XCP or complicate your existence with buying from dispensers. You'll be able to mint, send, and admire the NFTs in your



collection in a very simple interface. So here are the steps involved:

1. Go to https://github.com/loon3/Freeport-extension

2. If you're using Chrome, click on the URL below the "Install from Web Store" subtitle and follow the on-screen instructions. After you're done, you will notice the Freeport logo on the top-right side of your Chrome window, right next to the address bar and to the left of the options menu.

3. If you're using Firefox, you must use web-ext command line to install the file available at https://github.com/loon3/Freeport-extension/raw/dev/packages/freeport-0.3.0-fx.xpi. This is the more complicated way and you're going to have to read the syntax for instructions such as "web-ext run". However, if escaping Google's panopticon is what you're after, then it's going to be worth it.

4. Set up a new wallet with Freeport. By default, it's going to generate a 12-word BIP39 seed and you should also set up a passphrase (I recommend using both letters and numbers) to unlock your assets. This is basically a Bitcoin wallet, so treat it as such – take care of your seed phrase, never reveal it to someone else and write it down on a piece of paper or on metal sheets.

5. Once you're set up and logged in, you will see the Freeport main menu which features three buttons: Collect, Create, and Buy/Sell. In the top-left corner you will see your Bitcoin Counterparty address, and in the top-right corner you will find an orange button which displays the Bitcoin logo – this one allows you to check your BTC balance and send arbitrary amounts. Also notice that on the bottom menu you have a "Settings" button. You can use it to change your receiving/NFT minting address (a feature that you'll never find on Ethereum because it has no UTXOs by design), view your passphrase (never take screenshots), set transaction fees manually, and reset the app to load a different wallet.

6. Go to the "Create" menu and pick "Create New Item". A menu will pop to ask you to upload a gif, jpg, or png image. After you upload it to Freeport, it actually goes to Imgur servers and gets its own URL.

7. Next up, you will have to name your asset (keep in mind that this is the token description, not the token name), set the supply (for instance, the Leftist Tears collection has a limited supply of 21 cards per edition) and decide whether or not you want the asset to become divisible (is it going to be traded in whole units or also enable fractions?). After this, you must choose between a priority fee and an economy fee – these are estimations based on the wallet's own observation of the Bitcoin transaction mempool. To set the fee manually based on your own analysis and time preference, return to "Set transaction fees manually".

8. Once you're done setting the parameters, press the "Create" button. If you have enough BTC in your wallet to pay the fee, then the OP_RETURN transaction will get broadcast across the Bitcoin network and await confirmation. After your first network confirmation, your NFT will appear in Freeport's "Collect" section. You can send it to friends who share their Bitcoin addresses with you, but the Freeport wallet is not advanced enough to let you set up dispenser to sell it. You can also receive NFTs from friends by sharing one of your addresses with them. But if you want to unlock the full potential of the Counterparty protocol, you will have to use an advanced wallet like FreeWallet.io on desktop.

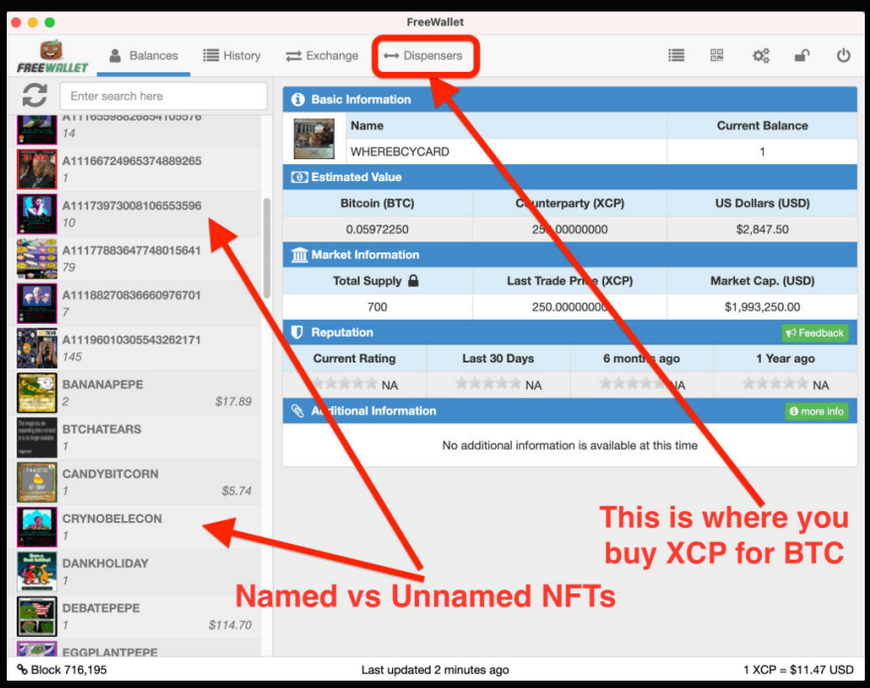
Create and manage your Bitcoin NFTs with FreeWallet.io on desktop (Mac, Windows, and Linux)

