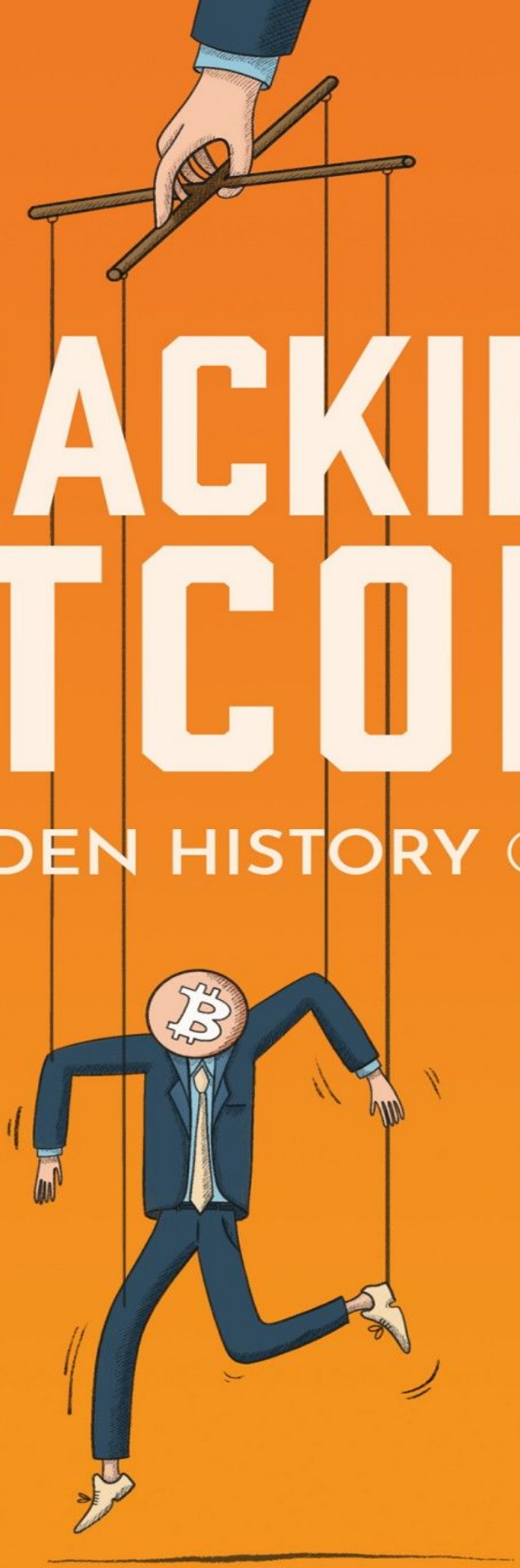
HIJACKING BITCOIN

THE HIDDEN HISTORY OF BTC



ROGER VER WITH STEVE PATTERSON

Hijacking Bitcoin

HIJACKING BITCOIN

THE **HIDDEN HISTORY** OF BTC

ROGER VER WITH STEVE PATTERSON

Published by Roger Ver

Rogerver.com

Co-written with Steve Patterson

Steve-patterson.com

ISBN 9798989492442 (Hardcover)

ISBN 9798989492435 (Paperback)

ISBN 9798989492428 (ePub)

ISBN 9798989492459 (Audiobook)

Cover design by Felix Diaz De Escauriaza

Contents

Foreword

By Jeffrey Tucker

The story you will read here is of tragedy, the chronicle of an emancipationist monetary technology subverted to other ends. It's a painful read, to be sure, and the first time this story has been told with this much detail and sophistication. We had the chance to free the world. That chance was missed, likely hijacked and subverted.

Those of us who watched Bitcoin from the earliest days saw with fascination how it gained traction and seemed to offer a viable alternative path for the future of money. At long last, after thousands of years of government corruption of money, we finally had a technology that was untouchable, sound, stable, democratic, incorruptible, and a fulfillment of the vision of the great champions of freedom from all history. At last, money could be liberated from state control and thus achieve economic rather than political goals—prosperity for everyone versus war, inflation, and state expansion.

That was the vision in any case. Alas, it did not happen. Bitcoin adoption is lower today than it was five years ago. It is not on a trajectory of final victory but on a different path to gradually increase in price for its earlier adopters. In short, the technology was betrayed by small changes that hardly anyone understood at the time.

I certainly did not. I had been playing with Bitcoin for a few years and was mainly astounded at the speed of settlement, the low cost of transactions, and the ability for anyone without a bank to send or receive it without financial mediation. That's a miracle about which I wrote rhapsodically at the time. I held a CryptoCurrency Conference in Atlanta, Georgia, in October 2013 that focused on the intellectual and technical side of things. It was among the first national conferences on the topic, but even at this event, I noticed two sides coalescing: those who believed in monetary competition and those whose sole commitment was to one protocol.

My first clue that something had gone wrong came two years later, when for the first time I saw that the network had been seriously clogged. Transaction fees soared, settlement slowed to a crawl, and vast numbers of on-ramps and off-ramps were closing due to high compliance costs. I did not understand. I reached out to a number of experts who explained to me about a quiet civil war that had developed within the crypto world. The so-called "maximalists" had turned against widespread adoption. They liked the high fees. They did not mind the slow settlements. And many were involving themselves in the dwindling number of crypto exchanges that were still in operation thanks to a government crackdown.

At the same time, new technologies were becoming available that vastly improved the efficiency and availability of exchange in fiat dollars. They included Venmo, Zelle, CashApp, FB payments, and many others besides, in addition to smartphone attachments and iPads that enabled any merchant of any size to process credit cards. These technologies were completely different from Bitcoin because they were permission-based and mediated by financial companies. But to users, they seemed great and their presence in the marketplace crowded out the use case of Bitcoin at the very time that my beloved technology had become an unrecognizable version of itself.

The forking of Bitcoin into Bitcoin Cash occurred two years later, in 2017, and it was accompanied by great cries and screams as if something horrible was happening. In fact, all that was happening was a mere restoration of the original vision of the founder Satoshi Nakamoto. He believed with the monetary historians of the past that the key to turning any commodity into widespread money was adoption and use. It's impossible to even imagine conditions under which any commodity could take on the form of money without a viable and marketable use case. Bitcoin Cash was an attempt to restore that.

The time to ramp up adoption of this new technology was 2013-2016, but that moment was squeezed in two directions: the deliberate throttling of the ability of the technology to scale and the push of new payment systems to crowd out the use case. As this book demonstrates, by late 2013, Bitcoin had already been targeted for capture. By the time Bitcoin Cash came to the rescue, the network had changed its entire focus from using to holding what

we have and building second-layer technologies to deal with the scaling issues. Here we are in 2024 with an industry struggling to find its way within a niche while the dreams of a “to-the-moon” price are fading into memory.

This is the book that had to be written. It is a story of a missed opportunity to change the world, a tragic tale of subversion and betrayal. But it is also a hopeful story of efforts we can make to ensure that the hijacking of Bitcoin is not the final chapter. There is still the chance for this great innovation to liberate the world but the path from here to there turns out to be more circuitous than any of us ever imagined.

Roger Ver does not blow his own trumpet in this book, but he truly is a hero of this saga, not only deeply knowledgeable of the technologies but also a man who has clung to an emancipatory vision of Bitcoin from the earliest days through the present. I share his commitment to the idea of peer-to-peer currency for the masses, alongside a competitive marketplace for free-enterprise monies. This is a hugely important documentary history, and the polemic alone will challenge anyone who believes himself to be on the other side. Regardless, this book had to exist, however painful. It’s a gift to the world.

Jeffrey Tucker

President, Brownstone Institute

Introduction

The past thirteen years of my life have been spent trying to make Bitcoin and other cryptocurrencies the money of the future. The technology has the potential to make the world a radically freer and more prosperous place, and it will end up being one of the most important inventions of all time. I have spent more than a decade evangelizing about the benefits of Bitcoin, funded numerous startups within the industry, built my own businesses around it, and have seen the price increase by more than 6,500,000%. Yet, this book is not a love story, and I wish it did not have to be written. The project I got involved with in 2011 has been hijacked and changed for the worse.

Bitcoin was designed to be digital cash, usable in everyday commerce, with minimal fees and fast transactions, and it worked that way for years. But today, Bitcoin is thought to be "digital gold," not meant for everyday commerce, with high fees and slow transactions—a complete reversal of the original design. It's discussed as a "store of value," with little care for its utility as a payment system. Some people even claim that Bitcoin cannot work as a payment system, because it does not scale. These common ideas are simply untrue. The reason that Bitcoin is no longer used as digital cash has nothing to do with the underlying technology. It's because a group of software developers took over the project, decided to change its design, and intentionally limited its functionality—whether due to incompetence, sabotage, or a mixture of both. The takeover happened from roughly 2014-2017, and it ultimately resulted in the network splitting in two and the cryptocurrency industry fracturing into a thousand pieces. The original design still exists and remains extremely promising, but it no longer trades under the ticker symbol "BTC."

As I travel and continue to speak around the world about the benefits of cryptocurrency, it has become apparent that hardly anybody knows the story of Bitcoin's takeover. The main discussion platforms online have been heavily censored for years and carefully control the information that people receive. Bitcoin Maximalists—the loud voices that insist all projects other than BTC are scams—also help to discourage critical investigation, mostly

by bullying people on social media. Anybody that questions their narrative is instantly mocked, and this has proven to be an effective tactic for silencing dissent. Since nobody speaks up, newcomers have almost no chance of hearing about Bitcoin's real history and design. This book provides that information.

Hijacking Bitcoin has three parts. Part I is a detailed look at the original design of Bitcoin and the radical changes made to it. Part II is the history of the takeover, including the many dirty tactics employed like censorship, propaganda, and attacks on businesses that dissented from the narrative. The final section, Part III, is about rescuing Bitcoin from its captors and providing a realistic vision for the future.

Getting involved early with a breakthrough technology is a dream of many entrepreneurs, and my journey has been filled with exciting moments and interesting stories. But this book is not a memoir. Its purpose is to educate. For the last few years, I have been sharing this information in private conversations, public speeches, and online videos, but now it's time to put it all in writing. The goal is to help people understand Bitcoin's current situation and how it got there. To the entrepreneurs and investors who are interested in bringing fast, cheap, reliable, and inflation-proof digital cash to the world: we can still do this. We just have to work together on the right project.

Part I:

An Ingenious Design

1

Altered Vision

The cryptocurrency revolution began when Bitcoin was released to the world in 2009. Over the past decade, Bitcoin has gone from being completely obscure to being an international sensation that spawned a new industry. Entrepreneurs are trying to use the technology to solve a wide range of problems, from simply improving online payments to rebuilding the global financial system. Between all the news coverage, Wall Street speculation, and online enthusiasm, cryptocurrencies are probably the most hyped technology of the twenty-first century. Yet, despite the hype and astronomical price increases, their real-world impact has been minor. In the future, they might serve as the foundation of a new financial system or become an alternative to government-issued money, but to date, the primary use of cryptocurrency has been financial speculation.

The situation reminds me of when I was living in Silicon Valley during the internet boom of the 1990s. Internet technology was predicted to revolutionize commerce around the world, which meant that any "internet company" with no infrastructure or plausible business plan could raise millions just by owning a premium domain name. The speculation was mind-boggling. Many of the biggest startups went bankrupt only a few years after going public. Yet, despite the infamous burst of the dotcom bubble, the world has indeed been revolutionized by the internet. The technology has become essential infrastructure for the global economy and an indispensable part of modern life, though its maturation process took longer than people had hoped. Cryptocurrencies are following a similar path. Despite the wild speculation and relative lack of usage, they look like an inevitable part of our future.

Any story of modern cryptocurrency must begin with Bitcoin, the grandfather of them all. My own life has been wrapped up with Bitcoin since discovering it in 2010. My first coins were purchased in early 2011 for less than $1 each. A few months later, the price spiked to $30, only to crash back to $2 by November that same year—the first of many extreme price fluctuations that have since become common for the industry. Rapid

price appreciation, followed by a crash of 80% or more, is a regular cycle that has been repeated several times in Bitcoin's short history. The volatility makes for good news headlines, since the general public is almost exclusively focused on price. But for me, Bitcoin has always been more than just a financial investment. It's a magnificent tool for increasing the amount of economic freedom in the world.

The early Bitcoin community was filled with eccentric people and unusual ideas. Like many others, I was particularly drawn to Bitcoin because of my political and philosophical ideals. I greatly value human freedom and believe individuals should have maximum control over their own lives. The more power any government has, the less power individuals have, and I knew from my study of economics and history that central banks' control over the money supply gives an enormous amount of power to governments. So, Bitcoin was naturally appealing to me, as it was designed to operate without a central, governing authority. People do not have to ask permission to use it. There's no "Bitcoin Central Bank" that controls the supply of coins, and the technology does not recognize international borders. Few things have more potential for increasing global freedom than fast, cheap, permissionless, inflation-proof digital money.

Futurism is the other primary philosophical motivation behind my enthusiasm for cryptocurrencies. Thinkers like Ray Kurzweil paint a compelling picture of the future in which humans radically improve their well-being through advanced technology. We might be able to greatly reduce the amount of suffering in the world, and even extend our own lifespans to enjoy more time on Earth, when we reach sufficient economic and technological development. In order to get there, it will require enough wealth and prosperity to continue financing research, as well as ongoing freedom to innovate. In my mind, Bitcoin gets us one step closer to a more technologically sophisticated future in which everybody's life is improved.

These beliefs were not unique in the early Bitcoin community. Online forums and message boards were the central hubs for discussion, and if you visited them, you would see endless discussions about Bitcoin being much more than a simple payment system or speculative investment. We all knew that the technology could be used to dramatically improve the world. Brian

Armstrong, the co-founder and CEO of Coinbase, captured this sentiment perfectly in an article entitled “How Digital Currency Will Change the World” by stating:

Digital currency may be the most effective way the world has ever seen to increase economic freedom. If this happens, the implications are profound. It could lift many countries out of poverty, improve the lives of billions of people, and accelerate the pace of innovation in the world… reduce wars, make the poorest 10% better off, overthrow corrupt governments, and raise happiness.[1]

My enthusiasm quickly turned into evangelism, and I was nicknamed “Bitcoin Jesus” for preaching the Gospel of Bitcoin to anybody who would listen—and to plenty of people who wouldn’t. My friends and family, the media, and businesses that I patronized would hear the same message: Bitcoin is fast, cheap, reliable money that was designed for the internet. With it, you can send any amount of money anywhere in the world instantly for around a single US cent or less. In fact, in the earliest days, most Bitcoin transactions were completely free and only included a small fee if your coins had recently been moved. People could immediately see the value in such a technology, regardless of their personal ideology. One of the best marketing pitches was to simply have people use Bitcoin, since the user experience was fantastic compared to other payment systems. I would get people to download a wallet onto their phones to send them a few dollars. After experiencing their first Bitcoin transaction, it would only take a few seconds to hear the inevitable “Wow!” after being dazzled by their first impression.

By 2015, Bitcoin had built up so much momentum that it looked unstoppable. Prominent companies, from Microsoft to Expedia, were starting to accept it for payment, and the young industry was growing exponentially. The successes started to pile up. Venture capital increased. Media coverage became positive. Bitcoin was on a direct flight to the moon.

Failure to Launch

Fast forward to today. Despite being a household name, Bitcoin has not yet taken over the world. In fact, there's a grim truth beyond the headlines and price charts: the actual usage of Bitcoin has declined since 2018, and many businesses have dropped it entirely as a payment option. On multiple occasions, the network has buckled and become almost unusable with huge transaction fees and unreliable payments. In times of network congestion, the average fee can reach more than $50 and transactions can take days or even weeks to process. And perhaps worst of all, these failures have pushed the industry to adopt so-called "custodial wallets," which are simply customer accounts managed by a company, similar to a regular bank account.

The entire purpose of Bitcoin is undermined by the mass usage of custodial wallets, because total control is given to a third party that can censor, track, and even confiscate coins—no different than an account balance at Venmo. Fraud also becomes easier. For example, when the FTX exchange collapsed in 2022, more than a billion dollars of customer funds instantly vanished. This was only possible because FTX ultimately controlled their customers' money. The integration of Bitcoin into Paypal is another prominent example of users being onboarded to custodial wallets instead of having full control over their funds. If regular people are all using custodial wallets, Bitcoin will have lost a key property that made it so revolutionary.

High fees, unreliable payments, custodial wallets, and less usage in commerce—by other metrics than price, Bitcoin has not landed on the moon; it hasn't even left orbit. So what happened?

The Official Story

The conventional explanation for these negative trends is that Bitcoin fell victim to its own success. As it gained in popularity, the network ran out of capacity. Inherent technological limitations caused the fees to skyrocket, payments to become unreliable, merchants to leave, and the industry to move towards custodial wallets. In response to these problems, the narrative surrounding Bitcoin has shifted towards being "digital gold" and a "store of value" instead of a digital currency. If Bitcoin is not supposed to be used in everyday commerce, then it does not matter whether it functions as a payment system.

Despite how often these ideas are repeated in the press and among popular commentators, they are completely incorrect. The real story is much more dramatic. Bitcoin was built for massive scale and did not run into inherent technological limitations. Instead, the project was taken over by a small group of software developers who redesigned the whole system. They intentionally limited its capacity and functionality, and they openly advocate for high fees and a backlog of transactions—the antithesis of the original design.

When I tell people about this today, they often think I'm exaggerating, but the developers say it themselves. For example, the influential Bitcoin developer Greg Maxwell has said quite plainly, "I don't think that transaction fees mattering is a failing-- it's success!"[2] Mark Friedenbach, another Bitcoin developer, stated that "Slow confirmation, high fees will be the norm in any safe outcome."[3] When the network nearly ground to a halt in December 2017, and the average transaction fee reached more than $50, they celebrated by "pulling out the champagne"[4] and were pleased to see the congestion, claiming that a consistent backlog was "the required criteria for stability."[5]

If you told me in 2012 that Bitcoin developers would eventually want high fees and slow transactions, I would not have believed you, nor would any of the early entrepreneurs that helped create the industry. The ideas are too bizarre. Expensive transactions and network congestion are not necessary for safety or stability. The opposite is true: high fees and unreliable payments push people into using custodial wallets, which undermines the whole purpose of Bitcoin in the first place.

On its current course, Bitcoin will not empower the average person. The project has stagnated over the past few years not because of technological failures, but because of human failures. Specifically, bad leadership and a flawed governance model. When I learned about Bitcoin back in 2010, it was so exciting that I almost felt a moral obligation to tell people about it and share the good news. Today, given the changes that have been made, I feel a moral obligation to tell people the bad news: Bitcoin was hijacked and no longer resembles the original project that inspired myself and countless others. But its story isn't over yet.

The Workaround

The original, scalable design of Bitcoin still exists, but it's not traded on cryptocurrency exchanges under the ticker symbol BTC. It's called "Bitcoin Cash" and is traded as BCH. For years, the industry was thwarted by the BTC developers, until 2017, when a new network was created to preserve the original vision of Bitcoin as digital cash with low fees, fast transactions, and without the need for custodial wallets. The BCH network is far less well-known than BTC, but it has already scaled its throughput capacity to more than thirty times BTC's, with plans to scale exponentially into the future.

The events leading to the creation of Bitcoin Cash were contentious and have since been named the "Bitcoin Civil War," and to this day, the BTC and BCH communities are often hostile towards each other. If you only follow Bitcoin casually, you will have exclusively heard the BTC side of the story; this book tells the other side, and it is filled with historical details, excerpts, and quotes from other early adopters who shared the same vision for Bitcoin as digital cash.

To distinguish between the different networks and groups, it's helpful to establish clear terminology. The BTC network is often referred to as "Bitcoin Core," while the BCH network is often referred to as "Bitcoin Cash." So, those are the terms used hereafter. The word "Bitcoin" by itself refers to the underlying technology that is used on both networks. Both Bitcoin Core and Bitcoin Cash use Bitcoin technology and share the exact same transaction history until their split in August 2017. The Bitcoin Core developers decided to pivot from the original design, while the Bitcoin Cash developers have stuck with it.

Avoiding Hazards

If this technology really is revolutionary, then it threatens the power of existing financial and political establishments. But on the current trajectory, if nothing changes, those institutions will assimilate cryptocurrencies and neutralize them. If Bitcoin is going to make the world a freer place, our window of opportunity is closing. The industry is approaching two failure scenarios. The first would be total capture by existing financial and

regulatory systems. Mass adoption of custodial wallets makes this possible, as transactions are easily tracked and controlled, and governments can force companies into compliance without difficulty.

The other failure scenario would be people simply giving up and abandoning the vision of inflation-proof digital cash altogether. I have seen many talented minds and competent businessmen prematurely conclude that Bitcoin cannot scale because of Bitcoin Core's failure. This disillusionment can be avoided if people realize that the original Bitcoin technology still exists, works well, and can scale to handle global adoption. Bitcoin Core simply pivoted from this design. Before losing faith in blockchain technology, entrepreneurs and developers need to first experience the original version. I am constantly trying out new cryptocurrencies, and Bitcoin Cash still provides me with one of the best user experiences after all these years.

Since Bitcoin stands at the intersection of international finance, political power, and disruptive technology, its story has to be one of the most dramatic of all industries, with enough material for several Hollywood productions. This book is just one piece of that story—the takeover of the development of Bitcoin and subsequent split into Bitcoin Cash, from the perspective of a businessman that has arguably used the technology in commerce more than anybody else in the world.

2

Bitcoin Basics

The world is inundated with bad information about Bitcoin, largely due to the power of social media. Honest investigation is discouraged online, and if a curious mind asks the wrong questions or expresses the wrong opinions, he can expect a wave of angry commenters attacking his intelligence, his reputation, or even his business. Bitcoin Maximalists—those who assert that BTC is the only legitimate cryptocurrency—are notorious for employing this tactic. They will blast out a list of reasons why any alternative project like BCH is a scam, insist the debate has already been settled, and question the sanity of anybody who disagrees. Most people do not have the time to investigate these claims, nor do they want to be targeted by online trolls, so they end up accepting the standard narrative.

To see past the narrative and truly understand the difference between Bitcoin Core and Bitcoin Cash, we must first understand how Bitcoin was originally designed. History can help us, because the creator of Bitcoin, Satoshi Nakamoto, had many public communications about his invention that explain its design. Other great minds and engineers that succeeded him, like Gavin Andresen and Mike Hearn, also explained the core ideas in a clear manner. Their writing, quoted throughout this book, is essential for anybody trying to understand Bitcoin at more than a superficial level. Before diving deeper, it's helpful to familiarize ourselves with three key concepts: the blockchain, miners, and full nodes.

The Blockchain

Bitcoin revolves around "blockchain" technology. The blockchain is simply a public ledger that keeps track of all Bitcoin balances, and it gets updated with new transactions approximately every ten minutes. These new transactions are packaged into "blocks" which are then "chained" together, one after the other, forming the "blockchain." The blockchain is unique because it's not maintained by a centralized authority. There's no single agency that processes all the transactions or determines the entries of the

ledger. Instead, it's maintained and updated by a decentralized network of computers around the world, giving it no central point of control or failure.

Blocks themselves are central to understanding the different philosophies in Bitcoin, which can roughly be split into two camps: "big-blockers" and "small-blockers." Big-blockers, as the name implies, want big blocks. The larger the blocks, the larger the transaction throughput of the network, and the more resources it takes to process each block. Small-blockers want to keep blocks small enough so that anybody can process them. We will cover this difference in more detail later.

Miners

Not just anybody can add blocks to the blockchain. This job is exclusive to miners. Miners update the ledger by bundling transactions together into a block and then adding a special proof. This proof is a solution to a math puzzle which is so difficult, it takes substantial computer power to figure out. All over the world, there are warehouses filled with specialized machines dedicated to solving these puzzles. Each one of these machines requires electricity, which means it costs money to be a Bitcoin miner!

Miners are financially rewarded for their services with two mechanisms: transaction fees and a block reward. Transaction fees are simply what users pay to get their transactions added to a block. The block reward is how new Bitcoins are minted. Every time a miner adds a block to the chain, he's given a small number of new Bitcoins. This reward is cut in half roughly every four years. In the earliest days, miners received 50 new bitcoins per block, but at the time of writing, the block reward is down to 6.25 coins. Eventually, the reward will be negligible, which will leave transaction fees as the only source of revenue for miners.

Big-blockers see miners as performing an essential service in the Bitcoin industry by protecting the network from attacks, maintaining the ledger, and processing all transactions. Miners frequently invest millions or even tens of millions of dollars to upgrade to more powerful equipment. In 2018, the company Bitmain announced plans to build the largest mining facility in the world in Texas and estimated their total investment to be more than $500 million.[1] Bitcoin mining has high investment and maintenance costs.

Because of this, most big-blockers think that miners should have the greatest say in the development of Bitcoin. Depending on the success of the coin they are mining, their capital investment could be entirely lost or generate a substantial return. So, they have a strong incentive to ensure Bitcoin remains useful and valuable.

Small-blockers tend to have a more skeptical or even hostile view towards miners. Because miners are the only ones that can add blocks to the network, they have substantial power and could become a systemic threat if mining becomes too centralized. If only a few major players dominate the market, that could make Bitcoin itself too centralized. Large mining facilities also introduce a political risk into the system. If governments decide to attack, regulate, or control the biggest miners, they might be able to disrupt or control Bitcoin. The role of miners is a central disagreement that led to the Bitcoin Cash split.

Full Nodes

Fortunately, if you want to use Bitcoin, you don't have to be a miner or run heavy-duty software. Regular users can access the network in easier ways. Satoshi Nakamoto described a method for Simplified Payment Verification (SPV) that allows users to send, receive, and validate their own transactions with minimal effort. For most of Bitcoin's history, the majority of wallets used either SPV or other similar methods for accessing the blockchain. This trend is reversing in BTC due to the proliferation of custodial wallets, but it remains the norm in BCH.

There's another option for accessing the Bitcoin network that takes more effort. Some users run "full node" software which downloads the entire blockchain and validates every single transaction that has ever taken place. The entire BTC blockchain contains around 800 million transactions and is currently around 450 gigabytes in size. For users running full node software for the first time, it can take several hours to sync up with the rest of the network. Furthermore, if a full node ever disconnects from the network, they have to download and validate all the latest blocks in order to use Bitcoin again. That's why SPV was such an important invention. It takes virtually no time or effort to use, and yet it still offers excellent security.

SPV allows you to validate your own transactions, while full nodes allow you to validate all transactions on the blockchain.

Arguably the biggest difference between the big-block and small-block philosophies is about the role of full nodes. Big-blockers think that the vast majority of activity on the network should be between miners and lightweight wallets that use SPV or similar technology. They think full nodes are only useful in special cases where you need to validate many people's transactions in a short period of time, for example if you're running a cryptocurrency exchange or payment processor. Since the network gives no financial compensation to full node operators—and since most people have no need to validate strangers' transactions—regular users do not have an incentive to run such heavy-duty software. Satoshi was unequivocally a big-blocker, and as he put it, "The design supports letting users just be users."[2]

Small-blockers, by contrast, think that full nodes are essential to the network. They think that users should run their own nodes, which is why having small blocks is essential, since the cost of running a node increases with the size of the blocks. In fact, the primary reason that small-blockers have claimed Bitcoin cannot scale is because big blocks are more expensive for node operators. Instead of concluding that regular users are not supposed to run full nodes, they concluded that Bitcoin cannot scale. From my perspective, this is one of the greatest confusions about Bitcoin and it will be analyzed in depth.

The Fundamental Five

A great deal has been made of Satoshi Nakamoto's original vision for Bitcoin. Supporters of it, like myself and other early adopters, thought that he designed a brilliant system that proved it worked in the real world. Because of this success, we did not see any reason to fundamentally change it. Critics of the original vision thought Satoshi was wrong in some key areas and wanted to change the protocol accordingly. The Bitcoin Core developers were such critics, despite their eventual governance over the project.

Bitcoin Maximalists often compare adherence to the original vision to a kind of blind faith, where any deviations from the founding ideas are not tolerated. But this is a weak criticism. The desire to stick with Satoshi's design is far from dogmatic. Bitcoin is a complex system, with many moving parts. In addition to the software and computer network, it's an entire economic system that requires an economic analysis in order to understand. When you look at the software components in addition to the economic components, it becomes clear that Bitcoin is finely-tuned and should not be tampered with lightly.

Instead of scaling Bitcoin by increasing the size of the blocks to allow for more transaction throughput, the Core developers decided that Bitcoin should scale by using multiple layers instead. According to them, the first layer should be composed of "on-chain" transactions, on which additional layers are built. These additional layers would be "off-chain," meaning the transactions would not be recorded on the blockchain, thereby avoiding the need to scale the base layer. The much-hyped "Lightning Network" is one of these second layers, but it has a host of fundamental issues that are discussed in detail in Chapter 9. One substantial problem is that it requires on-chain transactions in order to use. To simply connect to the Lightning Network, you have to make at least one transaction on the base layer, which might cost a hundred dollars if BTC is experiencing high usage. Despite this being a critical flaw, there is no proposed solution.

Bitcoin Core is betting everything on the viability of these additional layers. They inverted the original system to make base layer transactions slow and expensive, but they have not produced a satisfactory alternative that provides simple, reliable payments. The current version of the Lightning Network is neither reliable nor secure (which is why the most popular Lightning wallets are now custodial). So, any hope for BTC being the freedom-enhancing money of the future relies entirely on technology that has not yet been created.

At a conference in July 2021, Elon Musk also noted that BTC's transaction throughput could be a problem and defended the idea of scaling a cryptocurrency by expanding the size of its base layer:

There's some merit to considering something that has higher max transaction rates and lower transaction costs, and seeing how far you can take a single-layer network… I think you can probably take that further than people realize.[3]

Musk is a prominent supporter of BTC, but his engineering intuitions are aligned with the BCH philosophy. Scaling the base layer is the right idea and was always part of the original design.

Satoshi was not perfect, but as the upcoming chapters will explain, his ideas are compelling, well thought out, and deserve an honest examination. His design does not require the complexity of additional layers, though it is still compatible with them. Instead of blindly following any individual, group of developers, or ticker symbol, try to judge the ideas on their own merits. Listen to how Satoshi designed Bitcoin, listen to the Core developers, and make up your own mind.

The differences between the original design and Bitcoin Core's new design can be captured with five critical ideas:

1. Bitcoin was designed to be digital cash used to make payments over the internet.
2. Bitcoin was designed to have extremely low transaction fees.
3. Bitcoin was designed to scale with blocksize increases.
4. Bitcoin was not designed for the average user to run his own node.
5. Bitcoin's economic design is as important as its software design.

Each of these points is central to the original vision for Bitcoin that was shared by Satoshi and other early pioneers. But today, the prevailing narrative disagrees with almost every point. If you listen to commentators from network television to popular podcasts, you might believe that:

1. Bitcoin was designed to be a store of value, even if it doesn't work as a medium of exchange.
2. Bitcoin is supposed to have high transaction fees.
3. Bitcoin does not scale with blocksize increases.
4. Bitcoin's security depends on regular users running their own nodes.

5. Bitcoin's economic design was broken and needed to be fixed by software engineers.

All of these are incorrect. Even if you like the changes that Bitcoin Core has made, the historical record is clear that they radically differ from the original design. The following chapters will examine each of these claims in detail.

3

Digital Cash for Payments

The internet is the most powerful tool for information distribution that the world has ever seen. People can learn just about anything by using Google, Youtube, Wikipedia, and even social media. However, these channels can easily become polluted or even co-opted. For example, if you mention cryptocurrency on Twitter, you are guaranteed to hear from a hoard of random Twitter users pitching their preferred coin and trashing all others. If you look closely, many of these accounts have fake profile pictures, no followers, and seem to spend all day tweeting about their favorite crypto projects. Individually, they might seem irrelevant and powerless, but when there are hundreds or thousands of accounts doing this, it can sway public opinion. I have seen this firsthand. The cryptocurrency industry has been permanently affected by social media campaigns and online misinformation. These techniques have a particularly ugly history in Bitcoin.

While these tactics are immoral, they are undoubtedly effective. It is a testament to the effectiveness of the Bitcoin Core narrative that there's now disagreement and confusion about the very purpose of Bitcoin. Instead of being recognized as a payment system for everyday commerce, Bitcoin is almost exclusively spoken about as a "store of value" whose utility does not depend on it being used as cash. You can hear this claim repeated everywhere, even by academics. The description for the popular book The Bitcoin Standard reads:

Bitcoin's real competitive edge might just be as a store of value and network for final settlement of large payments—a digital form of gold with a built-in settlement infrastructure.[1]

I used to like the digital gold analogy until it got turned on its head. We used to say that Bitcoin is like digital gold because it's a currency that cannot be inflated by a central bank, and since it's digital, it can be sent anywhere in the world instantly at almost no cost. But that is not what people mean by "digital gold" anymore. Instead, they invoke that analogy to make the opposite point—that Bitcoin is like gold because it's expensive to transact

and not commonly used as a medium of exchange. Instead of being related to gold's monetary strengths, Bitcoin gets related to gold's monetary weaknesses.

Some Bitcoin Core proponents have taken this argument even further. Instead of merely claiming that Bitcoin makes a better store of value than it does a payment system, they claim that Bitcoin was intentionally designed as a store of value and not as a medium of exchange. According to Dan Held, the Director of Business Development at Kraken:

[T]hose pushing the 'Bitcoin was first made for payments' narrative insist on cherry-picking sentences from the white paper and forum posts to champion their perspective… Bitcoin was purpose-built to first be a Store of Value.2

While this brazen claim might gain social media likes and praise from cryptocurrency commentators, it does not stand up well against the facts. The historical record is clear that Bitcoin was designed for everyday payments.

In Satoshi's Words

What evidence do we have that Bitcoin was purpose-built to be a payment system? Well, everything that its creator wrote on the subject. In addition to the seminal whitepaper that introduced Bitcoin to the world, we have hundreds of online forum posts and more than fifty public email correspondences from Satoshi. They paint a clear vision for the technology. Let's start with the whitepaper, released in 2008, which presented and defined Bitcoin for the very first time. I recommend reading the entire whitepaper online. It is well-written, and many of the key concepts can be understood without technical knowledge. We will analyze the first few sections, starting with the title:

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi could have called it an "electronic store of value" if that's what he intended, but instead he called it an electronic cash system. Next, the very first sentence of the abstract reads:

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.[3]

"Online payments" are literally mentioned in the first sentence of the paper introducing Bitcoin to the world. After the abstract, the introduction begins:

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model…

In the first two sentences of the introduction, Satoshi mentions "commerce on the internet," "electronic payments," and "transactions." He continues:

Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for nonreversible services. With the possibility of reversal, the need for trust spreads... These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

In other words, existing online payment methods have high transaction costs due to the inherent trust required in the system. Credit cards, PayPal, and so forth, all depend on companies with expensive dispute resolution mechanisms. These costs make "small casual transactions" effectively impossible over the internet. By contrast, physical cash payments do not require trust in third parties, but there is no way to use physical cash online. Enter Bitcoin:

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud,

and routine escrow mechanisms could easily be implemented to protect buyers.

In other words, Bitcoin is like cash because the transacting parties can exchange directly with each other without going through a middleman. In the first few paragraphs, the whitepaper makes it clear that Bitcoin is about "commerce," "transactions," "payments," "merchants," "buyers," and "sellers." There is no mention of a "store of value" in the entire whitepaper.

Even in Satoshi's emails and forum posts, the concept of Bitcoin as a store of value can only be inferred a handful of times. Sam Patterson, co-founder of the cryptocurrency company OB1, wrote a popular article in which he catalogued every single mention of Bitcoin as a payment system versus a store of value. He concluded:

After reviewing all of Satoshi's writings, I can confidently state that Bitcoin was not purpose-built to first be a store of value. It was built for payments… Satoshi mentioned payments more than four times more frequently than store of value…

This evidence might be sufficient for you to disregard the claim "Bitcoin was purpose-built to first be a Store of Value." I can't see anyone honestly looking at Satoshi's words and really believing he didn't build this for payments.[4]

It's not just the whitepaper that makes it clear Bitcoin is about payments. Satoshi was equally clear in the online forums:

Bitcoin is practical for smaller transactions than are practical with existing payment methods. Small enough to include what you might call the top of the micropayment range.[5]

Micropayments

Just how small are "micropayments?" There is no universal definition, but in this context, they are transactions less than a single US dollar. Gavin Andresen, the developer that Satoshi chose as his successor, shared similar thoughts:

I still think the bitcoin network is the wrong solution for sub-US-penny payments. But I see no reason why it can't continue to work well for small-amount (between a US $1 and $0.01) payments.[6]

Bitcoin used to be considered practical for transactions in the range of a couple of cents to a couple of dollars. But since the transaction fees have risen, it's often impossible to send a transaction that small, since the fees end up larger than the actual balance being sent. If a Bitcoin address doesn't have enough funds to pay the miner fee, it effectively can't be used. Satoshi elaborates on micropayments:

While I don't think Bitcoin is practical for smaller micropayments right now, it will eventually be as storage and bandwidth costs continue to fall. If Bitcoin catches on on a big scale, it may already be the case by that time. Another way they can become more practical is if I implement client-only mode and the number of network nodes consolidates into a smaller number of professional server farms. Whatever size micropayments you need will eventually be practical. I think in 5 or 10 years, the bandwidth and storage will seem trivial.[7]

This quote is interesting for two reasons. First, Satoshi imagines Bitcoin eventually being used for "whatever size micropayments you need," and second, he predicts the network infrastructure will be consolidated into "professional server farms," which is especially relevant to the debate about bigger blocks.

Once [Bitcoin] gets bootstrapped, there are so many applications if you could effortlessly pay a few cents to a website as easily as dropping coins in a vending machine.[8]

Satoshi wanted Bitcoin to be used for "effortlessly paying a few cents to a website." Contrast this with what Core developer Peter Todd says:

I'd be very happy to be able to wire money anywhere in the world, completely free from central control, for only $20. Equally I'll happily accept more centralized methods to transfer money when I'm just buying a chocolate bar.[9]

Satoshi's and Todd's visions are incompatible with each other, as they disagree about the acceptable fee level by more than three orders of magnitude. $20 fees destroy every use-case for Bitcoin other than high-value transfers—a kind of digital gold extremism. We do have one quote from Satoshi that directly compares Bitcoin to gold. He was responding to questions about the apparent wastefulness of consuming electricity to mine Bitcoin:

It's the same situation as gold and gold mining. The marginal cost of gold mining tends to stay near the price of gold. Gold mining is a waste, but that waste is far less than the utility of having gold available as a medium of exchange.

I think the case will be the same for Bitcoin. The utility of the exchanges made possible by Bitcoin will far exceed the cost of electricity used. Therefore, not having Bitcoin would be the net waste.[10]

Gold is used as an analogy to illustrate that its utility as a medium of exchange outweighs the costs of mining it. Ironic, in hindsight.

Snack machine purchases are also discussed in one forum post, highlighting Bitcoin's capacity for instant, small-value payments. Since instant payments are not perfectly secure, Satoshi envisioned payment processors taking on the minor risk of fraud to handle them:

I believe it'll be possible for a payment processing company to provide as a service the rapid distribution of transactions with good-enough checking in something like 10 seconds or less.[11]

He was right, and it turns out that Bitcoin payment processors need only a couple of seconds to do good-enough checking.

All About Commerce

The forums are filled with similar discussions about using Bitcoin in commerce. Satoshi and others talked about creating interfaces for online merchants,[12] tools for physical merchants,[13] point-of-sale transactions,[14] use-cases where the customer is uneasy about using a credit card,[15] keeping small amounts of Bitcoin on mobile devices for incidental expenses,[16] and

so on. There is no doubt that Satoshi designed Bitcoin to be used for payments, even those as small as a few cents. In fact, the original 0.1.0 version of the software contained unfinished code for a peer-to-peer marketplace and even the basic framework for virtual poker.

The broader Bitcoin industry, too, was building on the assumption that Bitcoin was a fast, cheap, reliable payment system for the internet. Successful companies like BitPay, the largest Bitcoin payment processor in the world, had their entire business model challenged by unreasonably high fees. In an interview in 2017, CEO Stephen Pair said:

At BitPay, the Bitcoin blockchain has stopped working for us… and we have a couple of options. One is we start using a fork of Bitcoin. The second option is we start using a fork of Bitcoin. And the third option is we start using a fork of Bitcoin. We are really at a point where we have no choice, and that's what we have to do.[17]

For this reason, BitPay was one of the first companies that integrated Bitcoin Cash after the split. Brian Armstrong, the CEO of Coinbase, also shared the same vision for Bitcoin as digital cash for the world, and in a 2017 interview, he explained why BTC's failure to scale "broke his heart."

The reason why I got really passionate about Bitcoin and digital currency is that I want the world to have an open financial system… where all payments are fast, cheap, instant, and global… And Bitcoin ended up not scaling to be that.[18]

He goes on to explain that other projects like Bitcoin Cash are more likely to accomplish this goal:

I believe you could actually operate [the Bitcoin network], even at VISA scale, for maybe two to three orders of magnitude less than VISA is charging today. So it could be something on the order of one cent, or less, to send every payment in the world…

But I think other networks like Bitcoin Cash or Ethereum are all working on this, and so, that vision is going to be realized, but it was a little frustrating to not see the original Bitcoin get there.

Armstrong's opinion was common among early Bitcoin entrepreneurs and early Bitcoiners generally. I remember the online community would frequently compare Bitcoin with Western Union to highlight its superiority as a payment system. One of the most popular early infographics (pictured below) placed a Western Union ad beside an equivalent ad for Bitcoin. The Western Union ad read, "Send warm wishes today. For only $5, you can send up to $50 for pickup within the U.S. Moving money for better." While the Bitcoin ad read, "Send warm wishes 24/7. For only $0.01, you can send up to any amount for pickup anywhere. Moving money far better."

Figure 1: Early infographic comparing Western Union to Bitcoin

The Bitcoin.org website also marketed the advantages of using Bitcoin for everyday commerce. An archived version from 2010 stated that, "Bitcoin transactions are practically free, whereas credit cards and online payment systems typically cost 1-5% per transaction plus various other merchant fees up to hundreds of dollars."[19] Even as late as 2015, the website advertised "Zero or low processing fees" and "Instant peer-to-peer transactions."[20]

To pretend that Bitcoin was never created for everyday payments is a brazen attempt to rewrite history. Any person of integrity who was involved before 2014 will attest that the original plan was for a low-cost, digital cash system.

The people who thought Bitcoin should be an expensive, exclusive store of value were in the extreme minority.

4

Store of Value vs. Medium of Exchange

[T]he real advantage of Bitcoin lies in it being a reliable long-term store of value… not from its ability to offer ubiquitous or cheap transactions.[1]

—Saifedean Ammous, The Bitcoin Standard

It is surprising that so many people have uncritically accepted the idea that Bitcoin will store value even if it doesn't work as digital cash. The exact opposite is more likely to be true: if Bitcoin can prove itself as a superior currency over a long period of time, the market might accept it as a store of value. But it will take years of demonstrated utility and stability before that happens. Calling any existing cryptocurrency a "reliable long-term store of value" is premature, considering the wild price fluctuations that are a regular occurrence. The fact that BTC has greatly appreciated in price over the past ten years does not mean it is a store of value.

Don't Touch It

Saifedean Ammous has one of the most extreme versions of "digital gold maximalism" out there. He envisions a future in which regular people don't even touch the blockchain, and on-chain transactions are reserved for high-value transfers only. In The Bitcoin Standard, he writes:

Bitcoin can be seen as the new emerging reserve currency for online transactions, where the online equivalent of banks will issue Bitcoin-backed tokens to users while keeping their hoard of Bitcoins in cold storage...[2]

And in an online discussion, he writes:

Bitcoin on-chain payments aren't for the merchant; they're for central banks. You can have all the world's payment networks built on top of Bitcoin, only settling on chain. BTC is like central bank gold under a gold standard.[3]

This sentiment is echoed by popular Bitcoin commentator Tuur Demeester:

At full maturity, using the Bitcoin blockchain will be as rare and specialized as chartering an oil tanker.[4]

These ideas are now discussed as if they have been the dominant vision since the beginning. But compared to the original design, they are wild and unnecessary. I certainly never signed up for this version of Bitcoin, nor did the countless other entrepreneurs I worked with in the early days. In fact, a central part of the beauty of Bitcoin is precisely that the blockchain is accessible to everybody and not exclusive to bankers. Like so many other public personalities who speak with confidence about Bitcoin, Ammous and Demeester merely assume that additional layers will solve BTC's usability problems without any issue. Yet, when you actually look at second-layer technologies, their viability remains uncertain, especially if the base layer does not scale. These problems are generally not recognized by BTC enthusiasts, who instead believe that engineers will fix everything in the future, despite their poor track record so far.

Furthermore, a future of "Bitcoin-backed tokens" is a guarantee that arbitrary inflation will continue plaguing those of us who are not central bankers. History demonstrates that currencies inevitably lose their backing over time, and if people are forced to trade promises-of-Bitcoin instead of actual Bitcoin, it's only a matter of time before the promises are inflated far beyond the actual supply of Bitcoin. Second layers only make this inflation easier to conduct.

Narrative Shift

Within the Bitcoin community, the narrative started shifting from digital cash to a store of value over a period of several years. Even as late as 2016, the majority of Bitcoiners were still promoting the technology as an online currency—or as they liked to call it, "magic internet money"—which is why there would be celebrations whenever a new company announced that they were accepting it for payment. With each additional merchant accepting it, Bitcoin gained more credibility and utility. But after the fee spike in late 2017, rather than admit there was a problem, the most influential BTC proponents cleverly started to change the narrative—since

if Bitcoin is only a store of value, then high fees don't matter after all. In recent years, people have even been encouraged not to spend their coins in commerce, because BTC is for buying and holding indefinitely. My cynical take on the "buy, hold and never use" narrative is that it's a great way to pump the price by creating artificial scarcity. If enough people are convinced that they can get rich by buying and holding an asset with a finite supply, extreme price increases are the inevitable result.

In my judgment, the only hope that cryptocurrency has to become a real store of value is to have real-world utility. A cryptocurrency must be more useful than legacy systems, and high transaction fees immediately damage the usefulness of any coin. If BTC were the only cryptocurrency available, then perhaps it could still work as a store of value, but since the market has superior options to choose from, it seems unlikely that the slowest, most expensive, and least scalable cryptocurrency will end up being chosen as a reliable long-term store of value. For example, Bitcoin Cash has virtually all the properties of Bitcoin Core, except you can actually use it as digital cash. In the long run, the market will eventually figure out that they are paying extremely high fees on BTC for no good reason, since the same product can be offered at a fraction of the cost.

The Economics of Storing Value

To see the problems with the "store of value only" idea, we must dive deeper into economics. I was lucky to discover the Austrian School of Economics early in my life. Great thinkers like Ludwig von Mises and Murray Rothbard helped me understand the world through an economic lens, and the reason I knew that Bitcoin was going to become popular was because I had previously read their ideas on money. I could see that Bitcoin had the properties of extremely high-quality money, which meant I should buy some immediately.

Bitcoin's potential as a store of value is an interesting economic puzzle. For that matter, value itself is an interesting puzzle that perplexed economists for centuries. Why does anything have value in the first place? One of the insights from the Austrian School of Economics—that has since been incorporated into mainstream economics—is that value is subjective. Value is not found inside material goods; it's found inside human minds. Things

don’t possess value in themselves. We give them value because we believe they can be used to satisfy our desires.

A “store of value” cannot literally “store” value, as if it’s a physical box into which value is placed for later retrieval. Rather, if something is a store of value, that just means it has a consistent track record of being valued by humans. And because of its successful history, people have good reason to believe it will be valued in the future. So, it retains its purchasing power over time. Lots of things are used to store value. Cattle, for example, have been a store of value for a long time. Humans have good reason to believe that cattle can be used to satisfy their wants. You can milk them, eat them, use them for farm labor, and many other things. Because of this usefulness, if you want to sell your cattle, you’ll likely find buyers. Real estate is another popular store of value with a long track record. Humans have good reason to believe that owning land will benefit them. They can live on the land, use it to produce food, develop it, lease it, etcetera. A thousand years from now, it’s likely that cattle and real estate will still be valued by humans. The most popular store of value is money.

Money is a bit more complex as an economic phenomenon than cattle or real estate. In order to understand it, we have to grasp one more concept: the difference between direct and indirect exchange. Imagine a situation where a farmer raises chickens, and he lives next door to a tailor that produces shirts. If the farmer wants a shirt, and the tailor wants a couple of chickens, they can engage in the simplest kind of economic exchange called “direct exchange” or “barter,” which happens when the farmer trades his chickens directly for the tailor’s shirt. Barter tends to be clunky and inefficient, since it requires both parties to specifically want the item that the other person is trading. If instead of a shirt, the farmer wanted shoes, the exchange would not happen.

In contrast to barter, “indirect exchange” happens when the goods traded are not the final goods desired. So, the farmer might trade his chickens for some gasoline, not because he wants the gasoline, but because he can trade it to the tailor for the shirt he desires. In that situation, we would call the gasoline a “medium of exchange”—an intermediate step between the farmer and the final goods he desires.

Mediums of exchange are amazing. They enable huge networks of people to trade and collaborate without having to know each other, speak the same language, or share the same preferences. The most popular medium of exchange in an economy is money, and it essentially allows any product to be traded for any other. A farmer can turn his chickens into a Lamborghini if he first sells enough of them for money.

Money makes it far easier to plan, save, and invest. The farmer can sell his chickens in the summer for money that he plans to use in the winter. Or he can invest his money into projects that earn a return. Without money, investment is much harder to coordinate—a farmer would need to find projects that accept chickens directly as investment. Using money instead, he can sell his chickens for, say, Euros, then invest those Euros into other projects. Truly, money is a great invention that makes us all wealthier.

Money also makes an excellent store of value. The Austrian School of Economics provides the best explanation why. According to Ludwig von Mises:

The functions of money as a transmitter of value through time and space may also be directly traced back to its function as medium of exchange.[5]

Murray Rothbard also comes to the same conclusion:

Many textbooks say that money has several functions: a medium of exchange, unit of account, or "measure of values," a "store of value," etc. But it should be clear that all of these functions are simply corollaries of the one great function: the medium of exchange.[6]

In other words, it's precisely because money is the commonly used medium of exchange that it stores value. So, if Bitcoin is supposed to be money, then to claim it can store value without being a medium of exchange is to put the cart before the horse.

It's helpful to think of "storing value" as making a prediction. You're trying to guess which goods will be valued in the future. If something is useful to people—like real estate—it's more likely to be valued. If something is already being used as a medium of exchange—like paper currency—that's a

great sign that it will continue to be valued in the future. It's not a guarantee, since we see cases of paper currency being ruined by central banks inflating their money supply, but it's still a strong signal.

If people are less confident that something will be used as a medium of exchange in the future, they are less likely to use it as a store of value. Imagine that you are living on an island on which seashells are commonly used as a medium of exchange. One day, you hear on the radio that a groundbreaking new study shows that seashells are dangerous to hold and can cause cancer. You would expect far fewer people to accept those seashells as a medium of exchange, which means they are going to become a worse store of value. Even if the study was wrong and the seashells don't cause cancer, mere public belief that they might is sufficient to change a functioning money into something worthless. The Bitcoin Core network failures of 2017 and 2021—and subsequent anti-adoption from companies dropping it as a payment option—gave reasons to doubt that BTC can work as a medium of exchange, which makes it less likely to become a real store of value in the future.

Money and Value

While all money stores value, not all stores of value are money. Cattle and real estate are often considered stores of value without being money because they have other, non-monetary uses. This raises a key question: is Bitcoin like money that stores value because it's used as a medium of exchange, or is Bitcoin like cattle and real estate, which store value for non-monetary reasons? In 2010, Satoshi discussed this subject in the forums, where people were debating how Bitcoin could gain value and why. He stated:

As a thought experiment, imagine there was a base metal as scarce as gold but with the following properties:

- boring grey in colour

- not a good conductor of electricity

- not particularly strong, but not ductile or easily malleable either

- not useful for any practical or ornamental purpose

and one special, magical property:

- can be transported over a communications channel

If it somehow acquired any value at all for whatever reason, then anyone wanting to transfer wealth over a long distance could buy some, transmit it, and have the recipient sell it.

Maybe it could get an initial value circularly as you've suggested, by people foreseeing its potential usefulness for exchange. (I would definitely want some) Maybe collectors, any random reason could spark it.

I think the traditional qualifications for money were written with the assumption that there are so many competing objects in the world that are scarce, an object with the automatic bootstrap of intrinsic value will surely win out over those without intrinsic value. But if there were nothing in the world with intrinsic value that could be used as money, only scarce but no intrinsic value, I think people would still take up something.[7]

This is a great quote for a few reasons. First of all, in this context, Satoshi is using the term "intrinsic value" to mean non-monetary use value. Gold and silver, for example, make great mediums of exchange and can also be used in industry. Tobacco and salt, other historical mediums of exchange, can be consumed directly. Bitcoin does have some non-monetary value, which will be explained shortly, but Satoshi's thought experiment shows that even if Bitcoin had zero non-monetary uses, the mere fact that it is scarce and can be sent over a communications channel—i.e. the transaction costs are extremely low—could be sufficient to give it value because of "its potential usefulness for exchange." In other words, Satoshi thought Bitcoin might be able to bootstrap its own value by people recognizing that it could make an excellent medium of exchange. That makes Bitcoin a rather unique invention. It is a purpose-built payment system which uses a currency that was designed to have better monetary properties than any existing money.

Other Uses

At first glance, it doesn't look like Bitcoin can do anything other than be sent to somebody else. But it does have other uses. The Bitcoin blockchain is an online, public ledger that is maintained by a decentralized network of computers, and Bitcoin transactions control the entries on that ledger. This functionality can be used for various non-monetary purposes. For example, the blockchain can be used to store valuable data, though it's significantly more expensive than other methods for data storage. There are new social media companies that use this feature to create uncensorable platforms on the blockchain. Other applications could be things like asset registries, new systems for voting, or identity verification to improve online security. Relative to Bitcoin's utility as a general payment system, these abilities seem minor, but they do exist.

Thinking that Bitcoin qualifies as a "store of value" because of its non-monetary properties is like thinking US Dollar bills are a store of value because they can be used as kindling or toilet paper. Though that utility does exist, it's tiny when compared to the value of being a secure, international, frictionless medium of exchange. Satoshi understood that the transmissibility of Bitcoin was a central feature that gave it value. Yet, that feature was intentionally destroyed by the Bitcoin Core developers, giving BTC almost no unique value proposition when compared to other cryptocurrencies. Not only do other coins have lower fees, they also have superior non-monetary functionality.

Given the subjective nature of value, it is conceivably possible that the market could choose BTC as a store of value. But it's also conceivable that the market could choose smelly old gym socks as a store of value. Possible, but unlikely. It seems more reasonable to think that the cryptocurrency with the best chance of becoming a store of value needs to maximize all its positive properties and minimize its negative properties. Having clunky and expensive transactions is not a desirable feature of any store of value or medium of exchange. The famous internet entrepreneur Kim Dotcom, founder of MegaUpload, expressed similar sentiments in a conversation in January 2020, saying:

In order to be a very successful cryptocurrency you need to provide fast and cheap transactions, there's no way around that. It's nice to be a store of

value, but if you really want to succeed in this game, you need to be electronic cash.

Kim also pointed out that the vast majority of people still have no experience using cryptocurrencies, and in order to onboard them, fees need to be low, and reliability needs to be high.

[Most people] don't know anything about the current wars that are taking place or the current toxicity within the crypto community. They are going to go with the currency that gives them the cheapest fees, the fastest transactions, the most reliability, and currently, unfortunately, that is not Bitcoin [Core].8

Imagine a cryptocurrency with all the properties of BTC, except in addition, it allowed instant, nearly free transactions for the entire world and was a purpose-built medium of exchange for the twenty-first century. Its utility would be orders of magnitude greater than one without this functionality. That was the original plan for Bitcoin, and it remains the plan for Bitcoin Cash and other cryptocurrencies.

5

The Blocksize Limit

If you told me in 2011 that we would be sitting here in 2017 and we hadn't bumped up this block size, I would've said, "there's no way that could happen."[1]

—Stephen Pair, CEO of BitPay

A single technical parameter allowed the Bitcoin Core developers to turn Bitcoin into a different project: the "blocksize limit." The blocksize limit is simply the maximum size of blocks allowed on the network. Remember, transactions get bundled into blocks, so the more transactions, the larger the blocks. This makes the blocksize limit effectively a maximum throughput limit for Bitcoin. Bitcoin Core used a tiny blocksize limit to artificially throttle the capacity of the network to a fraction of its potential.

The blocksize limit was not supposed to be an important parameter, and the limit was not meant to be reached. It was supposed to stay far above the size of the average block. The blocks were never meant to be full, except in extreme circumstances.

Extra Space Needed

A full block means that there are more transactions trying to be processed than can fit into a single block, which immediately causes fees to spike and a backlog to develop. A BTC block can currently hold 2,000-3,000 transactions and is produced every ten minutes. If 18,000 people try to make a single transaction within a ten-minute period, the network must take at least six blocks to process them all. That's one hour to process every transaction in the queue if nobody else uses it during that time. If 150,000 people try to use Bitcoin at one time, it would require at least fifty blocks to process everything. That's more than eight hours of waiting.

Delayed processing is not the only problem during network congestion. When blocks become full, fees start rising. A higher fee does not guarantee

that your transaction will be processed quickly; it only allows you to cut in line in front of other transactions. Since the network cannot handle more than 3,000 transactions per block, a queue forms. Raising your fee increases the chance that miners will include your transaction in the next block, but if enough people pay more than you, your transaction gets pushed back farther in the queue. This makes fees rise exponentially and creates a horrible user experience. As soon as blocks become full, fees can rise from a dime to a dollar, then to five, ten, twenty, fifty dollars, or even more if enough people are using it. During the fee spikes in 2017 and 2021, some complex transactions cost more than $1,000 each, which I ended up paying multiple times. A quick search of the blockchain for transactions with fees from $900 to $1,100 returns nearly 35,000 results.2

Bitcoin is often analogized to email for its ability to instantly connect people over the internet. Imagine if email couldn't handle 150,000 people using it and took eight hours to send and receive messages. That would certainly be considered an embarrassing design flaw. Yet, in the middle of these network failures, transactions could be stuck for days, or even an entire week at the peaks. This is why the blocksize limit was supposed to stay far above the demand for transactions, as a distant technical limitation that wouldn't affect the functionality of the system. Bitcoin would scale with usage and the limit would either be increased or removed altogether.

Allowing the blocks to grow naturally would have kept Bitcoin as a digital cash system with low-fee transactions and universal access to the blockchain. But the Core developers wanted to turn Bitcoin into a settlement system for high-value transfers, so they refused to increase the blocksize limit. The only reason that fees spiked to astronomical levels and the network became unreliable was because the blocks were too small to handle demand.

Countless early developers, businesses, and enthusiasts knew that the blocksize limit needed to be raised. They knew that full blocks would cause a terrible user experience and could see that the blocks were becoming fuller as Bitcoin grew in popularity. Yet, despite endless arguments and pleas from the industry, the Core developers refused to increase the limit. They have still not meaningfully increased maximum transaction

throughput from 2010 levels. A single picture on your smartphone is bigger than an entire BTC block, sometimes significantly so depending on the quality of the image. This was ultimately the reason why the cryptocurrency industry fractured and Bitcoin Cash was created.

The Reason for the Blocksize Limit

By the time Satoshi Nakamoto left Bitcoin, there were many enthusiastic and talented developers working on the project, but two stand out as exceptional: Gavin Andresen and Mike Hearn. Andresen was chosen by Satoshi as his successor and the lead developer of the project. Naturally, he was also a big-blocker. Over the years, he wrote influential articles on his blog[3] about Bitcoin and scaling, developer culture, economics, and other topics.[4] He was soft-spoken, perhaps to a fault. Hearn, on the other hand, was a feistier developer who was more outspoken against the small-blockers whom he believed were disrupting the project. His previous work experience was especially relevant. Hearn left Google to work on Bitcoin. While at Google, he spent three years as a capacity planner for Google Maps—one of the most popular websites in the world. So, he was deeply familiar with network capacity issues. Like Satoshi and Andresen, Hearn was a big-blocker who didn't think Bitcoin had any inherent scaling problems. Between their blog posts, emails, forum conversations, and public interviews, Andresen and Hearn captured the original vision for Bitcoin better than anybody else. Their commentary is essential reading and is cited throughout this book.

When Bitcoin was originally coded, there was no explicit limit on the size of blocks that could be produced. That changed in 2010, when Satoshi added a blocksize limit to prevent a potential denial-of-service attack while Bitcoin was young. In his blog, Gavin Andresen explained the reasons for the initial limit:

> … [T]he limits were added to prevent a 'poisonous block' network denial-of-service attack. We have to worry about denial-of-service attacks if they are inexpensive to the attacker… The attack the limit is meant to prevent is much more expensive today…

On July 15th [2010], about eleven thousand bitcoin were traded at an average price of about three cents each. The block reward was 50 BTC back then, so miners could sell a block's worth of coin for about $1.50.

That gives a rough idea of how much it would cost an attacker to produce a 'poisonous block' to disrupt the network – a dollar or two. Lots of people are willing to spend a dollar or two "for the lulz" – they enjoy causing trouble, and are willing to spend either lots of time or a modest amount of money to cause trouble.[5]

The initial limit was set to one megabyte, allowing for a theoretical limit of seven transactions per second. In practice, the real limit is around three to four transactions per second, corresponding to 2,000-3,000 on-chain transactions per block—far above the actual usage of the network in those days. The plan was to simply increase the limit or eliminate it entirely. Andresen noted in the forums:

The plan from the beginning was to support huge blocks. The 1MB hard limit was always a temporary denial-of-service prevention measure.[6]

Ray Dillinger, another early Bitcoin pioneer, said the same thing:

I'm the guy who went over the blockchain stuff in Satoshi's first cut of the bitcoin code. Satoshi didn't have a 1MB limit in it. The limit was originally Hal Finney's idea. Both Satoshi and I objected that it wouldn't scale at 1MB. Hal was concerned about a potential DoS attack though, and after discussion, Satoshi agreed… But all 3 of us agreed that 1MB had to be temporary because it would never scale. [7]

Satoshi, Hal, and Ray being in unanimous agreement is particularly interesting since Hal Finney is often seen as a proponent of small blocks. But even he agreed the 1MB limit had to be temporary. Yet, to this day, the Bitcoin Core developers have refused to meaningfully increase the blocksize limit beyond the initial level set in 2010, despite the massive improvements in software, hardware, and networking technology. Virtually all the biggest companies in the industry tried, on multiple occasions, to increase the limit, but the Core developers refused, even after publicly agreeing to an increase. Instead, they changed the metric of blocksize into

“block weight” and claim the new limit is 4MB, but this is mostly an accounting trick and does not correspond to a quadrupling of throughput capacity.

Inverted Design

The simple reason the Core developers refused to increase the limit is because they wanted to change Bitcoin’s design. The sooner the blocks became full, the sooner the transaction fees would rise, which they viewed as desirable. Jorge Timón, a Core developer, stated, “I agree that hitting the limit wouldn’t be bad, but actually good for a young and immature market like bitcoin fees.”8 While Greg Maxwell stated bluntly, “There is nothing wrong with full blocks… Full blocks is the natural state of the system.”9

To appreciate just how radical these ideas are, contrast them with the ideas you would have encountered in the early days of Bitcoin, when the Visa network was often used as a comparison for transaction throughput. All the way back in 2009, Satoshi was asked about Bitcoin’s ability to scale and said:

The existing Visa credit card network processes about 15 million Internet purchases per day worldwide. Bitcoin can already scale much larger than that with existing hardware for a fraction of the cost. It never really hits a scale ceiling.10

This was the common understanding for years. Though today we would call it part of “Satoshi’s vision,” it was nearly everybody’s vision back then. For example, if you were researching Bitcoin in 2013, you would likely have come across its Wiki page. This is what the section on “scalability” had to say:

The core Bitcoin network can scale to much higher transaction rates than are seen today, assuming that nodes in the network are primarily running on high end servers rather than desktops. Bitcoin was designed to support lightweight clients that only process small parts of the block chain…

A configuration in which the vast majority of users sync lightweight clients to more powerful backbone nodes is capable of scaling to millions of users

and tens of thousands of transactions per second…

Today the Bitcoin network is restricted to a sustained rate of 7 tps by some artificial limits. These were put in place to stop people from ballooning the size of the block chain before the network and community was ready for it. Once those limits are lifted, the maximum transaction rate will go up significantly… At very high transaction rates each block can be over half a gigabyte in size.[11]

This was common knowledge. Everybody understood that the system was designed to scale with larger blocks, and it wasn't even controversial. Andresen stated that the scalability of Bitcoin was part of the allure that drew him to the project:

When I first heard about Bitcoin, it was small enough I could read everything, and I did, including all of those mailing list posts. The promise of a system that could scale up to rival Visa is part of the vision that sold me on Bitcoin.[12]

In 2013, Visa was handling, on average, around 2,000 transactions per second. To get 2,000 transactions per second on Bitcoin, the blocks would have to be roughly 500MB, which is an entirely manageable amount. Today's cell phones can easily record and upload HD videos that are gigabytes in size—that is, multiple times the size of a Bitcoin block that contains over a million transactions. Scaling to that level requires more than simply increasing the maximum blocksize, but there are no fundamental reasons why it can't happen. In fact, Bitcoin Cash has already successfully had multiple 32MB blocks, and a recent offshoot of Bitcoin Cash, Bitcoin SV, has even mined a 2GB block. These networks have not broken. Satoshi had a simple, final answer to questions about blocksize:

It would be nice to keep the [blockchain] files small as long as we can. The eventual solution will be to not care how big it gets.[13]

High Fees and Slow Transactions

Why would the Bitcoin Core developers want high fees? To the early Bitcoin enthusiast, or even to the average person, it sounds like an

obviously bad idea. But actually, high fees are the inevitable outcome of the small-block philosophy. To understand why, we have to analyze the system more closely. As explained in Chapter 2, miners get paid in two ways. They receive transaction fees and the block reward. Since the block reward diminishes over time, the only source of revenue will eventually be transaction fees. And since the Bitcoin Core developers want small blocks, the only way for miners to make money in their system is with extremely high transaction fees. Bitcoin cannot work without miners being paid, and if they can only process 3,000 transactions per block, fees need to be hundreds or thousands of dollars per transaction to maintain security. Core developer Jorge Timón spoke openly about this problem:

Bitcoin needs a competitive fee market in the long run to sustain [proof of work] once the subsidies are gone. I am very happy that we have it now….[14]

Pieter Wuille, another Core developer, said:

My personal opinion is that we—as a community—should indeed let a fee market develop, and rather sooner than later.[15]

They euphemistically call the backlog of high fee transactions a "fee market," where users outbid each other for the tiny amount of space inside blocks. This bizarre and unnecessary security model is why the Core developers celebrate and encourage high fees and a backlog of transactions. Greg Maxwell claimed:

Fee pressure is an intentional part of the system design and to the best of the current understanding essential for the system's long term survial [sic]. So, uh, yes. It's good.[16]

And when fees rose to $25 in December 2017, Maxwell infamously responded:

Personally, I'm pulling out the champaign [sic] that market behaviour is indeed producing activity levels that can pay for security without inflation, and also producing fee paying backlogs needed to stabilize consensus progress as the subsidy declines.[17]

Of course, Satoshi Nakamoto did not design Bitcoin this way. Miners were expected to recoup their costs by processing a high volume of low-fee transactions with big blocks. In the forums, Satoshi was asked about the long-term revenue model for miners. He explained:

In a few decades when the reward gets too small, the transaction fee will become the main compensation for [miners]. I'm sure that in 20 years there will either be very large transaction volume or no volume.[18]

Notice, he did not say "in 20 years, there will either be a large transaction volume or a small volume with extremely high transaction fees." That would have sounded dubious to anybody with common sense. He predicted either high volume or none at all.

The New Bitcoin

By artificially limiting the blocksize, the Bitcoin Core developers found a way to completely change the dynamics of the system. Not only did the user experience change from "nearly instant and free transactions" to "expensive and unreliable transactions," the underlying economic model was radically changed as well. BTC is gambling on the idea that future users will be willing to pay hundreds or thousands of dollars per on-chain transaction, despite having superior alternatives. Otherwise, miners will have to shut down most of their equipment because they won't generate a profit.

Given this, it's no exaggeration to say that BTC was hijacked, and the original design was replaced with a new, speculative one. This is why Vitalik Buterin, the co-founder of Ethereum, publicly said:

I consider BCH a legitimate contender for the bitcoin name. I consider bitcoin's *failure* to raise block sizes to keep fees reasonable to be a large (non-consensual) change to the "original plan", morally tantamount to a hard fork.[19]

Bitcoin Core's failure to increase the blocksize limit was not merely academic. It had real-world consequences for the businesses building on Bitcoin or merely accepting it for payment. After the 2017 fee spike, the

Bitcoin industry experienced anti-adoption for the first time. When the popular gaming platform Steam announced they were no longer accepting Bitcoin, they publicly shared their reasons why[20]:

As of today, Steam will no longer support Bitcoin as a payment method on our platform due to high fees and volatility in the value of Bitcoin… [T]ransaction fees that are charged to the customer by the Bitcoin network have skyrocketed this year, topping out at close to $20 a transaction last week (compared to roughly $0.20 when we initially enabled Bitcoin)…

When checking out on Steam, a customer will transfer x amount of Bitcoin for the cost of the game, plus y amount of Bitcoin to cover the transaction fee charged by the Bitcoin network. The value of Bitcoin is only guaranteed for a certain period of time so if the transaction doesn't complete within that window of time, then the amount of Bitcoin needed to cover the transaction can change. The amount it can change has been increasing recently to a point where it can be significantly different.

The normal resolution for this is to either refund the original payment to the user, or ask the user to transfer additional funds to cover the remaining balance. In both these cases, the user is hit with the Bitcoin network transaction fee again. This year, we've seen [an] increasing number of customers get into this state. With the transaction fee being so high right now, it is not feasible to refund or ask the customer to transfer the missing balance (which itself runs the risk of underpayment again, depending on how much the value of Bitcoin changes while the Bitcoin network processes the additional transfer).

At this point, it has become untenable to support Bitcoin as a payment option. We may re-evaluate whether Bitcoin makes sense for us and for the Steam community at a later date…

-- The Steam Team

It's impossible to fault Steam for their decision. Trying to use Bitcoin when the blocks are full can be an awful experience. Customers seeking refunds are guaranteed to lose money. If they are refunding a $30 game and the transaction fees cost $10 each, users can end up losing $20 and have

nothing to show for it. In my opinion, if you wanted to break Bitcoin, allowing blocks to become full would be the best way. If the high fees and processing delays were caused by a technical glitch, it probably would have been better for Bitcoin, since it's a new technology and the issue could have been considered a fluke. But instead, the public was told that high fees are perfectly fine, that you aren't supposed to use Bitcoin for everyday purchases, and that blockchains actually can't scale.

BTC supporters have a few standard responses to these criticisms. If they are unaware that high fees are part of the intentional redesign of Bitcoin, they often like to say, "Fees aren't really a problem. Look, at this very moment, fees are low!" But this is a weak argument. At any given moment, the fees might be low on BTC, but only because the network has little traffic. If more people use it, then congestion will build quickly, and the fees will spike again. It's like automobile traffic. Just because the roads are empty at 3am doesn't mean that Los Angeles has solved their traffic problems. If the BTC blocks are not full, then fees will be low, but if blocks are full and activity increases, then the fees will inevitably rise to extreme levels.

What About Second Layers?

The other attempt to rescue the small-block philosophy involves an appeal to secondary layers, since if most transactions are off-chain, then perhaps the fees can be low on the secondary layers. While it does make sense to build multiple layers in Bitcoin, in order to work correctly, the base layer must be scalable. If the base layer can only process seven transactions per second, it's not even close to being robust enough to build additional layers on top. Second layers still have to interact with the base layer, so high fees remain a fundamental problem. For example, the Lightning Network still requires occasional on-chain transactions to use, and those fees have to be paid by someone. Right now, many popular wallets are subsidizing these costs for their users, but if $50+ fees are the norm, that model is simply not sustainable.

Elon Musk is one person who seems to understand the value of scaling the base layer for cryptocurrencies. In a Twitter thread about network design, he shared his thoughts as an engineer:

BTC & ETH are pursuing a multilayer transaction system, but base layer transaction rate is slow & transaction cost is high… There is merit [to] maximizing base layer transaction rate & minimizing transaction cost… Block size & frequency should steadily increase to match broadly available bandwidth.21

If Musk had been around at the time, it sounds like he would have agreed with Satoshi, Andresen, Hearn, and most of the early Bitcoin entrepreneurs like myself. There is just no substitute for cheap, on-chain transactions.

The technical parameter that ended up splitting Bitcoin in two was the blocksize limit. Before the blocks became full, BTC enjoyed a market share in the cryptocurrency industry of around 95%. Once the blocks started filling up, the market share quickly dropped. At the peak of the network failure in January 2018, it dropped to 32%, and many users, businesses, and developers left BTC outright. As of March 2023, BTC market share is around 40% and will likely drop again with more network failures. If the Bitcoin Core developers had simply increased the blocksize limit to a reasonable level, I am confident that many competing cryptocurrency projects simply wouldn't exist, the industry would have remained unified around one coin, and BTC would have continued to be the premier digital cash system for the internet. Instead, the Bitcoin Core developers pivoted to a settlement system with high fees and unreliable transactions, leaving a void for digital cash that has not yet been filled.

6

Notorious Nodes

Bitcoin was designed to scale with larger blocks. So why would anybody think that big blocks are a problem? While it's impossible to know the internal motivations of the Bitcoin Core developers, this chapter will address their stated reasons for keeping the blocks small. All the objections to big blocks revolve around one core idea: as the blocksize increases, the cost to run a full node also increases. The more expensive it is to run a node, the fewer people will run them, and the more centralized the network will become. Therefore, by keeping blocks small, more people can run nodes, which keeps the network decentralized. Core developer Wladimir van der Laan stated it clearly in 2015:

I understand the advantages of scaling, I do not doubt a block size increase will *work* Although there may be unforseen [sic] issues, I'm confident they'll be resolved. However, it may well make Bitcoin less useful for what sets it apart from other systems in the first place: the possibility for people to run their own "bank" without special investment in connectivity and computing hardware.[1]

There are several problems with this idea. Most fundamentally, the idea that users need to run their own full nodes in order to "run their own bank" is incorrect. Bitcoin was designed so that regular people don't have to run their own full nodes. They can use lighter software. Remember, a full node downloads a copy of the entire blockchain and validates every single transaction on the network. This is unnecessary for almost everybody. Satoshi designed Bitcoin with Simplified Payment Verification (SPV) in mind, which allows users to verify their own transactions with a tiny amount of data. Using SPV, you cannot verify a stranger's transactions, nor can you verify every transaction ever made, but most people have no reason to do that. Satoshi was not foolish enough to design a cash system where every user had to download and verify the entire world's transactions. There's no way such a system could scale.

Second, the fact that the costs of validation increase with the size of blocks is not a problem. Satoshi could not have been clearer when he wrote:

The current system where every user is a network node is not the intended configuration for large scale. That would be like every Usenet user [running] their own NNTP server. The design supports letting users just be users. The more burden it is to run a node, the fewer nodes there will be. Those few nodes will be big server farms. The rest will be client nodes that only do transactions and don't generate.[2]

And also when he stated:

Only people trying to create new coins would need to run network nodes. At first, most users would run network nodes, but as the network grows beyond a certain point, it would be left more and more to specialists with server farms of specialized hardware.[3]

Satoshi was so clear about this that it's impossible to misinterpret. His idea made perfect sense. In every industry, businesses tend to specialize in what they do best. Maintaining Bitcoin's network is no different. Satoshi envisioned "big server farms" at the center of the network, with regular users connecting to them. It's fine to dislike this idea, but it's how Bitcoin was designed. It's analogous to email. Technically, it's possible for anybody to set up their own email server and connect to the global email network. But why would you? It's difficult to set up and maintain, and the vast majority of people have no reason to do so. So in most cases, we leave it to the specialists.

The Majority Opinion

Gavin, Mike, and Satoshi were not the only people who thought this way. The early forums are filled with other developers and users who also understood that the system does not require most people to run their own node. Alan Reiner, who created the popular Armory wallet, said in 2015:

The goals of "a global transaction network" and "everyone must be able to run a full node with their $200 dell laptop" are not compatible. We need to

accept that a global transaction system cannot be fully/constantly audited by everyone and their mother.[4]

Even supporters of Bitcoin Core have admitted that their perspective on nodes is quite different from the original one. “Theymos” is the pseudonym of the owner of the most popular discussion platforms for Bitcoin—who later played a central role in the censorship of big-blockers—but even he admitted:

Satoshi definitely intended to increase the hard max block size… I believe that Satoshi expected most people to use some sort of lightweight node, with only companies and true enthusiasts being full nodes. Mike Hearn’s view is similar to Satoshi’s view.[5]

Furthermore, it’s not even clear that the total number of people running nodes would be smaller if the costs increased. The total number of hobbyists running nodes would be smaller, but if Bitcoin was the new financial network of the globe, thousands of companies would have a financial incentive to run their own nodes. As Satoshi says in the whitepaper:

Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.[6]

The Full Node Religion

Let’s delve deeper into the reasons why small-blockers think full nodes are so important. The Bitcoin Wiki page has an entry on full nodes that explains their philosophy well. This long excerpt is a great summary:

Full nodes form the backbone of the network. If everyone used lightweight nodes, Bitcoin could not exist… Lightweight nodes do whatever the majority of mining power says. Therefore, if most of the miners got together to increase their block reward, for example, lightweight nodes would blindly go along with it. If this ever happened, the network would split such that lightweight nodes and full nodes would end up on separate networks, using separate currencies…

If all businesses and many users are using full nodes, then this network split is not a critical problem because users of lightweight clients will quickly notice that they can't send or receive bitcoins to/from most of the people who they usually do business with, and so they'll stop using Bitcoin until the evil miners are overcome…

However, if almost everyone on the network is using lightweight nodes in this situation, then everyone would continue being able to transact with each other, and so Bitcoin could very well end up "hijacked" by evil miners. In practice, miners are unlikely to attempt anything like the above scenario as long as full nodes are prevalent because they would lose a lot of money.

But the incentives completely change if everyone uses lightweight nodes. In that case, miners definitely do have an incentive to change Bitcoin's rules in their favor. It is only reasonably secure to use a lightweight node because most of the Bitcoin economy uses full nodes. Therefore, it is critical for Bitcoin's survival that the great majority of the Bitcoin economy be backed by full nodes, not lightweight nodes.[7]

These ideas have become the orthodoxy. Anybody trying to figure out Bitcoin today might not even know that this article is heavily biased towards a small-block perspective that the creator of Bitcoin himself would have disagreed with. There are two central points being made here:

1. Miners have an incentive to "hijack" Bitcoin by changing the rules in their favor; for example, increasing the block reward.
2. Miners are prevented from arbitrarily changing the rules because full nodes do not "blindly follow" the majority mining power.

Both of these claims are false. First, miners do not have an incentive to arbitrarily change the rules of Bitcoin. At first glance, it might seem like miners could profit from creating new coins out of thin air. However, this overlooks the reason why Bitcoins have value in the first place. Value is not intrinsic; it comes from a complex web of beliefs that people have about the entire Bitcoin network. If the miners decided to produce a billion new Bitcoins for themselves, they would destroy the underlying trust in the system, which would destroy the value of each Bitcoin. They might have a

billion more Bitcoins, but each one would be worthless. Mike Hearn understood this dynamic:

Rational miners shouldn't want to undermine the validity of their own wealth. Doing things that significantly reduce the utility of the system is self-defeating even over the medium term because it'd lead people to just give up on the system in disgust and sell their coins, driving down the price. I think it's fair to say that being unable to buy basic things like food or drinks in person would reduce the utility of Bitcoin for a lot of people.[8]

Hearn understood that miners are not a threat to the system. If anything, miners are least incentivized to break Bitcoin, since their only revenue comes from transaction fees and the block reward, both of which are denominated in Bitcoins that must be sold on the market.

The second major claim of the Wiki article is that full nodes can somehow prevent the rules of the network from changing. They cannot. Remember, full nodes cannot add blocks to the chain. They can only verify whether blocks and transactions are valid. Imagine that a new bug is discovered in the protocol that breaks Bitcoin in an important way and the software has to be upgraded in a short period of time. The miners will upgrade immediately, since their profits depend on the network running. But what would happen if everyone else running full nodes didn't upgrade? Would the miners be prevented from upgrading altogether? Not at all. Miners would continue on just fine adding blocks to the chain, and the full nodes would simply split themselves off the main network and onto their own new network. If their new network had no miners, they could not even add new blocks to their chain, and no transactions could be processed. If anything, this is a reason to use lightweight wallets, since you don't run the risk of being forked off from the main network.

Full nodes do not have any direct power to restrict miners from changing the rules. But it's correct to say they have indirect power to notify people that the rules have changed. According to the Wiki article, what prevents "evil miners" from changing the rules is that they know full nodes would catch them, and once the world learned about their evil deeds, the value of the whole system would be destroyed. So, the watchful eye of the full nodes keeps the miners in check. There's a superficial sense in which this is true.

Miners are indeed incentivized not to change the rules of Bitcoin arbitrarily because it would destroy the value of their coin. However, it doesn't require a large network of full nodes to notify people that the rules have changed. It only requires a single honest miner, or even a single honest node. Any one person can prove to the world that a particular block or transaction is invalid according to the old rules. Even if 100% of the miners were in collusion, a single full node could still demonstrate that the rules changed. That means any single miner, business, cryptocurrency exchange, researcher, or payment processor could prove that the rules changed. Therefore, it's essentially guaranteed that everybody would find out.

However, it would be an oversimplification to say that full nodes literally have no power, since not all nodes are created equal. Some full node operators are relevant economic actors. If the hobbyist running a node in his basement gets forked off the network, it doesn't matter. But if a large business or cryptocurrency exchange gets forked off, it does matter, and the value of the coin could be damaged. So, miners have a strong incentive to ensure that relevant economic actors support any proposed changes they want to make.

Honest and Dishonest Miners

It would also be an oversimplification to say that miners could never pose a risk to the integrity of Bitcoin. There is one clear scenario in which the actions of miners could be damaging. As explained in the whitepaper, Bitcoin requires that the majority of mining power—also called "hashrate"—is honest, meaning that it's not deliberately trying to destroy the system. Honest miners seek profit by maximizing the utility of the coin and growing the size of the network. Dishonest or malicious miners, on the other hand, pose a different kind of threat. Bitcoin was specifically designed to operate even among dishonest miners, but only if they constitute the minority. If the majority of hashrate became dishonest, then Bitcoin would indeed run into problems. For example, if a hostile government took control of the majority of hashrate, Bitcoin could be disrupted. But even in such a scenario, full nodes offer no protection. Since they cannot add blocks to the chain nor control the behavior of miners, they would simply be forked off

the main network. No matter how hard a full node tries, it just does not have the power to save a network with a majority of dishonest miners.

The fact that Bitcoin requires the majority of hashrate to be honest is not a unique design flaw. All proof-of-work blockchains have the same vulnerability. The real defense against dishonest miners is economic. It's the cost of mining. The more expensive it becomes to mine, the higher the costs to any bad actors trying to gain a majority of the hashrate. Therefore, the more successful Bitcoin becomes, the higher its overall level of security. Governments are generally the only ones that pose a real threat of gaining a majority of malicious hashrate, since they do not have to operate by the constraints of profit and loss. If a well-funded state actor tried to break Bitcoin in this way, the network would face a real challenge, regardless of how many full nodes there are.

The historical facts are clear. Bitcoin was not designed for regular users to run their own nodes. Satoshi was explicit about this on multiple occasions, saying:

The design outlines a lightweight client that does not need the full block chain… it's called Simplified Payment Verification. The lightweight client can send and receive transactions, it just can't generate blocks. It does not need to trust a node to verify payments, it can still verify them itself.[9]

Massive scaling was always possible with big blocks, and the infrastructure was supposed to be maintained by specialist "server farms." Despite this, the Bitcoin Core developers decided they didn't like Satoshi's design and thought they could improve it by having regular users download the entire blockchain and verify every transaction that takes place on it, even though they have no financial interest in doing so. That's currently the governing idea on the BTC network, and it's the reason transaction throughput is restricted and fees are high.

7

The Real Cost of Big Blocks

“I want to be able to run a full node from my home computer.” Does anybody actually care about that? Satoshi didn’t, his vision was home users running SPV nodes and full nodes being hosted in datacenters.[1]

—Gavin Andresen, 2015

Excessive concern about the cost of big blocks looks irrational when you run the numbers. It does not take more than back-of-the-envelope calculations to see that Bitcoin can scale far beyond 1MB blocks without substantially increasing costs. In fact, given the steep downward trajectory of the relevant costs involved, even at massive scale they would not be prohibitive for home users, even though Satoshi did not expect regular users to run their own nodes.

To have basic full node capability, the two major costs involved are data storage and bandwidth, both of which have plummeted for decades along with the costs of technology generally. I have watched these trends from the front line; my company MemoryDealers was built to sell computer hardware.

In The Bitcoin Standard, Ammous tries to explain why on-chain scaling is not feasible by going through the numbers:

For Bitcoin to process the 100 billion transactions that Visa processes, each block would need to be around 800 megabytes, meaning every ten minutes, each Bitcoin node would need to add 800 megabytes of data. In a year, each Bitcoin node would add around 42 terabytes of data... to its blockchain.[2]

This is correct. If Bitcoin processes roughly four transactions per second per MB block, then 800MB blocks equals around 3,200 transactions per second or a hundred billion transactions per year. Anybody familiar with computers will know that 800MB every 10 minutes is a surprisingly low number, considering that it enables Visa-level throughput. Yet, Ammous comes to the opposite conclusion:

Such a number is completely outside the realm of possible processing power of commercially available computers now or in the foreseeable future.[3]

I do not know where Ammous got his information, but he is apparently unfamiliar with the costs of technology. Even at massive throughput levels, neither storage nor bandwidth costs would be significant for running a basic full node.

Storage Costs

Let's start with the most basic calculations and then show how to reduce costs even further. In September 2023, a quick search for 8TB hard drives on Newegg.com shows its first result as a Seagate Barracuda drive selling for $119.99[4]—that's $15 per TB. If Bitcoin uses 42TB per year, that's $630, or $52.50 a month. If we want to include the cost of a consumer-grade, 6-bay NAS device to connect the drives together, that currently runs around $670.[5] Added together, that's a minuscule $1,300 per year—just over a hundred dollars a month—for storing 100,000,000,000 transactions.

Even though these costs are already low, the actual storage costs are even lower because of the clever way Bitcoin was designed. Put simply, full nodes do not need to store the entire transaction history. In fact, all they technically need is the running list of addresses with non-zero balances in them—called the "Unspent Transaction Output" set, or UTXO set. You can think of the UTXO set as the list of active cash balances without their corresponding histories. This makes the size of the UTXO set a tiny fraction of the historical record of all transactions. The record can be "pruned" away, where old, irrelevant information is discarded. Bitcoin miners often already run with a pruned blockchain. However, if a full node does want the historical record for some reason, it can easily keep as many months or years as it desires. Instead of storing all records going back to 2009, it could store just the last year's worth. So, instead of 42TB per year, it might only store 42TB in total, effectively turning the annual costs of storage into a one-time expense.

A full node running at Visa levels and keeping the entire blockchain history would still only incur minor storage costs with consumer-grade hardware. These calculations do not even consider the inevitable reduced costs of

technology in the future. Computer storage has a consistent record of massive price reductions over the past 70 years.

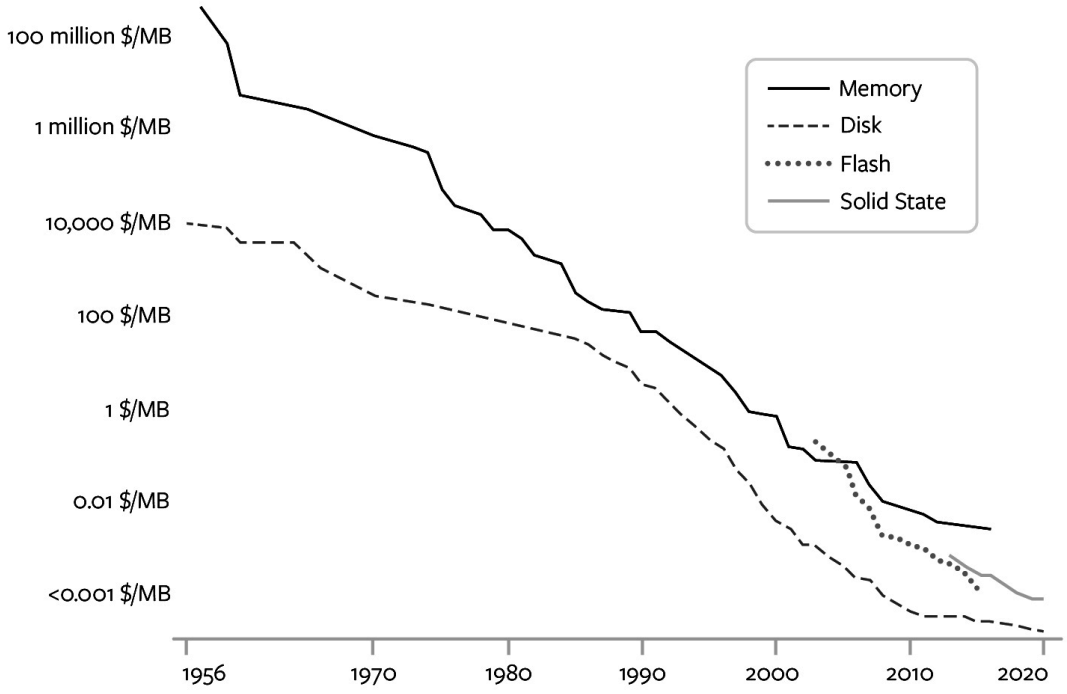


Figure 2: Computer memory and storage measured in US dollars per megabyte [6]

When Satoshi released Bitcoin at the beginning of 2009, computer storage cost roughly $0.10 per gigabyte. Since then, prices have come down more than 85% and are currently less than $0.015 per gigabyte.[7] Contrary to Ammous' claim that 800MB blocks would produce enough data to be "outside the realm of possible processing power of commercially available computers," the real storage costs would be affordable for consumers and minimal for most businesses.[*]

Bandwidth Costs

Storage costs are not a realistic concern. So, if there is any merit to the small block philosophy, it must be that bandwidth costs would be prohibitively expensive with big blocks. The Bitcoin Standard reads:

[A] node that can add 42 terabytes of data every year would require a very expensive computer, and the network bandwidth required to process all of these transactions every day would be an enormous cost that would be clearly unworkably complicated and expensive for a distributed network to maintain.8

Once again, Ammous makes confident pronouncements about the costs of technology, yet apparently without doing basic research on the topic. Satoshi himself addressed this concern all the way back in 2008, before he even released any code. He said:

The bandwidth might not be as prohibitive as you think. A typical transaction would be about 400 bytes… Each transaction has to be broadcast twice, so let's say 1KB per transaction. Visa processed 37 billion transactions in FY2008, or an average of 100 million transactions per day. That many transactions would take 100GB of bandwidth, or the size of 12 DVD or 2 HD quality movies, or about $18 worth of bandwidth at current prices.

If the network were to get that big, it would take several years, and by then, sending 2 HD movies over the Internet would probably not seem like a big deal.9

It's worth noting a couple of things from this quote. First, Satoshi gave an estimate of $18 per day—more than $6,500 per year—to demonstrate how low the costs of bandwidth could be at scale, again revealing that he did not expect regular users to run their own nodes. $18 per day is not an excessive amount, but it is enough to dissuade casual users who do not have a way to recover these costs. Miners would have no issues, however. If each of the hypothesized 100 million transactions had a $0.01 fee, that would result in $1 million per day split among miners, or roughly $41,500 per hour, more than enough to recover their costs for bandwidth.

Second, when Satoshi wrote that email in 2008, the average US cost of bandwidth was $9 for each megabit per second of data. Ten years later, it fell by a colossal 92% to $0.76.10 The cost of bandwidth varies across the world, but the trend is down everywhere, and there's every indication this will continue. AT&T is charging American customers only $80 per month

for one-gigabit service and $110 per month for two-gigabit.[11] People already using fiber optic internet might not even see their bandwidth costs increase at all.

To understand just how small these numbers are today, consider the data used by Netflix. Streaming an HD video from Netflix takes around 3GB of data per hour, and streaming a 4K video takes around 7GB per hour.[12] If we take Satoshi's estimates for 100GB per day, that works out to roughly 4GB per hour—around 43% less than the hourly bandwidth used when streaming 4K videos from Netflix. While it's true that not everyone in the world is currently able to stream 4K videos to their home, the point is that the costs are exponentially decreasing everywhere, and in the developed world they have reached a level where full node operators might not see their bandwidth costs increase at all. Undoubtedly, some nodes would not be able to handle the increased costs, but the capacity of the Bitcoin network should not be limited by those with the weakest internet connection. If Bitcoin only requires a gigabit-level internet connection in order to run a full node that can process Visa-level transaction throughput, the barrier to entry is not too high.

Bandwidth technology has rapidly improved for decades and shows no signs of slowing down. When Satoshi predicted that sending HD movies over the internet would eventually be normal, that was four years prior to the rollout of Google Fiber in 2012, which was the first mainstream service to bring gigabit internet connections to home users. Fiber promised to be nearly a hundred times faster than the average home connection at the time.[13] Future bandwidth technology looks equally as promising. In 2021, researchers in Japan set a new world record for internet speed, reaching an unbelievable rate of 319 terabits per second[14]—around 3.2 million times the current average US internet speed of 99.3 megabits per second.[15] It will take many years before that technology reaches the market, but it serves as another demonstration that exponential growth will continue to be normal, with many breakthroughs still ahead of us. Bandwidth is simply not a serious concern for Bitcoin at scale, and by the time global adoption is reached, the costs will be more trivial than they already are. This led Gavin Andresen to conclude that Bitcoin did not have any serious roadblocks to scaling. In 2014, he wrote:

According to my rough back-of-the-envelope calculations, my above-average home Internet connection and above-average home computer could easily support 5,000 transactions per second today.