The second and more difficult way to mint and manage Bitcoin NFTs involves a desktop wallet like FreeWallet.io. If you want your new asset to bear a certain name, you are interested in accessing dispensers, and you also want to pay dividends to your NFT holders, then you must make this upgrade.

Before getting into details, you should know that the mobile versions of the FreeWallet.io software haven't been maintained in years and will definitely cause unwanted bugs. They're fine for generating a wallet and receiving NFTs, but for every other feature you should use your desktop computer or laptop (or any device that runs MacOS, Windows, or Linux).

To name your assets, you're going to need 0.5 XCP (Counterparty's native utility token). And since exchanges no longer list it, the only way to acquire some XCP is from dispensers.

A dispenser is basically a vending machine: someone locks an arbitrary amount of an asset and enables everyone who sends the right amount of bitcoin to get ownership of the asset. You see what you want to buy, choose the deal you prefer, and then proceed to make the purchase.



Dispensers are a basic form of smart contracts. But their automated nature also comes with a tradeoff: there's always a risk that the dispenser gets emptied before your transaction confirms. So if you set a low transaction fee and therefore wait a couple of days until the first confirmation, you expose yourself to the risk of dealing with a closed or emptied dispenser. There is no way for the Bitcoin transaction to get unsent and there is no mechanism in place to return your money if the entire supply of Counterparty tokens gets sold out before you got your hands on your desired digital asset.

This is why you should ideally pay for a higher transaction fee, as a way to make sure that you're among the ones who get the fair deal. You should also try to only buy from dispensers created by addresses you recognize – if you know the owner and rely on their reputation, you're more likely to get your bitcoins back if the trade doesn't take place.

I've lost about $40 worth of bitcoin trying to buy XCP to name my NFTs: the first time, the dispenser got closed before I could receive my first confirmation (textbook exit scam); the second time, someone bought all the XCP from the dispenser before my first confirmation arrived. In both cases, I had no idea with whom I was dealing and didn't know how to reach out to the owner. This is unfortunate, but a part of any decentralized, unregulated, and free digital market.

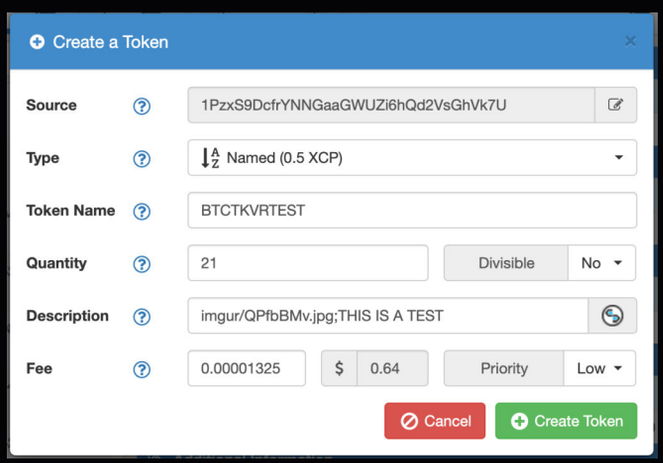
After you acquire your first XCP (remember, you need 0.5 per named NFT and you should use it ASAP as opposed to HODLing it speculatively), go to the "Actions" menu on the top right corner of the FreeWallet window and pick "Create a Token".

Here, you're going to have to select the source address and the asset type (named, subasset, or numeric). You must also input your token's name and supply (which can either be divisible or not).

Afterwards, you must set a description. And this is where you point your image file to FreeWallet. You're going to have to learn how to use proper syntax, as the structure is "imgur/imagename.jpg;DESCRIPTION OF YOUR TOKEN". Notice that you don't input the entire URL to your Imgur or YouTube asset, but use a shortened form. Also, there is no space before or after the semicolon. This is very important, as I've made this mistake before and the image was not being displayed properly and I had to send another transaction which changed the description.