That works out to 400 million transactions per day. Pretty good; every person in the US could make one Bitcoin transaction per day and I'd still be able to keep up.

After 12 years of bandwidth growth that becomes 56 billion transactions per day on my home network connection — enough for every single person in the world to make five or six bitcoin transactions every single day. It is hard to imagine that not being enough…So even if everybody in the world switched entirely from cash to Bitcoin in twenty years, broadcasting every transaction to every fully-validating node won't be a problem.16

The BTC network is producing blocks that are roughly 1MB† in size every ten minutes, which is comically small—even smaller than your average cell phone picture. We are constantly streaming videos that can be orders of magnitude larger than 1MB and transmitted over cellular networks, and the cost of data keeps falling. Bitcoin was intentionally designed so that regular users do not have to run their own node, but even at massive scale, the costs would not be prohibitive.

---

* Some specialized businesses that need ultra-fast performance, like cryptocurrency exchanges or payment processors, could see higher costs due to RAM requirements—though these can be mitigated also. See Gavin Andresen, "UTXO uh-oh…", http://gavinandresen.ninja/utxo-uhoh

† Technically, these numbers have increased slightly after changing the metric from "block size" to "block weight," but the total number of transactions per block is comparable. Explained further in Chapter 19.

8

The Right Incentives

I think most people see all the digital signatures and peer-to-peer networking technology but miss that much of the brilliance of Bitcoin is how the incentives are designed.[1]

—Gavin Andresen, 2011

Bitcoin is not merely a software project or a computer network. It is an enormous, complex system that millions of people around the world participate in. To understand it, we have to examine more than just its software. Some critical features of Bitcoin are not coded at all; they are built into its incentive structure. Users, miners, and businesses are all incentivized to use Bitcoin in a way that benefits themselves and the whole network at the same time. This economic coordination can be harder to see, but it's just as important as any other technical detail.

Why Run a Full Node?

Big-blockers and small-blockers disagree about the role of full nodes on the network, and this reflects a difference in thinking about incentives. In the small-block philosophy, full nodes are supposed to play a critical role, despite a lack of clear incentive. Regular users are encouraged to run their own nodes, downloading and validating the entire blockchain just to use Bitcoin, even though it's a burden. When running a node for the first time, it can take hours or even days to sync up with the rest of the network, and it also takes up hundreds of gigabytes worth of disk space. For this reason, full nodes are generally not run on smartphones, making BTC much less convenient to use. Users are not rewarded for running this software; they simply gain the ability to validate blocks of other people's transactions.

While this might sound like a great idea to a group of software engineers, it's not a realistic expectation for the rest of the world to follow. Most people will never run a full node because they have no reason to. It's too great a burden with too little a reward. If Bitcoin was designed so that

regular people were forced to run their own nodes for the security of the network, it would be a critical design flaw.

Compare this to Satoshi's SPV design, which allows wallets to be downloaded and synced instantly. You can use a BCH wallet on your smartphone as easily as any other app. BTC proponents like to claim that SPV has some theoretical security problems, but there have been no documented cases of users losing money because of it. It has a long, successful track record, and the most popular BTC wallet apps are actually using SPV or similar technology, or they are custodial wallets. Satoshi understood that heavy-duty infrastructure maintenance needed to be performed by people who are paid for their work—the miners, not everyday users.

Another example of economic misunderstanding was Bitcoin Core trying to protect the smallest nodes from getting kicked off the network. The developers had multiple opportunities to increase the blocksize limit, but they didn't want to risk kicking any nodes off the network, no matter how small. In fact, there's a whole movement of BTC supporters putting full nodes onto Raspberry Pis—computers so small that they cost about $30. So it's no surprise that BTC can't scale; every transaction on the network can still be processed with extraordinarily cheap equipment! From the perspective of scaling, the Core developers did the worst possible thing. They throttled the capacity of the network to the capacity of the smallest players and did not understand that it's perfectly healthy to have the smallest nodes kicked off the network as it grows. As Satoshi said, nodes will professionalize into "big server farms." That's what natural economic growth would look like.

The Hubris of Central Planners

Frederich Hayek is one of the best-known economists from the Austrian School. In 1974, he won a Nobel Prize in Economics for his academic work. One of his most famous books is called The Fatal Conceit, which is a brilliant examination of the problems with centrally-planned economies. He authored the famous quote:

The curious task of economics is to demonstrate to men how little they really know about what they imagine they can design.[2]

The more you learn about how free markets work, the more arrogant it seems to imagine that a better system could be designed by central planning. Markets are unbelievably efficient at coordinating scarce resources, and yet they do so without any central authority setting prices and production quotes for things. Hayek's famous quote continues:

To the naive mind that can conceive of order only as the product of deliberate arrangement, it may seem absurd that in complex conditions order, and adaptation to the unknown, can be achieved more effectively by decentralizing decisions and that a division of authority will actually extend the possibility of overall order. Yet that decentralization actually leads to more information being taken into account.[3]

In other words, free markets allow for a rapid flow of information between buyers, sellers, producers, consumers, growers, manufacturers, and every other participant in the economy. They are all trying to figure out what types of products to produce, in what quantities, out of what materials, for what costs, in which locations, through which manufacturing processes, and so forth. There's literally too much information for a central planning board to figure it all out. That's why it would seem silly for any one person to say, "The 'correct' price of shoes is $45 a pair." It depends on too many factors —what are the shoes made of, what is their quality, where are they being sold? Rather than having some committee decide the price of shoes for everybody, it's better to let individual entrepreneurs set prices themselves inside the marketplace, which results in more information being processed and better overall coordination.

These lessons are directly relevant to Bitcoin. Just like a free economy works better than a centrally-planned one, a free Bitcoin works better than a centrally-planned one. Bitcoin Core has been the central planning board for Bitcoin on many issues, whether it's imagining they know the "correct" blocksize, the "correct" level of transaction fees, or the "correct" number of nodes on the network. This is why Gavin Andresen said:

Central planning is why I would like to eliminate the hard, upper blocksize limit entirely, and let the network decide “how big is too big.[4]

In economic terms, the blocksize limit in BTC is a centrally-planned supply shortage. The demand for larger blocks is there, but miners are restricted from producing them because of an arbitrary limitation written into the software. BTC users are then forced to compete in an artificial “fee market” to get their transaction processed. The same thing happens in housing markets when central planners prevent new construction from being built. It causes a supply shortage and prices skyrocket. The basic economic principles of supply and demand apply to both the housing market and the cryptocurrency market. If left alone, miners will produce the best size block to meet demand.

The central planning tendency of the Core developers was not limited to the creation of unnecessary fee markets. They even used the blocksize limit to try and influence which projects other developers were working on. Core developer Wladimir van der Laan explained:

A mounting fee pressure, resulting in a true fee market where transactions compete to get into blocks, results in urgency to develop decentralized off-chain solutions. I’m afraid increasing the block size will kick this can down the road and let people (and the large Bitcoin companies) relax, until it’s again time for a block chain increase, and then they’ll rally Gavin again, never resulting in a smart, sustainable solution but eternal awkward discussions like this.[5]

Not only did the developers think themselves wise enough to set a mandatory maximum on the size of blocks, they also thought they could use high fees to incentivize people to work on their preferred projects. They were fine with the network buckling because it would create “urgency to develop decentralized off-chain solutions.” Talk about a fatal conceit! Of course, what actually happened was an exodus of developers from BTC who simply joined other projects that were more promising.

Trusting Incentives, not Individuals

The final part of Bitcoin's economic design that is commonly misunderstood is the role of trust. Just like the concept of "digital gold" has been taken too literally, the concept of "trustlessness" is also taken too literally. When Satoshi said that Bitcoin didn't require "trusted third parties," he did not mean that no trust in any humans whatsoever was required. Bitcoin is economic in nature, which makes it social in nature, which means it still requires some trust in humans. For example, a BTC enthusiast might run his own node, verify every transaction on the blockchain, and think he's operating without trusting anybody. But he's mistaken. He is actually trusting many people that he's never met. He trusts that the developers of his operating system did their jobs correctly. He trusts that the CPU manufacturers did their jobs correctly. He trusts that every single company involved in the production of his computer did not bug his hardware. He trusts that his ISP is connecting him to the internet in a secure way. He's essentially trusting thousands of people all over the world, though he's not trusting them individually. Instead, he's trusting the system of economic incentives that coordinates all of them to produce high-quality hardware and software. Even if the people in the production chain hate each other—or might even hate him personally—he trusts that the system will sufficiently reward good behavior and punish bad behavior to produce reliable products.

Bitcoin works the same way. The system was designed to operate without a central authority, so nobody has to trust any particular individual or company. But they do have to trust that the incentives are strong enough to create a reliable network. This trust cannot come from each individual analyzing the code for himself. It must come from seeing Bitcoin as a whole, which includes many humans and businesses acting in their own self-interest. When Bitcoin Core changed the incentives of the system, they fundamentally changed its whole design.

Satoshi's system was not perfect and did overlook a key problem: the governance and funding of Bitcoin's software development. Miners have strong incentives. Users have the correct incentives. But developers' incentives are murky and can result in conflicts of interest. In the case of Bitcoin Core, the structure of their decision-making process was flawed and ultimately derailed the entire project.

We have examined each of the Fundamental Five ideas for understanding the original design of Bitcoin:

1. Bitcoin was designed to be digital cash used to make payments over the internet.
2. Bitcoin was designed to have extremely low transaction fees.
3. Bitcoin was designed to scale with blocksize increases.
4. Bitcoin was not designed for the average user to run his own node.
5. Bitcoin's economic design is as important as its software design.

It should be clear that it's not a question of whether Bitcoin Core changed the original design. The question is whether you like their changes. In my opinion, their new design is not an improvement. In almost every way, other than price, it seems worse than the Bitcoin of 2013.

9

The Lightning Network

Even the most vocal Bitcoin Maximalists will admit that, in the long run, there needs to be a way to make Bitcoin usable as money in everyday commerce. But they do not want the base layer to provide that functionality. Instead, they want regular payments to be conducted on secondary layers like the Lightning Network. Small-blockers have been arguing that the blocksize limit does not need to be raised because the Lightning Network solves Bitcoin's scaling problems—they made this argument years before Lightning even existed. Despite the hype, the reality of the Lightning Network is grim. It has several critical design flaws that make it insecure, cumbersome, and unlikely to ever gain mainstream adoption. Each attempt at solving Lightning's problems has created new layers of complexity that come with new sets of problems—a terrible sign from the perspective of software development.

Here's a basic overview of the Lightning Network's design. The technology is based around "payment channels," which is essentially a running balance between two parties. Say Alice opens a payment channel with Bob and funds it with $10. The initial balance would be $10 for Alice and $0 for Bob. If she sends him a $3 transaction, the new balance would be $7 for Alice and $3 for Bob. Bob could send her back $1, and the new balance would be $8 for Alice and $2 for Bob. None of these transactions are recorded on the blockchain; their nodes keep track of the tally separately, off the chain. At any point, either party can close the channel, which then distributes the final balances to both people with an on-chain transaction.

Payment channels are a neat technology that has been worked on since the beginning, even by Satoshi himself. However, they were not being worked on as a scaling solution. Instead, they were being designed for tiny micropayments and high-velocity two-way transactions, which are used in special circumstances like machine-to-machine payments. Payment channels are great for micropayments because they allow tiny amounts to be sent back and forth between parties without incurring on-chain transaction fees.

The Lightning Network is an attempt to link payment channels together to create a secondary layer that can route everyday Bitcoin payments. So, if Alice wants to send money to Charlie, but she does not have a payment channel with him directly, she can route her payment through Bob, who does have a channel open with Charlie. For this service, Bob gets a tiny transaction fee. Ideally, the payments on Lightning would be instant, have extremely low fees, and could scale Bitcoin without having to increase the blocksize limit since most of the transactions are happening off-chain. Unfortunately, Lightning does not work well in practice because it has several system-breaking design flaws.

On-Chain Transactions

The most fundamental problem with the Lightning Network is that it requires on-chain transactions in order to use. Opening and closing a payment channel requires making on-chain transactions, and it is recommended to open multiple channels at the same time. These channels are not permanent; they require ongoing maintenance and are supposed to be refreshed annually. The requirement for on-chain transactions creates two critical problems:

1. Users must pay on-chain transaction fees just to open or close channels. If the base layer is being used as a settlement system between banks, these fees could cost hundreds or thousands of dollars just to connect to the Lightning Network.
2. Since onboarding to the Lightning Network requires on-chain transactions, it is mathematically impossible to onboard large numbers of people with 1MB blocks.

Problem (1) is straightforward, but it's often hidden from regular users. The most popular Lightning wallets are either custodial—which means users' funds are controlled by a company—or the wallet will commonly subsidize the on-chain transaction costs. Both situations are undesirable. Custodial Lightning eliminates all the benefits of using Bitcoin in the first place, and it's only possible for companies to subsidize on-chain transaction fees while they are low. If fees are consistently above $50 or $100, there is no way companies will continue subsidizing them. The Lightning Network does not avoid the pain of having high layer-one fees.

Problem (2) is also straightforward and has been recognized since the Lightning whitepaper was written. With extremely limited block space, even if every BTC transaction was solely used for opening a payment channel, there is not enough space to onboard more than a few thousand people per block. Paul Sztorc, a notable BTC supporter and developer, wrote an article breaking down the numbers in more detail. He concluded that even if 90% of the block space is dedicated to opening channels, only around 66 million people can be onboarded per year—that means it would take around 120 years to onboard the world to the Lightning network. He concludes:

In other words, each year we'd only onboard 0.82% of the world.

Worse: if channels last merely one year, then by Jan 1 2025, we will need to re-onboard the people who joined on Jan 1 2024. In that world, only 0.82% of Earth's population, max, can be bona fide Bitcoin users (at any one time).

Monetary network effects are very strong – you need to use the money that other people are using. So a 0.82% ceiling is not viable.[1]

Sztorc's proposed solution is to have a big block "sidechain" (explained in Chapter 13) that can onboard more users. My solution is to just use big block Bitcoin instead, which does not need the Lightning Network to be viable at global scale. The requirement to have larger blocks is why Joseph Poon wrote in the Lightning whitepaper:

If all transactions using Bitcoin were conducted inside a network of micropayment channels, to enable 7 billion people to make two channels per year with unlimited transactions inside the channel, it would require 133 MB blocks (presuming 500 bytes per transaction and 52560 blocks per year).[2]

This is the author of the whitepaper explaining that the Lightning Network at global scale would still require 133MB blocks! Unlike today's small-blockers, he then notes that 133MB blocks are still a feasible size:

Current generation desktop computers will be able to run a full node with old blocks pruned out on 2TB of storage.

The Lightning Network requires multiple on-chain transactions in order to use. Therefore, a 1MB, 2MB, or even 10MB blocksize limit would make it

impossible to be a real scaling solution. Regular users are not going to be eager to spend $50 or $100 to open a payment channel, but even if they were, the BTC blocksize limit is simply too small to accommodate mass usage.

Online Nodes

The Lightning Network requires users to run their own nodes. This fact famously perplexed Tone Vays, the popular Bitcoin personality. He apparently did not understand this basic feature, despite relentlessly promoting Lightning as an alternative to blocksize increases. In a YouTube conversation with Jimmy Song, he starts by fielding a question from the audience:

Vays: Here's a good question for you, Jimmy. Someone says "What benefit do I get from setting up my own Lightning node?"

Song: Uh, you can go and pay people, like in Lightning…

Vays: Wait a minute, I need clarification on that. Do I need to have a Lightning node in order to pay people through Lightning?

Song: Yes.

Vays: Really?

Song: Yes, because the only way you can pay anyone is by having a channel, and you can't have a channel unless you have a node.

Vays: But, do you need your own node, or do you need someone else's?

Song: You need your own node…

Vays: Oh wow, so every single person might need their own Lightning node?

Song: Yeah…[3]

The requirement to run your own node is difficult enough for everyday users because the nodes require ongoing monitoring and maintenance. But there's

an additional requirement that makes it crippling: each node has to remain online or they risk losing funds.

The way Lightning is designed, while a payment channel is open, both parties have a history of all the previous states the channel has been in—an individual record for when Alice had $10 and Bob had $0, then when Alice had $7 and Bob had $3, etc. When a channel closes, the "final" balance is broadcast by whichever party is closing the channel. However, instead of broadcasting the most recent balances, they can broadcast previous states of the channel, which allows Alice to potentially steal from Bob. Imagine that their last transaction resulted in a balance of $1 for Alice and $9 for Bob. If Alice closes the channel, instead of broadcasting the latest balance, she can broadcast an earlier state with an old balance, like when she had $10 and Bob had $0. If Bob does not catch her, then Alice will end up stealing a total of $9.

The Lightning Network tries to solve this problem by making it risky to publish old channel states. If Bob catches Alice within a two-week timeframe, he can broadcast a newer state, demonstrating that Alice published an old one. If this happens, all the funds in the channel go to Bob. This is supposed to provide an incentive to not cheat, but it's a weak one. If Alice already has a low or zero balance on the channel, she does not have much to lose by trying to steal. Also, in order to catch somebody, a node is required to be connected to the internet. If Bob's node goes offline, he cannot tell that Alice is stealing from him, and he can lose funds. This is why some Lightning proponents have suggested having a battery backup for nodes.

Lightning developers have tried to fix this problem by creating "Watchtowers," which are third parties that watch over the channel to make sure nobody is cheating, even if one node goes offline. This new system adds another layer of complexity, and it requires watchtowers to be trustworthy and competent, otherwise users can lose their funds. The problem of trust is simply pushed back one more step—i.e. the watchtowers need their own watchtowers.

In addition to the security risk, offline nodes cannot even accept payments, nor can they route payments for other people. Lightning requires both parties

to be online at the same time, and the sender cannot send any arbitrary amount of Bitcoin to the recipient. The recipient must generate a specific invoice for the sender to fill—hence, the requirement to be online.

The requirement to be online is also a security risk because it means the users' Bitcoin keys are held in a so-called "hot wallet," meaning it's connected to the internet. Standard security in Bitcoin has always been to keep the majority of your coins in offline "cold storage," while only keeping small amounts in wallets that are connected to the internet. Hackers are far more likely to succeed when targeting hot wallets, which the entire Lightning Network is composed of. The only way to get coins from the Lightning Network into offline cold storage is by making an on-chain transaction.

Liquidity and Routing Problems

Routing payments through the Lightning Network is another serious problem. Every payment needs to find a definite path from sender to receiver. If Alice wants to pay Donald but does not have a channel open with him directly, she has to find a route to him through other channels. She might have to send her payment through Bob first, who then sends it to Charlie, because Charlie has a channel open with Donald. If Donald is not well-connected enough with the network—if he does not have enough payment channels open with other well-connected parties—the software will not be able to find a path to him and the payment will fail.

But merely finding a route is not sufficient. Each channel along the path also needs to have sufficient liquidity within it for the payment to go through. If Alice wants to send a $100 payment to Donald that routes through Bob and Charlie, but the channel between Bob and Charlie has only $50 of liquidity in it, the payment cannot go through. In practice, this results in frequent payment failures, especially for large-value transactions.

To understand payment channels better, the best analogy is that of beads moving along a string. A channel is like a string connecting two people, and the beads are its liquidity. Let's say Alice opens a channel with Bob and puts 50 beads on the string. To pay for coffee, she moves five beads from her side over to Bob's. Then, to pay for a pack of gum, Bob moves one back to Alice.

When the payment channel closes, assuming neither person is trying to steal from the other, Alice and Bob will receive the correct distribution of beads based on their final location.

If there are not enough beads to process a payment, the network runs into liquidity problems. If Alice and Bob's channel only has 50 beads on it, it's impossible for them to route any payments that are larger than 50 beads—there's simply not enough beads to move. Compounding problems even further, to make a payment on the Lightning Network, a route must be found from Alice to Donald where every hop has sufficient liquidity, and these balances are constantly in flux. Every time a payment is routed through Bob's channel, its available liquidity changes. Therefore, not only are payment channels constantly opening and closing on the network, but their respective balances are also changing too. Imagine billions of people using this system, each having multiple payment channels open with constantly changing balances. The simple task of routing becomes an extremely complex one, which might even be impossible to solve without widespread centralization of the network. Rick Falvinge, the IT entrepreneur turned Swedish politician, concluded in a series of videos about Lightning:

Mesh routing is an unsolved problem in computer science, especially when you have adversaries in the network… I'm considering the Lightning Network a dead end... It is not going to gain adoption. It is going to remain a toy that will be tinkered with and eventually left by the wayside.[4]

Andreas Brekken, the founder of the popular Sideshift cryptocurrency exchange, came to a similar conclusion. I asked him about his experience using Lightning for his business, and he said:

Routing is a serious problem on the Lightning Network. Payments frequently fail to route, and the way I have tried to mitigate this problem is by being connected to the largest exchanges. But even that does not solve the problem completely. I have to use software that estimates the probability of a successful payment, and if the percentage is not high enough, I simply do not send the payment.

Frankly, large numbers of Bitcoin users are being tricked into thinking this thing can work, but after having incorporated it into my business, I just don't

think it will.

From a usability perspective, the best possible outcome for Lightning would be to have totally custodial wallets connected to the largest exchanges. But of course, that kind of defeats the purpose of Bitcoin in the first place.

Brekken is correct. If the Lightning Network is going to have any chance of success among the general public, it will require massive centralization into a “hub and spoke” network and widespread use of custodial wallets.

Hub and Spoke Model

Centralization is the one reliable way to lessen the severity of the problems with the Lightning Network. Custodial wallets eliminate the burden to run your own node and be online all the time. Routing is easier if everybody connects to the same giant hubs that have enough connectivity and liquidity to service millions of people—if everybody opens a channel with PayPal, then the chances of finding a route are high. Big companies will not merely participate in the Bitcoin economy, users will be forced to rely on them to have basic payment functionality, and just like with custodial wallets, they can be easily censored and cut off from the rest of the network.

The centralization of the Lightning Network is inevitable and has been predicted for years. In fact, it’s even been the subject of academic research. The structure of the network is called a “hub and spoke model”—resembling the spokes on a wheel— where small nodes connect to larger nodes, which are connected to a few super-nodes.

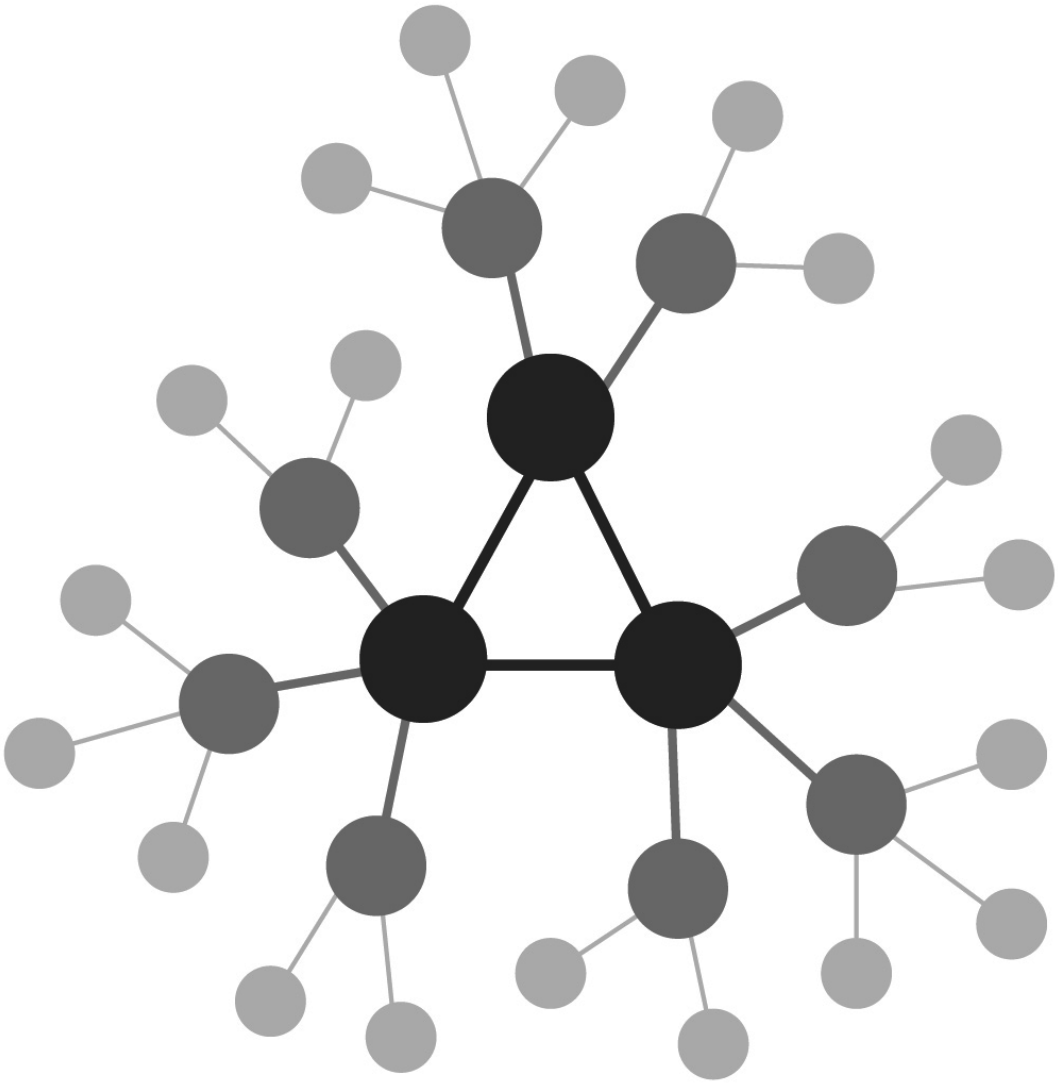


Figure 3: Diagram of a hub and spoke network

Crucially, this is not a distributed peer-to-peer network, where nodes connect directly to each other. With on-chain payments, Alice has a direct connection to Donald. With Lightning, Alice must go through Bob and Charlie first. The largest nodes become essential to the smooth functioning of the entire network, and these huge nodes will have the power to censor. They will be hosted by companies that are easy to regulate. And when they are taken

offline for whatever reason—due to failure, regulation, or simple maintenance—the connectivity of the network will be seriously damaged. Everyday users can be completely severed from the network if their link to a central hub goes down. Alice might not find any route to Donald without being forced to go through the equivalent of PayPal.

A group of academic researchers wrote about these risks in a 2020 paper entitled "Lightning Network: a second path towards centralisation of the Bitcoin economy."[5] They wrote:

[T]he BLN ["Bitcoin Lightning Network"] is becoming an increasingly centralised network, more and more compatible with a core-periphery structure. Further inspection of the resilience of the BLN shows that removing hubs leads to the collapse of the network into many components, an evidence suggesting that this network may be a target for the so-called split attacks.

These researchers put forward several mathematical and empirical arguments which demonstrated that the centralization tendency is inherent to the network design and concluded:

The tendency to centralisation is observable even when considering weighted quantities, as only about 10% of the nodes hold 80% of the bitcoins at stake in the BLN (on average, across the entire period)… These results seems to confirm the tendency for the BLN architecture to become "less distributed", a process having the undesirable consequence of making the BLN increasingly fragile towards attacks and failures.

Liquidity problems also add to these centralization pressures, along with the requirement to use a wallet that is always connected to the internet. Most people will not be willing to lock up thousands of dollars in their payment channels, especially because of the increased risk of being constantly online. This means large payments will inevitably be forced to route through large, corporate payment hubs that have sufficient liquidity and technical skills to ward off hackers.

The inevitable centralization of the Lightning Network is ironic, considering the mad crusade the Core developers took to avoid centralization by

overhauling Satoshi's original design. Not only is Lightning infinitely more complex, clunky, and less reliable than on-chain transactions, the network will end up being orders of magnitude more expensive for every user because the on-chain payments required to use it will cost hundreds or even thousands of dollars. And if a user ever gets banned from a central payment hub, they will be forced to make additional on-chain transactions to maintain connectivity to the rest of the network. If these transactions cost thousands of dollars each, then getting banned from the hubs will prevent most people from using Bitcoin at all.

With Satoshi's design, the network can be disrupted by an expensive 51% attack. With the Lightning Network, the cost of disruption will plummet. Governments or malicious actors can simply target the largest payment channels. If they can knock out a handful of critical hubs at once, then the network will become virtually unusable. Hashrate is not required.

A False Promise

The viability of BTC now relies on the development of secondary layers. If the secondary layers cannot deliver cheap, reliable payments, then BTC has no way of scaling—at least not without admitting spectacular failure and raising the blocksize limit, or by total centralization with custodial wallets. The way the technology currently stands, the Lightning Network will not be a serious solution to the problem of high on-chain fees, and it will not enable regular people to use BTC in commerce. Payment channels are a neat technology, but they are not a scaling solution. They might be helpful for micropayments, as Satoshi thought, but not for everyday transactions. Perhaps some future technology will be developed which would rescue BTC, but for now, the original design working on BCH remains the best system for fast, cheap, peer-to-peer payments online. The simplicity and elegance of the system are unmatched; fees remain low; there are no requirements to run your own node; payment hubs are not necessary, and there's nothing preventing secondary layers from being built on top of BCH —in fact, the larger blocksize allows for even better functionality of secondary layers.

I want Lightning to live up to its promises, because if it could, then the world would be a better place. But I currently have no reason to believe this

will happen. All signs point to it being a failed experiment, an embarrassment to the Core developers, and a demonstration that the Bitcoin Maximalists pushing this technology as a replacement for on-chain transactions were completely wrong and have misled millions of people.

It's hard to imagine a more effective way of disrupting Bitcoin than what actually occurred. Over the course of several years, BTC changed from the best payment system on the internet to a slow, expensive, unreliable one. Satoshi's brilliant design was discarded for the promise of a future technology which has not lived up to its hype. This failure has both innocent and malicious interpretations. Bitcoin's story might simply be an example of bad project management, but given the disruptive power of this technology, it looks more likely that Bitcoin was sabotaged by its enemies.

Part II:

Hijacking Bitcoin

10

Keys to the Code

Bitcoin is often spoken about as if it exists beyond the reach of human influence, as incorruptible as the laws of physics. The network is supposedly too large and decentralized for any group to control, no matter how powerful. According to The Bitcoin Standard:

Bitcoin's value is not reliant on anything physical anywhere in the world and thus can never be completely impeded, destroyed, or confiscated by any of the physical forces of the political or criminal worlds. The significance of this invention for the political realities of the twenty-first century is that, for the first time since the emergence of the modern state, individuals have a clear technical solution to escaping the financial clout of the governments they live under.[1]

This is a beautiful concept, and I truly wish Bitcoin worked this way, but unfortunately, history demonstrates otherwise. Bitcoin is very much a human project and is not immune from individual and institutional corruption. Social and political factors are overwhelmingly important and have been since the beginning.

A Reality Check

Confiscation has already become easy due to the trend towards custodial wallets. It happens all the time. Because the blockchain is public, governments can mark particular coins as suspicious and track them throughout the ledger. If the coins arrive at a centralized cryptocurrency exchange, as they usually do, the exchanges will freeze the corresponding accounts and notify the authorities. The coins in question can then be seized with a few clicks. Even if the coins do not move to a centralized exchange, they have likely moved from one, which—due to compliance with know-your-customer laws—gives the government the identity of at least one person who has touched those coins. From that point, they can surveil the blockchain to track the economic activity of that individual and work out plausible identities for anybody they have transacted with. This already

happens when Bitcoin is involved with large criminal cases, but there is no fundamental reason why it couldn't happen to everyday users.

The idea that Bitcoin is a "clear technical solution" to the threat of physical force from political actors is naive. If the government suspects you are hiding something, they can investigate as they would any other situation. They can demand you turn over your financial records, private keys, and electronics. If you refuse, they can gain entry to your home, imprison you, and confiscate your property. Bitcoin does not emancipate you from the physical world or prevent the government from threatening you with violence. A savvy technical user might be able to avoid confiscation or destruction of their savings, but average users will have a difficult time.

The financial freedom that Bitcoin does provide is maximized with non-custodial wallets. Though not perfect, the ability to track and confiscate coins is greatly reduced when regular users can access the blockchain for themselves at little cost and do not have to use centralized wallets or exchanges—analogous to using physical cash. Physical cash transactions are far harder to control than electronic transactions that go through banks or payment processors like PayPal, which is one reason why governments around the world want to move away from physical cash and towards digital currencies they control. That's why peer-to-peer digital cash is such a revolutionary concept; it keeps more power in the hands of regular people while giving them the convenience of electronic money.

The Governance of Bitcoin

Like the concepts of "digital gold" and "store of value," the famed "decentralization" of Bitcoin is more of a marketing slogan than a reality. In fact, one of the central stories of Bitcoin is how a small group hijacked the project despite the objections of most of the network. One group has consistently demonstrated they have more power and influence than any other: the software developers. The people that maintain and update Bitcoin's code are the people with the most influence over the network. For most cryptocurrency projects, not just Bitcoin, developers call the shots. And notably, software developers don't finance themselves. They have to get paid somehow. Therefore, the real power dynamics within a cryptocurrency project are determined by how its software developers make

decisions and get paid. The history of BTC is a cautionary tale of what happens when the incentives of developers become misaligned with the rest of the network.

Bitcoin is famously an "open-source" project, which means all the code is made public and anybody can freely view, use, and modify it without burdensome licensing constraints. This feature is often misrepresented by those who want to claim there are no centralized authorities controlling the software. All the rhetoric surrounding Bitcoin development makes it sound like the process is open and meritocratic—that if you write good code it will be automatically incorporated into the software. Even the Bitcoin.org website reads, "Bitcoin is free software and any developer can contribute to the project."[2] But that's simply not true. There are strict hierarchies that determine what code gets added to the software, and there are specific individuals who have the power to approve or reject code changes. If you have a different philosophy than these individuals—for example, if you agree with Satoshi and think the blocksize limit should be raised or eliminated—then no matter how good your code is, they won't incorporate it.

To contribute any code at all, you must persuade the right people. If they don't like your idea, or if they don't like you personally, they can simply ignore you. Bitcoin development is a social phenomenon like any other. Instead of saying, "Anybody can contribute to the project," it would be more accurate to say, "Anybody that agrees with the philosophy of a handful of Core developers and their vision for Bitcoin, accepts their development processes and hierarchies, and is socially approved by them can submit code for their evaluation!" But that doesn't sound like decentralization, does it? The reality of the situation was summed up well by Professor Hilary Allen from American University. In a congressional hearing in late 2022, she told a panel of US senators:

[We] typically hear that "crypto is different" because it's decentralized, but in fact, it's not decentralized. At every level, there are people controlling things.

We heard that Bitcoin is decentralized. Well, Bitcoin is controlled by a few core software developers—fewer than ten—and they can make changes to

the software, and then that software is implemented by mining pools, and there are just a few of them. So in all of these spaces, there are definitely people—often very few people—pulling the strings.[3]

She is not wrong, despite her conclusions invalidating the common narrative about Bitcoin's software development. The most insistent supporters who claim that the software is not centrally controlled will point out that, technically, anybody can download Bitcoin's source code, open it up, and modify it on their own computer. While this is true, it's misleading. Changing the code on your computer doesn't change the code that everybody else is running. If you modify the wrong parts, like the blocksize limit, you will get instantly forked off the network. The "official" software that everybody downloads—that approximately 99% of the industry uses—is controlled by a handful of people who hold the keys to the code. They ultimately determine what gets added, subtracted, and modified for everybody else.

The Succession of Keys

The mere fact that Bitcoin Core's software development has a governance structure is not inherently a bad thing. Decisions have to be made somehow. No software project could succeed if anybody could change the code on a whim. But given that hundreds of billions of dollars are now wrapped into this network, exactly who gets to update the code and how?

The keys to Bitcoin Core's development have gone through a specific progression. In January 2009, the governance was straightforward: Satoshi Nakamoto was the man in charge. All code changes had to be approved by him personally, and there were no objections to his authority. In an interview in 2015, Gavin Andresen recalled the early governance process:

If you go back in history, it was really simple. It was whatever Satoshi decided at the beginning, and that's really where we started. We had one source code. We had one pseudonym/person who made all the decisions about 'what should Bitcoin be', 'how should it evolve, 'what should it do.' That's where we started.[4]

By the end of 2010, Satoshi decided that he needed somebody else to run the project. So he chose Andresen, who shared the same vision for Bitcoin. On December 19, 2010, Andresen wrote in the forums:

With Satoshi's blessing, and with great reluctance, I'm going to start doing more active project management for bitcoin. Everybody please be patient with me; I've had a lot of project management experience at startups, but this is the first open source project of any size I've been involved with.[5]

Andresen became the figurative "heir" of Satoshi and was the Lead Maintainer until 2014. Unlike Satoshi, he was not the only person allowed to make code changes, because early on, he decided to give a handful of others this power. He explained why:

As soon as Satoshi stepped back and threw the project onto my shoulders, one of the first things I did was to try to decentralize that, so that if I got hit by a bus, it would be clear that the project would go on. And so that's why at this point there are five people who have commit access to the Github Bitcoin source tree.[6]

Andresen's decision was reasonable and well-intentioned, but unfortunately it had unforeseen consequences and looks like a strategic mistake in hindsight. He gave a handful of other people "commit access"—that is, the ability to change code on the official online repository—but they were not all aligned with Satoshi's vision for big blocks and low-fee transactions. Some apparently thought they could design a better system. Philosophical differences between the developers caused extreme development delays and factions to emerge. Eventually, one faction formed their own company, and shortly afterwards, the different groups turned into hostile camps.

In 2014, Andresen said he was shifting from the day-to-day maintenance of Bitcoin Core to higher-level research and chose Wladimir van der Laan as his successor. Van der Laan was an active contributor to Bitcoin's code, but he ended up being the most passive of the three project leaders, allowing critical decisions to go unresolved. Mike Hearn shared his frustration with the lack of competent leadership in Bitcoin Core in 2015:

What we've seen in Bitcoin Core is it started out as the traditional open source project. Satoshi was in charge. Then he delegated to Gavin, and Gavin was in charge, and then Gavin delegated to Wladimir, and Wladimir was in charge, and that's completely normal for any technical project. You have one leader who listens to input from people and makes the decision. Wladimir, unfortunately, prefers to not make decisions, I would say. I don't think he would disagree with his characterization. When there's a sort of dispute, he tends to stand back and try and hope that it resolves itself into a nice consensus, where everyone agrees, and when that doesn't happen, he just sort of ignores what's happening.

So Bitcoin Core sort of devolved over the last few years into this rule-by-consensus—but it's actually much closer to anyone who wants having a veto, because as long as anyone is objecting or making vaguely intellectual-sounding objections, then there's no consensus, and therefore change won't happen. [This] has become a huge problem, especially because some of the people who have commit access and love to make these sorts of arguments… they enjoy coming up with complicated theories and complicated proposals for redesigns of Bitcoin… and then what tends to happen is the more practical day-to-day needs of developers get lost.[7]

These issues were never fixed and eventually caused Hearn to leave the project altogether in 2016. On his departure, he published a fantastic essay entitled "The Resolution of the Bitcoin Experiment" which has since become mandatory reading for anybody trying to learn about the theory and history of Bitcoin. In it, he explains why the governance structure failed, causing BTC to fail from the perspective of its original design:

In a company, someone who did not share the goals of the organisation would be dealt with in a simple way: by firing him. But Bitcoin Core is an open source project, not a company. Once the 5 developers with commit access to the code had been chosen and Gavin had decided he did not want to be the leader, there was no procedure in place to ever remove one. And there was no interview or screening process to ensure they actually agreed with the project's goals.

As Bitcoin became more popular and traffic started approaching the 1mb limit, the topic of raising the block size limit was occasionally brought up

between the developers. But it quickly became an emotionally charged subject. Accusations were thrown around that raising the limit was too risky, that it was against decentralisation, and so on. Like many small groups, people prefer to avoid conflict. The can was kicked down the road. Complicating things further, [Core developer Greg] Maxwell founded a company that then hired several other developers. Not surprisingly, their views then started to change to align with that of their new boss…[8]

I agree with Hearn's analysis and have often wondered what would have happened if Andresen had chosen different developers to share his authority with, or if he had remained the only person with commit access, or if the industry had rejected the Bitcoin Core developers entirely and had chosen a different team—a situation that almost occurred in 2015, 2016, and again in 2017. To understand how the software development became so centralized, it's helpful to first understand where Bitcoin Core came from.

The Origins of Bitcoin Core

Before 2013, there was no such thing as "Bitcoin Core." Until then, everything was referred to as "Bitcoin"—the software, the currency unit, and the network—which caused unnecessary confusion for a project that already had a reputation for being confusing. So, in November 2013, a proposal was put forward to change the name of the software:

To remove the confusion between the Bitcoin network and the reference client implementation that we maintain in this repository, both confusingly named 'bitcoin', we'd like to rebrand the client.[9]

This proposal did not cause any controversy. Gavin Andresen agreed with it stating, "Now is a good time to change names, let's do it." From that point onward, the software was renamed "Bitcoin Core" and its developers became the "Bitcoin Core" developers. Despite what transpired over the subsequent years, the origins of Bitcoin Core were not nefarious.

After Satoshi's departure, Bitcoin Core was not even supposed to be the only software implementation of the Bitcoin protocol. The idea was to have multiple implementations, not just the Core software, so that specialization could happen. Miners, for example, might create their own version that

focused on fast transaction validation, while nodes could specialize on other features. During an excellent interview in 2015, Andresen explained:

It's really important for people to separate in their head "Bitcoin" the protocol—you know, Bitcoin the system that we're all using to transact—and the Bitcoin Core open-source software project that lives on Github and a bunch of people are contributing code to. They really aren't the same thing. I call Bitcoin Core the "reference implementation," and I've called it that for years, and that implies that there will be other implementations of the Bitcoin protocol.[10]

It's not hard to understand why having multiple implementations is a good idea. In addition to catching bugs that one team might overlook, having multiple implementations is the most straightforward way to prevent developer capture. For a project that is supposed to be about the decentralization of power, it would be a critical flaw to allow a single group to control the software development for the entire network. Andresen continues:

When we think of governance, we have to think about the governance of 'how will the protocol evolve' as separate from 'how will Bitcoin Core, the reference implementation code, evolve and be governed'. I think there are two separate governance processes, [but] because we started with this one source code that defined the protocol and was all anybody was ever running, in a lot of people's heads, they don't make that separation.

But I think it really is important to think of the protocol separately from this one source code… I've been saying for a while that I want to get to a point where there are multiple robust implementations.[11]

Mike Hearn shared this view and thought it was essential to having real decentralization. On the surface, it might seem that Hearn's desire to have a single person like Satoshi making final software decisions is at odds with the ability to maintain a decentralized project, but he explains why these two ideas are compatible:

Interviewer: If we assume that Bitcoin Core keeps having this [influence] determining the rules, then I find the argument a little bit strange that those

five people can agree, “Well let’s just give all the power to one person.” I mean, that may be fine as long as Gavin is there and he’s a rational guy, but that really seems to be in conflict with the whole idea of a decentralized system…

Mike Hearn: Not at all. The decentralization of Bitcoin doesn’t come from the fact there’s like five guys instead of three or two, right? Or even instead of one. [With] one to five people, you might as well say, “The central bank has a committee that sets monetary policy, so the Dollar is decentralized.” It doesn’t make any sense to view the system that way.

The decentralization in Bitcoin comes from the fact that everyone can audit the blockchain and check the rules for themselves. It comes from the fact that there’s a competitive market of implementations and, ultimately, from the fact that people can switch to other implementations and fork the blockchain if they want to.[12]

Other implementations did eventually arise in BTC. Once it became clear that the Core developers were refusing to increase the blocksize limit, the industry tried to upgrade to other implementations, on multiple occasions. But each time, these alternatives were attacked along with the businesses that supported them. Everything from denial-of-service attacks to fake app reviews, mass censorship, and social media smear campaigns were used to discourage people from using alternatives to Bitcoin Core—which is why their software is run by approximately 99% of nodes in BTC today and the people who want big blocks use alternative coins like Bitcoin Cash. The failure to decentralize software development resulted in a project totally dominated by a single group that maintains a single code repository on Github.

Now that the changes to Bitcoin’s design are understood, along with its centralized development structure, the history of Bitcoin can be reconstructed with more clarity.

11

The Four Eras

There will never be a single, authoritative history of Bitcoin because the story is too complex for any one person to see the whole truth. I can share my own perspective, memories, and personal experiences, which I know are similar to other early adopters and businessmen that worked with the technology from the beginning. In my mind, Bitcoin has gone through four different eras, each with its own culture, leadership hierarchy, level of industry development, and relationship to the general public. These eras blend into each other and do not have precise start or end dates, but they are still a helpful tool for reconstructing history to better understand the present moment.

Era:	First	Second	Third	Fourth
Culture:	Techies and libertarians	Growth-focused	Civil War	Price-focused
Leadership Hierarchy:	Satoshi Nakamoto	Gavin Andresen	Contested	Bitcoin Core
Industry development:	Non-existent	Young	Growing	Mainstream
Public awareness:	Unknown	Skeptical	Hyped	Mainstream

1) The First Era: Obscurity
From ~2009 through ~2011

The first era was defined by obscurity. With all the constant news coverage and hype today, it might be hard to believe that Bitcoin was virtually unknown for years. The entire community existed within a few online forums, cryptography mailing lists, and niche libertarian circles. It took

several years before it gained any serious public attention. In the earliest days, it wasn't clear that Bitcoin would even work, let alone become an international sensation. Even the original pioneers saw it as a technology with an uncertain future. Gavin Andresen warned on his blog in 2012:

DISCLAIMER: I've been saying this for a couple of years now, but it is still mostly true: Bitcoin is an experiment-- only invest time or money in it that you can afford to lose![1]

My experience of the first era began in late 2010, when I first heard about Bitcoin on the radio show Free Talk Live. The technology sounded too good to be true—fast, cheap, digital money that wasn't issued by a central bank or controlled by political forces. I knew if it worked as advertised, it could usher in a new era of global prosperity and freedom. So, I had to find out more. The next ten days were intense, as all my free time was spent learning about Bitcoin. I scoured the internet for every new piece of information—articles, blog posts, forum conversations, anything that discussed the new technology. My nights got later, and eventually my sleep turned into short naps. I would wake up and immediately continue researching.

My enthusiasm got me into trouble. While my mind loved learning about Bitcoin, my body did not. I wasn't eating enough food or getting enough sleep, and that pesky scratch in my throat kept getting worse. After ten days of this, my health deteriorated to the point where it couldn't be ignored. I was completely exhausted and couldn't even drive myself to the doctor. So I called my friend Kevin, and he took me to the hospital. Doctors are familiar with cases of binge-drinking, but I might be the first person admitted to a hospital for binge-reading! They told me that I needed to calm down and sleep. They gave me a sedative, and after sleeping for almost twenty hours straight, I felt much better. I left the next day and decided to resume my research (at a slightly slower pace, of course). That was the beginning of my journey with Bitcoin.

While the early pioneers were careful to not be overly optimistic about the new technology, I was not so careful. I thought Bitcoin was going to change the world and was convinced it would improve the lives of billions of people. I knew I needed to buy some, since such a valuable invention was practically guaranteed to increase in price. But in those days, it was difficult

to purchase any. Bitcoin was almost unheard of, and only a few enthusiasts were trading coins on obscure websites.