There is an important discussion to be had here about Imgur and other centralized services, as they can censor and remove your image. However, you can upload it somewhere else and change your token's description with a BTC transaction. This is why they say that the token is the art – because while the Counterparty asset is immutable and can't be renamed, the description can be changed anytime at the cost of an on-chain transaction.

Last but not least, you must set a transaction fee which fits your time preference. Ideally, you should make sure it confirms within two



weeks so most nodes don't drop it from their mempool. But the low or medium priority fee recommended by mempool.space should suffice.

Notice that you don't set your fee using the classic sat/byte or bit/kb system. Instead, you choose the total amount that you want to pay as fee. Keep in mind that these OP_RETURN transactions are generally larger than the average money transfer (they occupy more block space) and take a look at the dollar cost recommendations for a more accurate approximation. By default, FreeWallet won't let you pay a fee lower than 0.00001 BTC (10 bits, or 1000 sats) per transaction, but you can change it from the settings menu.

Once you've set all these parameters, click the "Create Token" button and you're good to go. Your NFT becomes available after its corresponding OP_RETURN transaction receives its first confirmation on the Bitcoin blockchain.

What can you do next? You can send it to friends, you can set up a dispenser to sell it, and you can even burn its supply to make it even more rare. If you value your token holders, you can also pay dividends to them.



As for the token itself, you are able to change its description and visual representation whenever you please. But the name remains forever. Just like in the case of domain names, something that's taken cannot be used by somebody else – except that no periodic renewal is necessary. Once you issue it, you own the asset name. And in reality, this is what people buy.

You can also list the token on exchanges for XCP – but this feature is available on wallets such as Counterwallet (eds.counterwallet.io). The liquidity for new NFTs is really small and you're probably better off opening dispensers which let you sell your tokens for BTC. But if you want to explore this financialization rabbit hole and do more with your XCP, you're free to give it a try.



Get your first Counterparty NFT

In Pokemon games, you get to choose between Charmander, Bulbasaur, and Squirtle. Inspired by this beginner's choice, I've set up dispensers that offer affordable Counterparty NFTs for everyone who wants to understand how this works.

You can grab one of the first three cards from the Bitcoin Heads series for only 23.45 bits (2345 sats, which at the December 29th rate means slightly more than $1). And you get to choose between VLADHEAD, JOSHUAHEAD, and NOPARAHEAD.

Why didn't I give them away for free? Well, because I technically can't – unless you send me your Bitcoin Counterparty address in a private message, I make a list, and then I batch transactions to the interested recipients. Also, the goal here is to teach you about how NFTs work in a quick and affordable way. All funds that I receive will be used to create more assets from the Bitcoin Heads series and give them away for free.

So after loading up your FreeWallet with at least 0.00002354 BTC (the minimum amount to buy one card) and about 0.00001000 BTC for the transaction fee, you can choose one of the three cards to add to your collection. Sure, you can get all three of them and even get greedy and accumulate as many as you can for speculative purposes. That's totally up to you.

But while I was experimenting with dispensers, I've discovered that some Counterparty wallets use the older BTC dust limit is 54.6 bits or 5460 sats. In the meantime, Core developers have set it to 5.46 bits/546 sats. But some Counterparty wallets may use the older policy.

This means that any transaction lower than 0.00005460 BTC may not broadcast to the network. If this happens, you'll need to get at least 3 cards in one transaction. While I could close the existing dispensers and reopen them at a higher price per card to eliminate any inconvenience, I thought this lesson about how Bitcoin works would be more useful to everybody.

Anyway, the goal of these NFTs is to help as many people get their first one on Bitcoin to figure out how it works. I don't encourage speculation, but what people do with the cards after they buy them is beyond my control and Bitcoin is a permissionless network which enables free and open markets.

I've also created QR codes that get you on the dispenser page for each one of the three NFTs. If you can't scan QRs and want to find the assets on your computer, go to xchain.io (the most popular Counterparty explorer) and type VLADHEAD, JOSHUAHEAD, and/or NOPARAHEAD in the search bar. After you click on the token's name, you're going to find a dedicated tab for dispensers.

In the future, you will find more of these creations at btcheads.com and nftears.com.



What's the point of NFTs?

Counterparty NFTs are a fun way to play with Bitcoin. You get to explore the features of an early protocol which sought to bring an entire spectrum of financial assets to Bitcoin. You also figure out where all of this craze started, join Telegram channels, and make friends with the OGs who created Rare Pepes and Spells of Genesis (whom you can also hear on season 10 of the Bitcoin Takeover podcast).