The first major Bitcoin exchange was actually a re-purposed website that was originally created to trade Magic: The Gathering playing cards. Compared to modern cryptocurrency exchanges, the user experience wasn't exactly smooth. To purchase my first Bitcoins, I couldn't use PayPal, an ACH deposit, or a credit card. Instead, I had to send a wire directly to the personal bank account of Jed McCaleb, the website owner. Fortunately, he came through, and I successfully acquired my first Bitcoin for less than a dollar each.

At the time, I couldn't really use my Bitcoin, since nobody accepted it as payment. So, I decided that my company MemoryDealers.com would be the first. We sold computer parts online, and to my knowledge, we became the first retailer to accept Bitcoins for payment. I knew from my experience with eCommerce that there was a huge demand for online currency that could be used anywhere with minimal fees—and the more that Bitcoin could be used in commerce, the more valuable it was going to become, and the more freedom it would bring to the world.

Selling our products for Bitcoin turned out to be a good decision, because Bitcoiners from around the world were eager to spend their new digital currency. Not only did our sales increase, but it was also a great way to accumulate more Bitcoin. Instead of sending personal bank transfers, I was simply selling goods online in exchange for Bitcoin. Shortly afterwards, we put up a now-famous sign in Silicon Valley proudly advertising that "We Accept Bitcoin." I'm sure 99.9% of the people who saw it had never heard of Bitcoin, but that was the point.

Figure 4: Our billboard declaring “We Accept Bitcoin”

For most of the first era, Satoshi provided the main ideological and technological leadership. In the early forum posts, he received many questions about Bitcoin’s design, especially about scaling, and he provided compelling answers which framed the vision that attracted so many people into the project.

2) The Second Era: Growth and Optimism
From ~2011 to ~2014

The second era was defined by the growth of a brand-new industry and the infectious optimism throughout the entire Bitcoin community. The foundations of a new financial system were being constructed, and I got to lay some of the bricks. It was one of the most exciting times in my entire

life. We Bitcoiners were a small group, but we had something special. Not only was there money to be made, but we all knew there was a huge opportunity to change the world in a positive direction.

At that time, there was no real commercial infrastructure; we were starting from scratch. We needed more merchants to accept Bitcoin, more exchanges to trade it, and easier tools for its usage. We needed new companies to be created, but in 2011, the venture capital industry hadn't yet discovered Bitcoin. So, I ended up being the world's first investor in Bitcoin startups. The market was so young that almost any successful investment benefitted everybody, especially if it tackled the basic problems we were all facing. For example, price volatility was a notorious issue that made merchants hesitant to accept Bitcoin for payment. So, I jumped at the opportunity to provide seed funding for BitPay, a startup that allowed merchants to accept Bitcoin and immediately convert it into fiat, eliminating the volatility risk. Their service proved crucial to gaining mainstream adoption, and BitPay has since become one of the most important companies in the entire cryptocurrency world.

Other early investments were in companies like Blockchain.info, which let users spend and receive Bitcoin without downloading any software by creating an online wallet that was accessible with a web browser. Kraken, BitInstant, and Shapeshift made it far easier for the public to acquire Bitcoin, while Purse.io allowed them to spend their coins on Amazon. Though the nickname "Bitcoin Jesus" has stuck, I like to think my role in Bitcoin's history is closer to being "Bitcoin Johnny Appleseed" for helping to seed many of the earliest companies with funding.

Perhaps the most fun problem to solve from this era was the simple lack of awareness about Bitcoin. Everywhere I traveled, I would ask people if they accepted it. Most of them, of course, had no idea what I was talking about. So I pitched it to them. I would try to persuade every business owner to accept the currency of the future—and enjoy the benefits of a popularity boost. If they announced that they were accepting Bitcoin online, they would immediately get a wave of new patrons who wanted to spend their coins. Early Bitcoiners were often eager to spend their new currency in commerce, since we all knew that if Bitcoin succeeded as a new form of money, we would all succeed. If a well-known company started accepting it, the

community would celebrate as if our team had just won the World Cup. Nowadays, if a big company announces that they accept cryptocurrency for payment, it barely makes the news. But back then, Bitcoin was battling for credibility, as its public reputation shifted between “obscure novelty for nerds” and “currency for criminals.” So, it was a real cause for celebration—and a serious milestone for the industry—when giants like Newegg or Microsoft decided to accept it.

The community was generally harmonious and unified around the same vision for Bitcoin as digital cash, built for low-fee transactions, accessible to anybody with an internet connection, and able to scale to reach mass adoption. Gavin Andresen was the lead programmer, and Mike Hearn became an influential technical leader—both of them shared the same vision. If you visited one of the many Bitcoin meet-up groups around the world, you would have heard the same story from all of them. If you spoke with the most influential entrepreneurs, you would have heard the same thing. But despite the broader industry unification, factions did start to emerge among the developers, with a small minority wanting to take Bitcoin in a different direction.

3) The Third Era: Civil War
From ~2014 to ~2017

The most important time in Bitcoin’s history was the Civil War Era. In fact, the entire present-day cryptocurrency industry is still defined by the events that took place between 2014 and 2017. This era was the ugliest of them all, filled with personal attacks, mass censorship, propaganda, social media engineering, failed conferences, broken promises, and eventual network failure and split into Bitcoin Cash. Shortly after Andresen made Van der Laan the Lead Maintainer of Bitcoin Core, the internal factions became more entrenched and hostile towards each other, and the blocksize debate went nuclear. Several key Core developers formed their own company called Blockstream—which has been, by far, the most influential company involved with Bitcoin’s software development and plays a central role in its capture. If you visited the biggest companies during that time, you would have heard near universal criticism of the Core developers for stalling Bitcoin’s growth and handicapping its utility. Several prominent developers even publicly warned that BTC was being hijacked while it was happening.

During this time, the industry tried desperately to keep the community together and scale the technology, with multiple attempts being made to bypass the Core developers, but these attempts were ultimately unsuccessful. Several conferences were organized to try and agree on a solution. In 2016, Brian Armstrong attended one of these conferences and wrote an article about his impressions:

I think the organizers of the conference were hoping for some sort of consensus, however it became clear by the end that the divide was too great. The conversations initially focused on various compromises to kick the can down the road on scalability. But as the conversations went on, I became less and less concerned about what short term solution we pick because I realized we all had a much bigger problem: the systemic risk to bitcoin if Bitcoin Core was the only team working on bitcoin.

The core team contains some very high IQ people, but there are some things which I find very concerning about them as a team after spending some time with them last weekend… They prefer 'perfect' solutions to 'good enough'. And if no perfect solution exists they seem ok with inaction, even if that puts bitcoin at risk. They seem to have a strong belief that bitcoin will not be able to scale long term, and any block size increase is a slippery slope to a future that they are unwilling to allow.

Even though core says they are ok with a hard fork to 2MB, they refuse to prioritize it… They view themselves as the central planners of the network, and protectors of the people. They seem ok with watching bitcoin fail, as long as they don't compromise on their principles… In my opinion, perhaps the biggest risk in bitcoin right now is, ironically, one of the things that has helped it the most in the past: the bitcoin core developers.[2]

Armstong's judgment was shared by the vast majority of large economic players at the time, including the miners. I recall attending one of these conferences and pleading with the biggest miners to raise the blocksize limit. They strongly agreed it should be raised, but because they wanted to avoid controversy, they ultimately deferred to Core. Many of them have since become huge Bitcoin Cash supporters.

During this period of extreme division, the general public remained mostly unaware, and in late 2017, another enormous wave of investment caused prices to spike amidst the chaos. One BTC eventually reached $20,000, while the average transaction fee spiked to more than $50, and average transaction confirmation times exceeded two weeks! For the first time in Bitcoin's history, anti-adoption happened, as various companies dropped support due to high fees and unreliable payments, and the narrative quickly started to shift to Bitcoin being a "store of value only" that did not require low fees. Instead of being a tool for regular people—especially helpful for those in the developing world with unstable currencies—the focus shifted towards appealing to central bankers and encouraging Wall Street to speculate. Blockstream executive Samson Mow captured this sentiment by flatly declaring that "Bitcoin isn't for people that live on less than $2 a day."[3]

4) The Fourth Era: Mainstream
From ~2018 to present

The fourth era started during the first run to $20,000, when the news started to cover Bitcoin non-stop. The hype was so extreme, I remember seeing a running ticker symbol in the corner of CNBC broadcasts that would track the price, even during unrelated segments or commercials—as if the most important financial news in the world was the price of one BTC. After almost a decade, the secret was finally out. Bitcoin hit the mainstream. Other cryptocurrencies, too, were enjoying the feverish Wall Street speculation. A new fundraising model allowed a wave of fresh startups to raise millions through ICOs (Initial Coin Offerings)—some with plausible business models, but many without.

The new narrative started to solidify with books like The Bitcoin Standard, which, despite making blunders on several critical concepts, has enjoyed widespread popularity. The same ideas have been uniformly repeated on all the most important discussion channels, making the small-block philosophy the only perspective that newcomers encounter when learning about Bitcoin. The original vision of big blocks and universal access to the blockchain was successfully demonized and its history obfuscated.

The culture is obsessively focused on the price of BTC, regardless of its underlying utility or usage. Every event, no matter how significant, gets judged based on its potential effect on price, rather than its potential to improve human freedom or wellbeing. For example, when the El Salvador government announced that BTC was going to become an official currency, there was almost no mention of the fact that their government was setting up purely custodial wallets for their citizens—meaning, the government will be able to track and censor transactions made through their app, freeze accounts, or easily confiscate coins if they decide to. State integration is great from the perspective of price appreciation and hype, but it's unclear whether the average El Salvador citizen will benefit at all.

One bright spot of the present era is the huge breadth of projects in the cryptocurrency industry. Investors from all over the world recognize that this technology is the future of finance. The credibility problem has finally been resolved. Even if BTC is no longer a decentralized project, the industry is decentralized, and people can choose from many competing options. No matter which projects are compromised in the future, so long as the freedom to choose remains, the market will sort out which coins are the best to use.

Despite Bitcoin's universal fame, the Mainstream Era has a similar feeling to 2011: there remains a serious awareness problem. The general public is aware of BTC, but they remain unaware of the original design and what's possible with big-block Bitcoin. I find myself once again evangelizing for the same technology that got me excited more than ten years ago! Except this time, the problem is not a complete lack of information, but rather an overwhelming amount of bad information. Amidst all the hype and celebrity endorsements, the basic concepts are still not understood.

The remainder of Part II is primarily focused on the time period in which Bitcoin's largest transformations took place: the Civil War, which lasted roughly from 2014 to 2017.

12

Warning Signs

It would be naive to think that a project as world-changing as Bitcoin would go unnoticed forever. International financial powers, whether public or private, have a lot to lose if cryptocurrencies succeed and remain outside their influence. Despite the optimism and unity within the Bitcoin community during the early days, there were signs early on that things were not idyllic or free from internal disruption. I remember as early as 2011, when the price shot up to $30, the main discussion forum Bitcointalk.org was flooded with spam, with bots suddenly posting endless threads of gibberish, making it impossible to use that forum to communicate. Somebody was paying attention and wanted to disrupt information flows, though it's not clear who.

Animation Information Manipulation

Perhaps the first undeniable sign of trouble came in May 2013. The blocksize debate had already started, but even the most conservative developers agreed that the 1mb limit had to be increased. The question was when and to what level. Various schemes were proposed. Some wanted a gradual increase to 2, to 4, then to 8mb. Others proposed an adjustable blocksize limit that automatically adjusted itself based on the average size of recent blocks, and still others wanted to remove the limit altogether. But nobody thought that a maximum throughput limit of seven transactions per second was a good idea. That is, not until the developer Peter Todd put out an animated video entitled "Why the blocksize limit keeps Bitcoin free and decentralized."

I consider Peter Todd's animation to be the first example of well-funded, blatant propaganda. It's so outrageous that it stretches credulity to think it was created from a mere difference in philosophy. The narrator explains how, in the name of decentralization, Bitcoin should cap itself to 1mb blocks forever:

We have an alternative to increasing the blocksize: off-chain transactions… you'll still use the blockchain for large transactions, but small exchanges will be handled by payment processors, which means small purchases like your morning coffee don't clog the whole system up…

Unlike a completely public blockchain where you can't pick who mines your transactions, or who you trust to do validation, off-chain transactions can be both instant, truly private, and you have complete control over who to trust.

What can you do to keep bitcoin decentralized? If you're a miner, only mine in pools that support keeping the blocksize limit, and ask your pool to publicly say so. If you are a user, ignore anyone trying to change the Bitcoin software you use to increase the 1mb blocksize, and tell people you transact with that you support keeping bitcoin decentralized and out of the hands of the existing corporate system.[1]

The absurdity of this proposal at the time cannot be overstated. While it sounds like something you might hear today, it was considered ridiculous in 2013, even by vocal small-blockers like Greg Maxwell, who wrote:

I do cringe just a little at the over-simplification of the video... and worry a bit that in a couple years it will be clear that 2mb or 10mb or whatever is totally safe relative to all concerns—perhaps even mobile devices with tor could be full nodes with 10mb blocks on the internet of 2023, and by then there may be plenty of transaction volume to keep fees high enough to support security— and maybe some people will be dogmatically promoting a 1MB limit because they walked away from the video thinking that 1MB is a magic number rather than today's conservative trade-off.[2]

Other Bitcoiners expressed anger and contempt for the animation throughout the online forums. Not only was the content of the video ridiculed, but the disturbing fact that it came from an insider—the influential developer Peter Todd—also raised eyebrows. The feelings of the Bitcoin community were made clear in the comment section of the video:

"I hope these morons don't ruin bitcoin by convincing people to keep the blocksize small. What better way to make sure that bitcoin remains a tiny

and irrelevant transactional medium…"

"Went from information to disinformation at 0:55, full cringe at 1:28, and straight up Orwell at 2:28."

"This video is dangerous propaganda and marketing hogwash. You're being misled, wake up!"

"What kind of shit lies is this!? It's ok up to 0:45 The rest describes a Bitcoin network that goes against the scaling abilities that Satoshi described, so keeping this limit would break that social contract with the users."

To understand the vitriol directed at the creators of this video, it's worth dissecting the script a little further, to see how it advocated the exact opposite of everything Bitcoin stood for. Consider this section:

We have an alternative to increasing the blocksize: off-chain transactions… you'll still use the blockchain for large transactions, but small exchanges will be handled by payment processors, which means small purchases like your morning coffee don't clog the whole system up…

In other words, the alternative to using Bitcoin is not using Bitcoin. Relying on third-parties to handle small payments is antithetical to the idea of digital cash. Small purchases do not "clog up" the system; the system was purpose-built for them. Restricting on-chain transactions to large amounts is restricting Bitcoin to wealthy users. Regular people cannot afford to pay an additional $5 for every cash transaction, much less $50 or $500+ dollars, and most countries around the world lack the infrastructure for cryptocurrency payment processing.

Large transactions are also more likely to be controlled and regulated by financial authorities, especially when people are forced to use custodial wallets. The blockchain would offer no significant improvement over existing systems, since most people are not going to be purchasing a car, a house, or cashing out part of their retirement without government oversight. If Bitcoin can't be used for cash, most of the world won't use it at all. The script continues:

Unlike a completely public blockchain where you can't pick who mines your transactions, or who you trust to do validation, off-chain transactions can be both instant, truly private, and you have complete control over who to trust.

Credit must be given to the creators for producing a truly impressive piece of propaganda! They create a problem out of a non-problem, then offer their novel solution, which is to not use Bitcoin in the first place. 99.9% of users have no reason to care who mines or validates their transactions. As long as their transactions are put into a block, that's what matters. And remember, users themselves can validate their own transactions without being a full node; they just can't validate the transactions of other people. Claiming that off-chain transactions are truly private is also false. In practice, the two off-chain solutions currently implemented—the Lightning Network and supposed "sidechains"—are both heavily centralized for regular users. The failures of both these technologies are discussed later.

Peter Todd's slick, misleading video was a milestone in Bitcoin's history, and it wasn't the only thing he did in 2013 that raised suspicions.

Instant Transactions? Too Risky

Digital cash needs to have instant transactions. It's unrealistic to imagine any successful cryptocurrency being used as cash if its transactions take more than a few seconds to process. By design, Bitcoin allowed for instant transactions from the beginning, and I used them every day in my business and when evangelizing about Bitcoin. But despite the obvious importance of this feature, some Core developers decided that instant transactions were "too risky" and intentionally broke Bitcoin's functionality to discourage them.

As explained in Chapter 2, Bitcoin transactions get bundled into blocks by miners. Each block builds on the one before it, adding more security with each additional block. Imagine a transaction has just been added to a block; we'll call the first block "Block 1." At that point, we would say the transaction has "one confirmation." When Block 2 gets produced, it adds to the security of all the transactions in Block 1, and we'd say our original transaction now has "two confirmations." The same is true for Blocks 3, 4,

5, and so on. Traditionally, in order to have extremely secure transactions, the rule-of-thumb is to wait until six blocks have been created, or six confirmations, which takes on average one hour.

What about transactions that have been created but have not yet been added to a block? These are called “zero-confirmation” transactions, or “zero-conf” for short. Zero-conf transactions take only seconds to send and receive, though they are inherently less secure. Less-than-perfect security is not a difficult concept to grasp, nor is it a unique idea to any entrepreneur, but some developers apparently thought it was unacceptable.

Let’s say we wanted to game the system by taking advantage of zero-conf transactions. Imagine that we have $200 worth of BTC. There are two stores in front of us, Alice’s and Bob’s, and we want to scam one of them. So, we walk into Alice’s store, purchase $150 worth of goods and pay a $40 transaction fee. Our transaction is seen on the network, but it has not yet been added into a block. So, we immediately walk into Bob’s store, spend the same $150 of BTC. Since the same coins are trying to be spent twice—a “double spend”—both transactions cannot be added into a block. Only one will be accepted and included in the blockchain, which means either Alice or Bob will be defrauded $150. The way Bitcoin is designed, this is theoretically possible, and occasionally double spends do happen. Does this mean the system is broken? Of course not.

The simple, elegant solution has been part of Bitcoin’s design from the beginning. It’s called the “first-seen rule.” Miners and nodes keep a running list of zero-conf transactions that are waiting to be added into a block. The first-seen rule says that whenever there are two conflicting transactions, whichever one was seen first wins. So, in our previous example, after sending the $150 to Alice, the Bitcoin network would already know about this transaction and simply reject the attempt to double spend it with Bob.

The first-seen rule was not mandatory or enforced at the protocol level. It was a simple, sensible policy for miners and nodes to abide by, since it allowed for instant transactions. However, it also allowed for elaborate theoretical schemes to defraud merchants, say, by collaborating with corrupt miners. Despite there being social and economic incentives which discourage this corruption, and despite the ability of entrepreneurs to

manage these risks as they already do with other payment methods, some developers thought that any theoretical insecurity was a design flaw that needed to be fixed at the code level. So, they came up with the idea of an undo button.

The Undo Button

Instead of the first-seen rule, Peter Todd proposed the "replace-by-fee" (RBF) patch, which said that when two conflicting transactions are seen, the one with the higher fee wins. So, after sending Alice the $150 transaction with a $40 fee, we could walk into Bob's store, spend the same $150 with a $50 fee, and the network would accept the second transaction as valid. Such a policy makes double spending easy, effectively breaking the reliability of zero-conf—which was the explicit goal of Todd. In the online forums, Peter Todd posted a thread entitled, "Reminder: zero-conf is not safe; $1000USD reward posted for replace-by-fee patch," in which he wrote:

> Someone by the name of John Dillon emailed the bitcoin-development email list earlier this morning offering a $500USD reward [later increased to $1000] to anyone who implements a transaction replacement-by-fee patch. That's an idea I posted on the email list two days ago:
>
> In any case, the more pressing issue… is changing fees attached to transactions after they have been broadcast…
>
> The more I think about the issue the more I think we should nip this zero-conf madness in the bud: change the relay rules so that transactions are replaced based on fees regardless of how that changes transaction outputs. Of course, this does make double-spending an unconfirmed transaction trivial. On the other hand… it lets us implement a limited 'undo' button for when people screw up….
>
> We keep saying over and over again to stop accepting zero-conf transactions, but people do it anyway because it seems secure. It's a very dangerous situation…
>
> Like it or not, zero-conf is dangerous when you don't trust the other party. I wrote the above replace-by-fee idea because I really think we run a risk if

we lull people into complacency. The blockchain and the proof-of-work system is how Bitcoin comes to a consensus about which transactions are or are not valid; trusting anything else is dangerous.[3]

It's worth walking through the logic of Todd's argument. He starts with the supposed problem of users getting their transactions stuck, which was only an issue for transactions with extremely low or zero fees. Though ironically, stuck transactions did become a real issue when the blocks became full and fees spiked in 2017. When users' transactions were stuck, sometimes for days or even weeks, RBF was indeed used to "unstick" those transactions. So with small blocks, high fees, and unreliable transactions, RBF starts to make more sense.

Then he gets to the real point: in his mind, zero-conf transactions aren't safe enough, and uninformed users just don't realize it. So, to prevent people from getting attached to zero-conf transactions, RBF would break their functionality once and for all—because, in his words, if the miners decided to implement something like RBF, zero-conf would break anyway. In other words, Bitcoin's instant payment functionality needed to be broken by developers at the software level, so that miners wouldn't end up breaking it in the future. That is, unfortunately, not an exaggeration of their position. John Dillon, the mysterious financier of this patch, explained:

I'm not offering this reward because I think an undo button is important… The problem is people like… Mike Hearn will be more than happy to screw up Bitcoin in a desperate attempt to stop double spends when it becomes a big issue… By breaking zero-conf security now there won't be pressure to implement [his centralized] crap. The most badly affected will be Satoshidice and they should not be using the blockchain the way they do.[4]

And in 2015, while this debate was still ongoing, the well-known programmer Bram Cohen agreed:

To say that zeroconf doesn't work is an oversimplification. Zeroconf works okay… for now. But if it's used at any meaninful [sic] scale an unstoppable conspiracy will inevitably emerge to exploit those relying on it. Rather than wait for disaster to strike, Bitcoin development should plan to cease zeroconf support in a scheduled and orderly manner, with the changeover

happening before either the conspiracy gets built or harm is done to the functionality which zeroconf support conflicts with.[5]

Solutions Outside Code

It shouldn't be surprising that software developers try to solve problems with software. But this tendency can turn into myopia if left unchecked, or as Gavin Andresen put it, "Engineers are great at not seeing the forest for the trees. They get stuck on details and lose track of the bigger picture."[6] The bigger picture, in this context, is the world outside Bitcoin's code. Entrepreneurs have been solving problems with less-than-perfect payment security for thousands of years, using far inferior technology than cryptocurrency. A great insight into this was written by Justus Ranvier, an engineer with real-world experience, who replied to Peter Todd's forum post about RBF by saying:

Security in this context is being inappropriately treated like a binary concept. There's an entire consumer economy out there based around charge cards which, in bitcoin terms, take 90 days to confirm transactions. Trillions of dollars are being transacted out in the real world via payment methods that are no less insecure than zero-confirmation Bitcoin transactions. Accepting zero-conf transactions is an issue of risk management and business planning, not a case of "secure" vs "insecure".

And elsewhere writes:

You've spent too much time playing The Sims and forget that both merchants and pool operators are sentient, intelligent beings instead of automatons. If the risks of zero conf double spends are worth expending resources to reduce or eliminate then the merchants will find a way to get it done.[7]

Indeed, cryptocurrency payment processors are well-aware of the risks of double-spending and have various options for managing it. The simplest option is for the payment processor to take on the risk for their customer in return for a fee—payment insurance, essentially. Or they can require customers to use a particular wallet app to pay for goods, which makes it more difficult to execute a double-spend. Without RBF, pulling off a

double-spend is difficult and not worth the hassle to steal small amounts, but for large purchases it might be expected that customers have to wait for a confirmation or two. In fact, companies like SatoshiDice that were providing gambling services on Bitcoin had already implemented a system that allowed instant transactions for small amounts, but large amounts required confirmations.

Zero-conf transactions are especially important for brick-and-mortar payments. Given that only a tiny percentage of customers try to steal from businesses in-person, some merchants might simply accept the risk of double-spends themselves. Traditional options for mitigating the risk of fraud or theft still work. If they already have security systems in place, for example, they might be able to get footage of the criminal. These are just a handful of ideas to address zero-conf security concerns. I'm sure even better solutions would have been found if double-spends ever became a real problem. Markets are exceptionally good at discovering and managing risk.

Replace-by-fee prompted many people to speak out against it. Charlie Lee, who was the engineering manager at Coinbase said:

Coinbase fully agrees with Mike Hearn. RBF is irrational and harmful to Bitcoin.[8]

Jeff Garzik, an early Bitcoin Core developer agreed:

Repeating past statements, it is acknowledged that Peter's scorched earth replace-by-fee proposal is aptly named, and would be widely anti-social on the current network.[9]

Gavin Andresen said flatly:

Replace-by-fee is a bad idea.[10]

Even Adam Back, who later played a big role in derailing Bitcoin agreed:

I agree with Mike & Jeff. Blowing up 0-confirm transactions is vandalism.[11]

Yet, in late 2015, RBF was successfully added to Bitcoin Core. At present, RBF transactions are created with a flag, so merchants can refuse to accept them if they are careful, but developers are currently debating whether to change this default setting. If the flag is ever removed, zero-conf payments on BTC will effectively have zero security. Zero-conf payments are understood to be an essential feature in Bitcoin Cash, and developers have been actively working on ways to further improve their security and reliability.

Sheer Propaganda

Despite the controversy surrounding RBF, if you try to research it today, you will undoubtedly encounter misleading information. On the Bitcoin Core website, there is a Q&A section on RBF. One question reads:

Was the opt-in RBF pull request controversial?

Not in the slightest. After extensive informal discussion stemming back months, the PR was opened on October 22nd [2015]. It was subsequently discussed in at least four Bitcoin development weekly meetings…

In the PR discussion, 19 people commented, including people working on at least three different wallet brands, and 14 people explicitly [agreed with] the change, including at least one person who had been very outspoken in the past against full RBF. No clearly negative feedback was provided in the PR, or elsewhere that we are aware of, while the PR was open.[12]

This section is carefully worded so the casual reader walks away thinking RBF was not controversial. Notice the question is about the "pull request" (PR), not the overall concept of RBF—that is, if you only look at the comment section for that particular action on Github, the majority of people on that thread agreed with it. But that's only because an enormous amount of debate simply took place in other venues. The dates involved are also misleading. They claim the informal discussion stretched back "months" from the end of 2015, but as the Bitcointalk.org forum thread demonstrates, RBF was being hotly debated as early as 2013.

The Q&A says, “No clearly negative feedback was provided in the PR, or elsewhere that we are aware of, while the PR was open.” (My emphasis.) But the pull request was opened in October 2015! Mike Hearn wrote an extensive dissenting article on his own website criticizing replace-by-fee in March 2015,[13] seven months prior.

In a different section, the Q&A asks, “I heard Opt-in RBF was added with little or no discussion,” and it answers with a list of a dozen links to “Recent RBF discussions going back to May 2015.” It entirely omits the fact that RBF was a bubbling controversy only two months earlier. This careful control of information is designed to mislead newcomers about Bitcoin, and it makes it exceptionally difficult to discover the truth about its history.

Who Was John Dillon, Anyway?

The history of Bitcoin is intertwined with mysterious figures, starting with its unknown creator, Satoshi Nakamoto. But Satoshi is not the only shadowy figure. John Dillon is another, and not much is known about him. Dillon was the man who offered to pay $1,000 to develop the replace-by-fee patch proposed by Peter Todd. As it turns out, Dillon also supported and paid Todd for his work creating the infamous 1mb-forever animated video. When Todd announced he was working on the video, Dillon wrote:

It is so important that you are taking this message to the people. Bitcoin is much bigger than this little forum…I suspect there is a lot more Bitcoin activity going on that doesn’t give a damn about Bitcoin as a payment system. Peter mentioned Silk Road which is brilliant I think. It is an off-chain transaction system already.

As a serious Bitcoin investor I also care about the store of value, not stupid micropayments, and I know my partners feels [sic] the same way. We also know that Bitcoin’s value has very little to do with being a payment system...[14]

Once the infamous animation was produced, Dillon wrote:

I finally got a chance to see your new video. It's solid professional work, you have done a great job. You'll soon get another 2.5BTC from me by the same method I used before. Nice to see that big 10BTC donation you got, and from an address with 125BTC! It really says something how many of the donations you have been getting all come from addresses with large balances of Bitcoins, about 250BTC and counting right now. It just goes to show how the people most heavily invested in Bitcoins are the ones with the most to lose from centralization and regulation. Keep up the fight.[15]

Dillon was not just any enthusiastic small-blocker. He was apparently having extensive conversations with some Core developers, and at one point, Gavin Andresen remarked, "I've started to suspect jdillon is a very sophisticated troll with the ulterior motive of destroying bitcoin."[16]

Gavin's suspicions might have been correct. In November 2013, Dillon was apparently hacked by some angry Bitcoiners, when his Bitcointalk account posted its own thread entitled, "'John Dillon' We can leak things too you trolling piece of shit." The post contained a single link to an archive of private correspondence from Dillon, as well as conversations about him from other developers. The authenticity of the leak has not been disputed. Dillon appears to be coordinating with Todd and funding multiple projects that supported transforming Bitcoin into an expensive settlement system. Peter Todd himself was apparently aware that people had become suspicious of his connection to Dillon. In an IRC chat, Todd and Greg Maxwell wrote:

<petertodd> Everyone knows John and I "know" each other, if anything I'd like my PGP signature on his key to make the nature of that relationship understood.

<gmaxwell> (I think half the people think you and John are the same person. :P)

<petertodd> ha, I know, I'll admit he kinda creeps me out a bit sometimes... he's admitted he reads all my posts religiously.

But by far the most interesting exchange is an email between Dillon and Todd, in which Dillon claims to be involved with the intelligence

community, saying:

Just so you know this stuff about Tor has me worried... Please don't make this public, but my day job involves intelligence, and I'm in a relatively high position.

You know, I went into the job years ago with very different thoughts about it than I do now. The last, well, decade really has changed a lot of minds in this field, in totally different ways. Myself I am on the side of Snowden and Assange, but... lets just say when you have a family your willingness to be a martyr diminishes. The same is true of many of my colleagues.

Hopefully my support for Bitcoin can help undo some of the damage we've done, but I do have to be careful and it's tough to take all the precautions I need to be able to communicate. If it was found out that I was involved with Bitcoin that way I have been, let's just say there would be consequences…

To which Todd seems to respond concerned:

I mentioned your status to a friend of mine who is a former spook and well aware of the dangers of the business to anyone with a sense of ethics.

He told me to tell you this, word for word: "An old crow strongly advises you to consider the risks to yourself and your family, and stop what you are doing." I trust his judgement, and just as importantly, his ethics.

Be careful. Myself, I suggest you think hard about whether or not what you are doing has had enough of an impact on your goals to be worth it - I can't answer that question for you.[17]

These emails read like something out of a spy novel. It's impossible to know whether Dillon was telling the truth, but it's worth noting how suspicious the whole situation is. "John Dillon" is the pseudonym of an unknown person who paid Peter Todd, a Core developer, to produce a video promoting the restriction of Bitcoin's throughput to seven transactions per second. He offered a bounty to develop replace-by-fee, which was intended to "break zero-conf security now"—that is, to break the functionality of instant transactions. Gavin Andresen publicly speculated that Dillon had an

ulterior motive to destroy Bitcoin, and later it turns out, in leaked emails, that Dillon claimed to be in a high position within an intelligence agency. (But not to worry, because he also claimed to have a change of heart and really wanted Bitcoin to succeed!) All of this happened around the most revolutionary financial invention in history, which directly challenges established governmental, financial, and banking powers around the world. Readers can come to their own conclusions, but in my mind, by late 2013, Bitcoin had already been targeted for capture.

13

Blocking the Stream

Open-source software development is notorious for lacking a straightforward business model. It's often unclear how programmers should get paid for their work when their final product is free and open to the public. Some projects will ask users for voluntary donations. Others will offer premium support for companies and institutions. Cryptocurrency projects are especially tricky because the software is a financial product. Any mistakes can directly affect the wallets of millions of people. Different groups have tried different strategies to finance their own development. A simple donation model has worked for some. Others will set aside a large pile of coins at their genesis to create a foundation that oversees development. Some projects will give a percentage of the block reward straight to the programmers. Lots of creative models have been tried.

Bitcoin development is yet another open-source project with an awkward business model. Given its world-changing importance, scale, and complexity, every setup that has been tried has caused controversy—for good reason, since the integrity of the entire system depends on the mechanism by which the developers get paid. Funding and governance go hand-in-hand, and potential conflicts of interest among developers are a critical threat, as the most straightforward way to corrupt a project is to corrupt its funding mechanism.

The Bitcoin Foundation

Unlike many of the development groups today, Bitcoin started out as a project among volunteers. As it grew in popularity, questions about compensation naturally arose. The earliest attempt to create a more formal organization around the maintenance of the software came in 2012, with the creation of the Bitcoin Foundation, which modeled itself on the Linux Foundation. The Bitcoin Foundation accepted donations from large companies and other interested parties. I myself donated to it and was a founding board member. Its most important goal was to provide funding for

Gavin Andresen as the Chief Scientist and Lead Maintainer for Bitcoin Core. In an interview with The New Yorker, Andresen explained:

The Linux Foundation provides a bit of a center for Linux, and to pay the lead developer, Linus Torvalds, so that he can do nothing but concentrate on the kernel… It's a tricky thing, once you get to be a certain size as an open-source project, how do you sustain yourself? Linux is the most successful open-source project in the world, so we thought it would make sense to use that as a model.[1]

Another goal of the Foundation was to improve the reputation of Bitcoin with regulators and the general public, since it was frequently smeared as a currency for criminals at that time. Andresen stepped down as Lead Maintainer in early 2014 to focus more on scientific research and duties with the Bitcoin Foundation. That April, he wrote:

A few years ago I created a Google Scholar alert for "bitcoin." And I was happy if I got one alert per month. Today, I find it harder and harder to keep up with all of the great Computer Science or Economics papers related to bitcoin and other crypto-currencies; in just the last week Mr. Google told me about 30 new papers I might be interested in reading…

To be clear: I'm not going to disappear; I'll still be writing and reviewing code and offering my opinions on technical matters and project priorities. I enjoy coding, and I think I'll be most effective as Chief Scientist if I don't lose touch with engineering reality and make the mistake of building huge, beautiful, theoretical castles that exist only as whitepapers.[2]

Unfortunately, Andresen did not have much time before the Foundation started to fall apart due to bad management, a lack of transparency, and a series of petty scandals. By the end of 2014, the organization was dysfunctional, with some board members getting into trouble with the law. In April 2015, it was announced that the Foundation was effectively bankrupt and would not be able to raise enough money to continue funding development.[3] So later that month, Andresen joined a new project at MIT's Digital Currency Initiative, where he would continue to develop Bitcoin along with two other Core coders, Wladimir van der Laan and Cory Fields.[4]

With the failure of the Bitcoin Foundation, and with Van der Laan as the Lead Maintainer, Bitcoin would slowly be transformed into a different project over the next three years. In a different world, if the Foundation had succeeded, it's unclear whether this transformation could have ever happened. Reflecting on this question, Mike Hearn would later write:

One of the problems with cryptocurrency, philosophically, is that the commitment to decentralisation tended to be interpreted as (or spun as) a general rule against institutions and processes of any kind. Both me and Gavin were involved in setting up the Bitcoin Foundation early on, but it sputtered out. Partly due to being set up too fast and too many rum characters getting involved, but mostly because the pseudo-libertarians bent themselves towards the goal of wrecking it on the grounds that Bitcoin shouldn't have a foundation or a formalised development process.

This left the community not with a decentralised utopia but rather with a vague, informal and cliquey development process driven by back channel dealing, manipulative attempts to define individual positions as "consensus" and the purchasing of developers. If the community had rallied around Gavin's attempt to organise the community with a set of institutions, things might have worked out differently, as it'd have had greater built in resistance to being hijacked.[5]

While the failure of the Bitcoin Foundation was significant, the most important changes to the software development structure came in late 2014, when some Core developers formed their own company called Blockstream.

Blockstream is Founded

Blockstream would end up being the most influential company in Bitcoin's history. Its co-founders were Adam Back, Gregory Maxwell, Pieter Wuille, Matt Corallo, Mark Friedenbach, Jorge Timón, Austin Hill, Jonathan Wilkins, Francesca Hall, and Alex Fowler. Unlike the Bitcoin Foundation, Blockstream was founded as a for-profit company—a fact that made other Bitcoiners immediately curious about their business model. Greg Maxwell was asked about it during an "Ask Me Anything" session on Reddit and provided a handwavy answer:

[W]e believe there is a vacuum in the industry (not just Bitcoin, but computing in general) for cryptographically strong trustless technology… We think there is a tremendous business potential in building and supporting infrastructure in this space, some connected to Bitcoin and some not. E.g. by acting as a technology and services provider for other businesses in helping them migrate to a more Bitcoin-like way of doing business.

Right now our focus is on building out the base infrastructure so that there is actually a place to build the revenue producing business we'd like to have, and then we hope to circulate that back into building more good technology.[6]

Blockstream was successful in creating a revenue-producing business, but it turned out to be a serious conflict of interest. Instead of building out the base infrastructure, it crippled the base infrastructure and now offers paid solutions to the problems it created. The fact that Maxwell would be employed to work on critical infrastructure is ironic, given his admission that he previously thought the key technological mechanism used by Bitcoin was not even possible:

When bitcoin first came out, I was on the cryptography mailing list. When it happened, I sort of laughed. Because I had already proven that decentralized consensus was impossible.[7]

When Blockstream was initially formed and raised their first round of fundraising, I initially thought it was a good sign that more investors were discovering Bitcoin. But as time went on—and it was revealed that their biggest investors came from the establishment banking industry—I became more skeptical, along with countless other Bitcoiners. Now, in hindsight, I consider the founding of Blockstream the beginning of the Civil War era. Shortly after its formation, the culture shifted, disagreements turned hostile, and the most radical small-block position—which hardly anybody had taken seriously—became more vocal and aggressive. Blockstream engineers started to insist that Bitcoin could not scale the way it was originally designed, while censorship began in the online forums. The passivity of the lead developer Van der Laan, who wanted to avoid conflict, started to be exploited in favor of the status quo. The Core developers

became adamant that “consensus” was needed among them in order to raise the blocksize limit, effectively giving them a complete veto over scaling the protocol.

Why would a group of developers form a company to take over a project and then prevent it from scaling? The answer turns out to be simple: their business model depends on Bitcoin not scaling its base layer. The less Bitcoin can do, the more Blockstream can do for a fee.

The Business Model

Blockstream raised suspicions soon after it was founded and has been the subject of innumerable conspiracy theories, some more plausible than others. For years, people have speculated that the bizarre behavior of the Core developers is best explained by a conflict of interest—if either Blockstream or their investors profit by throttling Bitcoin. But today, we no longer have to speculate, because they speak openly about it. In a Forbes interview, CEO Adam Back shared one part of their monetization strategy, saying, “Blockstream plans to sell sidechains to enterprises, charging a fixed monthly fee, taking transaction fees and even selling hardware.”[8]

What are “sidechains”? The company’s whitepaper explains the general idea:

We propose a new technology, pegged sidechains, which enables bitcoins and other ledger assets to be transferred between multiple blockchains. This gives users access to new and innovative cryptocurrency systems using the assets they already own. By reusing Bitcoin’s currency, these systems can more easily interoperate with each other and with Bitcoin, avoiding the liquidity shortages and market fluctuations associated with new currencies. Since sidechains are separate systems, technical and economic innovation is not hindered.[9]

In other words, sidechains are an attempt to link different blockchains together by connecting entries on one ledger with entries on another. It’s a neat idea, and in theory it could allow for more creative experimentation. Different rules and networks could operate on different ledgers but remain interoperable with Bitcoin. This is why sidechains have been proposed as an

alternative method for scaling Bitcoin, since different projects can still be pegged to the Bitcoin blockchain without being directly built on top of it.

Let's take an example to make the concept of sidechains clearer. Imagine a new blockchain designed for nanopayments of a millionth of a penny or less—smaller than even the original Bitcoin was designed for. Let's call it "NanoBits" or "NBT." Instead of being a totally isolated blockchain, NanoBits could have a sidechain integration with the Bitcoin blockchain, allowing users to lock up their Bitcoin in exchange for NBT. For example, by locking up 0.001 BTC, you could unlock a billion NBT. Then, if users want to trade their coins back to the BTC blockchain, they could swap the billion NBT back into BTC. If done correctly, this type of system would allow for more innovation, since the sidechains can operate with totally different rules, allowing different development teams to experiment without needing to persuade the entire community to add their changes. Plus, this innovation can occur without fear of breaking the main chain, since any new failures and flaws would be isolated to the sidechain. That's how it might work in theory. In practice, it's a different story.

The idea of sidechains has always appealed to me, and I have personally funded their development on BTC with the DriveChain project, led by Paul Sztorc. Like any software project, creating a working implementation has proven much more difficult than creating a nice-sounding idea.

Done correctly, sidechains should not require any trust in centralized authorities in order to work, which is what the DriveChain project is trying to do. Blockstream has released their version of a sidechain called the "Liquid Network," but it works very differently. The Liquid Network is a "federated" sidechain, which is better understood as a centralized sidechain or even an altcoin. The basic security of their network requires trust in a small, hand-selected group they call the Liquid Federation. According to their website:

The Liquid Federation is a group of cryptocurrency businesses, including exchanges, trading desks, infrastructure companies, game developers, and more. The federation fulfills a number of tasks that are integral to the Liquid Network's operation.[10]

There are currently only fifteen members of this federation, and if more than a third of them became dishonest, the security of the network would break and users could lose their money. Not only is the network centralized, but after swapping your BTC for Liquid tokens, you are no longer using the Bitcoin network. Instead, you are using Blockstream's proprietary Liquid Network, and every single transaction fee goes to a wallet controlled by them.11 It's a lucrative system. Liquid is a sidechain, which means transaction fees are not paid to Bitcoin miners; they are paid directly to Blockstream.

Why would somebody choose to swap their BTC for Liquid tokens? One reason is quite simple: the fees on BTC are too high! Adam Back, the CEO of Blockstream, has brazenly advertised his Liquid Network as a solution to the problem of high fees on the main network, saying on Twitter:

If you are actively trading and don't like high fees, use exchanges with [Liquid] integration, or complain to an exchange that doesn't. Pay 1-2c to clear in 2 min final, while others are paying 50c—$2.50 for 1hr+ transfer… Be part of the solution.12

To be clear, this is the CEO of Blockstream—the company that employed a majority of the most powerful Bitcoin Core developers during its most critical time period—directing people to his proprietary blockchain to "be part of the solution" to high fees and network congestion. Meanwhile, the BTC network only has poor performance because the Bitcoin Core developers refused to increase the blocksize limit in the first place. The conflict of interest is enormous. It certainly looks like Blockstream is selling a paid solution to problems they caused, and it's not even clear whether the Liquid Network would have a reason to exist if Bitcoin had big blocks.

A Banker's Dream

Capturing all the transaction fees from the Liquid Network is not the only way that Blockstream profits from it. They also charge a monthly fee to companies integrating Liquid and are releasing tokens on their network. In 2020, Blockstream announced that they had become technical partners with

a new startup called Avanti, which is trying to be a cryptocurrency-friendly bank. According to their website:

Avanti is a new breed of bank — a software platform with a bank charter, built to connect digital assets with the legacy financial system. Our team is deeply experienced in both. We're not just a bank — we're a depository institution, which means we're eligible to become a U.S. dollar clearing bank at the Federal Reserve.[13]

Within the small-block vision, banks continue to play a critical role in the future financial system by being the primary entities that access the blockchain. So, it makes sense for Blockstream to position themselves as key players in that system, offering technical services, consultation, and their own proprietary network as an alternative to Bitcoin. This strategy has worked so far. Avanti recently announced they were entering the lucrative digital asset market by issuing tokens ("Avit") that they claim will be redeemable for one US dollar, though not fully backed by dollars. A Coindesk article explains:

While Avit would not be pegged one-to-one to the U.S. dollar – because it's a new digital asset, not a digital representation of a real-world asset – the currency would be 100% backed by a reserve of traditional U.S. assets.[14]

In other words, Avanti Bank will issue tokens that are redeemable for a dollar without actually being backed by dollars. The real assets backing their token will provide them with yield instead. While there is nothing inherently wrong with this business model, it's another example of cryptocurrencies being assimilated into the traditional financial system without taking advantage of crypto's unique properties. Bank tokens backed by "a reserve of traditional U.S. assets" are not inflation-proof, censorship-resistant, or disruptive to the status quo. Because they provide yield, they even come with risk of default. If the bank issuing the tokens goes bankrupt, users will end up losing money, once again demonstrating why currencies that do not require trusted third parties are so attractive.

Considering that the narrative surrounding Bitcoin is that it's disruptive to the established financial industry, there is some irony in the fact that Blockstream is integrating with banks to help them issue digital dollars. In

addition, they are even starting to integrate directly with governments and help them with fundraising. In El Salvador, Blockstream has helped to create a "Bitcoin Bond" to help the state raise a billion dollars, paying out an annual dividend to holders. Both the Bitcoin Bond and Avit Tokens will be built on the Liquid Network, diverting even more traffic from BTC to Blockstream's sidechain.15

The conflict of interest between Bitcoin Core developers and Blockstream is easy to see. With such perverted incentives, it's no surprise that Satoshi's vision of cheap, peer-to-peer transactions on the base layer was abandoned; big blocks would kill their business model. By contrast, on Bitcoin Cash, anybody can create tokens and transact them on-chain with minimal fees. Sidechains and custodial wallets are not needed to scale, since the base layer can handle a much higher transaction throughput. Though, if desired, sidechains and custodial wallets still work with big blocks and would perform better.

Conspicuous Fundraising

The details of Blockstream's multiple rounds of fundraising have not helped their image nor quelled the conspiracy theories surrounding the company. To date, they have raised around $300 million from investors. Nearly a third of a billion dollars is a substantial amount for any company to raise, but especially for one working on open-source software.

In early 2016, eyebrows were raised when Blockstream completed a $55 million round of Series A funding.16 One of the primary investors was a venture capital firm called AXA Strategic Ventures, a branch of the French multi-national firm AXA—the eleventh largest financial services company in the world according to Fortune Global 500.17 At the time, the CEO of AXA was Henri de Castries, a magnate of the international financial system. In a 2015 news article, The Guardian newspaper described De Castries as follows:

Henri de Castries might just be the most powerful man in the world. He is chief executive and chairman of one of the world's biggest insurers, Axa, and a member of France's illustrious noble house of Castries. But De Castries is also chairman of the Bilderberg group, a collection of political

and business leaders from Europe and North America that meets in private every year to debate “megatrends and major issues facing the world” – or which is secretly running the world if you are a conspiracy theorist.[18]

As if the mysterious John Dillon wasn’t enough fodder for conspiracy theories, Bitcoin’s history also includes a real connection to the Bilderberg group. For decades, the Bilderberg group has been controversial, due to its highly secretive meetings and their attendance by some of the most powerful people in the world—a who’s-who of elites from across political, financial, academic, and media industries. The organization has been operating since the 1950s and includes far too many powerful attendees to name, ranging from heads of state like Tony Blair and Bill Clinton, to European royalty like the kings of Belgium, Norway, and Spain, business magnates like Bill Gates and Jeff Bezos, and a long list of CEOs and founders of large companies, banks, and news outlets across the world.[19] Naturally, when a large number of powerful people get together and hold secretive meetings, conspiracy theories are inevitable, whether or not they are justified. We know from history that some conspiracies are real, and it’s naive to think meetings like this are not influencing world affairs to some extent—that’s why they hold them in the first place! Their real-world impact is unknown, but it is definitely greater than zero.