But to me, it's important to prove that Bitcoin is so much more than a financial tool. It's also a distributed computer network which enables free speech. Messages that would otherwise get censored or suppressed can find their way on the Bitcoin network – at the expense of a transaction fee, of course. But the intentions are not always financial and there are plenty of ways to express oneself via Bitcoin (Counterparty NFTs being one of them).



As US First Amendment attorney Justin Wales mentioned in S5 E4 of the Bitcoin Takeover Podcast, Bitcoin is free speech and should be protected under the provisions of the US Constitution and the Bill of Rights. So if we make non-financial uses of the Bitcoin network more common, then we strengthen this thesis and win important battles against regulators that seem to only lend their ear to oversimplified narratives. Bitcoin is not a commodity, it's not a security, it's unlike anything legal systems have ever seen and can be used to exercise free speech and have fun.

Of course, these use cases are not for everyone. If you're into hoarding and HODLing BTC, then you won't "get" NFTs. And that's completely fine, not everyone aspires to collect trading cards and finds value in arbitrary tokens on the Bitcoin network that may also have a jpeg attached.

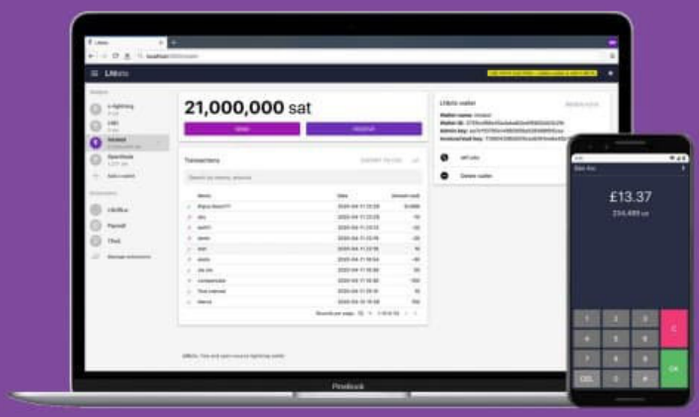
NFTs aren't an asset class, they are not "coins", and they aren't entirely like baseball cards either. They're provably rare collectibles which tell a story, mean something to the collector, or else simply enable wealthier bitcoiners to support the work of a young artist. And even though there's a market for NFT speculation, their purpose isn't always speculative – sometimes it's all about having fun in a pretty nerdy and costly way.

Not all NFTs are built equally and that's the entire point of something "non-fungible". It's unique in its own way, has some particularities that others may find appealing to the point that they'd willingly pay money, and evokes a certain feeling or memory. Some are historic, others are amusing, but all of them are reminders that the Bitcoin community is really fun and diverse.

So next time someone tells you about this cool Ethereum or Solana collection, remind them that Bitcoin did it first and does it better with Counterparty. And if you ever want to send me some of your creations, my address is 1PzxS9DcfrYNNGaaGWUZi6hQd2VsGhVk7U.

LNbits

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



Free sats!
(Scan with bitcoin lightning wallet)

Coinflip!
(Scan with bitcoin lightning wallet)

LNbits can be used as:

- Accounts system, each wallet with their own API keys
- Extendable platform via LNbits accessible extension framework
- Part of a development stack via LNbits excellent API
- Your own branded lightning wallet
- Instant wallet for LN demonstrations

LNbits can run on:

RASPI BLITZ Clightning LND
LNPay.co LNTXbot myNode
opennode spark Umbrel

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



Preview: BTCTKVR Podcast Season 10

The Bitcoin Takeover Podcast keeps on keeping it real with season 10. This time around, we have 16 guests whose topics of expertise push the boundaries of Bitcoin maximalism by presenting what everyone's favorite internet currency can do outside of the narrow "digital gold" framework. It's so blasphemous that Saifedean would choke on his steak if he listened to it!

Each one of the 12 episodes is an exploration of lesser known rabbit holes that teach us about what Bitcoin can become in the future thanks to momentarily-unpopular but seemingly-emerging use cases: from privacy-friendly DeFi on top of the Lightning Network and NFTs on the Counterparty layer to improving CoinJoins to make bitcoin transactions truly fungible, it's all there for your enjoyment.

The structure is seemingly-chaotic, but oddly symmetrical and characteristically rich in critical thinking: the first four episodes are about Bitcoin's more mature approach to DeFi and NFTs, the next four are about Bitcoin privacy, the upcoming one bridges the two realms with a little bit of rational analysis of what scams are, and the grand finale consists of a hard-hitting succession of interviews with Rare Pepe scientists.