Ultimately, it is impossible to know the significance of these connections. It could be a delightful coincidence that Blockstream was funded by a venture capital firm whose parent company is one of the largest financial companies in the world, whose CEO is the chairman of the Bilderberg group. I truly do not know, but at the very least, the connection is too intriguing not to mention here and is another part of Bitcoin’s colorful history.

Researchers have tried to follow the money flowing into Blockstream over the years, and while there are plenty of interesting connections and possible conflicts of interest, nothing is unambiguous. For example, the Digital Currency Group is another venture capital firm which has raised suspicions after investing in a huge range of cryptocurrency projects, Blockstream included. When the firm was created in 2015, their initial funding came from establishment financial companies, including MasterCard—a direct competitor of Bitcoin.[20] Yet, there’s nothing definitive that links

MasterCard to a nefarious plot to capture Bitcoin's development. While they undoubtedly knew about Bitcoin's potential for disruption, it's impossible to know the intentions behind their investment. Perhaps they just wanted to ride the wave of cryptocurrency investment and innovation, or perhaps they wanted influence over the company with the most control over Bitcoin's code. I can easily imagine both scenarios.

Blockstream's largest fundraising round came in 2021, when it raised over $200 million in Series B funding, bringing its valuation to $3.2 billion.[21] This enormous haul came several years after the capture of key Bitcoin Core developers, a significant loss of total market share of BTC, the Bitcoin Cash split in 2017, and multiple network failures which saw skyrocketing transaction fees and dramatically increased confirmation times. One interpretation, from a purely business perspective, is that investors believe Blockstream's alternative network will generate significant revenue in the future by competing with the main BTC network for transactions. A less charitable interpretation is that Blockstream received a large payoff for crippling Bitcoin's development at a critical time and fundamentally changing it to resemble the existing financial system. A few hundred million dollars is nothing compared to what the banks might lose if Bitcoin were running at its full potential.

Early Bitcoin adopter and internet personality Stefan Molyneux had this concern as early as 2014, when he predicted that existing financial and political interests would recognize Bitcoin as a threat and try to slowly capture it. He said:

It's really important for people to understand how big the behemoth is that Bitcoin is facing. There will be efforts on the part of the financial-government complex to keep the technology at bay… [by saying] 'Let's not kill it outright, because it's big enough now that people will see what we've done…'

Instead, what they're going to try to do is throw little bits of sand in it until most people find it too cumbersome to use, and then say 'Well, it was an interesting idea, but it didn't quite work out the way people wanted.' I think that is the great danger.[22]

Molyneux might have been prescient. Regardless of whether malice was involved, we can say with confidence that the Bitcoin of 2024 is far less threatening to existing powers than the Bitcoin of 2014. It is a cumbersome network that pushes users to secondary, controlled layers to have a better experience. Custodial wallets are also easy to control and inject the need for trusted third parties back into the system. In the big picture, Bitcoin's re-design looks remarkably similar to the existing monetary system, where everyday users do not have ultimate control over their own funds and require companies to provide financial services for them. The benefits of this new system are primarily enjoyed by early adopters who benefitted from the enormous price appreciation.

From the perspective of the original design and purpose of Bitcoin, Blockstream's influence over the protocol has been disastrous. BTC looks nothing like the original Bitcoin, and it's unlikely to in the future. Fortunately, Blockstream does not have a monopoly over all cryptocurrency development, and Bitcoin Cash developers successfully routed around them in 2017—though the process was not easy and involved an enormous amount of pain and drama.

14

Centralizing Control

The centralization of control over Bitcoin's software did not happen overnight. It took a few years, and during that time, dissenting views were common. Criticisms of Bitcoin Core and Blockstream were everywhere, especially after Gavin Andresen stepped down as the Lead Maintainer of Core. In hindsight, while it seems clear that Bitcoin's development was compromised, the process was unclear as it was happening. Outright accusations of development capture were less common, because most of the important actors in the industry were desperately trying to keep the network together. Also, since Blockstream's business model was not revealed until a few years after its creation, the glaring conflicts of interest could only be speculated about. Though, the curious absence of a clear business model was noticed immediately in a Wall Street Journal article about the company's investors in 2014:

Blockstream has no clear roadmap on how it will turn an open-source software engineering project into a corporate money-maker. Instead, investors took a leap of faith, mostly based on the reputations of the company's co-founders… [T]he indeterminate nature of Blockstream's business model made it a complicated investment for many venture capitalists, who typically must justify returns to their investors.

The manager of one fund said he turned down the pitch because he couldn't invest in such a vague plan. Mr. Hoffman said he invested via his personal not-for-profit foundation… because he felt strongly that Blockstream's first funding round "had to be invested in the development of the bitcoin ecosystem and not have, as its primary focus, economic returns…"

[S]ome commentators have worried that a private company with such intellectual clout could have undue influence in a bitcoin network that's supposed to be community-owned and decentralized. [Co-founder Austin Hill] said that's why it was paramount that Blockstream was set up in a transparent way, as "a public utility, and not a way to hijack bitcoin."[1]

Regardless of Austin Hill's personal intent, Blockstream ultimately did turn into a way to hijack Bitcoin. Hindsight provides us with 20/20 vision, but when reconstructing Bitcoin's history, it's important to be aware of the lack of clarity at the time. It took years before the Liquid Network was openly promoted as an alternative to the Bitcoin blockchain—a smart strategy by Blockstream, since if they immediately advertised their proprietary network as a scaling solution, they would have been met with laughter and overwhelming resistance.

Instead, Bitcoin Core and Blockstream's centralization of power was somewhat slow and methodical. They took advantage of small opportunities to give themselves more control over the network. They took advantage of Van der Laan's weak leadership and desire to avoid controversy. Perhaps most importantly, they leveraged the idea of "developer consensus" to effectively give themselves veto power over the software—even if their veto radically changed the structure and economics of the entire system. Jeff Garzik warned about this in a public email about their refusal to increase the blocksize limit, saying:

This is an extreme moral hazard: A few Bitcoin Core committers can veto [an] increase and thereby reshape bitcoin economics, price some businesses out of the system. It is less of a moral hazard to keep the current economics (by raising block size) and not exercise such power.[2]

Programmable Money or Spam?

The blocksize limit was not the only area in which the Core developers asserted their power. Another great example was the notion of so-called "spam transactions" and the utilization of Bitcoin for smart contracts. Though it's been stripped out of the BTC software and nearly forgotten about today, Bitcoin was originally designed to handle smart contracts—the sorts of complex computations that Ethereum is known for. The smart contracting system in Bitcoin was clunkier than more recent cryptocurrencies, but it still had broad functionality, much of which has been reactivated on Bitcoin Cash.

The Core developers not only destroyed Bitcoin's utility as digital cash, they also stripped out basic functionality from the original technology itself.

Why would they do that? For the same reason they refused to increase the blocksize limit: it did not fit their new vision for Bitcoin. They did not like Satoshi's vision, so they created their own where the blockchain is only used for high-value transactions. Everything else, whether small payments or smart contracts, is at risk of being designated as "spam" and restricted by the Core developers. The Counterparty team found this out the hard way.

Counterparty was one of the first groups to take advantage of Bitcoin's broader technical functionality. They effectively built a decentralized, digital asset register on top of Bitcoin. Users could mint and trade their own tokens directly on top of the base layer. The technical details of how they accomplished this are not relevant, except for one particular feature. Since Bitcoin's beginning, users have been able to add bits of data to the blockchain, allowing it to handle more than simple monetary transactions. The Counterparty developers, among others, used this feature to build their products. Unfortunately for them, the Core developers were aggravated by people using the technology this way, because they thought it "bloated" the size of the blockchain. However, because it's impossible to completely prevent users from doing this, the Core developers decided to make an explicit feature to add small amounts of data to the blockchain in the least disagreeable way possible, which they called the "OP_RETURN" function.

When OP_RETURN was originally announced, it was supposed to allow for 80 bytes of data to be added to transactions—which could then be easily discarded by miners and nodes. Working with this 80-byte number, the Counterparty developers would build out a new version of their platform. However, when OP_RETURN was finally released, its size was cut in half, effectively crippling the projects that were being built for 80 bytes[3]. This sparked a heated controversy and debate among the public, the Core developers, and the Counterparty developers.[4]

The Core developers' decision left a bad taste in many people's mouths and was considered anti-innovative. It was noticed by none other than Vitalik Buterin, who credited the controversy as one of the reasons he created Ethereum on an entirely separate blockchain instead of building on Bitcoin. He wrote:

The OP_RETURN drama preemptively pushed me toward building ethereum on Primecoin instead of Bitcoin. The primecoin plan was scrapped because we ended up getting more attention and resources than we expected, and so we could build our own base layer...[5]

And elsewhere he stated:

The very earliest versions of ETH protocol were a counterparty-style metacoin on top of primecoin. Not Bitcoin, because the OP_RETURN wars were happening at the time and given what certain core developers were saying… I was scared that protocol rules would change under me (eg. by banning certain ways to encode data in txs) to make it harder, and I did not want to build on a base protocol whose development team would be at war with me.[6]

Greg Maxwell would respond to Buterin, clearly upset at the claim that the behavior of the Core developers contributed to Buterin's decision to leave Bitcoin. Maxwell said:

[C]an you show even a single piece of evidence supporting this? How would OP_RETURN have anything to do with ethereum, it does nothing by definition[7]

To which Buterin replied:

You don't remember the OP_RETURN drama? The point is that I took things like the reduction to 40 bytes as an act of war against [Counterparty-style] meta-protocols using the bitcoin blockchain (which is what Ethereum would have been).[8]

Pushing Away Talent

Many of the key Counterparty developers, along with countless other creative minds, would eventually shift their focus from the Bitcoin blockchain to the Ethereum blockchain instead. Today, Ethereum is still known for having a culture and platform more open to innovation. Cryptocurrency entrepreneur Erik Voorhees would later write:

Unfortunately I think the [Bitcoin Maximalists] made Bitcoin pretty unwelcoming to experimentation and app developers, they all went to Ethereum, and the network effect now exists clearly there. I don't think the Maxis care though, they have their gold 2.0 narrative, for better or worse.[9]

By pushing people away from Bitcoin, the Core developers reinforced their position as a centralized power over the entire network. They could determine how much creative experimentation would be allowed. They could also determine which projects were possible or impossible depending on what features they added—which made any personal connections with the Core developers valuable. They also ended up setting the culture around Bitcoin's development—which was often unnecessarily dramatic and hostile towards innovation. Regardless of whether they were permissive or strict, the important fact is that they had this influence in the first place.

The hostility of the Core developers towards creative usages of the blockchain is particularly ironic considering the popularity of the narrative that Bitcoin is "programmable money." Revisiting the OP_RETURN feature less than a year later, Greg Maxwell would write:

I think OP_RETURN has shown itself to be seriously problematic; and we continue to have problems with people beleving [sic] that storing non-bitcoin related data in the chain… is an approved, correct, non-antisocial use of the system.[10]

In Maxwell's vision, users are supposed to behave like members of a congregation, following a list of approved behaviors handed down by their superiors. This level of rigidity and control is not conducive to creativity, nor is it realistic for a network that, if allowed to scale, could comprise of billions of people. Individuals cannot be expected to know what the "approved" usage of a technology is; they will just use whatever functionality is helpful to them.

Entrepreneurs and creative professionals need assurance that the protocol they are building on will not suddenly break due to some developers changing their minds or deciding that a particular usage of the blockchain is unacceptable. In practice, the more constraints put on Bitcoin, the more users have been pushed to alternative systems that provide them with

additional functionality. As Gavin Andresen speculated in 2014, this was perhaps an intended result:

There is a small minority of people who believe that it would be BETTER if transactions moved to fiat currency, an altcoin, or some more-centralized off-blockchain solution. I strongly disagree.[11]

Fortunately, when Bitcoin Cash was released, OP_RETURN was one of the first things upgraded and increased to 220 bytes. This additional space, when coupled with significantly bigger blocks, enables more creative usages of the blockchain than are feasible with BTC. Increased data usage is not a significant concern within the big-block philosophy, since regular users do not have to run their own nodes, and miners can easily discard this data. Everyone is encouraged to take advantage of this feature and find new uses for it, even if Greg Maxwell would not approve!

Low fees are also critical to the long-term success of programmable money. The attitude towards high fees has shifted today, but originally, even a five-cent transaction fee was considered laughably high. In a famous interview, Vitalik Buterin commented:

Right now, a Bitcoin transaction costs five cents, which is… fine right now, because PayPal's fees are even stupider. But, you know, the internet of money should not cost five cents a transaction. [Laughter] It's kind of absurd.[12]

Despite how high the fees are across the cryptocurrency industry, Buterin was right. It is kind of absurd and unnecessary to have fees of more than a cent for the vast majority of transactions. If the utility of programmable money is hampered by five cent fees, imagine how much it's hampered by $50 fees. Stephen Pair of BitPay shared a similar opinion, commenting on Bitcoin's competitiveness as a payment system: "A penny for an average on-chain transaction is probably too expensive to be competitive."[13] There's no technical reason why that can't be achieved. It already is on the Bitcoin Cash network.

A Core Loss of Faith

The controversy surrounding OP_RETURN and other minor features was nothing compared to the anger that resulted from the refusal to increase the blocksize limit—especially since key Core developers had previously agreed that raising the limit was necessary, even if they did not want it entirely removed. Pieter Wuille wrote in 2013:

I'm in favor of increasing the block size limit in a hard fork, but very much against removing the limit entirely… My suggestion would be a one-time increase to perhaps 10 MiB or 100 MiB blocks (to be debated), and after that an at-most slow exponential further growth.[14]

Despite their words, their actions were stalling Bitcoin's growth at a critical time, and eventually, their small-block philosophy became even more radical. Bitcoiners everywhere were becoming impatient by 2013, louder by 2014, and were completely fed up in 2015. Nobody captured this sentiment better than Mike Hearn, in a public email thread with Greg Maxwell. Hearn started the email by quoting Maxwell, who was trying to argue that tiny blocks were always the plan from the beginning:

"It was well... understood that the users of Bitcoin would wish to protect its decenteralization [sic] by limiting the size of the chain to keep it verifyable [sic] on small devices."

No it wasn't. That is something you invented yourself much later. "Small devices" isn't even defined anywhere, so there can't have been any such understanding. The actual understanding was the opposite… Please don't attempt to bullshit me about what the plan was…

If Satoshi had said from the start, "Bitcoin cannot ever scale. So I intend it to be heavily limited and used only by a handful of people for rare transactions. I picked 1mb as an arbitrary limit to ensure it never gets popular."

... then I'd have not bothered getting involved. I'd have said, huh, I don't really feel like putting effort into a system that is intended to NOT be popular. And so would many other people…

He finished the email by suggesting Maxwell create his own altcoin rather than hijack and re-engineer Bitcoin to fit his personal preferences:

Look, it's clear you have decided that the way Bitcoin was meant to evolve isn't to your personal liking. That's fine. Go make an alt coin where your founding documents state that it's intended to always run on a 2015 Raspberry Pi, or whatever it is you mean by "small device". Remove SPV capability from the protocol so everyone has to fully validate. Make sure that's the understanding that everyone has from day one about what your alt coin is for.

Then when someone says, gee, it'd be nice if we had some more capacity, you or someone else can go point at the announcement emails and say "no, GregCoin is meant to always be verifiable on small devices, that's our social contract and it's written into the consensus rules for that reason".

But your attempt to convert Bitcoin into that altcoin by exploiting a temporary hack is desperate, and deeply upsetting to many people. Not many quit their jobs and created companies to build products only for today's tiny user base.[15]

Nobody put it better than Mike Hearn, then or now. Though he and Gavin Andresen shared a similar technical vision for Bitcoin, Hearn was clearly the more confrontational of the two. After seeing the failures of Bitcoin and what it's turned into today, I think Hearn's anger and frustration were justified, and he was certainly not alone.

"Our New Overlords"

Andreas Antonopoulos, who has since become a popular advocate for Bitcoin and cryptocurrencies, also expressed his frustration at the behavior of the Core developers—and Mr. Maxwell in particular—in the online forums, saying:

[Maxwell] has previously posted several misattributed quotes and then failed to retract them or apologize… Treat any quotes he posts with extreme suspicion, especially if they are selective, short, out-of-context and attempting to slander - ie, his usual schtick. He rationalizes his opinion as

the only one that matters, [a] somehow "neutral" opinion that we'd all accept if we weren't so dumb…

The only thing that mattered in this debate was the opinion of the 3-4 developers who did not want any process that… resulted in anything but what they had already decided. They twisted, turned and rationalized, but in the end did exactly what they intended from the beginning: censorship of particular opinions by exclusion and decree.

All hail our new overlords. They're not just coders, they are press directors and OWN bitcoin. As they often say, if you don't like it... fork.[16]

In late 2014, while Gavin Andresen was still working at the Bitcoin Foundation, he would write an article laying out a roadmap for scaling. After writing countless forum posts, blog posts, and email threads explaining why the blocksize limit needed to be raised, he concluded that it was finally time to move forward:

The next scaling problem that needs to be tackled is the hardcoded 1-megabyte block size limit that means the network can support only approximately 7-transactions-per-second… The intent has always been to raise that limit when transaction volume justified larger blocks…

"Because Satoshi Said So" isn't a valid reason [by itself]. However, staying true to the original vision of Bitcoin is very important. That vision is what inspires people to invest their time, energy, and wealth in this new, risky technology.

I think the maximum block size must be increased for the same reason the limit of 21 million coins must NEVER be increased: because people were told that the system would scale up to handle lots of transactions, just as they were told that there will only ever be 21 million bitcoins.[17]

Only a few months after this post was written, it became unmistakably clear that the Core developers were not going to raise the blocksize limit. If big-block Bitcoin was going to exist as Satoshi designed it, Hearn and Andresen would have to take matters into their own hands.

15

Fighting Back

Endless debates did not work. Bitcoin was not scaling, and small blockers were not interested in compromise. In May 2015, Core developer Matt Corallo wrote:

Personally, I'm rather strongly against any commitment to a block size increase in the near future. Long-term incentive compatibility requires that there be some fee pressure, and that blocks be relatively consistently full or very nearly full. What we see today are transactions enjoying next-block confirmations with nearly zero pressure to include any fee at all…[1]

So, later that year, it was resolved that the Core developers had to be routed around. A different software implementation would have to be created, and if a majority of hashpower switched to it, the network would successfully bypass Core altogether. Since the long-term goal was always to have competing implementations, the intransigence of Core provided a great reason to start the competition—a decision that would permanently change Bitcoin's history.

BitcoinXT and BIP101

Mike Hearn and Gavin Andresen had previously created an alternative implementation called BitcoinXT to make some non-critical changes to the software. BitcoinXT was still compatible with Bitcoin Core—they both connected users to the same network—but it allowed Hearn to work on another project called Lighthouse, which was a crowdsourcing platform that used Bitcoin as its currency. To get Lighthouse to work correctly, he needed minor changes made to the Core software, but since that proved nearly impossible, he just decided to make his own implementation instead. It was this alternative implementation that was chosen to be the big-block replacement of Bitcoin Core. The blocksize limit would be increased on BitcoinXT, making it incompatible with Core, and if a critical mass of miners used it, the network would be successfully upgraded, at long last, to

allow for larger blocks. Satoshi described this upgrade mechanism in the whitepaper, stating:

[P]roof-of-work also solves the problem of determining representation in majority decision making… Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it…

[Miners] vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.[2]

Not only would BitcoinXT upgrade the network from a technical perspective, it would also end Bitcoin Core's dominance over the source code, making XT the main repository online. The bad decision-makers and broken decision-making process within Core would no longer matter. A journalist for the New Yorker asked Andresen about this in an interview:

I asked Andresen whether, if XT were to achieve full acceptance, he would then include all the earlier Bitcoin core devs in the new XT team. He replied that "[XT] will have a different set of developers. Part of the reason for forking is to have a clear decision-making process for the software development.[3]

Readers who are sympathetic to the original vision might be thinking to themselves, "It's about time!", but keep in mind that the decision to route around Bitcoin Core was an extremely difficult one to make. Nearly the entire cryptocurrency world, at that time, was unified within one Bitcoin community and network. In my many conversations with Bitcoin entrepreneurs, the frustration at Core was almost universal, but the desire to keep the network together was even stronger. If the situation got messy, it could fracture the community and economy.

Keep it Together

The risk of a community fracture had to be compared to the risk of a network failure. If blocks became full, fees skyrocketed, and the network

could not handle the transaction load—an unprecedented event at the time—the user experience would become torturous and unreliable, and it could permanently turn people off from Bitcoin. In 2015, the technology had still not become mainstream yet, and lots of people from the financial world were eager to see it fail. So, the blocksize limit had to be raised to avoid a crisis; the Core developers had to be fired, but the industry needed to wait until the right moment. In hindsight, now that we've seen multiple cases of network failure on BTC, it's clear that the public can tolerate it—though perhaps because they have accepted the Core narrative and do not know better. Sky-high fees are certainly bad for BTC, but so far, they have not permanently destroyed its credibility.

Within Bitcoin development, there was a formal way to propose new changes to the software. Programmers would write "Bitcoin Improvement Proposals," otherwise known as "BIPs." BIPs ranged from trivial improvements to substantial changes. After a BIP was created, if there was any disagreement, a debate would ensue to figure out whether the proposal should be accepted or rejected. Various BIPs had previously been created to allow for blocksize increases. Some were modest increases; others were radical increases. None were accepted into Bitcoin Core.

Mike Hearn and others would create BIP101, proposing an immediate increase of the blocksize limit to 8mb, followed by tiny increases every block, resulting in a doubling of the limit every two years up to a new maximum size of 8GB by 2035—allowing for approximating 40,000 transactions per second (which was several times larger than Visa's throughput at the time). Hearn would later reflect on the proposal:

In August 2015 it became clear that due to severe mismanagement, the "Bitcoin Core" project that maintains the program that runs the peer-to-peer network wasn't going to release a version that raised the block size limit… So some long-term developers (including me) got together and developed the necessary code to raise the limit. That code was called BIP 101 and we released it in a modified version of the software that we branded Bitcoin XT. By running XT, miners could cast a vote for changing the limit. Once 75% of blocks were voting for the change the rules would be adjusted and bigger blocks would be allowed.[4]

The upgrade mechanism was simple and straightforward. Miners running BitcoinXT could cast a vote, and if a supermajority of the hashrate voted in favor of BIP101, then it would be activated after a two-week grace period. BIP101 was considered a "hard fork" upgrade because it would be incompatible with previous versions of the software—as opposed to a "soft fork" which maintains compatibility. Because of the way Satoshi hastily added the blocksize limit, it would take a hard fork to increase it. The Core developers would make loud protestations at the notion of a hard fork, claiming it could cause a network failure or split. In fact, many of them claimed it would be less risky to change the entire economics of Bitcoin than to have a hard fork. Pieter Wuille from Bitcoin Core stated:

If we are willing to go through the risk of a hard fork because of a fear of change of economics, then I believe [the Bitcoin] community is not ready to deal with change at all.[5]

In hindsight, the drama surrounding hard forks looks overblown. Nearly every cryptocurrency project undergoes hard forks, because they are an essential mechanism for upgrading critical code, fixing bugs, and reducing technical baggage. Ethereum regularly undergoes hard forks. Bitcoin Cash has undergone several since its release. But back in 2015, this precedent was not yet established, and Core was able to stoke fears that a hard fork could break the network. In reality, even if there was a software bug in the upgrade and the network was disrupted, it would simply be fixed, as other critical bugs have been in the past. The risks of disruption are negligible compared to the risks of overhauling the entire system—akin to taking chemotherapy to protect yourself from a common cold!

In my opinion, the real reason for the fear surrounding BIP101 was because it would have resulted in Bitcoin Core losing control over development and no longer holding the keys to the code repository online. Since XT would add BIP101, and Core would not, the two implementations would become incompatible with each other on the protocol level, resulting in the minority implementation being "forked off" the main network. Though this would be devastating for Core and their supporters, by requiring 75% of miners to support the change, it would ensure minimal disruption for regular users. The remaining miners would either have to upgrade their software to allow for larger blocks or create their own separate blockchain.

The history of BitcoinXT would permanently disprove the idea that Bitcoin is somehow beyond the reach of human influence. Instead, it is deeply social, and its history is not shaped by software code writing itself—it's shaped by individuals making difficult decisions in a social, economic, and political context. Though nearly every serious businessperson was supportive of a blocksize increase, some thought that firing Core outright would be too divisive. Instead, they would publicly support BIP101 and urge Bitcoin Core to merge it into their software. Several of the largest non-mining Bitcoin companies issued a joint statement endorsing BIP101 and 8MB blocks without explicitly endorsing BitcoinXT. Signatures included Stephen Pair, the CEO of Bitpay, Peter Smith, the CEO of Blockchain.info, Jeremy Allaire, the CEO of Circle.com, Wences Casares, the CEO of Xapo.com, Mike Belshe, the CEO of Bitgo.com, among others. The statement read:

Our community stands at a crossroads… After lengthy conversations with core developers, miners, our own technical teams, and other industry participants, we believe it is imperative that we plan for success by raising the maximum block size.

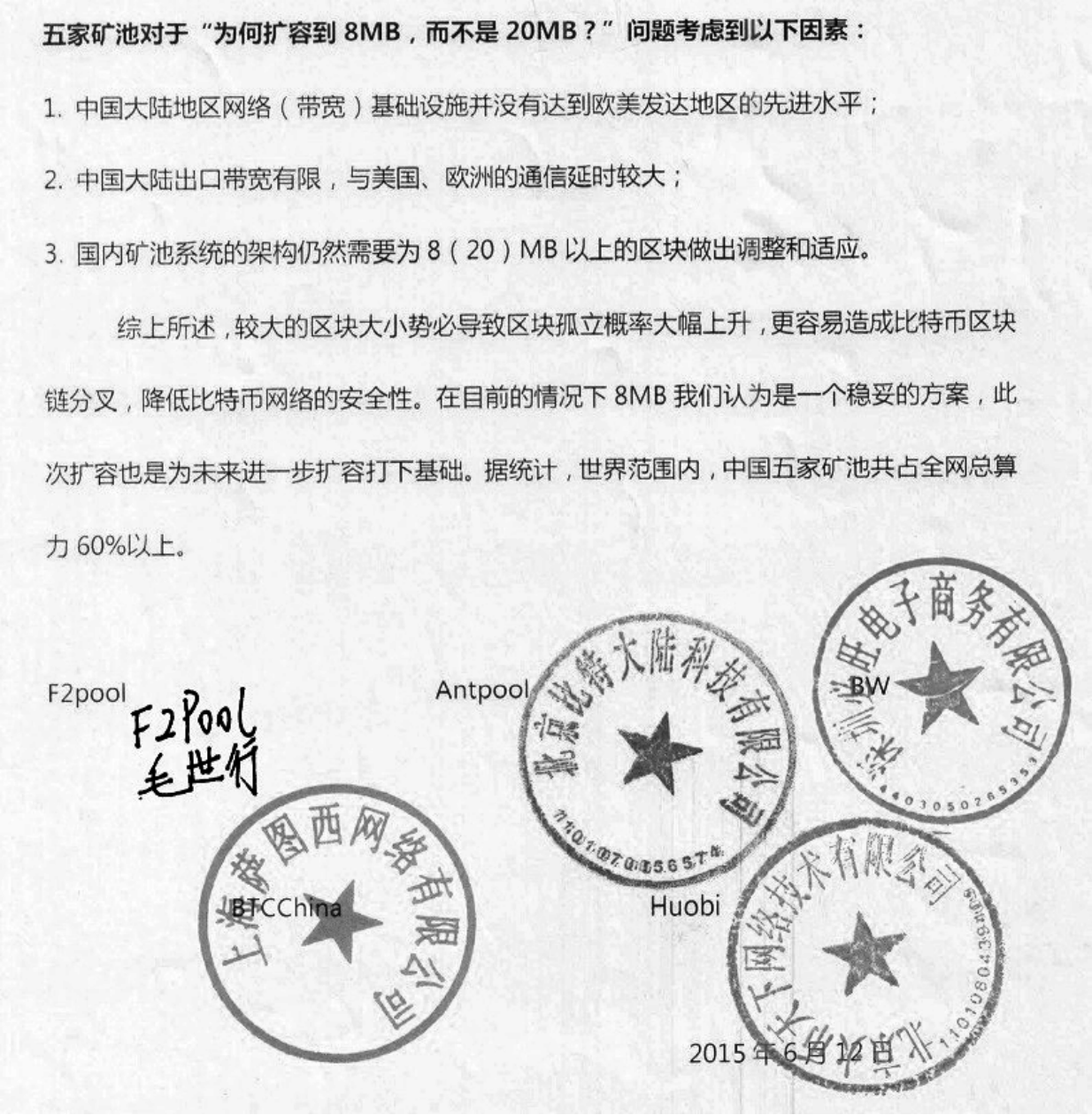
We support the implementation of BIP101. We have found Gavin's arguments on both the need for larger blocks and the feasibility of their implementation — while safeguarding Bitcoin's decentralization to be convincing. BIP101 and 8MB blocks are already supported by a majority of the miners and we feel it is time for the industry to unite behind this proposal.

Our companies will be ready for larger blocks by December 2015 and we will run code that supports this… We pledge to support BIP101 in our software and systems by December 2015, and we encourage others to join us.[6]

BitcoinXT is the unspoken part of this letter. "We will run code that supports BIP101 in December" translates to, "If Bitcoin Core does not allow this upgrade, we will switch to XT."

Some of the biggest miners at the time released a similar statement. In it, they not only expressed their support for larger blocks, they specifically

refuted one argument that Bitcoin Core had been promoting—that 8MB would be too large for Chinese miners who were stuck behind the famous "Great Firewall of China." Core had previously argued that 8MB would cause bandwidth and latency issues. But several large Chinese mining companies—representing more than 60% of Bitcoin's total hashrate[7]—signed a letter stating they were ready for 8MB blocks.



五家矿池对于"为何扩容到 8MB，而不是 20MB？"问题考虑到以下因素：

1. 中国大陆地区网络（带宽）基础设施并没有达到欧美发达地区的先进水平；

2. 中国大陆出口带宽有限，与美国、欧洲的通信延时较大；

3. 国内矿池系统的架构仍然需要为 8（20）MB 以上的区块做出调整和适应。

综上所述，较大的区块大小势必导致区块孤立概率大幅上升，更容易造成比特币区块链分叉，降低比特币网络的安全性。在目前的情况下 8MB 我们认为是一个稳妥的方案，此次扩容也是为未来进一步扩容打下基础。据统计，世界范围内，中国五家矿池共占全网总算力 60%以上。

F2pool

F2Pool 毛世行

Antpool

BW

BTCChina

Huobi

2015 年 6 月 12 日

Figure 5: Industry letter signed by Chinese miners

One translated section reads:

If the current network is incapable of supporting blocks larger than 1MB, then Core's insistence on the block size limit is understandable. But actually, even with the Great Firewall in place, Chinese mining pools have all said they want an 8MB block size.8

With the widespread international agreement that the blocksize limit must be raised, the power and influence of Bitcoin Core looked like it was coming to an end.

Time to Fork Off

On August 15th 2015, Mike Hearn wrote another landmark article in Bitcoin's history entitled "Why is Bitcoin Forking?" that explained why a split had to happen.9 The entire article is worth reading, and several excerpts are quoted here:

So this is it. Here we are. The community is divided and Bitcoin is forking: both the software and, perhaps, the block chain too. The two sides of the split are Bitcoin Core and a slight variant of the same program, called Bitcoin XT… Such a fork has never happened before. I want to explain things from the perspective of the Bitcoin XT developers: let it not be said there was insufficient communication…

Satoshi's plan brought us all together… It's the idea of ordinary people paying each other via a block chain that created and united this global community. That's the vision I signed up for. That's the vision Gavin Andresen signed up for. That's the vision so many developers and startup founders and evangelists and users around the world signed up for. That vision is now in jeopardy.

In recent months it's become clear that a small group of people have a radically different plan for Bitcoin… They see a golden, one-time opportunity to forcibly divert Bitcoin from its intended path and onto a wildly different technical trajectory.

He then explained that, given the enormous difference between the competing visions, the most sensible resolution would for small blockers to

create their own alternative coin rather than hijack Bitcoin by exploiting what he called a “temporary kludge”—i.e. the blocksize limit. However, it was clear that the small block faction would not leave to create their own independent project, nor would they compromise by even slightly increasing the limit. Hearn saw this as evidence of structural flaws within Bitcoin Core:

Why can this dispute not be resolved in some more civilised manner than an outright split? Put simply, the decision making process in Bitcoin Core has broken. In theory, like almost all open source projects, Core has a “maintainer”. The job of a maintainer is to shepherd the project and make decisions about what goes in and what doesn’t. The maintainer is the boss. A good maintainer gathers feedback, weighs arguments and then makes decisions. But in the case of Bitcoin Core the block size debate has been allowed to drag on for years.

The problem is that any change, no matter how obvious, can be nixed entirely if it becomes “controversial”, meaning another person with commit access objects. As there are five committers and many other non-committers who can also make changes “controversial” this is a recipe for deadlock. The fact that the block size was never meant to be permanent has ceased to matter: the fact that removing it is debated, is, by itself, enough to ensure it will not happen. Like a committee with no chairman, the meeting never ends…

After sharing a long list of key companies and individuals that were supportive of Hearn and Andresen, he then pointed out the enormous asymmetries of power between the Core developers and the rest of the entrepreneurs and engineers throughout the Bitcoin industry. No matter how much support a particular proposal received, it could be rejected by a handful of people with veto power:

Companies represent many of Bitcoin’s most passionate, devoted and technical people. They provide critical infrastructure. Yet the views of the people who build them are considered “misleading to the sense of consensus”. What about wallet developers? They are the people most exposed to the needs of day to day users. Never asked. When they spoke up anyway, it made no difference; their views are considered irrelevant…

It's become clearer and clearer that the "consensus" that's so often talked about in the Bitcoin Core community really means the views of a tiny handful of people, regardless of what anyone else in the wider community might think, how much work they have done, or how many users their products have.

Put another way, "developer consensus" is marketing, wool pulled over the eyes of Bitcoin users to blind them from the truth: just two or three people acting in concert can break Bitcoin in whatever way they see fit.

Hearn ended his article by illustrating that forks are the only way to prevent development capture, as they provide competitive pressure to keep developers from going rogue:

In short, they believe that the only mechanism that Bitcoin has to keep them in check should never be used. I don't think they really mean it to come across this way, but it does. Their view is that there shouldn't be any alternative to their decisions. That anything they object to, for whatever reason, is killed forever … and that Bitcoin is thus their toy to do with as they please.

This state of affairs cannot go on. The Bitcoin Core project has shown it cannot reform and so it must be abandoned. That is why Bitcoin has forked. We hope everyone understands.

Once again, nobody summed up the situation more accurately than Mike Hearn. His article was considered a brilliant articulation of the problems within Bitcoin, as well as a justification for forking off from Bitcoin Core. To small-blockers, however, it was considered an act of war. If a supermajority of miners followed Hearn and Andresen, the small-block vision of Bitcoin would be relegated to an altcoin, and the Core developers would effectively be fired. So, there was an immediate, widespread campaign to shut down XT before it gained too much momentum.

16

Blocking the Exit

Bitcoin looks the most decentralized when observed from a distance. Upon closer examination, it becomes clear that there are a small number of critical positions that have overwhelming influence over the network. Control over the software keys has already been established as one example. Another is the control of information flows online. BTC's powerful narrative, repeated everywhere in the media, did not spontaneously emerge, nor was it the result of free and open discussion among Bitcoin enthusiasts. The two most important discussion platforms, on which the overwhelming majority of conversations happened, were bitcointalk.org and the r/Bitcoin subreddit, both of which still enjoy immense popularity. Both platforms happen to be controlled by the same person, known by the pseudonym "Theymos." He also owns The Bitcoin Wiki (Bitcoin.it). That's one person with enormous power to shape narratives and direct the flow of information, and when the time came, he was not hesitant to exercise this power.

The Censorship Begins

Bitcoin.org used to be considered a neutral page for people learning about Bitcoin. It had basic introductory information, links to companies and services within the industry, and other resources that newcomers would find helpful. However, since it was controlled by hardcore Bitcoin Core supporters, this veneer of neutrality quickly evaporated once BitcoinXT started to threaten the dominance of the Core developers. On June 16th 2015, Bitcoin.org announced their official "Hard Fork Policy," which read:

It appears that the recent block size debate will likely result in a contentious hard fork attempt… The danger of a contentious hard fork is potentially so significant that Bitcoin.org has decided to adopt a new policy:

Bitcoin.org will not promote any software or services that will leave the previous consensus because of a contentious hard fork attempt.

This policy applies to full node software, such as Bitcoin Core, software forks of Bitcoin Core, and alternative full node implementations. It also applies to wallets and services… which release code or make announcements indicating that that will cease operating on the side of the previous consensus…[1]

In other words, any companies siding with BitcoinXT over Core would have their listings removed from the site. Since Bitcoin.org was, and still is, often considered the "official" website for Bitcoin, this policy would help create the narrative that any "contentious forks" away from Core are illegitimate by default. The announcement was immediately blasted by many Bitcoiners, Mike Hearn among them saying:

You want to ensure new users don't learn about Bitcoin XT. Why not just say that outright? Your position is wrong and will just reduce bitcoin.org's utility as a place to learn important information. What's more, you are inherently supporting a status quo in which a tiny number of people can veto any change to Bitcoin regardless of how widely supported it is by the rest of the community. That's not decentralisation. And it is ultimately far more dangerous to Bitcoin.

If you try and shut down the only method the community has to reject the decisions of this tiny group, you're effectively dooming the project to the whims of whoever happened to be around early on in the project and ended up with commit access.[2]

Hearn also noted the absurdity of the policy, given the enormous support for bigger blocks across the industry:

…it says you will delist any wallet or service that announces it will operate on the other side of the "previous consensus". Currently every single wallet bar GreenAddress that we've polled has told us they support bigger blocks. Additionally, every major payment processor we've talked to has also said that. Plus the major exchanges. So to be consistent with this policy you will have to delete every wallet and all major services (except GreenAddress) from the website.

Fellow Bitcoiner Will Binns wrote:

Bitcoin.org should try to [stay] as non-biased as possible in the midst of publicly debated issues. Hundreds of people, if not thousands, are coming to this site every day, many of which are new users learning about Bitcoin for the first time. For existing users in the space, this website is also an incredible resource in most cases.

It seems like this post would be in an effort to sway public opinion more-so than anything else. It doesn't provide a complete context nor link to a wider array of information about the underlying issues it references so the reader can form their own opinion - it comes across as forcing a biased one.[3]

This new Hard Fork Policy would not be the last time the Bitcoin.org website was used to mislead people into thinking that Bitcoin Core was the "official" software and that any competitors were illegitimate. Though, the impact of this particular policy was negligible compared to what happened to the online discussion forums.

Reddit Gets Captured

For months, it was common on the r/Bitcoin subreddit for users to complain about their posts being censored and removed from the platform. One of the most highly upvoted threads in the forum's history called for the moderators to step down and be replaced.[4] Shortly after this thread was posted it was removed, and the very next day in August 2015, Theymos announced a new moderation policy on r/Bitcoin that censored all discussion of BitcoinXT. The post is lengthy, but recommended reading, as it marked another milestone in Bitcoin's history. The key message was that all hard forks are illegitimate without a "consensus" of Core developers. Because of this, BitcoinXT was not really Bitcoin and therefore could no longer be discussed on the platform. Excerpts from the announcement are provided below:

r/Bitcoin exists to serve Bitcoin. XT will, if/when its hardfork is activated, diverge from Bitcoin and create a separate network/currency. Therefore, it and services that support it should not be allowed on r/Bitcoin…

There's a substantial difference between discussion of a proposed Bitcoin hardfork… and promoting software that is programmed to diverge into a

competing network/currency. The latter is clearly against the established rules of r/Bitcoin, and while Bitcoin's technology will continue working fine no matter what people do, even the attempt at splitting Bitcoin up like this will harm the Bitcoin ecosystem and economy.

Theymos further explains the decision in the form of a Q&A session:

Why is XT considered an altcoin even though it hasn't broken away from Bitcoin yet?

Because it is intentionally programmed to diverge from Bitcoin, I don't consider it to be important that XT is not distinct from Bitcoin quite yet…

Can I still talk about hard fork proposals on r/Bitcoin?

Right now, not unless you have something really new and substantial to say. After this sticky is removed, it will be OK to discuss any hardfork to Bitcoin, but not any software that hardforks without consensus, since that software is not Bitcoin.

How do you know that there is no consensus?

Consensus is a high bar. It is not the same as a majority. In general, consensus means that there is near-unanimity. In the very particular case of a hardfork, "consensus" means "there is no noticeable probability that the hardfork will cause the Bitcoin economy to split into two or more non-negligible pieces".

I know almost for certain that there is no consensus to the change in XT because Bitcoin core developers Wladamir, Greg, and Pieter are opposed to it. That's enough to block consensus…

But with such a high bar, 8 MB blocks will be impossible!

If consensus can never be reached on one particular hardfork proposal, then the hardfork should never occur. Just because you want something doesn't mean that it's ever reasonable for you to hijack Bitcoin from the people who don't want it, even if your side is the majority (which it isn't in this case).

This isn't some democratic country where you can always get your way with sufficient politicking. Get consensus, live without the change, or create your own altcoin…

Towards the end of his announcement, he added that it does not matter if everyone disagrees with him or despises the censorship:

If 90% of r/Bitcoin users find these policies to be intolerable, then I want these 90% of r/Bitcoin users to leave. Both r/Bitcoin and these people will be happier for it.[5]

The Bitcoin community was livid. Theymos's announcement was another dark milestone in Bitcoin's history, and it generated a huge reaction. The thread accumulated more than a thousand comments. A small sample of them provide the general tone of responses:

"[C]alling XT an altcoin is ridiculous, clinging to semantics at best. This topic deserves to be allowed to be hashed out, and banning further discussion of it is a gross disservice to the community."

"Please change this sub to r/bitcoincore if that's all that will be discussed here. Calling it r/bitcoin but banning discussions about alternative clients and consensus rules is misleading…"

Another user couldn't help but be sarcastic about the situation:

Congrats r/bitcoin, I am glad you have finally settled on the Bitcoin CEO, now you have that central authority that you always wanted that will tell you exactly how you are supposed to think and act. No more having to think and decide for yourself, you have theymos to tell you exactly what is bitcoin, what the laws and rules are about bitcoin, what the devs think… So if you are ever unsure about bitcoin Theymos will from now on make all the decisions for you..

One user speculated that the moderators might have been compromised:

I think it's worth discussing the possibility that the mod team has become compromised and banks (or whomever) could stand to make money

controlling the discussion.

Theymos was not shy about his decision, and he revealed his censorship strategy in conversation that would eventually be leaked:

You must be naive if you think it'll have no effect. I've moderated forums since long before Bitcoin (some quite large), and I know how moderation affects people. Long-term, banning XT from r/Bitcoin will hurt XT's chances to hijack Bitcoin. There's still a chance, but it's smaller. (This is improved by the simultaneous action on bitcointalk.org, bitcoin.it, and bitcoin.org)… I do have power over certain centralized websites, which I've decided to use for the benefit of Bitcoin as a whole…[6]

Regardless of the moral status of his decision, Theymos was correct that moderation can be effectively used for manipulation. It can teach people that questioning the official narrative is unacceptable and will be punished, and in this case, it was critical to establishing the popularity of small-block ideas. To this day, newcomers have no idea they are only being presented with one perspective—a perspective that Satoshi himself would strongly disagree with. When the average person encounters the same information on multiple platforms, on the Bitcoin Wiki, and throughout the discussion forums, he will not even be aware that there is another perspective, much less have an informed opinion about it. Over time, that kind of information control is immensely powerful.

Ripple Effects

The decision to censor all discussion of BitcoinXT did not just infuriate regular Bitcoiners. It also upset fellow moderators. A few days after Theymos' announcement, a dissident moderator "jratcliff63367" wrote a sharply critical article entitled, "Confessions of an r/Bitcoin moderator." One section reads:

When theymos decided to use his centralized authority of r/bitcoin to stifle all debate and discussion of bitcoin-xt, he violated a core principle. As a decentralized peer-to-peer network, any point of centralized control is problematic… This one single person holds absolute centralized control of

the two largest communications platforms for the community to discuss the future and evolution of bitcoin...

He exercises absolute power of what is, or is not, allowed to be discussed; including complete and total censorship power over the narrative in the two largest media outlets.[7]

Only ten days after jratcliff63367's public criticism of Theymos, he was removed as a moderator from r/Bitcoin. He would later speculate that his removal was because of suggesting that the Core developers might be compromised:

It is not at all unreasonable to suppose that core-devs have been contacted by the 'spooks' and are applying influence. Crippling bitcoin so that almost all of the value has to flow through side-channels and only large institutions can access the core network would be a great solution to what world governments consider as a major problem…

The government doesn't actually care if there is some new 'asset class' like bitcoin. There are zillions of asset classes, what do they care if it is bitcoins or beanie babies? What they care about is people transferring that value without their ability to track and intercept. If the only people who can directly access the blockchain are big-banks...well you get the idea.[8]

The same heavy-handed censorship still exists today, and the amount of people caught within this information bubble is much larger. The impact of these controls cannot be overstated. The enormous confusion surrounding Bitcoin exists, in large part, because of the deliberate efforts of a handful of people to filter out all information that challenges their narrative—and, ultimately, challenges their power. Unfortunately, mass censorship and propaganda were not the only tactics used against BitcoinXT. More aggressive measures were taken, too.

The DDoS Attacks Begin

SlushPool was one of many mining pools in Bitcoin. A mining pool is the standard way for miners to regulate their income. Without a pool, individual miners must wait until they personally find a block in order to earn any

Bitcoins. But with a pool, miners put their hashing power together and share the block rewards, smoothing out their income considerably. Virtually all miners are part of a pool. So, when SlushPool was hit with a DDoS attack after allowing voting on BIP101, it affected a lot of people. On August 25th, 2015, Slushpool received a letter from the perpetrators, telling them the attacks would continue until they stopped supporting BitcoinXT.[9] According to the MIT Technology Review:

Alena Vranova… said the company received a message saying that the attack would end once it turned off the ability for customers to declare support for Andresen's idea. [They were] forced to comply with that demand because the attack was powerful enough to cause connectivity problems for some Slush Pool miners. "This is a destructive behavior," says Vranova. "I would admire someone who stands out, explains, and promotes his idea. [But] this is just cowardly"…

Another victim was the Web hosting company ChunkHost, based in Los Angeles. It didn't receive a message, but the attack was focused on one customer who had recently switched the software powering a Bitcoin ATM to BitcoinXT. "It seemed pretty clear. As soon as he switched, he got attacked," says Josh Jones, a founder of ChunkHost.