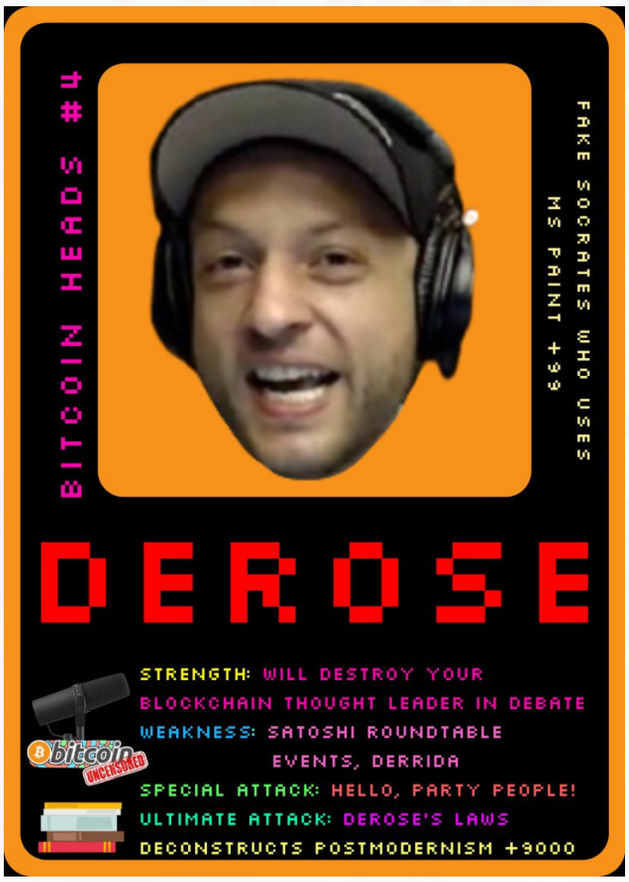
Yes, there is a lot of Counterparty shilling – because the protocol hosts the most valuable and historically-relevant NFTs, which were born back in the bear market of 2014. You know, long before ETH even existed and back in the day when NFTs were only known as "tokens". Even if you didn't pay much attention to it, 2021 has been the year when Counterparty came back from the dead to start producing the dankest tokenized memes while bringing transaction fees to Bitcoin miners and making digital artists rich enough to buy fast cars and lavish mansions.



If the first meme that comes to your mind after reading the above is Carlos Matos' prophetic "that's a scam!" moment, then rest assured: season 10 also offers you a debate on the nature of scamminess and what happens when the scams get built on Bitcoin. The special guest of this one is none other than Toximus

Decimus Meridius himself, Giacomo Zucco: the man whose 2018 speech from the Baltic Honeybadger conference did to Bitcoin maximalism what Elvis Presley has done to rock n roll.

It's important to ask ourselves to which extent we're achieving progress or if we inevitably end up scamming ourselves, as many use cases are making their way back on the most secure network which uses the hardest money. Some of the same people who call out ICOs and NFTs for being fraudulent (and even sell "toxic maximalist" hats) will launch similar products and services on Bitcoin layers and sidechains. This begs the relevant question: is the scam in the practice itself, or in the network which propagates it?



If you're a fan of sarcastic internet frogs that depict all sorts of phenomena from popular culture, then you'll most likely feel delighted by the selection of guests and topics. Furthermore, if you're concerned about Bitcoin's limited privacy and ever-extending KYC/AML policies, then you'll also find at least four episodes that will make you feel better about the progress that's being made. And if you long for the good old days when Bitcoin Uncensored was the biggest podcast around and a $100 price swing was a big deal, you'll also find a recording with a certain fake Socrates who uses MS Paint and refers to his listeners as "party people".

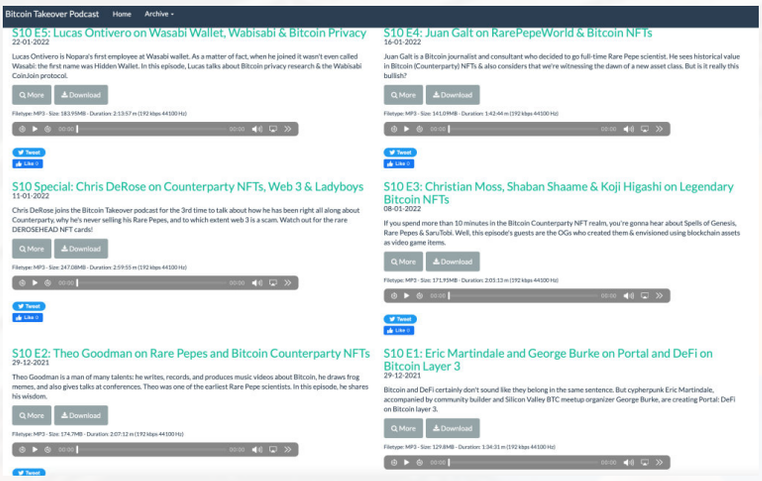
In a realm that's filled with smugness and like-mindedness, the Bitcoin Takeover podcast builds bridges between various subcultures of bitcoiners in order to paint a panoramic picture of where this magic internet money project is at and where it might be heading. So don't expect to find too much LARPing and regurgitation of popular talking points, prepare yourself to disagree, and always be ready to learn something new to expand your horizons.

The maximalist thesis to which Bitcoin Takeover adheres isn't that the project is already perfect and everything else is a scam. On the contrary, it's about maximizing Bitcoin's potential by bringing all interesting use cases to the network that's most secure and issues/transacts the world's hardest form of money.

So we should always be on the look-out for new and exciting technologies, as their more mature and refined embodiment will easily get included on top of the Lightning network or on some sidechain, statechain, or even drivechain. When we say that Bitcoin will eat up all alts, the statement shouldn't only refer to their investors and market caps – but also to their interesting technologies and use cases.

As always, the episodes are available across all streaming platforms: Spotify, Apple, Google, Breaker, PodcastIndex, Sphinx, and pretty much every service which grabs the RSS feed. However, my recommendation is that you open bitcoin-takeover.com/audio in Tor browser: this way, you'll listen for free without requiring any kind of registration and you benefit from the greatest amount of privacy. The show's sponsors are fine with not knowing who listens to the podcast, so I'm not interested in collecting any data about who you might be.

Speaking of sponsors, thanks to the appreciation that Joshua Scigala and Adam Ficsor (Nopara73) have expressed for the project, both Vaultoro and Wasabi wallet are back for another round. Nik Oraevskiy also seems to like Bitcoin Takeover's grand master plan, so Bitcoin Reserve has also joined the



party. Now you have the complete picture: a place from where you can buy bitcoin for fiat, a wallet which helps you mix those coins to get better transaction privacy, and an exchange that lets you trade with hard money (bitcoin, gold, and silver) to maximize your purchasing power during all market cycles. Hope you'll like their musical presentation during the episodes, as I wrote and recorded an original song for each one of the companies.

Last but not least, we need to address this season's graphics: for the second time in a row, I'm vandalizing a Renaissance painting by Rafael. This time around, it's The Parnassus: a fresco from the Palace of Vatican, which represents poetry. Because, you know, Rare Pepes and Spells of Genesis are also poetic to some extent.

The early 16th century fresco depicts Apollo playing the lira next to Calliope, the muse of epic poetry. But in the BTCTKVR version, it's me entertaining the crowd while being inspired by a Bitcoin-headed lady.

In Rafael's painting, you can also see 9 muses, 9 ancient poets, and 9 contemporary poets. In the BTCTKVR version, you can see (clockwise, from the bottom to the top): Karo Zagorus (@btcdragonlord), Alex Nita (@BitcoinTom21), 8-bit Britney Spears (aka "Bitney"), Ben (@coinspawner), Joshua Scigala (JScigala), Duck Avenger (@griptoshi), Vic (@vicariousdrama), Decentralized Dad (@DecentralizedD1), Lex, Pob (@kryptokatt), Lady Picasso (@art_and_nfts), Lily (@lilyxbtc), Mir (@mir_btc), Eugenia (@BitcoinLady99), Bekka (@BitcoinBekka_), Track Bender (@trackbender), Beggi Jonsson (@BeggiJonsson), Cipherhoodlum (@Cipherhoodlum), David St-Onge (@DavidStOnge), Skateboarder Pleb (@Janitols), Volodya (@Voodolodya), Nik Oraevskiy (@BTCReserveHQ), and Adam Ficsor (@Nopara73).

Though I'm the one who added the heads to the painting, I must thank Mihnea Niță and Golshid from Vaultoro for providing me early assistance with the graphics. Also, thanks to everyone who contributed with suggestions and feedback.

Without further ado, here's a presentation of each episode:

S10 E1: In this season premiere, Eric Martindale and George Burke talk about their Portal DeFi project and why they're building it as a layer 3 on top of the Lightning network. It's a really interesting conversation about how Bitcoin's second layer is capable of making Ethereum obsolete. Oh, and did I mention that George runs the world's oldest Bitcoin meetup and Eric has made significant contributions to Blockstream's Elements project?