Others running BitcoinXT reported the same thing. One user wrote on the forums:

It would seem that the conflict has taken a nasty turn, and some of the more extreme Core supporters have started just straight out DDoS attacking XT nodes… Looking at a recent drop-off at XTNodes.com, it seems that this has started during the last 24 hours, and one of my nodes was hit three times in that period, on a dedicated IP that only runs a Bitcoin node and nothing else…

Is this really how some people think they are going to "resolve" the situation? If this continues, I can easily see people starting to declare open season on non-XT nodes, and then we have a war going that no one wants.[10]

Over the following weeks, the forums started filling up with similar stories. Another user claimed his entire small town was knocked offline by one such attack:

I was DDos'd. It was a massive DDoS that took down my entire (rural) ISP. Everyone in five towns lost their internet server for several hours… because of these criminals. It definitely discouraged me from hosting nodes.[11]

Mike Hearn would join in some of the threads. On one post, he added:

The attackers have been telling pools to stop mining BIP 101 voting blocks if they want the attacks to stop. It's very clearly a Russian Bitcoiner who believes that everyone should use Core no matter what.[12]

No Competition Allowed

The Core developers were not happy about the idea of letting miners decide what the main software implementation should be. Just like with the blocksize limit, they argued that it would harm Bitcoin's decentralization. Hearn pointed out that without such a mechanism, the obvious threat to decentralization would be Core's monopoly over the protocol:

Right now the people doing the most to hurt decentralisation of Bitcoin are Blockstream and Wladimir, by telling people that using the block chain as a voting mechanism (as was done in the past) is reckless and will destroy Bitcoin's value. The logical implication of this argument is that only Bitcoin Core developers, and really only Wladimir, can change big chunks of the Bitcoin protocol. And thus that they are effectively the "CEOs of Bitcoin". Which is the opposite of decentralisation.

I mean, what is the point of open source, if you aren't supposed to fork it and modify the code when the original project does something wrong? How is Bitcoin's decentralisation even meant to work, with such a belief?[13]

A moderator of r/Bitcoin, user Hardleft121, reacted positively to Hearn's post, saying that "everyone should read this. it wasn't supposed to be like this. Mike and Gavin are right." Hardleft121 was also removed from his position as a moderator by Theymos.

Brian Armstrong was interviewed by Bitcoin Magazine about Coinbase's position with regards to BIP101 and BitcoinXT. He responded:

We are open to evaluating all proposals which increase the block size… In my view, Bitcoin XT is the best option I've seen so far. Not just because it has working code, but also because it has a simple implementation that is easy to understand, the block-size increases seem about right to me, and I have confidence in the people behind the project.

My preference at this point would be to have Gavin step up as the final decision-maker on Bitcoin XT, and have the industry move to that solution with help from Mike Hearn, Jeff Garzik and others that wish to do so…

We will upgrade regardless of whether Bitcoin Core is updated... I've been disappointed to see how slow Bitcoin Core has moved on this issue, and we're open to switching forks.14

The day that interview was published, it was linked to on r/Bitcoin, upsetting Theymos who immediately warned that Coinbase could be punished and censored from the online forums for their act of disobedience:

If Coinbase promotes XT to customers on coinbase.com and/or switches all of its full nodes to BIP 101 software, then Coinbase is no longer using the Bitcoin currency, and it doesn't belong on r/Bitcoin. This also applies to bitcointalk.org (where Coinbase would be restricted to the altcoin section). Bitcoin.it and bitcoin.org have similar policies. In fact, Coinbase was already almost removed from bitcoin.org due to your past statements in this matter.15

In December 2015, Coinbase announced that they were running BitcoinXT on their servers and supporting BitcoinXT, though they were still open to other proposals.16 In response, the owners of Bitcoin.org promptly removed Coinbase from their website—a remarkable move considering that Coinbase might have on-boarded more people to Bitcoin than any other company in the world! The removal was made by one of the owners of Bitcoin.org, another shadowy figure known by the pseudonym "Cobra" who stated:

Coinbase is now running Bitcoin XT in their production servers. XT is an contentious hard fork attempt that will create a new altcoin and split the community and blockchain should it ever go into effect. If this ever happens, Coinbase's customers may find that they no longer own any actual Bitcoin.

This pull request removes Coinbase from the "Choose your Wallet" page to protect new users from being on the wrong end of a blockchain fork. Bitcoin.org should only promote Bitcoin services. Companies that use XT don't meet this criteria because they support forking off the blockchain and switching to a new incompatible currency without broad consensus.17

This announcement again raised the ire of many Bitcoiners. Developer Jameson Lopp wrote:

The potential for forking does not an altcoin make. Until such time as a BIP101 fork occurs, companies running XT are definitely running Bitcoin. If a hard fork does occur, said companies may still be running Bitcoin - it would have to be judged which fork is the winner post-fork. Removing companies as "not running Bitcoin" when no fork has occurred is jumping the gun.18

Bitcoin veteran Olivier Janssens claimed that the move was retaliation for Coinbase having "dared to speak up against CoreDev."19 However, just as with the decision to censor, not every response was critical. One user expressed support for the move, saying it would establish a precedent for keeping companies in line with Core:

We definitely need to coerce Coinbase into switching back to Bitcoin Core. If we do not take any action, we're setting a dangerous precedent where other wallets and services are allowed to break apart from the consensus.20

There is something funny about the use of the term "consensus" to describe the position of a handful of Core developers as opposed to the overwhelming majority of industry participants. If there was any actual consensus in 2015, it was that the blocksize limit needed to be raised immediately. But despite the general backlash, Coinbase was successfully

removed from the Bitcoin.org website and was taken offline by a DDoS attack the very next day.21

17

Hotwired for Settlement

It scares me what the Bitcoin community is turning into. Any opinion that's not the party line is being stamped out.[1]

—Charlie Lee, Creator of Litecoin

BitcoinXT posed a real threat to small-blockers. So, they attacked it, claiming it risked the integrity of the entire Bitcoin network. Because the Core developers did not approve, XT was deemed "controversial" and therefore too risky, or even reckless, for anyone to support. Yet, this way of upgrading Bitcoin was described by Satoshi himself, all the way back in 2010. When asked by a forum member how to increase the blocksize limit, he responded:

It can be phased in, like:

if (blocknumber > 115000)

maxblocksize = largerlimit

It can start being in versions way ahead, so by the time it reaches that block number and goes into effect, the older versions that don't have it are already obsolete. When we're near the cutoff block number, I can put an alert to old versions to make sure they know they have to upgrade.[2]

Satoshi's method was simple and straightforward, as usual. He recommended creating a hard-fork upgrade that would increase the blocksize limit at a predetermined time in the future. That way, miners would have sufficient time to upgrade their software. Satoshi was not concerned with "consensus"—if a minority of miners did not upgrade their software, they would simply be kicked off the network.

Not only was forking expected, it was understood to be an integral part of the governance of Bitcoin. In the middle of the XT controversy, Wired Magazine wrote:

Bitcoin XT provides an unusually clear window onto the world of open source, an extreme example that demonstrates why, despite or even because of the current strife, this idea is so effective—why it's so quickly changing the way our world works. Bitcoin XT exposes the extremely social—extremely democratic—underpinnings of the open source idea, an approach that makes open source so much more powerful than technology controlled by any one person or organization.[3]

Charlie Lee also commented on the elegance of forking as a governance mechanism:

Like others have said, XT will only fork with [a] supermajority of miner votes. If it does get supermajority… then XT will be Bitcoin. That's how Satoshi designed the system.[4]

While in theory, the ability to fork is an excellent check on the power of development teams, in practice, it still requires extensive coordination among the miners, industry, and userbase. If switching to a new implementation is too risky, too painful, or too controversial, miners might decide to avoid forking altogether to avoid drama—which is what ended up happening with BitcoinXT.

Despite the open support for larger blocks, and BIP101 in particular, some miners started to get cold feet due to the controversy created by Core supporters. In an interview with CoinTelegraph, AntPool—a mining pool accounting for roughly 20% of the hashrate at the time—stated:

We like the idea of increasing the maximum block size, but if Bitcoin XT is too contentious, we also don't want the community to be divided. [5]

BTCChina's Director of Engineering wrote:

We think Gavin's proposal is a well-balanced solution that we all can stand behind and support. The initial 8 megabyte block size increase was also the agreed number amongst all mining operators in China. BTCChina Pool will unfortunately not be running Bitcoin XT due to its experimental nature, but we are looking forward to see[ing] this patch merged into Bitcoin Core.[6]

It's not hard to understand why miners would prefer the easiest option, which would have been Core coming to their senses and raising the blocksize limit. The entire industry desired the same thing, which is why it took years before BitcoinXT was created. However, as time went on, it became clear that Core would not change their minds, and to believe otherwise was simply wishful thinking. More decisive action had to be taken.

Bitcoin Core would find another way to obfuscate and delay by organizing a series of "Scaling Bitcoin" conferences that tried to persuade miners to keep running Core's software. At these conferences, they agreed that the blocksize limit had to be raised, but only to 2MB instead of 8MB. Miners were urged to keep trusting Core and wait a little longer for more substantial upgrades. In August 2015, the CEO of Blockstream Adam Back wrote: "My suggestion 2MB now, then 4MB in 2 years and 8MB in 4years then re-asses. [sic]"[7] And later in December of that year added: "There is consensus from developers, miners that 2MB is next step."[8]

A 2MB blocksize limit might have only been a quarter of what miners wanted, but it still would have doubled Bitcoin's throughput, allowing a little more time before blocks became full and fees skyrocketed. Over the following years, this 2MB compromise was agreed to several times, with Core ultimately breaking their agreements every time.

While the desire to avoid controversial forks is understandable, Satoshi's design requires that miners assert themselves, especially when faced with development capture. This is a mechanism to balance power within Bitcoin, but ultimately, it's one that depends on human choices and cannot be enforced by the software itself. So, when XT failed, Mike Hearn considered it a demonstration that Bitcoin could not overcome the human, social, and psychological barriers limiting its own success. He would later write:

[Regarding] the miners specifically I called some of them via Skype… One or two refused point blank to talk to me. One miner said he supported me, but couldn't be seen to do so in case it hurt the price. Another conversation went like this:

Miner: “We agree the block size should be raised and we agree Core is not going to do so.”

Me: “Great! So when will you start running XT?”

Miner: “We aren’t going to run XT.”

Me: “Er, but you just said you agree with our policies and don’t think Core will come around.”

Miner: “Yes, we agree that you are right, but we will never run anything except Core. To do that would be to leave the consensus…We can’t run XT, that’d be crazy. We will wait for Core to change their minds.”

That was the point where I decided it had all become a waste of my time. The vast majority of mining hash power was controlled by people who were psychologically incapable of disobedience to perceived authority.[9]

“The Resolution of the Bitcoin Experiment”

Amid the vitriol, censorship, DDoS attacks, and lawsuit threats, the number of miners running BitcoinXT steeply declined. And once it became clear that the 75% miner threshold would not be reached, Mike Hearn decided he had enough. If Bitcoin could not overcome Core’s centralized power and increase its tiny blocksize limit beyond 1MB, then in his mind, Bitcoin had failed.

On January 14th, 2016, Hearn penned the last of his excellent essays, entitled “The Resolution of the Bitcoin Experiment.”[10] In it, he explained why he considered Bitcoin a failed project:

It has failed because the community has failed. What was meant to be a new, decentralised form of money that lacked “systemically important institutions” and “too big to fail” has become something even worse: a system completely controlled by just a handful of people… there’s no longer much reason to think Bitcoin can actually be better than the existing financial system.

Think about it. If you had never heard about Bitcoin before, would you care about a payments network that:

- Couldn't move your existing money
- Had wildly unpredictable fees that were high and rising fast
- Allowed buyers to take back payments they'd made after walking out of shops, by simply pressing a button (if you aren't aware of this "feature" that's because Bitcoin was only just changed to allow it)
- Is suffering large backlogs and flaky payments
- Which is controlled by China
- And in which the companies and people building it were in open civil war?

I'm going to hazard a guess that the answer is no.

Hearn then explained the situation with the blocksize limit and placed heavy blame on the Chinese miners for their inaction—since at the end of the day, the miners did have the ability to break Core's stranglehold:

Why are they not allowing [the blockchain] to grow?

Several reasons. One is that the developers of the "Bitcoin Core" software that they run have refused to implement the necessary changes. Another is that the miners refuse to switch to any competing product, as they perceive doing so as "disloyalty"—and they're terrified of doing anything that might make the news as a "split" and cause investor panic. They have chosen instead to ignore the problem and hope it goes away.

Hearn then points out another potential conflict of interest. If the Great Firewall of China actually makes big blocks unfeasible for Chinese miners, that gives them "a perverse financial incentive to actually try and stop Bitcoin becoming popular." Instead of miners having an incentive to process more transactions to earn the transaction fees, a crippled internet connection would make limited transaction throughput and high fees more profitable—a desirable outcome from the perspective of the Core developers!

In the article, he blasts the rampant censorship and propaganda online, the DDoS attacks against XT nodes, and the "bogus conferences" that were designed to stall progress and persuade people to keep trusting Core. Specifically commenting on the "Scaling Bitcoin" conferences, he wrote:

Unfortunately, this tactic was devastatingly effective. The community fell for it completely. When talking to miners and startups, "we are waiting for Core to raise the limit in December" was one of the most commonly cited reasons for refusing to run XT. They were terrified of any media stories about a community split that might hurt the Bitcoin price and thus, their earnings.

Now the last conference has come and gone with no plan to raise the limit, some companies (like Coinbase and BTCC) have woken up to the fact that they got played. But too late.

Hearn draws a pessimistic conclusion, saying that the mining centralization in China would remain a problem, even with a different development team in charge:

Even if a new team was built to replace Bitcoin Core, the problem of mining power being concentrated behind the Great Firewall would remain. Bitcoin has no future whilst it's controlled by fewer than 10 people. And there's no solution in sight for this problem: nobody even has any suggestions. For a community that has always worried about the block chain being taken over by an oppressive government, it is a rich irony.

After airing his grievances, he ends on a more optimistic note:

[I]n the past few weeks more members of the community have started picking things up from where I am putting them down. Where making an alternative to Core was once seen as renegade, there are now two more forks vying for attention (Bitcoin Classic and Bitcoin Unlimited). So far they've hit the same problems as XT but it's possible a fresh set of faces could find a way to make progress.

If we judge Hearn's final essay from an investment perspective, he was clearly wrong. The price of BTC has appreciated more than 100-fold since

his essay was published. But his arguments still stand when judging BTC by its utility. The technology remains capped at an outrageously tiny transaction throughput level. The development is still dominated by one group that explicitly rejects Satoshi's original vision. Custodial wallets have become common, giving governments easy surveillance and control over regular users' coins. If BTC is to be judged by its usage as an alternative currency for regular people, it can only be called a failure. The best we can say is that it made early investors incredible amounts of money, and it sparked the creation of the cryptocurrency industry which might someday deliver sound, digital money for the masses.

Breaking the Narrative

Though Mike Hearn lost his patience and resigned from the project, the battle for Bitcoin was far from over. The entire industry still had an existential problem on its hands: would they even exist if the blocks became full? Buterin complained about fees when they were five cents—how would everyday users react if transaction fees were ten, twenty, or fifty dollars each? This uncertainty was unacceptable, and most companies knew they had to continue pushing for a blocksize increase. The industry would need to better coordinate and alert the general public to the takeover happening within Bitcoin. The information and narrative battle had to be fought.

During this time, several more excellent articles were written by proponents of the original vision. Jeff Garzik and Gavin Andresen penned another famous essay entitled "Bitcoin is Being Hot-wired for Settlement." They warned that Bitcoin was being transformed into a different system by leveraging the artificial blocksize limit:

> Getting stuck at 1M core block size transforms a historic DoS limit into an accidental policy tool…. we have a disappointing situation where a subset of dev consensus is disconnected from the oft-mentioned desire to increase block size on the part of users, businesses, exchanges and miners. This reshapes bitcoin in ways full of philosophical and economic conflicts of interest…
>
> Inaction changes bitcoin, sets it on a new path…. Stuck-at-1M risks reversing bitcoin's network effect by pricing users out of the core

blockchain, forcing them onto centralized platforms…

[T]o remove long term moral hazard, core block size limit should be made dynamic, put in the realm of software, outside of human hands. Bitcoin deserves a roadmap that balances the needs of everybody who has worked hard over the last six years to grow the entire ecosystem.

Garzik and Andresen also commented on the Scaling Bitcoin conferences, saying that the conferences did not accomplish their stated goals and were only helpful to identify that a 2MB limit was low enough to reach universal agreement:

One of the explicit goals of the Scaling Bitcoin workshops was to funnel the chaotic core block size debate into an orderly decision making process. That did not occur. In hindsight, Scaling Bitcoin stalled a block size decision while transaction fee price and block space pressure continue to increase.

Scaling Bitcoin was useful in surveying consensus on core block size. 2M appears to be the consensus most common denominator.[11]

Stephen Pair also entered the fight, writing on behalf of BitPay, the largest Bitcoin payment processor in the world, which was on pace to handle over a billion dollars' worth of BTC transactions in a single year.[12] Over a series of articles, Pair wrote about the blocksize limit, BitPay's analysis of the network's power dynamics, and his total rejection of the idea that Satoshi's design was broken and in need of revision by the Core developers:

Some people believe that Bitcoin is best suited as a settlement system rather than a payment system. This notion is rooted in a view that it's not possible to have a truly decentralized, trustless payment system that can handle the day to day payments needs for the population of people on this planet. They think that Satoshi's vision of Bitcoin as a purely peer-to-peer version of electronic cash is unattainable.

That's nonsense. It can be done.

He then went on to explain that Bitcoin's value proposition comes from it first being a payment system, then, once successful, a settlement system in

the future:

History suggests settlement systems must start out as widely accepted payment systems… Bitcoin will make a fine settlement system if it first works well as a payment system. Bitcoin should only be limited by actual processing constraints and not arbitrarily chosen caps.[13]

Pair also addressed the notion that miners are somehow a threat to the security of the system and need their power removed. In an article entitled "Miners Control Bitcoin… and that's a good thing," he defends Satoshi's design and explains how it keeps Bitcoin decentralized:

A few weeks ago, I had a conversation with someone who expressed a notion that some control should be taken out of the hands of miners. I found that interesting. It begs the question, if you take some power out of the hands of miners, who are you giving that power to?

Should one person own the Bitcoin trademark? Should they have the power to set the official Bitcoin™ consensus rules? Perhaps miners should sign their blocks such that only those that have been certified to follow the official, trademark protected, Bitcoin™ consensus rules are allowed to create blocks. If you follow this line of thought to its logical conclusion, you end up with a centrally managed system with no need at all for mining.

He then explained the power of Bitcoin's incentive system, how it keeps miners from misbehaving, and why the miners are the most critical part of the network's security:

Individually, miners control very little, but collectively, they control everything about bitcoin. This is an important and fundamental property of Bitcoin… [O]ne miner alone, operating on a different set of rules, would produce blocks that are rejected by other miners. They wouldn't earn any reward for their efforts. So, while miners are competing with one another to produce blocks most efficiently, miners also have a need to cooperate…

Bitcoin places all power over the operation of the network in the hands of miners, and anyone can become a miner. This collective, coordinated action is what makes Bitcoin a powerful, novel and revolutionary system. To

undermine the power that miners have over Bitcoin is to undermine everything that is Bitcoin.

Despite the power assigned to miners by Satoshi, Pair acknowledges that this power can be surrendered if the miners refuse to make decisions, or if they simply do not realize that they possess such power in the first place:

Miners can delegate their power. They may choose to let a mining pool produce the blocks they mine, thus letting the pool enforce the consensus rules or censor transactions if they desire. Miners can also let others influence or control what software they run and the rules that software enforces. The only reason developers, mining pools or any other non-mining constituents have any say in the matter regarding consensus rules is that miners have chosen (consciously or negligently) to delegate their power.14

Pair's perspective was a commonly held one in 2016, but it's nearly unheard of today. In fact, if newcomers are trying to learn about Bitcoin's design, they will more than likely encounter the Bitcoin Wiki page which is dedicated to this exact topic, entitled "Bitcoin is Not Ruled by Miners." Readers are told that full nodes set and control Bitcoin's rules, not miners. According to the article, the ability for nodes to not upgrade their software keeps miners in check:

[I]f miners produce blocks which break the consensus rules, then to everyone running a full node, it will be as if these blocks never existed; these blocks create no bitcoins and confirm no transactions. Since most of the economy is in some way relying on a full node to verify transactions, this prevents the miners who are creating invalid blocks from actually breaking any rules with any sort of real-world effectiveness, even if 100% of miners are doing so…15

As explained in Chapter 6, if the majority of miners decide to change the software they run, while some nodes run incompatible software, the nodes simply get forked off the network. Full nodes, by themselves, do not have the power to generate blocks, and therefore do not have the power to process transactions by themselves. The network can run fine without these nodes, but it would come to a screeching halt without miners. It is absurd to

imagine Bitcoin was designed so that hobbyists running nodes in their basement could prevent 100% of miners—who spend hundreds of millions of dollars on infrastructure—from upgrading their software. Yet, the article doubles down and further claims that the network requires most participants to run their own nodes, otherwise the whole system becomes insecure:

If not much of the economy is running independent full nodes, then Bitcoin is ruled by someone. If most of the economy is using SPV-style lightweight nodes… then Bitcoin is ruled by miners and therefore insecure.

After articulating the opposite of Satoshi's philosophy, the article concludes with another absurdity:

The result of all this is that there is no "Bitcoin governance"; Bitcoin is not governed. No person or group can force their views on anyone else, and even things like the definition of a bitcoin can be subjective… [A]chieving this non-governance was one of the primary motivations behind Bitcoin, it continues to be one of its biggest advantages over traditional systems, and both the system itself and the Bitcoin community will vigorously resist any attempt to weaken this feature of Bitcoin.[16]

No one who understands the history and network design of Bitcoin could say it exists without governance. The term "non-governance," like "digital gold," is nothing more than a catchy slogan that misleads people about Bitcoin's true design. Readers should not be surprised to learn that this article on the Bitcoin Wiki—which claims to speak on behalf of the Bitcoin community—was written by the same person who has control over all the major discussion platforms: Theymos himself.

18

From Hong Kong to New York

The fact that Bitcoin Core has allowed the network to reach this point is incredibly negligent, and I think says a lot about their motivations and competency as a team.[1]

—Brian Armstrong, CEO of Coinbase

At the beginning of 2016, more than 90% of the network hashrate expressed support for increasing the blocksize limit to at least 2MB.[2] While BitcoinXT was not chosen as the implementation to make the increase happen, another quickly took its place. Bitcoin Classic, led by Gavin Andresen and Jeff Garzik, immediately gained popularity as a conservative alternative to Bitcoin Core by only increasing the limit to 2MB. Like XT, Classic would increase the blocksize limit only after reaching a threshold of 75% of the hashrate. Just days after Classic's website was created, 50% of the hashrate stated their support for the new implementation.[3] The Wall Street Journal quickly took note:

[A]nother proposal, this one called Bitcoin Classic, has emerged from the ashes of the XT/Core debate. It is a version of bitcoin that would allow for a two-megabyte limit, with rules put in place to raise it over time. It appears to be quickly winning support.[4]

Despite its instant popularity, not everybody was ready to fork away from Core. The BTCC mining pool were early skeptics of Classic, though they supported a blocksize limit increase. Their preference was to avoid the controversy by having Core simply increase the limit themselves:

We support a 2 MB increase but we will not sign on to support Bitcoin Classic… Just because people are gravitating to something doesn't mean you automatically jump on board without some serious analysis… The ideal situation for us is to have the 2 MB increase done in Core, followed by [SegWit].[5]

“SegWit” stands for “Segregated Witness” and will be explained later.

The strategy of waiting for Core to increase the blocksize was not one with a good track record. Eric Voorhees, the creator of the extremely popular Satoshi Dice game and the ShapeShift exchange, would comment on BTCC’s position, urging them to support Classic—if only to pressure Core into compromise:

The only circumstance under which Core would go to 2MB is if they feel an imminent hard fork toward Classic (or something else). If your desire is to get Core to add 2MB, signing on to Classic is probably the most effected [sic] path.[6]

By the end of February 2016, it looked like the pressure was starting to work. An emergency conference was organized in Hong Kong with several large miners, companies, and key Core developers.

The Hong Kong Agreement

The goals of the industry were clear: find a way to scale Bitcoin to avert the impending network failure and do it without fracturing the community into pieces. The goals of the Core developers were different. First and foremost, they had to protect their own jobs, since they were under the threat of being fired and replaced by Bitcoin Classic. So, they promised a small blocksize increase in exchange for miners pledging to only run Core software. On February 20th, an agreement was reached, now called the “Hong Kong Agreement” or “HKA.”[7] The two key components of the HKA were:

1) A hard-fork upgrade to raise the blocksize limit to 2MB.

2) A soft-fork upgrade to enable SegWit.

The miner pledge read, “We will only run Bitcoin Core-compatible consensus systems, eventually containing both SegWit and the hard-fork, in production, for the foreseeable future.” The agreement also came with a timeline. SegWit would be released in April 2016, the code for the hard-fork in July, and the hard-fork would be activated around July the following year. Since Classic was a 2MB upgrade, and Core promised the same, the agreement made sticking with Core more palatable to miners—if they could

just hold on another few months, they would get to 2MB without all the controversy.

In contrast with the relatively simple blocksize increase, SegWit is a much more complicated change to the software which alters the way transactions are structured. SegWit slightly increases transaction throughput, but its primary purpose is to make second layers like the Lightning Network easier to build. Significant criticisms have been leveled at SegWit from people like Dr. Peter Rizun and others.[8] Critics have pointed out potential security weaknesses, and everyone acknowledges the code comes with serious "technical debt"—permanent increases in software complexity. The more complex the software, the more difficult it is to work with, and the more bugs will inevitably be created, and SegWit was a huge increase in complexity. Every wallet in the industry had to be written in order to accept SegWit transactions safely—a complaint brought up by several different companies at the time.

Despite the criticisms, I have never had a strong opinion about the merits of SegWit. To me, the most important part of Bitcoin is having fast, cheap, reliable transactions that cannot be censored by a third party. If SegWit can increase those qualities, then it's a good idea. If it detracts from those qualities, then it's a bad idea. However, by itself, it's not sufficient to increase transaction throughput by a meaningful amount. But given the urgency of the situation in 2016, it seemed like a tolerable compromise to get a blocksize limit increase without splitting the network in two—that is, assuming Core would follow through on their promises.

While the HKA did not get unanimous support, it did garner the signatures of several key players involved with mining, including AntPool, Bitmain, BTCC, and F2Pool, comprising a significant percentage of the total hashrate. A few cryptocurrency exchanges signed on, too. Five Core developers added their signatures, along with the CEO of Blockstream Adam Back. Brian Armstrong was a notable critic, and he flew back from Hong Kong convinced that Bitcoin Core needed to be replaced as soon as possible. Shortly after attending the conference, he would write an article that warned of "the systemic risk of Core being the only team working on the protocol" and urged switching to Bitcoin Classic:

We need to communicate with the Chinese miners about this upgrade path. They have been misled to believe that only 4–5 people in the world can safely work on the bitcoin protocol, when in fact it is this group that poses the greatest risk for their businesses…

By upgrading to BitcoinClassic it does not mean we need to stay with the Classic team forever, it simply is the best option to mitigate risk right now. We can use code from any team in the future.

The article also reaffirmed the importance of having multiple software implementations to keep Bitcoin healthy and avoid development capture:

My general view (which I articulated at the roundtable last weekend) is that bitcoin will be far more successful with a multi-party system working on protocol development than a single team with the limitations I mentioned above. I think we can make this happen. In fact, we must make this happen…

Long term, we need to form a new team to work on the bitcoin protocol. A team that is welcoming of new developers to the community, willing to make reasonable trade offs, and a team that will help the protocol continue to scale.[9]

The Hong Kong Agreement did not dissuade bad actors from targeting Bitcoin Classic nodes, as they had previously done to BitcoinXT. Another round of DDoS attacks would punish anybody running alternatives to Core, and the online forums started to fill up again with stories of the attacks. Blocky.com reported:

The current attack is the latest to show that a simple disagreement over scalability has descended into chaos and has brought to [the] surface criminal elements within our community. The disagreement follows recommendations to increase capacity to 2MB as an emergency measure to release the pressure on transactions which are currently operating at maximum capacity with blocks being full.[10]

Bitcoin.com was also attacked, leading to our ISP shutting down a server for several hours. Our CTO at the time, Emil Oldenburg, wrote about the

motivation behind the attack:

The purpose of this attack is to intimidate anyone running Bitcoin Classic. It's the same modus operandi we saw with Bitcoin XT. This comes at a time when miners have started to mine Bitcoin Classic blocks and already have way more support than XT ever had.

Someone, or some people, are buying DDOS attacks towards Classic in an attempt to stop the growth of Classic nodes and blocks. Some Core developers, and Adam Back, have stated that 'Bitcoin is not a democracy', while this description is correct for the current governance model; with the censorship, character assassinations, attacks against anyone who disagrees with the party line and sabotage against free choice, the current governance is more similar to North Korea.[11]

The magazine CoinTelegraph covered the story of F2Pool, a Chinese mining pool accounting for more than a quarter of Bitcoin's total hashrate, being attacked immediately after allowing their miners to run Classic:

The attacks began to target the F2Pool Bitcoin mining pool almost immediately after the F2Pool team announced their decision to "test" Bitcoin Classic by launching a subpool in which miners can mine Bitcoin Classic blocks.[12]

Once again, the attacks proved remarkably effective. Bitcoin Classic enjoyed its highest support around the middle of March 2016 before rapidly declining.

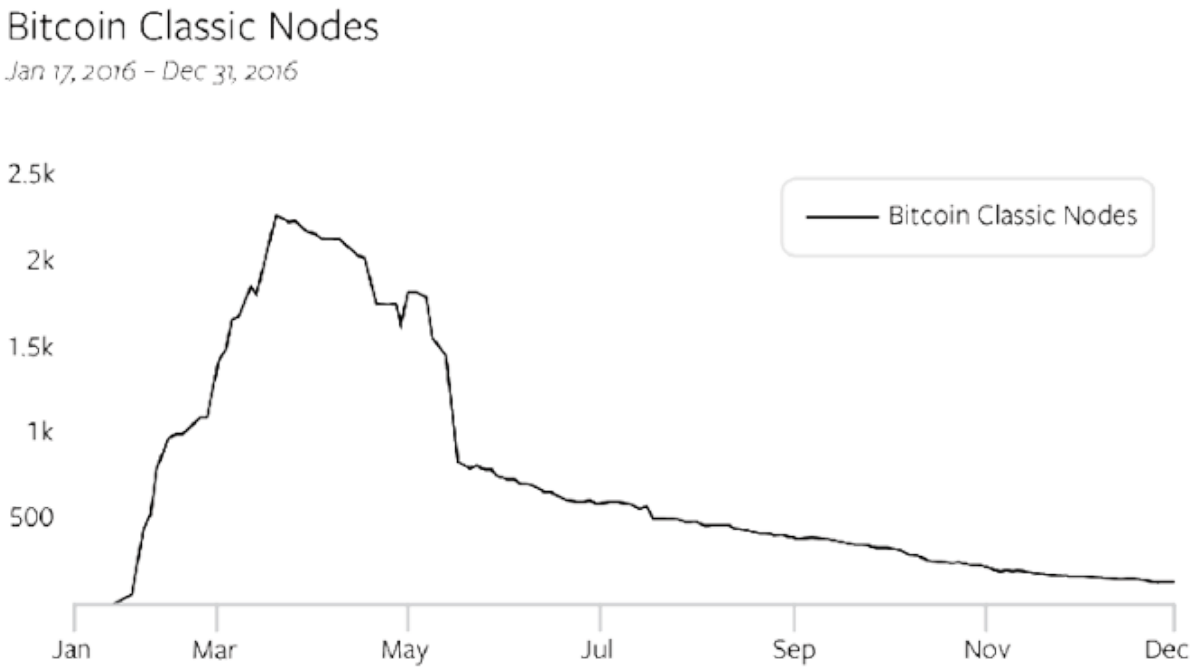


Figure 6: Number of active Bitcoin Classic nodes[13]

It's not hard to understand why. Running Bitcoin Classic was controversial and risked forking the network in two, and it was an open invitation to DDoS attacks. Plus, Classic only upgraded to 2MB blocks, which were already promised by Core at the HKA. So, to a large number of miners, trusting Core seemed like a safer option. Unfortunately, their trust was misplaced, and Brian Armstrong's criticisms would prove prescient. The Core developers missed their deadlines for both the SegWit upgrade and blocksize increase. They did not adhere to the HKA, and the blocks kept getting fuller.

Tighter Information Controls

Meanwhile, the war to control Bitcoin's dominant narrative was raging. Rampant censorship was not the most extreme tactic used. The owners of key informational websites became even more brazen. In July 2016, the Bitcoin.org owner "Cobra" came up with an idea: perhaps newcomers could be prevented from learning about Bitcoin's original design by changing the whitepaper itself:

I've been noticing that the Bitcoin paper… is getting a lot of traffic… Almost all the people reading the paper are probably reading it for the first time, and using it as a learning resource. However since the paper is so outdated, I believe it doesn't do a good job anymore of giving people a firm understanding of Bitcoin…

I feel like the Bitcoin described in the paper and the Bitcoin described on bitcoin.org are starting to diverge. At some point, I think the paper will start to do more harm than good, because it tricks people into believing they understand Bitcoin.

Cobra then makes the extraordinary claim that the whitepaper is not meant to explain Satoshi's original design but rather to explain how the present Bitcoin Core software works:

I have seen people promote toxic and crazy ideas, and then cite parts of the paper in an effort to justify it. Academics are also regularly citing the paper and basing some of their reasoning and arguments on this outdated paper…

I believe the paper was always designed to be a high level overview of the current reference implementation, and that we should update it now that the paper is outdated and the reference implementation has changed significantly from 2009.[14]

By Cobra's logic, even if the Core developers wildly changed the code to lose all resemblance to the original Bitcoin, the whitepaper should be altered to reflect those changes. Theymos immediately commented on the thread, agreeing that the whitepaper misleads people:

Interesting suggestion. The paper is definitely outdated, and I do often see people saying "just read the whitepaper!" as if the paper is still a good way to learn about Bitcoin…[15]

Fortunately, this proposal was met with sufficient resistance to block the change, though it would not stop them from trying again in the future. Theymos would later make another outrageous proposal, that companies should be required to pledge their allegiance to the small-blocker narrative in order to have their products listed on the Bitcoin.org website:

[S]everal companies said that miners control Bitcoin. This belief is one of the most dangerous threats to Bitcoin… I've been thinking that bitcoin.org should somehow act against this more than it is already. For example, maybe bitcoin.org should require that wallets and services sign a very simple pledge that acknowledges that Bitcoin is not ruled by miners in order to be linked from bitcoin.org.16

Cobra chimed in, again criticizing the whitepaper and calling for it to be revised or replaced altogether:

The whitepaper is to blame for all these dangerous beliefs. We seriously need to rewrite it, or produce a completely new whitepaper and call that the Bitcoin whitepaper.17

These quotes are shocking in their brazenness. Two unknown people who control the most prominent websites in Bitcoin are eager to censor, propagandize, and even rewrite history to push their narrative. The average user does not even know of the existence of Theymos and Cobra, much less so the history of how they pushed a version of Bitcoin that is diametrically opposed to the original one—neither do prominent investors that I have spoken with in private, because it takes significant independent research or long-term involvement in the industry to figure out.

BU, NYA, S2X, and Other Acronyms

2016 came and went without SegWit or a blocksize increase, and the next year would become the craziest in Bitcoin's history. In January 2017, blocks were regularly running at 90%+ capacity, occasionally bumping into the 1MB limit, and by March, the average transaction fee passed $1—an increase of more than 1,000% in less than a year. Early Bitcoin entrepreneur Charlie Shrem wrote:

If we don't implement bigger blocks ASAP, Paypal will be cheaper than #bitcoin. I already pay a few dollars per tx. Stop hindering growth.18

The next alternative implementation started to gain steam. The Bitcoin Unlimited (BU) team wanted to replace the hard-coded blocksize limit with something they called "emergent consensus." The basic idea was simply to

allow miners and nodes to set their own limit without needing approval from anyone. Economic incentives, they thought, were strong enough to keep the network coordinated and functional. I agreed with their analysis.

Despite gaining momentum in early 2017, BU was hated by the typical characters and subject to attacks. On Reddit, multiple anonymous users shared their intentions to exploit any bugs they could find for maximum effect.19 They succeeded, and in the middle of March, over half the Bitcoin Unlimited nodes were successfully brought down in a coordinated attack. The bug did not cause much damage itself, but it did damage the reputation of the BU developers at a critical time. A Bloomberg article covering the attacks wrote:

While the exploit was quickly patched, it is validation to critics who say Unlimited programmers lack the experience to fix bitcoin's complicated congestion issue. Unlimited had in recent weeks won the backing of influential miners, as some decided to give up on reaching a community consensus after more than two years of discussion. The bug raises uncertainty about whether miners will follow through on their support.20

During all the drama, BTC's market share also started crashing. At the beginning of the year, BTC enjoyed about 87% of the total market cap of all cryptocurrencies. By May, it plummeted below 50%. The Bitcoin industry was finally starting to feel the consequences of delaying scaling for years. So, another conference was organized, this time in New York. The largest economic players were invited, along with key Core developers.

An agreement was quickly reached—a conservative one, resembling the HKA that was previously agreed upon. SegWit would be activated with an 80% miner threshold, and a 2MB blocksize increase would happen within six months. This would become known as the New York Agreement, or "NYA." Famously, all the Core developers refused to show up for the conference, so the industry had to find agreement amongst themselves. My company Bitcoin.com signed the NYA, though I was unable to attend personally. Had I been there, I would have objected to one glaring problem with the whole plan: the blocksize increase was supposed to happen after SegWit was activated. What if, after accepting SegWit, another campaign was organized to attack all alternatives to Core? Would the miners finally

commit to an alternative implementation? It was an enormous gamble that turned into an enormous blunder.

The New York Agreement gained signatures from 58 companies from 22 different countries, representing 83% of the hashpower, over $5 billion of monthly on-chain transaction volume, and more than 20 million Bitcoin wallets.[21] The support was so universal, that even prominent critics of Core and SegWit signed on. For example, the mining pool ViaBTC had written a scathing article the month prior explaining why they did not support SegWit as a scaling solution, saying:

Network capacity is now the most urgent issue for Bitcoin… SegWit, which is a soft fork solution for malleability, cannot solve the capacity problem… Even if SegWit after activation can slightly scale up block size with new transaction formats, it's still far behind the demand for the development of Bitcoin network.

Second-tier networks such as Lightning Network (which relies on SegWit) cannot be considered as a block scaling solution. LN transactions are NOT equal to Bitcoin's peer-to-peer on-chain transactions and most Bitcoin use scenarios are not applicable with Lightning Network. LN will also lead to big payment "centers", and this is against Bitcoin's initial design as a peer-to-peer payment system. It can be a good method though for frequent and small Bitcoin transactions in certain cases. But we cannot rely on it as a cure for Bitcoin scaling.

Their article then explains how SegWit will strengthen Core's dominance over the Bitcoin protocol:

As an implementation reference for Bitcoin, Bitcoin Core was of significant influence in the community. However, their influence has long been overrated by their actions. By abusing their previous influence, they've obstructed Bitcoin block size increase from happening, against the will of the community. Core team has in some cases explicitly, supported censorship of Bitcoin's mainstream forums, along with banning of many prominent developers, businesses, and community members who have different opinions with Core's current roadmap. Today, Bitcoin is in urgent need of

diversified dev teams and implementations to achieve decentralization in Bitcoin development.

Should SegWit be activated, Bitcoin will have no choice but to proceed with Core's current roadmap in the coming years, which will further intensify the impacts of an incompetent dev team on Bitcoin community and rule out the possibilities for Bitcoin to grow in multiple directions.[22]

Yet, despite their strong criticism, they still signed on to the NYA to try and keep the community unified around the same coin and preserve hard-won network effects. By June 2017, transaction fees continued to skyrocket to over $5 on average—now up more than 5,000% from the previous year.

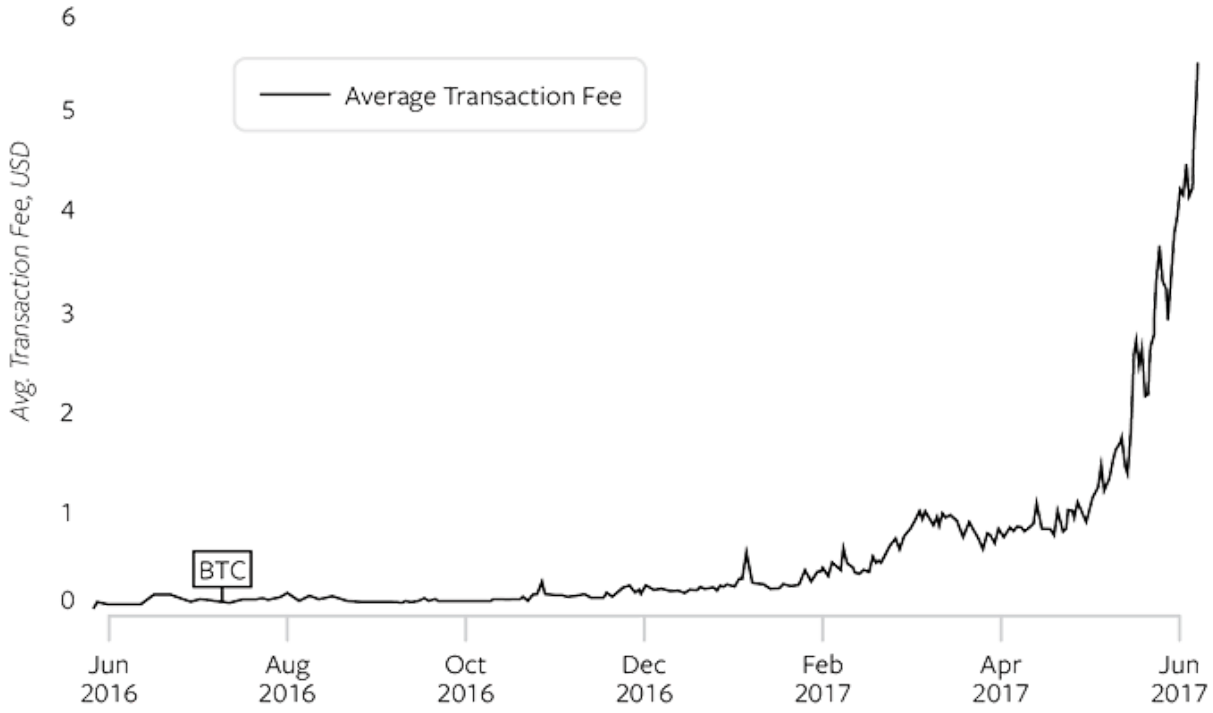


Figure 7: Average BTC transaction fee June 2016 - June 2017

BTC's relative market cap also hit a new low of 38%, as more people were choosing alternative chains like Ethereum which offered better performance. The overwhelming majority of the industry agreed that upgrading Bitcoin's capacity was urgent, but the Bitcoin Core developers were absolutely unwilling to increase the blocksize limit at all. So, other developers would

have to make it happen on a different software repository. Jeff Garzik was chosen as the lead developer for this new project, and the code he was working on would be called “SegWit2x” or “S2X.”

Once again, Core was at risk of being fired. If the majority of miners, running SegWit2x, produced a block larger than 1MB, the miners running Core would be forked off the network. Perhaps more importantly, the keys to Bitcoin’s code would finally be ripped from Core’s hands. So, another campaign was waged to demonize anybody supporting SegWit2x, which was simply the code to reflect the HKA and NYA. Greg Maxwell wrote:

[A] couple of well meaning dipshits went to China a few months back to learn and educate about the issues and managed to let themselves get locked in a room until 3-4 am until they would personally agree to propose some hardfork after segwit.[23]

Forum user httpagent commented about the hostility of Core towards anyone outside of their circle:

I’ve noticed a “know-nothing” strategy recently adopted by [Bitcoin] core - basically, the idea is that community members claim that everyone who isn’t part of core development is naive and has no valid position in debating the future of bitcoin.[24]

The remainder of 2017 would end up being a showdown between Blockstream/Core and the rest of the industry. Despite claiming for years—in the name of unity—that a fork should be avoided at all costs, Core supporters demonstrated that they had no real desire for cooperation. When the time came, they were ready to divide the community and attack their opponents by whatever means necessary.

19

The Mad Hatters

When Bitcoin Core released the SegWit code, they required 95% of the hashrate to signal for its activation before it would be implemented—essentially giving veto power to a 5% minority of miners. Core was heavily criticized for setting this threshold too high, since if enough miners dissented, they could block SegWit activation indefinitely, which is why the required percentage was brought down to 80% with the NYA. However, a different plan had already been hatched before the NYA happened, in order to try and force the miners to adopt SegWit.

Cut off Your Nose to Spite Your Face

Pseudonymous developer ShaolinFry announced his idea for a "User-Activated Soft-Fork" (UASF) in February 2017,[1] though the plan did not initially gain much attention. UASF was an attempt to explicitly challenge the power of miners by threatening to disrupt the network if SegWit was not quickly adopted.[2] Nodes running UASF code would refuse to accept blocks that did not signal for SegWit activation. Therefore, if miners produced blocks that were incompatible with the UASF code, the nodes would end up forking themselves off the network. While this sounds like a self-evidently bad idea, it could theoretically cause problems if they were able to recruit enough nodes with economic influence to run their code—say, from exchanges, payment processors, or wallet providers. Users could end up on a separate blockchain from the majority of miners, without their knowledge or consent, potentially losing funds or having their payments fail.

The UASF architects tried to appeal to economic incentives to gain momentum behind their idea. In addition to the possible pain caused by network disruption, they also argued that miners could make more profits by adopting SegWit, since it allowed for new transaction types. Fees could be earned from transactions in the original format plus the new one. The goal was to make immediate SegWit adoption the easiest path for miners, since they were already planning on adopting it anyway.

Both the UASF and its proponents had many detractors. The co-founder of OB1, Dr. Washington Sanchez, claimed that the "UASF is a fancy name for a Sybil attack."[3] A Sybil attack is where participants in a network cannot discern honest from dishonest actors. Since Bitcoin nodes are easy to create, it's possible to flood the network with dishonest nodes to make it harder for honest ones to connect with each other. Ironically, the proof-of-work requirement in Bitcoin is intentionally designed to protect from Sybil attacks. Nodes are cheap and easy to create, but miners are not. By requiring miners to demonstrate proof-of-work, it makes the cost of attacking the network exponentially higher, and this high cost is what allows honest actors to find each other. UASF tries to overcome this protection by threatening to fork off economically-relevant nodes from the network.