S10 E2: If you're a fan of Rare Pepes, then you're going to love this episode. Theo Goodman is an OG frog meme "scientist" who is responsible for some of the most memorable art pieces in the entire NFT world. He created his iconic works on Bitcoin's Counterparty protocol and feels only slightly amused about the fact that these digital collectibles may just end up paying for a significant chunk of Bitcoin's security budget via on-chain transaction fees.

S10 E3: Speaking of Counterparty NFTs secured by the Bitcoin blockchain, this episode features three of the biggest names in the field: SaruTobi creator and ZEBEDEE co-founder Christian Moss (aka MandelDuck), Spells of Genesis mastermind Shaban Shaame, and Bitcoin Dungeon master Koji Higashi. It's the first four-way discussion in the history of the podcast, which highlights the origins of Bitcoin NFTs. Halfway into the episode, Christian also presents Pieter Wuille's take on how Counterparty NFTs can potentially impact Bitcoin's security.

S10 E4: When we recorded this interview, Juan Galt told me that he had put his Bitcoin consultancy gig on pause to go full-time Rare Pepe card collector and trader. This episode reflects a little bit of the euphoria that we had at the peak of 2021's bull cycle, but also provides useful information on why some NFTs have historical significance and will most likely never go out of style.



S10 E5: Lucas Ontivero is Nopara73's first employee at Wasabi wallet. He's so OG that when he initially joined the project, it was still called Hidden wallet. In this episode, he tells the story about why privacy matters to Bitcoin and how we're going to see significant advancements thanks to the development of WabiSabi. Our conversation starts out slowly, but gets more intense as it progresses. We even discuss controversial views about potentially hard forking privacy into Bitcoin.

S10 E6: My initial plan for this season was to interview only lesser known European Bitcoin-only services that do an excellent job but usually end up flying under the radar due to the American-centric media bias. So when I reached out to Nik Oraevskiy, he was keen on joining the show to talk about what it's like to lead a principled Bitcoin-only exchange in Europe. For roughly 78 minutes, we spoke about some of the most pressing issues in the Bitcoin space (including El Salvador's custody situation). After we stopped recording, Bitcoin Reserve expressed interest in sponsoring Bitcoin Takeover. Hunky dory!

S10 E7: Yuval Kogman (also known as nothingmuch) is a coder and privacy professional whom I first met in November 2021, during my visit at Wasabi wallet HQ. I quickly became intrigued by his role in optimizing the WabiSabi CoinJoin protocol and I knew I wanted to have him on the Bitcoin Takeover podcast. Yuval is so committed to making Bitcoin private that he's working on a separate experimental WabiSabi implementation which brings some extra features that he finds essential. He also gives an interesting answer to the question: "If Bitcoin was to undergo an emergency hard fork to fix a critical bug, would you support also adding Confidential Transactions?".



S10 E8: Ever used Tor? It's pretty good for online privacy, but it has some known issues and limitations. Thankfully, there's a lot of ongoing research which concerns IP address and data transmission obfuscation, and Harry Halpin finds himself at the avant-garde of the cypherpunk mission with Nym: a decentralized project which uses mixnets. Harry has been so good at pitching Nym, that he was even able to leverage geopolitics in order to convince the European Commission to finance Nym – they wouldn't want to let the USA control the internet and surveillance, right? This episode will serve as a pretty good crash course on cypherpunk privacy projects and how you can hide your identity on the internet.

S10 E9: After talking about DeFi and tokens on a Bitcoin podcast, it seemed about right to make a confession to Giacomo Zucco, the maximalist priest himself. But as a proponent of RGB Spectrum (a layer 3 project which does all the tokenization stuff from Counterparty), he was extra forgiving and provided some nuance to the debate. Giacomo even went as far as ranking token-issuing platforms according to their degree of scamminess. If you listen carefully, you can even hear about the shitcoin that first attracted Giacomo Zucco in 2013.



S10 E10: Joe Looney and Shawn Leary are the kind of people who literally memed their wealth into existence. As Rare Pepe scientists, they created one of the world's most impressive networks of green frog drawings. They were there when the project started, and in the process they created the proper infrastructure to take Pepe to the Moon: the Rare Pepe Directory, Rare Pepe Wallet, and even Free Port (the easiest way to mint Bitcoin NFTs). If you want to learn more about the significance and history of Rare Pepes, you gotta listen to Joe and Shawn.