Miners Versus Full Nodes

There are several critical problems with the UASF concept. Most fundamentally, given Bitcoin's design, it still requires miners to participate. Even if the UASF nodes successfully forked themselves off the main network, without any miners cooperating, their chain would not be able to produce any new blocks. So, it would be immediately unusable. If they brought 5% of the hashrate with them, their chain would only be able to produce blocks at 5% the normal rate—instead of each block taking ten minutes on average, it would take two hundred minutes. They would also be subject to "51% attacks." A 51% attack is where a majority of hashrate is dishonest or malicious and can cripple a blockchain. If the UASF supporters took 5% of the hashrate to a new chain, it would mean 95% stayed on BTC. That means it would only take another 6% of miners to move to the UASF chain to attack it. 89% of the total hashrate would be on BTC, and 11% would be on the UASF chain. Of that 11%, more than half would be hostile and could wreak havoc. At the end of the day, Satoshi's design gives miners the power to determine whether the blockchain is functional or not.

While the UASF concept might have been flawed, it did bring up an important question: do miners connect to a network of full nodes, or do full nodes connect to a network of miners? Thankfully, the answer is "both."

While miners form the technical backbone of Bitcoin, they do not operate independently from a broader economic network. Miners are still profit-driven, and that means they must consider what other parties want. They cannot simply ram through changes without undermining the credibility (and price) of the coin they mine. However, being excessively concerned with minority opinion can also be counterproductive in the long run, especially if it prevents the blockchain from scaling.

UASF had no traction at the beginning, but it eventually gained supporters after the most extreme small-blockers took up the cause, people like Samson Mow, the CSO of Blockstream, and Luke Dashjr, a Blockstream contractor. Mow organized a public fundraiser for the best UASF proposal,[4] and over the next few months, support for UASF grew, especially on social media, though it was never clear how much support was real versus manufactured. On Twitter, for example, hundreds of accounts would swarm public discussions about Bitcoin, aggressively promoting the UASF idea. A remarkably high number of these accounts were new, had cartoon profile pictures, almost no followers, and apparently used their Twitter accounts to solely share their strong opinions about Bitcoin—which they seemed to do for several hours a day, for multiple months. Meanwhile, at real-world meetups and conferences, there were never more than a couple of UASF supporters in any group, despite their loud online presence. They quickly gained a reputation for being the most hostile and disruptive Bitcoiners at conferences and could be identified by their matching camouflage hats emblazoned with “UASF” which were produced by Blockstream.

Eventually, a few companies like BitFury and Samurai Wallet would show support for the UASF, but the movement never reached a critical mass, and it never had to. Miners simply accelerated their timeline for adopting SegWit as part of the NYA. SegWit was scheduled to activate in late August 2017, and the 2x blocksize increase was scheduled for November of the same year.

The drama surrounding SegWit and UASF did have another consequence, however. It spurred on a group of miners to finally create a backup plan. If SegWit turned out to be a bad idea, or if its adoption caused a chain split, or if the 2X blocksize increase failed to occur, there had to be a Plan B. So, an

alternative implementation was created to safely split off from BTC and form a separate chain, without SegWit, and with an immediate increase of the blocksize limit to 8MB. This implementation was called Bitcoin ABC—the "ABC" standing for "adjustable blocksize cap," which would allow miners to set their own limits without needing the approval of developers. Bitcoin ABC brought about a new network, and therefore a new coin, called Bitcoin Cash. That's how BCH started, not as an immediate replacement for BTC, but as a contingency plan by the biggest miners in case the BTC upgrades failed. It turned out to be a good idea.

The "Enemies of Bitcoin"

Almost immediately after SegWit was activated, a new campaign took the place of UASF. Social media engineers, information controllers, and prominent Blockstream employees started to agitate for "NO2X"—rejecting the "2X" part of SegWit2x and keeping the blocksize limit at 1MB. They certainly had their work cut out for them, since almost all the major businesses still planned on the 2x upgrade, and miner signaling swelled to over 90%. The near-universal industry support would be smeared as a "corporate takeover," which was rather ironic since the NYA was needed to overcome the corporate influence that Blockstream held over the Core developers. According to Adam Back:

[P]eople who want to corporate take-over Bitcoin are anti-Bitcoin ethos and anti-Bitcoin; they are *enemies* of Bitcoin.[5]

Core developer btcdrak echoed this sentiment and claimed SegWit2x would actually centralize Bitcoin's development even further:

I am utterly appalled by this proposal both technically, ethically, and by the process which it has adopted… For all the talk of how important "alternative implementations" are, how does this rash and rushed action promote an ecosystem of multiple implementors? By encouraging fast upgrades, you are actually centralizing the ecosystem even further.[6]

The push to prevent the 2x upgrade—and therefore route around Core—was predicted beforehand by many veterans who were familiar with the tactics of the aggressive small block faction. The topic was being discussed

in the uncensored forums, with some people claiming that expecting the hard fork to never happen was akin to a conspiracy theory. User jessquit responded to this idea, saying:

Where do I take whatever drug you're on that makes you completely forget the last N years of broken promises by malactors in this space? Because you clearly are able to completely block out all the history here and just let your imagination take you away…

[I]s it possible that SW2X stays on track and gets 80+% to activate and then stays on track for the HF? Yes. It is definitely possible. It just requires an astonishing suspension of disbelief.[7]

Another user chimed in, agreeing:

I do not believe Blockstream and Core will be honest, did they not already prove that from the Hong Kong agreement? They blatantly reneged on an agreement already right? It's like, fool me once shame on you, fool me twice… and I deserved it.

One particularly dishonest tactic was to claim that the SegWit upgrade was a blocksize increase, implying that Core had already followed through on their promise made in Hong Kong. Samson Mow started this narrative on Twitter with a short dialogue:

SegWit activation would put a definitive end to the perceived Bitcoin 'Civil War' and threat of a network splitting hard-fork.[8]

Edmund Edgar responded with skepticism:

What they mean by this is, once they get segwit, there will be no block size increase, ever.[9]

Which Mow responded to, claiming:

SegWit is a block size increase. Prove it isn't.[10]

This claim would be shamelessly repeated by the usual characters, including Adam Back,[11] Peter Todd,[12] Greg Maxwell,[13] Eric

Lombrozo,[14] and even on the segwit.org website.[15] The reason they could make this claim was because of the way SegWit restructured transactions. The technical details are not important, but they accomplished this by changing the metric of "blocksize" to "block weight," essentially weighing different parts of the transaction differently. By this new accounting method, the literal size of blocks could be increased slightly beyond 1MB—the average is currently 1.3MB—but without a substantial increase in transaction throughput capacity. Stating that this qualified as a 2MB blocksize increase was deceptive—as if the proponents of SegWit2x simply wanted to have blocks containing more data, irrespective of whether it allowed them to process more transactions per block. Using "block weight" metrics, SegWit2x would have resulted in a 8MB block weight limit, though the throughput capacity would essentially be the same as a 2MB blocksize limit. SegWit on its own only allowed for 50% of the capacity the industry was planning on after the Hong Kong and New York Agreements. If SegWit really was a blocksize increase by the usual definition, then the SegWit2x controversy would not have existed at all.

Everyone is Guilty

Theymos and Cobra once again leveraged their control over key websites in order to push the Core-only narrative. Another push was made on Bitcoin.org to delist companies that supported SegWit2x. Cobra wrote:

For now, let's just remove any mention of Coinbase and Bitpay (and their associated products), and put out an alert telling users to BEWARE of Coinbase and Bitpay because they plan on switching over to something that we believe isn't actual Bitcoin. The alert can have instructions telling users how to get their BTC off these services and recommend alternative companies that are committed to using the real Bitcoin.[16]

A couple of days later, Cobra would share plans for adding a "Segwit2x Safety Alert" to warn users of "what these insidious companies are planning so we can prevent them quietly pushing it through."[17] These insidious companies were comprised of most of the largest, oldest, most successful, and most respected participants in the industry—nearly everyone outside the Blockstream/Core bubble. Yet, only a week later, Bitcoin.org announced their intentions to blacklist most of the companies in Bitcoin[18]:

Bitcoin.org is planning to publish a banner on every page of the site warning users about the risks of using services that will default to the so-called Segwit2x1 (S2X) contentious hard fork. S2X companies will be called out by name… By default, we will be using the following list of companies known to support S2X in our warning:

-1Hash (China)

-Abra (United States)

-ANX (Hong Kong)

-Bitangel.com /Chandler Guo (China)

-BitClub Network (Hong Kong)

-Bitcoin.com (St. Kitts & Nevis)

-Bitex (Argentina)

-bitFlyer (Japan)

-Bitfury (United States)

-CryptoFacilities (UK)

-Decentral (Canada)

-Digital Currency Group (United States)

-Filament (United States)

-Genesis Global Trading (United States)

-Genesis Mining (Hong Kong)

-GoCoin (Isle of Man)

-Grayscale Investments (United States)

-Jaxx (Canada)

-Bitmain (China)

-BitPay (United States)

-BitPesa (Kenya)

-BitOasis (United Arab Emirates)

-Bitso (Mexico)

-Bixin.com (China)

-Blockchain (UK)

-Bloq (United States)

-BTC.com (China)

-BTCC (China)

-BTC.TOP (China)

-BTER.com (China)

-Circle (United States)

-Korbit (South Korea)

-Luno (Singapore)

-MONI (Finland)

-Netki (United States)

-OB1 (United States)

-Purse (United States)

-Ripio (Argentina)

-Safello (Sweden)

-SFOX (United States)

-ShapeShift (Switzerland)

-SurBTC (Chile)

-Unocoin (India)

-Veem (United States)

-Civic (United States)	-ViaBTC (China)
-Coinbase (United States)	-Xapo (United States)
-Coins.ph (Phillipines)	-Yours (United States)

In 2017, this list represented the closest thing to consensus within the Bitcoin community, since it encompassed nearly the entire industry. Yet, according to the owners of Bitcoin.org, this was merely a list of "insidious companies" that were in fact leaving the consensus, hell-bent on capturing Bitcoin for themselves to irresponsibly change the software to allow for 2MB blocks. The absurdity of the situation was nicely captured in the title of a trustnodes.com news article: "Bitcoin.org Plans to 'Denounce' Almost All Bitcoin Businesses and Miners."[19]

By Any Means Necessary

Instead of avoiding forks, Bitcoin looked like it would split into three different chains by the end of 2017: the Segwit1x chain (S1X), the Segwit2x chain (S2X), and Bitcoin Cash (BCH). The fight between S1X and S2X brought about a critical question: which chain would keep the name "Bitcoin" and the ticker symbol "BTC"? If "Bitcoin" is identical to the network brought about by the Bitcoin Core software, then obviously that would mean S1X is Bitcoin. But if Bitcoin is the network brought about by the miners and greater industry—and is not synonymous with one software implementation—then S2X would obviously be Bitcoin.

Most of the industry adopted the same policy, often considered the neutral one. The name "Bitcoin" would be assigned to whichever chain accumulated the most hashrate, regardless of whether it was S1X or S2X. Not only was this consistent with Satoshi's design, it also made sense in terms of giving customers maximum stability. A minority hashrate chain is not simply unreliable, it could result in lost funds. While this policy was reasonable, it was also an existential threat to Blockstream and the Core

developers. By September 2017, roughly 95% of the hashrate was signaling for S2X,[20] practically guaranteeing that the Bitcoin name, ticker symbol, and network effects would go with the 2MB chain. And unless the Core developers put in additional protections—like the ones put in place when Bitcoin Cash forked off—they risked having their chain entirely wiped out. However, putting those protections in place would concede that they were a minority fork and had lost the battle for Bitcoin. So, instead of admitting defeat, they became even more aggressive and tried to get the government involved.

Core developer Eric Lombrozo called S2X a "serious cyber attack" and threatened to take legal action against it, stating:

A good portion of the community wants to keep the legacy chain… attempts to destroy it will be treated as an attack on the property of all these people. It constitutes a serious cyberattack and decisive action against it, both technical and legal, has been prepared.[21]

Blockstream co-founder Matt Corallo wrote directly to the SEC to ask them to intervene and provide "consumer protection" from the fork:

I am Matt Corallo, a long-time developer of Bitcoin… an expert on Bitcoin's operation, vocal Bitcoin advocate, and strong proponent of the availability of a Bitcoin Exchange-Traded Product (ETP). I have very grave concerns with the proposed rules for the maintaining of Bitcoin deposits and the lack of consumer protection in the event of Bitcoin Network rule changes in the current filings.

As described in the S-1 filing for the "Bitcoin Investment Trust" (BIT), a "permanent fork" of Bitcoin may occur when two groups of users disagree as to the rules which define the system (its "consensus rules"). More specifically, such a "permanent fork" is likely to occur when one group of users wish to make a change to Bitcoin's consensus rules, while another group does not…

[I]t is important to note that, in the event of a permanent fork, there is likely to be significant market confusion as investors, businesses, and users decide which cryptocurrency they will term "Bitcoin"… In such a scenario, the

BIT could cause significant longer-term market confusion, effectively misrepresenting itself to consumers, all while complying with its currently-proposed rules and filings.[22]

Samson Mow took to Twitter, suggesting that Coinbase was breaking the laws of the "BitLicense" in New York. Tagging both Coinbase and the New York Department of Financial Services, he wrote:

Is @coinbase breaking the terms of the #BitLicense? Endorsing 2x fork definitely raises safety concerns. @NYDFS[23]

And later he continued:

Did @NYDFS superintendent give prior written approval for Coinbase to sign #NYA?[24]

In addition to lawsuit threats, they also used more direct ways of attacking businesses that did not define "Bitcoin" by Bitcoin Core's software. Wallet providers, for example, could face waves of fake one-star reviews on their apps, warning users of potential "lost funds" or "malware" because their company would not support the "real" Bitcoin. Bitcoin.com was placed on a list for malicious email bombing, where all of our @bitcoin.com email addresses would be sent thousands of spam emails every day. Another round of DDoS attacks started against NYA supporters. The constant demonizations, character assassinations, and online harassment extended even to people who were guilty of associating with declared enemies. When Bitcoin.org was discussing the removal of the BTC.com wallet from their website, Cobra responded:

They're associated with that monster Jihan Wu, so I don't mind if they get removed because of this, they're terrible people. I definitely feel like a line has been crossed here.[25]

Jihan Wu is the co-founder of Bitmain, the largest chip manufacturer for Bitcoin miners. He was also the first person to translate the whitepaper into Chinese. Despite getting involved in 2011 and building one of the most successful Bitcoin companies in the world, Wu was smeared as a monster for his lack of total obedience to Bitcoin Core. In fact, since nearly all the

miners were supporting S2X instead of Core, the narrative quickly shifted to outright hostility towards miners generally—as if Segwit2x was a "miner takeover" of Bitcoin. The proper role of miners was no longer to protect, secure, and scale the network; it was to quietly run software provided to them by the Core developers.

The Mob Wins

Once again, the pressure started to work. Companies were being seriously harmed by the organized campaigns against them. While the censorship of big-blockers remained on the online forums, posts that attacked S2X-supporting companies were promoted, no matter how integral they had been to the Bitcoin economy. Brian Hoffman from OB1 was one of the first to publicly retract his support for S2X, not because he supported S1X, but because he was exhausted by the attacks against his company. In an article entitled "SegWit2X: You're f***ed if you do, you're f***ed if you don't," he wrote:

> Another reason I supported SegWit2x is because I hoped that by making SegWit a reality that we could somehow bring a fractured Bitcoin community tighter together when it needed it most. I was wrong. I no longer feel this is a reality. The Bitcoin community does not care about unity other than to preserve the wealth already accumulated by so many early holders and wealthy investors.

He then wrote about the huge culture shift that had taken place within Bitcoin. Instead of celebrating mass adoption and usage, the culture had become hostile towards people spending their Bitcoins at all:

> I am constantly bombarded with messages from people telling me that I'm harming Bitcoin by encouraging users to spend their Bitcoin on OpenBazaar. Someone actually flagged our Crypto is Currency Day effort as a malicious effort because they did not believe in usage of Bitcoin as a form of payment. It is disappointing that people are so petty, but once again this is reality… So in closing you can officially put me in the #Whatever2X column. I'm more interested in creating positive situations in the world, not fighting trolls and assholes in the community.[26]

Amid the controversy and confusion, the cryptocurrency exchange BitFinex—which notably did not sign the NYA—found a way to raise the costs of following through with Segwit2x. Unlike most of the industry, they decided that the ticker symbol BTC would not be assigned based on hashrate. Instead, it would be given to the "incumbent implementation." Their announcement read:

As the proposed consensus protocol Segwit2x project appears likely to activate, we have elected to designate the Segwit2x fork as B2X, for now. The incumbent implementation (based on the existing Bitcoin consensus protocol) will continue to trade as BTC even if the B2X chain has more hashing power… For the time being, BTC will continue to be labeled as "Bitcoin," and B2X will be labeled as "B2X." This will remain the case unless and until such time that market forces suggest an alternative, more appropriate, labeling scheme for one or both chains.[27]

A few other smaller exchanges would soon follow the same policy. That meant users could find themselves trading "BTC" for one price on BitFinex, a wildly different price on Coinbase, and payment processors like BitPay might not even recognize their coins at all—essentially a nightmare scenario for the average user. Imagine a transaction processor like BitPay trying to explain this situation to merchants or to customers asking why their BTC payments did not go through. The headache would be enormous, which is why on November 8th, 2017, roughly a week before the planned fork, BitPay wrote a letter calling for the cancellation of Segwit2x.[28] Shortly afterwards, a joint announcement was made by some of its strongest backers, including the lead developer Jeff Garzik:

Our goal has always been a smooth upgrade for Bitcoin. Although we strongly believe in the need for a larger blocksize, there is something we believe is even more important: keeping the community together. Unfortunately, it is clear that we have not built sufficient consensus for a clean blocksize upgrade at this time. Continuing on the current path could divide the community and be a setback to Bitcoin's growth. This was never the goal of Segwit2x.

As fees rise on the blockchain, we believe it will eventually become obvious that on-chain capacity increases are necessary. When that happens,

we hope the community will come together and find a solution, possibly with a blocksize increase. Until then, we are suspending our plans for the upcoming 2MB upgrade.29

And with that, the New York Agreement failed, just like the Hong Kong Agreement did before it, and like Bitcoin Unlimited, Classic, and XT before that. The threat of disruption was too great a risk, especially for only a 2MB limit which would only provide a fraction of the throughput capacity needed for mass adoption. The failure of S2X would demonstrate, once and for all, that Bitcoin Core had totally captured BTC and would permanently overhaul its design. Anybody adhering to the original vision for Bitcoin as digital cash would be forced to move to a different project. Fortunately, Bitcoin Cash immediately provided that outlet as big-block Bitcoin without the burdens of Blockstream and the Core developers. Three days after the cancellation of Segwit2x, Gavin Andresen identified BCH as the continuation of the original Bitcoin project:

Bitcoin Cash is what I started working on in 2010: a store of value AND means of exchange. 30

Bitcoin's darkest time was during its Civil War era, and it resulted in a successful hijack of the original project. But fortunately, its story does not end there. Maximalists will insist that the battle for Bitcoin is over, that the Core developers are now the final authority, and that the price appreciation of BTC has vindicated the small block philosophy. None of these things are true. Bitcoin technology is still new, and with big blocks, it can compete against any cash system in the world. The Core developers might control BTC, but they do not have any control over BCH. The price of each coin depends on the quality of information within the economy. If misinformation is currently widespread, then prices are destined to adjust as better information becomes known. Bitcoin's original, ambitious goal was to be a fast, cheap, reliable payment system for the internet without needing to trust a centralized authority. That project is alive and well. It just got delayed a few years.

Part III:

Taking Back Bitcoin

20

Challenger for the Title

No cryptocurrency project is beyond corruption, no matter how promising the technology, because all cryptocurrencies depend on software—and therefore humans—for their existence. Individuals can always be compromised, and software can always be rewritten. The successful capture of Bitcoin Core was a clear demonstration of this unfortunate truth. While cryptocurrencies will likely be the money of the future, it remains an open question whether they will make the world a freer place. On its current trajectory, the technology might end up completely corrupted. Instead of being used to empower individuals and give them more financial freedom, it might be used for the opposite purpose—to empower governments to track, surveil, and control people. This negative outcome is much more likely if people cannot access the blockchain and are forced to rely on second layers instead. Peer-to-peer cash is an incredible tool for promoting human freedom; a permissioned blockchain is an incredible tool to restrict it. Whether Bitcoin ends up being a peer-to-peer cash system or a control system within a dystopian nightmare depends on what decisions we make going forward.

The Real Bitcoin

By the end of 2017, Bitcoin started its transition from the Civil War era to the present Mainstream era. The failure of Segwit2x sent a clear message that Satoshi's design would never be implemented on the Bitcoin Core network. Small blocks had become a fundamental feature of BTC. So, anybody wanting to scale Bitcoin with big blocks was forced to switch from BTC to BCH. Because of this, I immediately dedicated all of my efforts to promoting Bitcoin Cash, since it was the continuation of the project I had been working on for the previous seven years. It did not take long before the largest companies like BitPay and Coinbase integrated BCH into their services to allow people to purchase and pay with BCH instead of BTC.

Right away, a competition began between Bitcoin Cash and Bitcoin Core, and they were not just competing for users. The mere existence of Bitcoin

Cash posed a fundamental challenge to Bitcoin Core, because it held a legitimate claim to the title of "the real Bitcoin." For the first year of Bitcoin Cash's existence, BTC and BCH were battling for the very title of "Bitcoin." While today, the industry norm is to call BTC "Bitcoin," that convention was not established for some time, and when you understand the technology and its history, it becomes clear why. The battle over the name "Bitcoin" was, and still remains, critically important, and no group can ever be allowed to monopolize it. Vitalik Buterin echoed this sentiment back in 2017, even though he thought it was premature to call BCH "Bitcoin," writing on Twitter:

I consider BCH a legitimate contender for the bitcoin name. I consider bitcoin's *failure* to raise block sizes to keep fees reasonable to be a large (non-consensual) change to the "original plan", morally tantamount to a hard fork…

That said, *right now*, I think trying to claim "BCH = bitcoin" is a bad idea, as it *is* a minority opinion in the "greater bitcoin community".[1]

Three Critical Questions

The BCH fork raised three critical questions that every Bitcoiner must answer:

1) Is Bitcoin identical to what the Bitcoin Core developers produce?

Even the most rabid Bitcoin Core supporters have to admit that Bitcoin cannot simply be whatever the Core developers produce. It takes little imagination to see how such a project could be corrupted. For example, imagine that the main Github accounts associated with Bitcoin Core are compromised and change the code to require every transaction to pay a fee to an unknown address. Obviously, that would suggest Bitcoin Core had been hijacked, and "the real Bitcoin" would have to continue with a different software implementation. Since the threat of hijack is always present, that means Bitcoin must remain separate from the Bitcoin Core implementation to protect the network's integrity. But this brings up the next question:

2) When does forking away from Bitcoin Core become necessary?

The Bitcoin ecosystem must always be prepared to switch software implementations if necessary—otherwise, there is no defense against the corruption of developers. So there must be some criteria for determining when a fork is required. If every transaction is suddenly required to pay a fee to a mysterious entity, that's an obvious sign it's time to fork, but not every situation is so clear. For example, if the fundamental design of Bitcoin is changed to restrict people's access to the blockchain, that might also be a sign. Or, if the most powerful developers form a company that diverts traffic from Bitcoin onto their proprietary sidechain—that too could be a sign. The centralization of development is a permanent concern, and ironically, even the top developer Van der Laan admitted so in 2021. In a blog post announcing that he no longer wanted to lead the project, he wrote:

I realize I am myself somewhat of a centralized bottleneck. And although I find Bitcoin an extremely interesting project and believe it's one of the most important things happening at the moment, I also have many other interests. It's also particularly stressful and I don't want it, nor the bizarre spats in the social media around it, to start defining me as a person.[2]

When the lead developer admits they have become a centralized bottleneck, that also might be a sign that it's time to fork. The fact that forks are justified and necessary in certain situations raises the next critical question:

3) When does a fork earn the title of "the real Bitcoin"?

By itself, the ability to fork the software does not prevent development capture. Forking the software must also come with the threat of capturing pre-existing network effects—each side of a fork must compete for the title of "the real Bitcoin" and the "BTC" ticker symbol. The integrity of the entire system depends on it.

Most people do not realize that the ticker symbols (BTC, BCH, ETH, XMR, etc) are separate from the underlying blockchain they are attached to. In fact, in the first days of Bitcoin Cash's existence, it traded on some cryptocurrency exchanges as "BCC" before the "BCH" convention was adopted. These ticker symbols are a large part of the network effects for any

coin. In practice, whatever is traded on the exchanges under the “BTC” ticker is what people refer to as “Bitcoin.” So, it is critically important that forks can compete for the dominant ticker symbol too. If Bitcoin Core always inherits these network effects, it’s an enormous advantage and a substantial step toward totally capturing Bitcoin, since any new competitor would have to build up their own network from scratch. If the existing infrastructure defaults to Bitcoin Core no matter what, then all serious competition has been lost, and the Core developers can never really be fired or replaced.

Despite their importance, the preceding three questions are rarely asked. Asking them in public raises the ire of the social media engineers who desperately want to keep control of Bitcoin’s narrative. If the general public ever recognizes that developer capture is an existential threat to any cryptocurrency project, they might realize that Bitcoin Core has already captured Bitcoin—and that Bitcoin Cash is the attempt to reclaim it.

Reverse the Situation

Immediately after the failure of Segwit2x, there was a real possibility that Bitcoin Cash would simply replace BTC as the real Bitcoin. I was not the only one who thought so. Within a month, the price of BCH went from around $650 to an inter-day high of over $4,000! For a brief period, it looked like Bitcoin was going to free itself from Core once and for all. The momentum did not continue, however, and in the face of suffocating information control, the price of BCH has steadily decreased relative to BTC for the past few years. Bitcoin Core supporters are eager to declare a victory because of the large price difference between the two coins, but this is premature.

In my view, the higher price of BTC is almost entirely due to the inheritance of network effects, not because people were excited about small blocks—since years later, there is still hardly anybody who understands the difference between big and small blocks. Forum user MortuusBestia illustrates this point with a thought experiment imagining that BTC were a fork of BCH, not the other way around:

Reverse the situation.

Imagine the dominant bitcoin had 32mb blocks with a fleshed out scaling plan including successful testing of GB+ blocks , support by every major crypto business, project, and service, guaranteed sub-cent fees and a more the merrier growth strategy for true global adoption.

Now imagine some upstart devs forked off and reduced block size to 1mb, heavily restricting transactional capacity to create a fluctuating fee market intended to produce long term fees in excess of $100+ driving users to a second layer system of fee taking government regulated financial intermediaries they call “hubs”.

Would this new high fee coin see any traction whatsoever?

It needs to be understood that the current BTC price is the result of incumbency, not merit. Any suggestion that the market could never come to the realisation that the Blockstream/Core redesign of bitcoin was a mistake is pure cult ideology.[3]

This is a great point. It’s hard to take seriously the idea that the small block, high fee chain would have had any real momentum behind it. It would be fine as an experiment or a sidechain, because it’s effectively a new idea when compared to Satoshi’s vision. I fully support such experimentation, but it should not have inherited the network effects of BTC—the entire industry has been stalled for years because their experiment has largely failed from a technological perspective.

“You Didn’t Call it Bcash”

The most potent weapon in the arsenal of BTC maximalists has always been narrative control. So immediately, they went to work using their old tactics of smearing people and directing the flow of information online. My nickname of “Bitcoin Jesus” was inverted to “Bitcoin Judas,” as if I was a great betrayer of Bitcoin, despite my ideas remaining constant since 2011. A campaign was created to only refer to Bitcoin Cash as “bcash” to discredit and distance BCH from the Bitcoin brand. Nobody within the BCH community used “bcash” to refer to Bitcoin Cash, but that did not matter. They even created a fake Reddit page called “r/bcash”—controlled by small blockers—and would direct people to it from the popular r/Bitcoin page to

mislead them.[4] Honest discussion about Bitcoin Cash was once again heavily suppressed and often censored outright.

Having seen these tactics before, many big blockers assumed the bcash campaign was coordinated by the same bad actors, and leaked conversations strengthened that suspicion. In a Slack conversation between Adam Back and Cobra—the pseudonymous co-owner of the Bitcoin.org domain—Back tries to convince Cobra to hand over the domain to somebody else because he accuses Cobra of being secretly sympathetic to the big block philosophy. To make his case, Back points out that Cobra "just said bcash has advantages and didnt call it bcash"—as if merely not using the term bcash was suspicious behavior.[5] Despite being extremely petty, this tight coordination of language among Maximalists has proven effective for reinforcing the narrative that Bitcoin Cash is not a project to be taken seriously.

BCH developer Jonald Fyookball wrote an article summarizing his thoughts about the motivation behind the "bcash" campaign. He explained:

It's simple: They want to disassociate Bitcoin Cash from Bitcoin. They don't want to allow Bitcoin Cash to use the Bitcoin brand name. And that's completely hypocritical given the fact that the Core group has used every dirty trick in the book (censorship, corporatism, lies and stalling) to usurp the Bitcoin project to their own ends...

They are hoping new users won't even realize there's another version of Bitcoin. They are hoping those users won't realize that Bitcoin was originally peer to peer electronic cash (not this settlement layer that Core is pushing.)

And ultimately, they are hoping people don't see that Bitcoin has changed course, and that there's a version of Bitcoin that stayed with the original formula.[6]

Jonald's thoughts accord with my own, and I know many who agree in private.

21

Bad Objections

The Bitcoin Maximalist playbook should be clear by now—relentlessly push a narrative and attack anybody that questions it. Censor discussion and revise history if necessary. Utilize social media to harass, shame, and bully people into submission. I expect these tactics will continue in the future because they have been effective so far, and also because the Bitcoin Core narrative is quite fragile. Anybody willing to dig beneath the surface will quickly find holes in their story. While there are endless examples of outrageous, deceptive behavior, not every criticism of Bitcoin Cash comes from bad actors. Information has been tightly controlled online for several years, so most people are simply confused because they have only heard one side of the story. The most common criticisms of BCH are easy to refute but still worth addressing.

"Serious Technical Problems"

The Bitcoin Standard is one of the biggest contributors to the confusion because it contains some basic errors. Ammous' claims about scaling have already been addressed, but he also makes dubious claims about BCH. After noting the large price differential between BTC and BCH, he writes:

> Not only is [Bitcoin Cash] unable to gain economic value, it is also dogged with a serious technical problem that renders it almost unusable.[1]

This appears to be an exaggerated reference to the Emergency Difficulty Adjustment (EDA) that Bitcoin Cash briefly used after its creation. Before the 2017 fork occurred, it was unclear how much hashrate the BCH chain would have, so the EDA was created to ensure that the blockchain would remain functional even with a small number of miners. The downside was that the EDA could cause oscillations of hashrate, alternating between excessively fast block production and excessively slow. These fluctuations were not a "serious technical problem." They were expected beforehand, though their magnitudes were underestimated. However, it did become

disruptive, and after a couple of months, the EDA was simply removed and replaced with a better algorithm, as planned.

“It’s Roger Ver’s Coin”

I have lost track of the number of times I’ve been called the “creator” of Bitcoin Cash due to my promotion of it. But this claim is quite simply false. I had nothing to do with the creation of Bitcoin Cash. In fact, I supported Segwit2x because I did not want the industry to fracture in two. My first preference was to keep BTC together, and it was only after S2X failed that I decided to throw my full support behind Bitcoin Cash.

Even more fundamentally, I refuse to pledge allegiance to any particular coin. I have always been in support of a multi-coin future in which users can choose from many options. Competition is healthy, and if BCH loses the competition to another coin—and that project increases the total amount of economic freedom in the world—I fully support it. Bitcoin Cash looks promising because of its underlying technical capability, but if another coin has better fundamentals, then I support its use and adoption too.

Plus, since I personally witnessed the capture and corruption of BTC, I am painfully aware that it can happen to BCH or to any other project. No technology or community is perfect, and success is never guaranteed. So, my focus is on the general utility of cryptocurrency to improve the world and not any particular coin for its own sake. I am not the creator of Bitcoin Cash, but I am one of its biggest proponents.

“Only A Handful of Miners”

Another popular objection is to say that only a handful of miners control Bitcoin Cash. Concern over miner centralization is a valid one for proof-of-work blockchains—51% attacks are always possible—but this criticism falls flat because it’s not applied consistently. Large mining pools do control a significant percentage of the hashrate, due to Satoshi’s design, but this fact is true for BTC, BCH, BSV, and any other proof-of-work chain that uses the SHA-256 algorithm. In fact, the exact same miners will switch between the chains as the profitability of mining them fluctuates. The following chart shows the mining centralization on BTC, as of March 2023:[2]

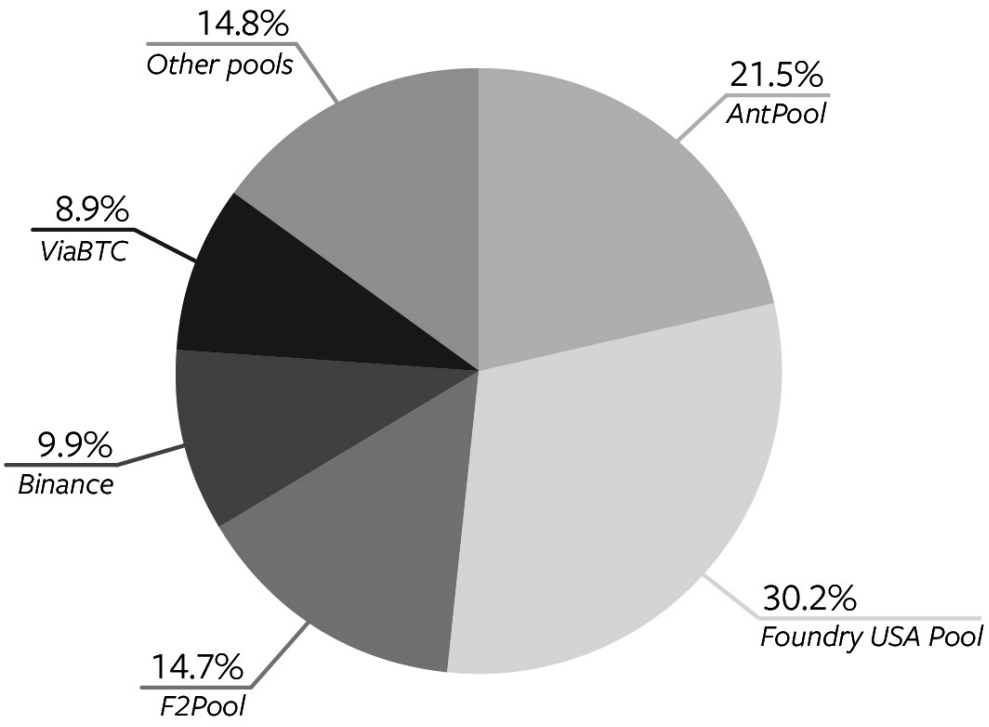


Figure 8 : Latest BTC blocks by mining pool (one week)

This diagram shows three mining pools with over 65% of the total hashrate. If you include the next two biggest pools, the total is over 85%. Bitcoin mining is simply not that decentralized. While this is a valid concern, the actual risks should not be overstated. Mining pools do not directly control the miners connected to them. For any reason, the individual miners—and the machines they operate—can switch to a different pool. So even if a pool operator wanted to coordinate a 51% attack, they have no mechanism to force individual miners to go along with it. Any criticism of Bitcoin Cash for its mining centralization needs to be applied consistently across all SHA-256 chains.

Also, it's worth remembering one of Satoshi's messages to Mike Hearn in 2011, when he wrote:

As things have evolved, the number of people who need to run full nodes is less than I originally imagined. The network would be fine with a small number of nodes if processing load becomes heavy.[3]

Satoshi understood that some degree of centralization is unavoidable, and that pattern is repeated across different industries. The problem is not centralization for its own sake, but rather the risks of 51% attacks. As the mining industry grows, it becomes less realistic to imagine that the largest participants would coordinate a malicious attack on a network into which they have invested hundreds of millions of dollars.

"The Developers Are Bad"

Bitcoin Core supporters are famous for claiming that they have the best developers of any cryptocurrency project—but especially better than the Bitcoin Cash developers. For the first year after the Bitcoin Cash fork, this was one of the most popular smears against BCH, but it has become notably less common since an event in late 2018, when a BCH developer named Awemany discovered a catastrophic bug in the Bitcoin Core software. In his Medium article explaining what happened, Awemany wrote:

Six hundred microseconds. That is about the time that Matt Corallo wanted to shave off of block validation with his pull request in 2016 to Bitcoin Core… This 600 microsecond optimization now resulted in CVE-2018–17144. Certainly the most catastrophic bug in recent years, and certainly one of the most catastrophic bugs in Bitcoin ever.

This bug was initially suspected to potentially cause inflation, was reported because it led to reliable crashes and confirmed by closer analysis… to be actually allowing inflation!

Of all the possible bugs in Bitcoin, inflation bugs are one of the worst—if exploited, it could have allowed somebody to secretly create new coins out of thin air! Awemany was so shocked by the severity of the bug, and the fact that it passed peer-review from people like Van der Laan and Greg Maxwell, that he wondered whether it was intentional:

I also have to be honest, this change creates an unavoidable element of suspicion in me… I [would] like to qualify that this is not what I assert nor think is happening, but definitely crosses my mind as a potentiality…

I always feared that someone from the bankster circles, someone injected into the Bitcoin development circles with the sole goal of wreaking unsalvageable havoc, would do exactly what happened. Injecting a silent inflation bug. Because that is what would destroy one of the very core advantages that Bitcoin has over the current status quo…

Now, again, I am definitely not saying this is the case with PR 9049 for sure. I actually think the explanation of a young, cocky Core developer, a new "master of the universe" wreaking havoc by sheer arrogance and hubris, is the more likely explanation.[4]

Awemany discovered this bug in September 2018. Despite experiencing the hostility of the Core developers for years, he decided to disclose the bug to them privately and not exploit it for financial gain. He could have seriously damaged the reputation of Bitcoin Core—and the credibility of BTC—but chose not to. His goodwill was not returned, and instead of gratitude, his disclosure was met with more criticism, and the individuals involved refused to take responsibility for the catastrophic bug. He wrote:

I have yet to see anything resembling an admission of being imperfect by the developer in question, or any other prominent Core developer for that matter.

After this event, Maximalists still refused to give Awemany the respect he deserved, but it did quiet down claims that Bitcoin Core had a monopoly on all the competent developers.

Free to Innovate

Forking away from Bitcoin Core allowed the Bitcoin Cash developers to improve more than just the blocksize limit. Other features that Satoshi built into the original design have been reactivated, and other innovations have improved BCH's capacity to create smart contracts, seamlessly issue tokens, and maximize transaction privacy. Entrepreneurs and developers now have more tools available for them to build directly on Bitcoin without having to worry about their product breaking due to the extreme limitations of small blocks.

Restoration and Improvement

The Bitcoin Cash developers quickly uncapped some of the unnecessary restrictions placed on Bitcoin. The software functions by using operation codes ("opcodes") to construct and process transactions. One of these opcodes, "OP_RETURN," was previously mentioned in Chapter 14. OP_RETURN allows data to be added to the blockchain in an easy, scalable way. The size of OP_RETURN was tripled in BCH, allowing it to be utilized much more easily. Different companies have already used this feature to build next-generation internet services like decentralized social media platforms.

Early in Bitcoin's history, some of Satoshi's original opcodes were deactivated as a precaution, but the Core developers never bothered to reexamine or reactivate them. The Bitcoin Cash developers successfully reactivated several of them in May 2018, further expanding functionality. They also added a brand-new opcode called OP_CHECKDATASIG which allows the software to incorporate data outside the blockchain to be used within smart contracts.[1] Since then, even more opcodes have been added, including a host of new "Native Introspection opcodes" that combine together to greatly increase the sophistication of BCH's smart contracting system and help make the code simpler, smaller, more efficient, and more powerful.

Freed from Bitcoin Core's roadmap, the BCH developers could finally return to the original focus and purpose of Bitcoin: as a digital cash payment system. The controversial Replace-By-Fee (RBF) feature—that allowed zero-confirmation transactions to be easily reversed—was removed, making instant transactions much more reliable for merchants and payment processors.

Bitcoin is complex, and the more complex it becomes, the more difficult it is to build wallets and other tools. RBF added unnecessary complexity, but that paled in comparison to the changes introduced by Segwit. Among other complexities, Segwit used a new address format, leading to difficulties in transacting between wallets which didn't support Segwit and the new format. Most big blockers thought Segwit was unnecessarily complex and not a solution for scaling, so when the Bitcoin Cash split happened, they intentionally forked off before Segwit was activated, thus ensuring they did not have to bother removing it from the codebase. This decision proved to be a wise one. The developers, merchants, and users of Bitcoin Cash remain completely unaffected by the complexity introduced by Segwit.

Security and Privacy

The amount of computer power required to mine Bitcoin is an essential part of the system's security. If mining is too easy, then malicious actors will find it easier to disrupt the network. If mining is too difficult, then blocks will take too long to produce, slowing down confirmation times and processing speed. This difficulty level regularly adjusts to keep the system self-regulating, but it has sometimes proved inconsistent. Therefore, a Difficulty Adjustment Algorithm (DAA) was added for more stability and was upgraded in 2020. The network has enjoyed even smoother difficulty level adjustments since the new algorithm took over.

Privacy is always somewhat of a challenge for blockchains, since every transaction is public. But every once in a while, a new innovation occurs which gives users a bit more privacy in their transactions. Schnorr signatures are one such innovation that upgrades the cryptography used in Bitcoin. The technology offers several advantages over the older signature method, such as solving the long-standing problem of transaction malleability. Most importantly for privacy, it allows for multiple parties to

create a joint transaction using only one signature. This means that an external observer looking at the blockchain would see a single transaction and would not easily recognize that there were multiple parties involved, giving all participants a higher level of privacy.

This upgrade led to the creation of CashFusion, a privacy protocol which does exactly as described above, in addition to other techniques for enhancing privacy. In 2020, Kudelski Security performed an independent security audit of CashFusion and concluded:

Overall, we believe that CashFusion addresses an existing problem in managing anonymized transactions in Bitcoin Cash by adopting a reasonable security tradeoff… [I]n general we believe that CashFusion offers a practical way to recombine fragmented anonymous transactions in a secure way without the server being able to steal the funds or deanonymize users.2

At the time of writing, this protocol has been used for more than 190,000 transactions totaling more than 17 million BCH on the network.3

Serious Scale

Bitcoin Cash can already support far more transactions than the stagnant Bitcoin Core blockchain, but development continues in order to achieve the vision of global digital cash. There are several proposals which have received some community support, though it's not certain they will make it into the code. Some of them are minor changes to increase the security of the system, but one proposal, CashTokens, continues the push to make BCH even more useful for smart contracts. If the technology works as promised, CashTokens would enable decentralized applications on BCH in a similar fashion to the Ethereum network, with the added scalability of big-block Bitcoin.

Researchers have long been interested in pushing the limits of on-chain scaling. Bitcoin Cash already has a 32MB blocksize limit, but that's obviously not sufficient for global adoption. All the way back in 2017, Dr. Peter Rizun used the BCH "testnet"—a sandbox for testing without affecting the main chain—and successfully mined a 1GB block.4 Given the

pace of development of computer technology, Satoshi's statement that "It never really hits a scale ceiling" looks correct. In fact, one researcher wanted to see whether the Raspberry Pi 4—an extremely small and cheap single-board computer—could verify a 256MB block in under ten minutes. It took less than two minutes.[5]

Far from the claims of Bitcoin Core supporters, the original Bitcoin has extreme scaling capability, and it is finally being realized on the Bitcoin Cash network. Right now, miners can choose to increase the blocksize limit themselves. If a majority of hashrate wants to triple the limit, they can simply change the settings within the BCH software without needing permission from a centralized group of developers. Discussion is currently taking place about whether the blocksize limit can finally be removed altogether, as was considered by both Mike Hearn and Gavin Andresen years ago. Despite the technology being designed back in 2009, big-block Bitcoin remains one of the most scalable—if not the most scalable—cryptocurrencies in the world.

Every cryptocurrency has supporters that loudly proclaim that their coin is superior for one reason or another. Instead of making abstract arguments or a marketing pitch, I strongly suggest readers experiment with Bitcoin Cash for themselves. The fees are extremely low, which means you will not lose a bunch of money in transaction fees by playing around. We have put a huge amount of work into our Bitcoin.com wallet that can be downloaded in the App Store, and users can experience for themselves the Bitcoin that Satoshi envisioned, with sub-penny fees and instant transactions. The experience is so good when compared to other projects, it speaks for itself.

23

Still Forking Around

Bitcoin Cash is not the perfect cryptocurrency, and it does not have a perfect community surrounding it. There are still real problems present, some of which can only be managed, never resolved. While the technology is incredible, it has not solved the difficult social problems that emerge whenever large numbers of people are working together on a project, and questions about proper governance have not disappeared. The problems we forked away from with Bitcoin Core have resurfaced to a lesser degree in Bitcoin Cash. As a result, two more forks have happened since the split with BTC in 2017. Neither fork was motivated primarily by technological disputes, but rather from the personalities involved. From my perspective, the least attractive part of Bitcoin Cash is the fact that these splits have occurred and have splintered the big block community even further. Despite this serious problem, the forks also demonstrated that the Bitcoin Cash community will not tolerate attempts to hijack the protocol, unlike what happened with Bitcoin Core.

Forks are not inherently a bad thing. In hindsight, Bitcoin would probably have been better off forking away from Core several years earlier. When irreconcilable differences occur within a community, forking is a way for each side to develop its own project independently. It's like an evolutionary process, with different groups branching off to find their own unique form. If they make positive changes, then their projects will have a better chance of success; if they make negative changes, their projects will naturally die off. These forks come at a cost though, because they necessarily splinter the network effects into smaller parts, and network effects are a huge part of any cryptocurrency's success. Forks also reduce the pool of talent and energy within a project, and they seem to inevitably cause bitterness and rivalry between the camps—another loss of energy and focus on productive goals. Merchants, too, can be harmed by forks, since there is often drama involved, and they have to figure out whether they will take a side or stay neutral.

Forks can be extremely valuable if they are necessary, but they can be extremely harmful if not. So, given the stakes involved, what was so serious to have caused two further forks within the big block community? The story is similar to what happened in BTC: a few self-appointed leaders tried to take full control of the software development, but this time both attempts failed—unfortunately not without fracturing the network even further.

"Satoshi's Vision"

Big blockers were finally unified around Bitcoin Cash after the split from BTC in 2017. We all recognized the genius of the original design and wanted to break free from Bitcoin Core to scale the technology immediately. However, discussions about scaling did not disappear. Just how fast should the blocksize limit be raised and to what levels?

The first split to occur was between different Bitcoin Cash implementations. The most popular implementation was still Bitcoin ABC led by Amaury Sechet, the main programmer behind the 2017 BCH fork. But some people thought the roadmap of Bitcoin ABC was too reserved and did not scale aggressively enough. So a separate development team was formed called "Bitcoin SV." The "SV" stands for Satoshi's Vision, since they claimed to be implementing the vision of Bitcoin's creator. While this may have been a laudable goal, the effort was complicated by the leadership of a man who claimed to actually be Satoshi himself: Craig S Wright (CSW).