S10 E11: When I first interviewed JScrilla in S3 E11 of the Bitcoin Takeover podcast, he was best known in the community for his "Sound Money" album. He did say something about selling the music on Counterparty, but few people listened. Two years later, his DJ Pepe cards are evaluated at $10.000 a piece and people mostly know him for the frog memes he draws – even though he is just as active with his music. In this episode, we talk about how and why he created the Fake Rare movement.

S10 Special: The plan for Chris DeRose's third appearance on the Bitcoin Takeover podcast was to allow him to host the episode. But when the moment to record finally came, he hadn't prepared any topics. So we backtracked from his early involvement in Counterparty (which precedes the Bitcoin Uncensored podcast), joked about how he once again was ahead of his time, and then ended up debating to which extent the NFT mania is a case of elite behavior being adopted by the lower classes to irreversibly destroy the meaning of value. As always, it's a fun but very intellectually-stimulating conversation.

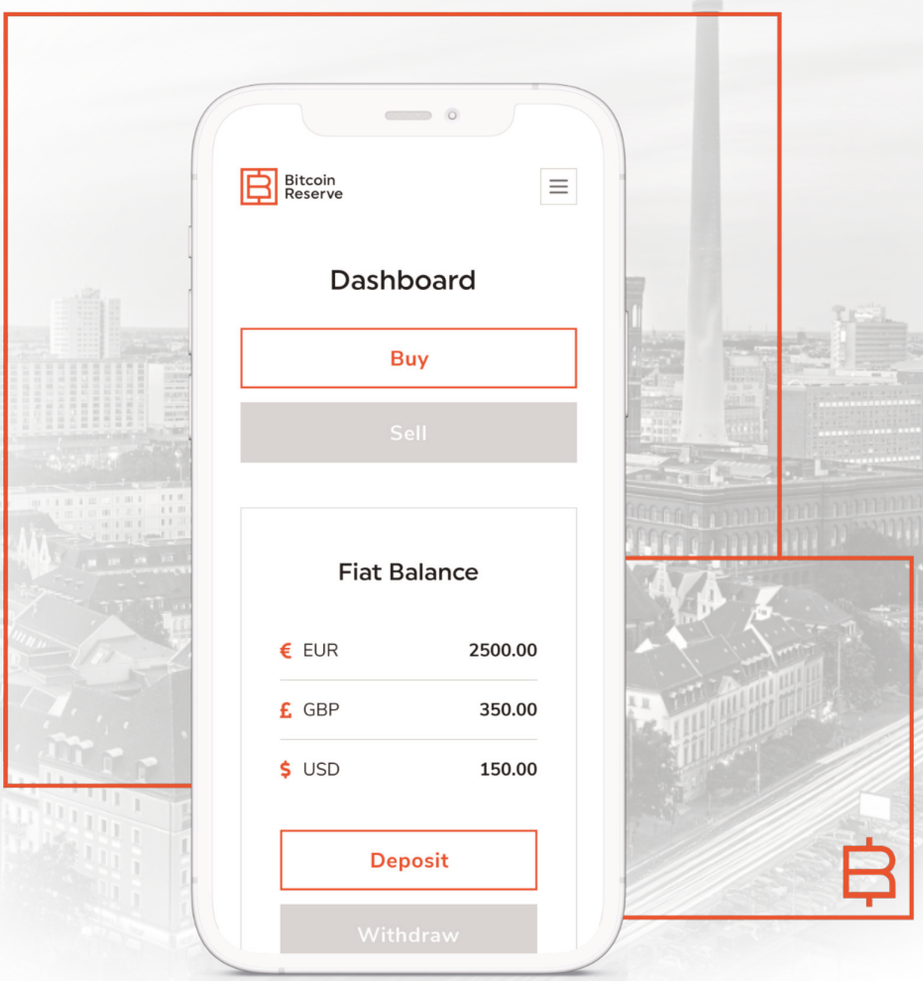
Europe's only non-custodial Bitcoin exchange where you can buy any amount

FLASH

Fast, simple and secure bitcoin buying from €10 up to €50,000. With rapid oboarding, users can get started in seconds.

CONCIERGE

White glove service for HNWIs and institutions in Europe and beyond, looking to buy over €50,000 in bitcoin.



Bitcoin Reserve

www.BitcoinReserve.com

BTCTKVR STATS

magazines:	2
magazine pages:	342
podcast episodes:	121
podcast minutes:	11562
podcast hours:	192.7
days passed:	1096
bull markets:	1
bear markets:	1
lambos bought:	0
bitcoins lost:	all of it