CSW is a unique character, and most people are extremely skeptical of his claim. However, for some time, I did think he might actually be Satoshi. I have great respect for Gavin Andresen, and Gavin once claimed that he thought Craig was Satoshi, even though he could not be sure. After a handful of other respected minds within Bitcoin said the same thing, I trusted their judgment—plus it helped that Craig was unabashedly a big blocker who knew Bitcoin had the potential to scale massively. However, since that time, an enormous amount of controversy has erupted around his claim to be Satoshi, and the evidence he has provided publicly is extremely suspicious. Whether or not his claims are true, he was able to successfully rally a community of people around his vision for Bitcoin's future. One prominent Bitcoin SV supporter was Calvin Ayre, a successful businessman

with a background in online gambling, who ended up providing the financial resources to develop the Bitcoin SV software.

Unfortunately, some technical details of Bitcoin SV and Bitcoin ABC were incompatible, and it did not look like either side was eager to compromise. So in August 2018, a group of miners and entrepreneurs met in Thailand in order to see if another split could be avoided. At that time, I thought Bitcoin ABC's implementation was more promising, but I was optimistic that we would find common ground. I attended and had a reasonable discussion with Ayre over dinner the night before the conference. But I was upset to discover that the next morning Ayre's media outlet published an article claiming that the miners present at the conference had all agreed to follow the SV implementation—even though discussions had not even started! My distrust grew when CSW stormed out of the conference only a few hours later, preventing any further effective discussion or compromise. These underhanded tactics left a bad taste in my mouth.

Over the next couple of months, bitterness grew between the camps. Another contentious hard fork looked likely, though this time it was unclear how it would be resolved. Bitcoin SV and Bitcoin ABC were compatible with each other until either side made fundamental changes to their software, and even then, two incompatible implementations would not necessarily yield two separate blockchains. Another possibility was that, with sufficient hashrate, one side could completely defeat the other, with the minority chain being destroyed outright. Though this sounds like a more disruptive outcome, it might be preferable, since in a winner-takes-all scenario, the victor preserves all the existing network effects. If two separate, viable blockchains emerge, that means the existing network effects are split between them, and two separate coins will emerge from the fight. This kind of competition has been called a "hash war," since the battle is about who can gain the support of the most miners.

Bitcoin ABC and Bitcoin SV looked like they were on a collision course to fight a hash war. Since my focus has always been on using Bitcoin for payments, I knew the credibility of Bitcoin Cash could take a hit if the network experienced significant disruption. So, I spent more than a million dollars renting mining equipment to ensure ABC secured more hashrate

than SV. As a further precaution, Amaury Sechet added code that prevented re-organizations of the ABC chain that were larger than ten blocks in size. However, this code never came into effect, as the ABC chain accumulated more hashrate than the SV chain, and both sides ended up existing as separate networks. Bitcoin SV ended up creating a new coin that gained the ticker symbol "BSV." While I was pleased that my side won the battle—and we successfully got rid of the extremely divisive Craig Wright—the victory came at the cost of shrinking the size of our network even further. After the BSV split, big block Bitcoiners were no longer unified around one project.

Since that split in November 2018, BSV has fallen further behind BCH in terms of price and hashrate. As a result, their strategy seems to have shifted towards relying on patent trolling and lawsuits. I have been sued repeatedly by Craig, as have a long list of people in the cryptocurrency industry. These tactics have been widely condemned, and as a result, BSV has one of the poorest reputations of all cryptocurrencies. Most exchanges have banned BSV's coin from their platforms, further hampering its acceptance. While I completely support and encourage competition between projects, I find it impossible to overlook the fact that BSV's leadership has decided to weaponize the legal system to harass and harm people, myself included. In February 2023, Gavin Andresen updated his personal blog with a note to readers. At the top of his famous article from 2016 that explained why he thought Craig was Satoshi, he added:

I don't believe in rewriting history, so I'm going to leave this post up. But in the seven years since I wrote it, a lot has happened, and I now know it was a mistake to trust Craig Wright as much as I did. I regret getting sucked into the "who is (or isn't) Satoshi" game, and I refuse to play that game any more.[1]

ABC, Another Bitcoin Core?

Every big blocker saw that the funding model for Bitcoin Core developers was broken. Blockstream corrupted several key programmers who worked with conflicts of interest. However, just because we can see the problems in Bitcoin Core does not mean we have found a perfect solution in Bitcoin Cash. Unresolved questions still remain about the best mechanism for

funding development. These questions have occasionally surfaced since 2017, and they ended up causing yet another split in 2020.

Amaury Sechet was the lead developer of Bitcoin ABC, which was the leading software implementation of BCH until 2020. Sechet had a reputation for being technically competent, however his leadership skills had been called into question for years. The cryptocurrency industry is a complex mixture of people and computers; good leaders need to have both soft and hard skills. For whatever reason, the industry tends to attract workers who are on either extreme—either extremely skilled with people or extremely skilled with computers, but rarely both. Sechet had built up a reputation for being difficult to work with, and he frequently expressed discontent with the amount of funding ABC was receiving.

In 2019, the question of developer funding was raised in BCH, and the community responded with a fundraiser that donated more than 800 BCH to different teams. I have personally donated millions of dollars to different teams over the years, including around $500,000 to Bitcoin ABC. In early 2020, the issue re-emerged again.

In response, a group of miners representing the majority of hashrate proposed an “Infrastructure Funding Plan” (IFP), which would divert 12.5% of the block reward for six months into a fund marked for development. The fund would be controlled by an independent corporation in Hong Kong, and they initially estimated the IFP would raise around $6 million. The miners described their proposal in an article:

a) There is no “masternode” voting or any other voting. This is a decision by miners to fund development directly.

b) The initiative shall last 6 months (May 15th 2020 — November 15th 2020)

c) The initiative is under the direction and control of the miners, who can at any time choose not to continue.

d) This is not a protocol change. Instead this is a decision by miners on how to spend their coinbase rewards and which blocks should be built on.[2]

This seemed like a fine plan to me, since it was the miners organizing it amongst themselves and would only be temporary. But the reaction among the broader Bitcoin Cash community was mixed. Some people thought that 12.5% was too high, and others pointed out—rightly so—that the miners were vague on the details about just how the funds would be distributed.

After some deliberation, Bitcoin ABC added the code for the IFP into their software with a compromise: the reward would be reduced to 5%, and a certain threshold of miners would have to agree before the change was activated. If miners did not vote, then it would fail.

The whole idea proved unpopular and sparked the creation of a competing software implementation called Bitcoin Cash Node (BCHN) which did not support the IFP. The BCHN team also provided an alternative to Amaury Sechet's leadership, which had been weakened after attacking and alienating the people around him. With increasing miner support behind BCHN and decreasing support of ABC and Sechet, the IFP failed.

In response, Sechet announced in August 2020 that Bitcoin ABC would be implementing a new version of the IFP that November. His new version changed some key variables: the percentage of the block reward going to development was increased from 5% to 8%, became permanent, did not require a threshold of miners to activate, and perhaps most outrageously, the funds would be sent to a single address, controlled by Sechet himself or somebody closely affiliated with him. In other words, Amaury Sechet decided his Bitcoin ABC implementation should be funded straight from the BCH block reward indefinitely. Not even Bitcoin Core was that brazen!

In an article announcing the new plan, Sechet made it clear that he did not care who disagreed. The plan would move forward without discussion:

While some may prefer that Bitcoin ABC did not implement this improvement, this announcement is not an invitation for debate. The decision has been made and will be activated at the November upgrade.[3]

A large portion of the Bitcoin Cash community was outraged. Bitcoin ABC wanted to position itself as Blockstream / Bitcoin Core 2.0 and secure a whopping 8% of the block reward for itself indefinitely into the future—a

great financial opportunity, if the BCH network allowed it. Researcher Dr. Peter Rizun wrote flatly, “Amaury Sechet is literally modifying the BCH protocol to issue coins to him and his friends.”[4]

More frustration came from fellow BCH developers like Jonathan Toomim, who chimed in:

For 3 years, Amaury Sechet was the single most productive developer in the BCH full node space. This was true because, as the maintainer of Bitcoin ABC, he was able to prevent anybody else from getting much of anything done.[5]

Despite the criticism, Sechet did not budge, and his new code was incorporated into Bitcoin ABC which was scheduled to go live in November 2020. So, three years after the split from Bitcoin Core—in which BCH became the minority chain and had to build its network effects from scratch—a similar situation arose again. If Sechet succeeded in effectively hijacking Bitcoin Cash, I admit that I would have become extremely pessimistic about the viability of big-block Bitcoin—not for any technical reason, but because it would have demonstrated a systemic weakness to developer capture.

However, to my delight, the Bitcoin Cash community would not accept his takeover, and neither would the miners. More hashrate moved over to BCHN, and when November rolled around, Bitcoin ABC failed to secure enough support and forked itself off the main network. Amaury Sechet was fired, and his project took on a new name “eCash” that exists on a separate blockchain.

On the one hand, these forks have been damaging for the continuity and growth of Bitcoin Cash. Every time there is a contentious split, the network shrinks, bitterness grows, the user experience gets worse, and talented individuals leave due to the drama. However, on the other hand, Bitcoin Cash successfully fired a development team that tried to hijack the protocol for their own gain. That’s a great sign. Bitcoin Cash is now free from Blockstream, Craig Wright, and a disgruntled Amaury Sechet. I challenge anybody to find a blockchain more resistant to developer capture.

24

Conclusion

We are at the beginning of a monetary revolution. From a historical perspective, the blockchain is still a brand-new invention, and like any powerful new technology, it can make the world a considerably better or worse place. If we are not careful, it might be co-opted and used to track and control people at an unprecedented level. But if we unlock its potential for good, it will usher in a new era of sound money, personal freedom, and prosperity. The benefits of sound digital money are enormous—as enormous as the risks of unsound digital money. If I have learned anything in the last decade, it's that this power has not gone unnoticed. The political and financial establishment has taken note of Bitcoin and other cryptocurrencies because they are an existential threat to the status quo.

Transactions that are not peer-to-peer require third parties to facilitate them, and the old financial system is largely composed of third parties—banks, payment processors, credit card companies, regulatory agencies, and central banks manipulating the money supply. Middlemen are everywhere, profiting in some way from every transaction they touch. Satoshi's version of Bitcoin—used for everyday commerce, with large blocks and universal access to the blockchain—routes around these intermediaries. The Bitcoin Core version does not. In fact, BTC now depends on the old system in order to work for the average person. Even the Lightning Network depends on trusted third parties, since nearly everybody must use custodial wallets, which are merely account balances held with a company. There is nothing revolutionary about that. At the end of 2021, Cointelegraph wrote an article that demonstrated this point well:

South Korean crypto exchange Coinone has announced it plans to no longer allow withdrawals of tokens to unverified external wallets starting in January...

Coinone said users would have from Dec. 30 to Jan. 23 to register their external wallets at the exchange, after which time it would restrict withdrawals. The exchange specified that crypto users could only register

their own wallets, and the verification process “may take some time” and could change in the future.

According to Coinone, it planned to verify users’ names and resident registration numbers — issued to all residents of South Korea — to ensure crypto transactions were “not used for illegal activities such as money laundering.”[1]

The world is trending in this direction, where companies are forced to comply with regulations that completely strip their customers of privacy. One way to fight this trend is to keep transactions peer-to-peer and not use custodial wallets. However, this is not feasible if the cryptocurrency being used does not scale to allow everybody to access the blockchain.

We may never know the true motivation behind Bitcoin Core’s decision to overhaul Satoshi’s design. Maybe it happened in good faith. Maybe it happened because Core was infiltrated. Regardless, the result is the same: a small-block version of Bitcoin that is considerably less disruptive to the status quo. If interested parties did not directly corrupt Bitcoin, they certainly benefit from its corruption. The same can be said for the rampant censorship online, the widespread information control, and the social media engineering that surrounds this topic—even if the opposition did not cause it, they certainly benefit from it.

Finding the Balance

First-generation Bitcoiners, like myself, who wanted to see Bitcoin widely adopted as a peer-to-peer electronic cash system have failed so far. However, our mistakes can be learned from. The vision for fast, cheap, reliable, inflation-proof digital cash is still alive, but it requires a network of people to bring it into existence. Software alone cannot improve the world; humans are still required!

The next generation of digital cash enthusiasts will need to have a more sophisticated philosophy than we had in the early days. To build such a philosophy, we should start by analyzing the different tensions that exist within systems. Every cryptocurrency project is faced with an endless list of problems, and these problems never have perfect solutions. Instead, there

are tradeoffs that must be balanced against each other. Analyzing these tradeoffs is critical for improving our overall understanding.

The first tradeoff is between focusing our efforts on one cryptocurrency project versus multiple. In the big picture, having competition between multiple projects is a great thing. We should never pledge allegiance to any particular coin. However, our time, attention, and resources are scarce. If any cryptocurrency is going to compete against existing financial systems, we need to coordinate with each other. The more coordination that exists on the same project, the stronger it will become over time. If everybody builds on a separate network, none of those networks will succeed. This is why I am focusing primarily on Bitcoin Cash right now, because I know the underlying technology can scale, and it has already been battle-tested in the real world. Until there is clear evidence that there's a genuinely superior option—not merely the theoretical possibility of one—I will continue to promote BCH as the most promising cryptocurrency for becoming digital cash.

A similar tension exists between the need to have multiple software implementations and the need for strong, competent leadership. The hijack of Bitcoin Core and the attempted hijack of Bitcoin Cash demonstrated that a single development team cannot be trusted in perpetuity. Bitcoin must remain separate from any particular implementation. However, this does not mean that every developer needs to create his own separate implementation. Competent leaders should have a team around them that respects the professional hierarchy, as Mike Hearn suggested. Having a lead implementation is fine, so long as the system remains meritocratic. Otherwise, it will degrade into another case of development capture.

The same can be said for contentious hard forks. On the one hand, the ability to fork is a critical part of the governance of Bitcoin. On the other hand, forks are extremely disruptive and damaging to network effects. They must remain a last resort, otherwise a community will fork itself into irrelevance. Mike Hearn commented on some of these ideas in a fantastic Q&A in 2018. When asked about Bitcoin Cash's community and development structure, he responded:

My view is that Bitcoin Cash strongly resembles the Bitcoin community of 2014. This is not good. That experiment was tried and it didn't work. It's tempting to think that what happened was a freak one-off occurrence, but I don't think it was. I think it was inevitable given the structure and psychological profile of the community at the time.

So just trying to "get back on track" as I see it, is nowhere near radical enough. If I could get one message across to you in this session it's this: be bold. Be willing to accept that what happened was not just bad luck.[2]

Once again, history proved Hearn right, and since he wrote these comments, BCH has split two more times. Any more could prove disastrous. Those underlying structural problems must be fixed. One way is to reduce the number of critical parameters that developers control. For example, all the drama surrounding the blocksize limit can be avoided by simply removing the limit altogether and letting miners determine the size of blocks to produce. The more decisions we can put into the hands of miners and businesses, and not protocol developers, the better.

More fundamentally, a successful project will need to demonstrate stability over time. Adding new features can be attractive, especially for computer programmers, but it comes at the cost of stability. Businesses simply cannot build on unstable platforms, and if the payment technology they are using changes every few months, it quickly becomes more of a hassle than a benefit. A global digital cash system must be rock solid. Once the core features are set, they should not be changed unless absolutely necessary. There are plenty of other cryptocurrencies that are trying to be like Ethereum and provide a universal platform for smart contracts and other complex functionality. But not every coin needs to be like Ethereum; we need some project(s) to focus on simple, effortless cash transactions that can reach global scale.

One more feature that is unique to Bitcoin is worth addressing. Both BTC and BCH have diminishing block rewards over time, which means that before long, miners will receive the vast majority of their revenue from transaction fees, not newly minted coins. This poses a serious challenge to BTC because of small blocks, where high fees are necessary in order to maintain security. But BCH miners will continue to have a straightforward

profit mechanism thanks to Satoshi's original design. Simply by scaling the user base and processing more transactions, they can get paid well. For example, if half a billion people are transacting with Bitcoin Cash twice a day, that's one billion daily transactions. With a $0.01 fee per transaction, that's around $10 million per day of revenue, or over $3.5 billion per year split among miners. This provides a great incentive to keep scaling the network indefinitely.

The Pursuit of Freedom

The cryptocurrency industry is notorious for being toxic and divisive, where competing projects are viewed as mortal enemies. But in the bigger picture, most of us are on the same side. We want more human freedom and less centralized control over our lives. The world is ready for peer-to-peer electronic cash. The Bitcoin Core narrative—despite its many factual errors—has inspired millions of people who are eager to see the separation of money and state. The concept of digital gold has proven popular; just wait until people realize they can have digital gold and digital cash at the same time, on the same network, with the same currency.

Most people simply do not know the story of Bitcoin Core. They do not know that blockchains can scale just fine and that the Bitcoin network was intentionally redesigned to have high fees. They do not know that Blockstream profits by diverting traffic onto their own proprietary blockchain. They do not know about the failures of the Lightning Network and the inevitable proliferation of custodial wallets. They do not know that the information they consume online has been tightly controlled and censored for years to promote a single, dominant narrative. But they are totally on board with the idea of sound digital money that is not controlled by a centralized authority—a beautiful vision that simply cannot be realized on the BTC network. So in one sense, despite the widespread misinformation, the hardest sell is already done. Switching from one blockchain to another is easy compared to getting sold on the idea of cryptocurrencies in the first place.

The last decade has been a whirlwind for me personally. I have seen the birth of a breakthrough technology and its subsequent corruption. I helped to plant the seeds of an emerging industry, saw them grow, and have made

lifelong friends on the way. My enthusiasm for promoting Bitcoin got me the nickname “Bitcoin Jesus,” only to be demonized a few years later as “Bitcoin Judas” for preaching the same message. I have watched the value of my assets rise and fall millions of percent. It has truly been a wild ride. I hope it will be clear in thirty years’ time that the physical, mental, financial, and emotional investments put into this industry have made the world a dramatically better place. The success of Bitcoin and cryptocurrencies should not be measured by how expensive the coins are, nor how rich the early investors become, but rather how much freer the world has become by utilizing this wonderful new technology.

Notes

1. Altered Vision

1 “How Digital Currency Will Change The World”, Coinbase, August 31, 2016, https://blog.coinbase.com/how-digital-currency-will-change-the-world-310663fe4332

2 DishPash, “Peter Wuille. Deer caught in the headlights.”, Reddit, December 8, 2015, https://www.reddit.com/r/bitcoinxt/comments/3vxv92/peter_wuille_deer_caught_in_the_headlights/cxxfqsj/

3 Chakra_Scientist, “What Happened At The Satoshi Roundtable”, Reddit, March 4, 2016, https://www.reddit.com/r/Bitcoin/comments/48zhos/what_happened_at_the_satoshi_roundtable/d0o5w13/

4 Gregory Maxwell, “Total fees have almost crossed the block reward”, Bitcoin-dev mailing list, December 21, 2017, https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2017-December/015455.html

5 CoinMarketSwot, “Hey, do you realize the blocks are full? Since when is this?”, Reddit, February 14, 2017, https://www.reddit.com/r/btc/comments/5tzq45/hey_do_you_realize_the_blocks_are_full_since_when/ddtb8dl/

2. Bitcoin Basics

1 “Bitmain Chooses Rockdale, Texas, for Newest Blockchain Data Center”, Business Wire, August 6, 2018, https://www.businesswire.com/news/home/20180806005156/en/Bitmain-Chooses-Rockdale-Texas-Newest-Blockchain-Data

2 Satoshi, “Re: Scalability and transaction rate”, Bitcoin Forum, July 29, 2010, https://bitcointalk.org/index.php?topic=532.msg6306#msg6306

3 BITCOIN, “Bitcoin: Elon Musk, Jack Dorsey & Cathie Wood Talk Bitcoin at The B Word Conference”, Youtube, July 21, 2021, https://youtu.be/TowDxSHSClw?t=8168

3. Digital Cash for Payments

1 Saifedean Ammous, The Bitcoin Standard, New Jersey: Wiley, 2018. Description inside back flap.

2 Dan Held (@danheld), Twitter, January 14, 2019, https://twitter.com/danheld/status/1084848063947071488

3 Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008, https://www.bitcoin.com/bitcoin.pdf

4 Samuel Patterson, “Breakdown of all Satoshi’s Writings Proves Bitcoin not Built Primarily as Store of Value”, SamPatt, June 6, 2019, https://sampatt.com/blog/2019/06/06/breakdown-of-all-satoshi-writings-proves-bitcoin-not-built-primarily-as-store-of-value

5 Satoshi, “Re: Flood attack 0.00000001 BC”, Bitcoin Forum, August 4, 2010, https://bitcointalk.org/index.php?topic=287.msg7524#msg7524

6 Gavin Andresen, “Re: How a floating blocksize limit inevitably leads towards centralization”, Bitcoin Forum, February 19, 2013, https://bitcointalk.org/index.php?topic=144895.msg1539692#msg1539692

7 Satoshi, “Re: Flood attack 0.00000001 BC”, Bitcoin Forum, August 5, 2010, https://bitcointalk.org/index.php?topic=287.msg7687#msg7687

8 Satoshi Nakamoto, “Bitcoin v0.1 released”, Metzdowd, January 16, 2009, https://www.metzdowd.com/pipermail/cryptography/2009-January/015014.html

9 Peter Todd, “How a floating blocksize limit inevitably leads towards centralization”, Bitcoin Forum, February 18, 2023, https://bitcointalk.org/index.php?topic=144895.0

10 Satoshi, “Re: Bitcoin minting is thermodynamically perverse”, Bitcoin Forum, August 7, 2010, https://bitcointalk.org/index.php?topic=721.msg8114#msg8114

11 Ilama, “Re: Bitcoin snack machine (fast transaction problem)”, Bitcoin Forum, July 18, 2010, https://bitcointalk.org/index.php?topic=423.msg3836#msg3836

12 Molybdenum, “CLI bitcoin generation”, Bitcoin Forum, May 22, 2010, https://bitcointalk.org/index.php?topic=145.msg1194#msg1194

13 Satoshi, “Re: The case for removing IP transactions”, Bitcoin Forum, September 19, 2010, https://bitcointalk.org/index.php?topic=1048.msg13219#msg13219

14 Satoshi, “Re: URI-scheme for bitcoin”, Bitcoin Forum, February 24, 2010, https://bitcointalk.org/index.php?topic=55.msg481#msg481

15 Satoshi, “Re: Porn”, Bitcoin Forum, September 23, 2010, https://bitcointalk.org/index.php?topic=671.msg13844#msg13844

16 Satoshi, “Re: Bitcoin mobile”, Bitcoin Forum, June 26, 2010, https://bitcointalk.org/index.php?topic=177.msg1814#msg1814

17 Stephen Pair, Consensus 2017, https://s3.amazonaws.com/media.coindesk.com/live-stream/Day1_Salons34.html

18 This Week in Startups, “E779: Brian Armstrong Coinbase & Tim Draper: crypto matures, ICO v VC, fiat end, bitcoin resiliency”, Youtube, November 17, 2017, https://youtu.be/AIC62BkY4Co?t=2168

19 “Bitcoin P2P Cryptocurrency”, Bitcoin, January 31, 2009, https://web.archive.org/web/20100722094110/http://www.bitcoin.org:80/

20 “Bitcoin is an innovative payment network and a new kind of money.”, Bitcoin, March 23, 2013, https://web.archive.org/web/20150701074039/https://bitcoin.org/en/

4. Store of Value vs. Medium of Exchange

1 Ammous, The Bitcoin Standard, p.212

2 Ammous, The Bitcoin Standard, p. 206

3 Saifedean Ammous (@saifedean), Twitter, https://twitter.com/saifedean/status/9392176589978542

4 Tuur Demeester (@TuurDemeester), Twitter, May 29, 2019, https://twitter.com/TuurDemeester/status/1133735055115866112

5 Ludwig von Mises, The Theory of Money and Credit, Germany: Duncker & Humblot, 1912

6 Murray N. Rothbard, What Has Government Done to Our Money?, Alabama: Mises Institute, 2010

7 Satoshi, "Re: Bitcoin does NOT violate Mises' Regression Theorem", Bitcoin Forum, August 27, 2010, https://bitcointalk.org/index.php?topic=583.msg11405#msg11405

8 Tone Vays, "On The Record w/ Willy Woo & Kim Dotcom - Can't All 'Bitcoiner's' Just Get Along?", Youtube, January 16, 2020, https://www.youtube.com/watch?v=mvcZNSwQlRU

5. The Blocksize Limit

1 Stephen Pair, Bitcoin.com podcast", Reddit, April 5, 2017, https://www.reddit.com/r/btc/comments/63m2cp/if_you_told_me_in_2011_that_we_would_be_sitting/

2 "Bitcoin transactions", Blockchair, August 18, 2023, https://blockchair.com/bitcoin/transactions?s=fee_usd(desc)&q=fee_usd(900..1100)#

3 Gavin Andresen, GAVIN ANDRESEN, August 18, 2023, http://gavinandresen.ninja/

4 Gavin Andresen, GavinTech, August 18, 2023, https://gavintech.blogspot.com/

5 Gavin Andresen, “One-dollar lulz”, GAVIN ANDRESEN, March 3, 2016, http://gavinandresen.ninja/One-Dollar-Lulz

6 Gavin Andresen, “Re: Please do not change MAX_BLOCK_SIZE”, Bitcoin Forum, June 03, 2013, https://bitcointalk.org/index.php?topic=221111.msg2359724#msg2359724

7 Cryddit, “Re: Permanently keeping the 1MB (anti-spam) restriction is a great idea ...”, Bitcoin Forum, February 07, 2015, https://bitcointalk.org/index.php?topic=946236.msg10388435#msg10388435

8 Jorge Timón, “Răspuns: Personal opinion on the fee market from a worried local trader”, Bitcoin-dev Mailing List, July 31, 2015, https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-July/009804.html

9 User <gmaxwell>, bitcoin-wizards chat log, January 16, 2016, http://gnusha.org/bitcoin-wizards/2016-01-16.log

10 Bitcoincash, “Satoshi Reply to Mike Hearn”, Nakamoto Studies Institute, April 12, 2009, https://nakamotostudies.org/emails/satoshi-reply-to-mike-hearn/

11 “Scalability”, Bitcoin, September 11, 2011, https://web.archive.org/web/20130814044948/https://en.bitcoin.it/wiki/Scalability

12 Gavin Andresen, “Re: Bitcoin 20MB Fork”, Bitcoin Forum, January 31, 2015, https://bitcointalk.org/index.php?topic=941331.msg10315826#msg10315826

13 Satoshi, “Re: Flood attack 0.00000001 BC”, Bitcoin Forum, August 11, 2010, https://bitcointalk.org/index.php?topic=287.msg8810#msg8810

14 jtimon, Reddit, December 13, 2016, https://www.reddit.com/r/Bitcoin/comments/5i3d87/til_4_years_ago_matt_carollo_tried_to_solve/db5d96z/

15 Pieter Wuille, “Bitcoin Core and hard forks”, Bitcoin-dev mailing list, July 22, 2015, https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-July/009515.html

16 User <gmaxwell>, “bitcoin-wizards” chat log, Gnusha, January 16, 2016, http://gnusha.org/bitcoin-wizards/2016-01-16.log

17 Gregory Maxwell, “Total fees have almost crossed the block reward”, Bitcoin-dev mailing list, December 21, 2017, https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2017-December/015455.html

18 Satoshi, “Re: What’s with this odd generation?”, Bitcoin Forum, February 14, 2010, https://bitcointalk.org/index.php?topic=48.msg329#msg329

19 Vitalik Buterin (@VitalikButerin), Twitter, November 14, 2017, https://twitter.com/VitalikButerin/status/930276246671450112

20 “Steam is no longer supporting Bitcoin”, Steam, December 6, 2017, https://steamcommunity.com/games/593110/announcements/detail/1464096684955433613

21 Elon Musk (@elonmusk) Twitter, July 10, 2021, https://twitter.com/elonmusk/status/1413649482449883136

6. Notorious Nodes

1 Wladimir J. van der Laan, “Block Size Increase”, Bitcoin-development mailing list, May 7, 2015, https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-May/007890.html

2 BitcoinTalk, “Re: Scalability and transaction rate”, Satoshi Nakamoto Institute, July 29, 2010, https://satoshi.nakamotoinstitute.org/posts/bitcointalk/287/

3 Cryptography Mailing List, “Bitcoin P2P e-cash paper, Satoshi Nakamoto Institute, November 3, 2008, https://satoshi.nakamotoinstitute.org/emails/cryptography/2/

4 Alan Reiner, “Block Size Increase”, Bitcoin-development mailing list, May 8, 2015, https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-May/008004.html

5 Theymos, “Re: The MAX_BLOCK_SIZE fork”, Bitcoin Forum, January 31, 2013, https://bitcointalk.org/index.php?topic=140233.msg1492629#msg1492629

6 Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, https://www.bitcoin.com/bitcoin.pdf

7 “Full node”, Bitcoin Wiki, April 8, 2022, https://en.bitcoin.it/w/index.php?title=Full_node

8 Mike Hearn, “Re: Reminder: zero-conf is not safe; $500USD reward posted for replace-by-fee patch”, Bitcoin Forum, April 19, 2013, https://bitcointalk.org/index.php?topic=179612.msg1886471#msg1886471

9 BitcoinTalk, “Re: Scalability”, Satoshi Nakamoto Institute, July 14, 2010, https://satoshi.nakamotoinstitute.org/posts/bitcointalk/188/

7. The Real Cost of Big Blocks

1 Gavin Andresen, “Re: Bitcoin 20MB Fork”, Bitcoin Forum, March 17, 2015, https://bitcointalk.org/index.php?topic=941331.msg10803460#msg10803460

2 Ammous, The Bitcoin Standard, p. 233

3 Ibid.

4 “Seagate BarraCuda NE-ST8000DM004”, NewEgg, September 2023, https://www.newegg.com/seagate-barracuda-st8000dm004-8tb/p/N82E16822183793

5 “QNAP TS-653D-4G 6 Bay NAS”, Amazon, September 2023, https://www.amazon.com/QNAP-TS-653D-4G-Professionals-Celeron-2-5GbE/dp/B089728G34/

6 John McCallum, “Historical cost of computer memory and storage”, Our World in Data, 2022 https://ourworldindata.org/grapher/historical-cost-of-computer-memory-and-storage

7 “Disk Drive Prices 1955+”, Jcmit, September, 2023, https://jcmit.net/diskprice.htm

8 Ammous, The Bitcoin Standard, p. 233-234

9 Satoshi Nakamoto, “Bitcoin P2P e-cash paper”, Bitcoin.com, November 3, 2008, https://www.bitcoin.com/satoshi-archive/emails/cryptography/2/#selection-29.1597-29.2053

10 “The Shrinking Cost of a Megabit”, ncta, March 28, 2019, https://www.ncta.com/whats-new/the-shrinking-cost-of-a-megabit

11 Michael Ken, “AT&T Starts Offering 2-Gigabit and 5-Gigabit Home Internet Amid Cost Hike”, PC Mag, January 24, 2022, https://www.pcmag.com/news/att-starts-offering-2-gigabit-and-5-gigabit-home-internet-amid-cost-hike

12 Nick Perry, “How much data does Netflix use?”, digitaltrends, June 19, 2021, https://www.digitaltrends.com/movies/how-much-data-does-netflix-use/

13 Blair Levin and Larry Downes, “Why Google Fiber Is High-Speed Internet’s Most Successful Failure”, Harvard Business Review, September 7, 2018, https://hbr.org/2018/09/why-google-fiber-is-high-speed-internets-most-successful-failure

14 Kristin Houser, “Japan breaks world record for fastest internet speed”, Big Think, November 13, 2021, https://bigthink.com/the-present/japan-internet-speed/

15 Alex Kerai, “State of the Internet in 2023: As Internet Speeds Rise, People Are More Online”, HighSpeedInternet.com, January 30, 2023, https://www.highspeedinternet.com/resources/state-of-the-internet

16 Gavin Andresen, “A Scalability Roadmap”, Bitcoin Foundation, October 6, 2014, https://web.archive.org/web/20141027182035/https://bitcoinfoundation.org/2014/10/a-scalability-roadmap/

8. The Right Incentives

1 Gavin Andresen, “R e: Microsoft Researchers Suggest Method to Improve Bitcoin Transaction Propagation”, Bitcoin Forum, November 15, 2011, https://bitcointalk.org/index.php?topic=51712.msg619395#msg619395

2 F. A. Hayek, The Fatal Conceit : The Errors of Socialism, edited by W. W. Bartley III, Chicago: University of Chicago Press, (1988), p. 76

3 Ibid.

4 Gavin Andresen, “Re: Please do not change MAX_BLOCK_SIZE”, Bitcoin Forum, June 03, 2013, https://bitcointalk.org/index.php?topic=221111.msg2359724#msg2359724

5 Wladimir J. van der Laan, “Block Size Increase”, Bitcoin-development mailing list, May 7, 2015, https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-May/007890.html

9. The Lightning Network

1 Paul Sztorc, “Lightning Network -- Fundamental Limitations”, Truthcoin.info, April 4, 2022, https://www.truthcoin.info/blog/lightning-limitations/

2 Joseph Poon and Thaddeus Dryja, “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments”, January 14, 2016, https://lightning.network/lightning-network-paper.pdf

3 Tone Vays, “Bitcoin Brief w/ Jimmy Song - Bitmain, BTC Apartments in Dubai & $10k Price Talk”, Youtube, February 15, 2018, https://www.youtube.com/watch?v=9_WCaqcGnZ8&t=2404s

4 We Are All Satoshi, “Rick Reacts to the Lightning Network”, Youtube, February 18, 2018, https://www.youtube.com/watch?v=DFZOrtlQXWc

5 Jian-Hong Lin, Kevin Primicerio, Tiziano Squartini, Christian Decker and Claudio J. Tessone, “Lightning Network: a second path towards centralisation of the Bitcoin economy”, June 30, 2020, https://arxiv.org/pdf/2002.02819.pdf

10. Keys to the Code

1 Ammous, The Bitcoin Standard, p. 200

2 “Bitcoin development”, BitcoinCore, August 18, 2023, https://bitcoin.org/en/development

3 Level39 (@level39), Twitter, December 15, 2022, https://twitter.com/level39/status/1603214594012598273

4 Epicenter Podcast, “EB94 – Gavin Andresen: On The Blocksize And Bitcoin’s Governance”, Youtube, August 31, 2015, https://www.youtube.com/watch?v=B8l11q9hsJM

5 Gavin Andresen, “Development process straw-man”, Bitcoin Forum, December 19, 2010, [https://bitcointalk.org/index.php?topic=2367.msg31651#msg31651

6 Epicenter Podcast, “EB94 – Gavin Andresen: On The Blocksize And Bitcoin’s Governance”, Youtube, August 31, 2015, https://www.youtube.com/watch?v=B8l11q9hsJM

7 Epicenter Podcast, “EB82 – Mike Hearn - Blocksize Debate At The Breaking Point”, Youtube, June 8, 2015, https://youtu.be/8JmvkyQyD8w?t=3699

8 Mike Hearn, “The resolution of the Bitcoin experiment”, Medium, January 14, 2016, https://blog.plan99.net/the-resolution-of-the-bitcoin-experiment-dabb30201f7

9 Lannwj, “Rebrand client to ‘Bitcoin Core’ #3203”, Github, November 5, 2013, https://github.com/bitcoin/bitcoin/issues/3203

10 Epicenter Podcast, “EB94 – Gavin Andresen: On The Blocksize And Bitcoin’s Governance”, Youtube, August 31, 2015,https://www.youtube.com/watch?v=B8l11q9hsJM

11 Ibid.

12 Epicenter Podcast, “EB82 – Mike Hearn - Blocksize Debate At The Breaking Point”, Youtube, June 8, 2015, https://youtu.be/8JmvkyQyD8w?t=3845

11. The Four Eras

1 Gavin Andresen, “Is Store of Value enough?”, GAVINTHINK, July 11, 2012, https://gavinthink.blogspot.com/2012/07/is-store-of-value-enough.html

2 “What Happened At The Satoshi Roundtable”, Coinbase, March 4, 2016, https://blog.coinbase.com/what-happened-at-the-satoshi-roundtable-6c11a10d8cdf

3 Samson Mow (@Excellion), Twitter, October 6, 2016, https://twitter.com/Excellion/status/783994642463326208

12. Warning Signs

1 Keep Bitcoin Free!, “Why the blocksize limit keeps Bitcoin free and decentralized”, Youtube, May 17, 2013, https://www.youtube.com/watch?v=cZp7UGgBR0I

2 Gmaxwell, “Re: New video: Why the blocksize limit keeps Bitcoin free and decentralized”, Bitcoin Forum, May 17, 2013, https://bitcointalk.org/index.php?topic=208200.msg2182597#msg2182597

3 Peter Todd, “Reminder: zero-conf is not safe; $1000USD reward posted for replace-by-fee patch”, Bitcoin Forum, April 18, 2013, https://bitcointalk.org/index.php?topic=179612.0

4 Peter Todd, “Reminder: zero-conf is not safe; $1000USD reward posted for replace-by-fee patch”, Bitcoin Forum, April 18, 2013, https://bitcointalk.org/index.php?topic=179612.0

5 Bram Cohen, “The inevitable demise of unconfirmed Bitcoin transactions”, Medium, July 2, 2015, https://bramcohen.medium.com/the-inevitable-demise-of-unconfirmed-bitcoin-transactions-8b5f66a44a35

6 Gavin Andresen, “A definition of “Bitcoin””, GAVIN ANDRESEN, February 7, 2017, http://gavinandresen.ninja/a-definition-of-bitcoin

7 Etotheipi, “Re: Reminder: zero-conf is not safe; $1000USD reward posted for replace-by-fee patch”, Bitcoin Forum, May 09, 2013, https://bitcointalk.org/index.php?topic=179612.80

8 Mike Hearn, “Replace by fee: A counter argument”, Medium, March 28, 2015, https://blog.plan99.net/replace-by-fee-43edd9a1dd6d

9 Ibid.

10 Ibid.

11 Ibid.

12 “Opt-in RBF FAQ”, BitcoinCore, August 18, 2023, https://bitcoincore.org/en/faq/optin_rbf/

13 Mike Hearn, “Replace by fee: A counter argument”, Medium, March 28, 2015, https://blog.plan99.net/replace-by-fee-43edd9a1dd6d

14 Peter Todd, “Bitcoin Blocksize Problem Video”, Bitcoin Forum, April 28, 2013, https://bitcointalk.org/index.php?topic=189792.msg1968200

15 Benjamindees, “Re: New video: Why the blocksize limit keeps Bitcoin free and decentralized”, Bitcoin Forum, May 18, 2013, https://bitcointalk.org/index.php?topic=208200.20

16 User <gavinandresen>, IRC chat log, August 30, 2013, http://azure.erisian.com.au/~aj/tmp/irc/log-2013-08-30.html

17 “Untitled”, Pastebin, November 16, 2013, https://web.archive.org/web/20131120061753/http://pastebin.com/4BcycXUu

13. Blocking the Stream

1 Maria Bustillos, “The Bitcoin Boom”, The New Yorker, April 1, 2013, https://www.newyorker.com/tech/annals-of-technology/the-bitcoin-boom

2 Gavin Andresen, “Bitcoin Core Maintainer: Wladimir van der Laan”, Bitcoin Foundation, April 7, 2014, https://web.archive.org/web/20140915022516/https://bitcoinfoundation.org/2014/04/bitcoin-core-maintainer-wladimir-van-der-laan/

3 Oliver Janssens, “The Truth about the Bitcoin Foundation”, Bitcoin Foundation, April 4, 2015, https://web.archive.org/web/20150510211342/https://bitcoinfoundation.org/forum/index.php?/topic/1284-the-truth-about-the-bitcoin-foundation/

4 Gavin Andresen, “Joining the MIT Media Lab Digital Currency Initiative”, GavinTech, April 22, 2015, https://gavintech.blogspot.com/2015/04/joining-mit-media-lab-digital-currency.html

5 “The philosophical origins of Bitcoin’s civil war (Mike Hearn, written 2016 but released 2020)”, Reddit, December 13, 2020, https://www.reddit.com/r/btc/comments/kc2k3h/the_philosophical_origins_of_bitcoins_civil_war/gforyhb/?context=3

6 Adam3us, “We are bitcoin sidechain paper authors Adam Back, Greg Maxwell and others”, Reddit, October 23, 2014, https://www.reddit.com/r/IAmA/comments/2k3u97/we_are_bitcoin_sidechain_paper_authors_adam_back/clhoo7d/

7 Daniel Cawrey, “Gregory Maxwell: How I Went From Bitcoin Skeptic to Core Developer”, CoinDesk, December 29, 2014, https://www.coindesk.com/markets/2014/12/29/gregory-maxwell-how-i-went-from-bitcoin-skeptic-to-core-developer/

8 Laura Shin, “Will This Battle For The Soul Of Bitcoin Destroy It?”, Forbes, October 23, 2017,

https://www.forbes.com/sites/laurashin/2017/10/23/will-this-battle-for-the-soul-of-bitcoin-destroy-it

9 Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón, and Pieter Wuille, "Enabling Blockchain Innovations with Pegged Sidechains", October 22, 2014, https://blockstream.com/sidechains.pdf

10 "What is the Liquid Federation?", Blockstream, August 18, 2023, https://help.blockstream.com/hc/en-us/articles/900003013143-What-is-the-Liquid-Feder

11 "How do transaction fees on Liquid work?", Blockstream, August 18, 2023, https://help.blockstream.com/hc/en-us/articles/900001386846-How-do-transaction-fees-on-Liquid-work-

12 Adam Back (@adam3us), Twitter, May 23, 2020, https://twitter.com/adam3us/status/1264279001419431936

13 Avanti, January 27, 2022, https://web.archive.org/web/20220127022722/https://avantibank.com/

14 Nate DiCamillo, "Unpacking the Avit, Avanti Bank's New Digital Asset Being Built With Blockstream", CoinDesk, August 12, 2020, https://www.coindesk.com/business/2020/08/12/unpacking-the-avit-avanti-banks-new-digital-asset-being-built-with-blockstream/

15 Blockstream Team, "El Salvador to Issue $1B in Tokenized Bonds on the Liquid Network", Blockstream, November 21, 2021, https://blog.blockstream.com/el-salvador-to-issue-1b-in-tokenized-bonds-on-the-liquid-network/

16 Paul Vigna, "Bitcoin Startup Blockstream Raises $55 Million in Funding Round", The Wall Street Journal, February 3, 2016, https://www.wsj.com/articles/bitcoin-startup-blockstream-raises-55-million-in-funding-round-1454518655

17 “Global 500”, Fortune, August 18, 2023, https://fortune.com/global500/2021/search/?sector=Financials

18 Graham Ruddick, “Axa boss Henri de Castries on coal: ‘Do you really want to be the last investor?’”, The Guardian, August 7, 2015, https://www.theguardian.com/business/2015/aug/07/axa-boss-henri-de-castries-on-coal-do-you-really-want-to-be-the-last-investor

19 “List of Bilderberg participants”, Wikipedia, August 18, 2023, https://en.wikipedia.org/wiki/List_of_Bilderberg_participants

20 Fitz Tepper, “Barry Silbert Launches Digital Currency Group With Funding From MasterCard, Others”, TechCrunch, October 28, 2015, https://techcrunch.com/2015/10/27/barry-silbert-launches-digital-currency-group-with-funding-from-mastercard-others/

21 “Blockstream Raise $210 Million Series B With $3.2 Billion Valuation”, FinTechs.fi, August 18, 2023, https://fintechs.fi/2021/08/24/blockstream-raise-210-million-with-3-2-billion-valuation/

22 Crypto Me!, “Stefan Molyneux predicts Blockstream takeover of Bitcoin”, Youtube, May 7, 2018, https://www.youtube.com/watch?v=q-sMbf2OzOY

14. Centralizing Control

1 Michael J. Casey, “Linked-In, Sun Microsystems Founders Lead Big Bet On Bitcoin Innovation”, The Wall Street Journal, November 17, 2014, https://web.archive.org/web/20141201173917/https://blogs.wsj.com/moneybeat/2014/11/17/linked-in-sun-microsystems-founders-lead-big-bet-on-bitcoin-innovation/

2 Jeff Garzik, “Block size: It’s economics & user preparation & moral hazard”, Bitcoin-dev mailing list, December 16, 2015, https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-December/011973.html

3 Tim Swanson, “Bitcoin Hurdles: the Public Goods Costs of Securing a Decentralized Seigniorage Network which Incentivizes Alternatives and Centralization”, April 2014, http://www.ofnumbers.com/wp-content/uploads/2014/04/Bitcoins-Public-Goods-hurdles.pdf

4 “Make Master Protocol harder to censor”, Github, September 2014, https://github.com/OmniLayer/spec/issues/248

5 “Vitalik Buterin tried to develop Ethereum on top of Bitcoin, but was stalled because the developers made it hard to build on top of Bitcoin” Reddit, February 1, 2018, https://np.reddit.com/r/btc/comments/7umljb/vitalik_buterin_tried_to_develop_ethereum_on_top/dtli9fg/

6 Joseph Young, “Vitalik Buterin Never Attempted to Launch Ethereum on Top of Bitcoin”, CoinJournal, May 22, 2020, https://coinjournal.net/news/vitalik-buterin-never-attempted-launch-ethereum-top-bitcoin/

7 “Vitalik Buterin tried to develop Ethereum on top of Bitcoin, but was stalled because the developers made it hard to build on top of Bitcoin” Reddit, February 1, 2018, https://np.reddit.com/r/btc/comments/7umljb/vitalik_buterin_tried_to_develop_ethereum_on_top/dtli9fg/

8 Ibid.

9 Erik Voorhees (@ErikVoorhees), Twitter, January 5, 2021, https://twitter.com/erikvoorhees/status/1346522578748370952

10 Laanwj, “Change the default maximum OP_RETURN size to 80 bytes #5286”, Github, February 3, 2015, https://github.com/bitcoin/bitcoin/pull/5286

11 Gavin Andresen, “Re: Gavin Andresen Proposes Bitcoin Hard Fork to Address Network Scalability”, Bitcoin Forum, October 19, 2014, https://bitcointalk.org/index.php?topic=816298.msg9254725#msg9254725

12 Crypto Me!, ""The Internet of Money should not cost 5 cents per transaction." -Vitalik Buterin", Youtube, December 19, 2017, https://www.youtube.com/watch?v=unMnAVAGIp0

13 Stephen Pair, "Bitcoin as a Settlement System", Medium, January 5, 2016, https://medium.com/@spair/bitcoin-as-a-settlement-system-13f86c5622e3

14 Pieter Wuille, "Re: How a floating blocksize limit inevitably leads towards centralization", Bitcoin Forum, February 18, 2013, https://bitcointalk.org/index.php?topic=144895.msg1537737#msg1537737

15 Mike Hearn, "Why Satoshi's temporary anti-spam measure isn't temporary", Bitcoin-dev mailing list, July 29, 2015, https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-July/009726.html

16 Aantonop, "Re: Roger Ver and Jon Matonis pushed aside now that Bitcoin is becoming mainstream", Bitcoin Forum, April 29, 2013, https://bitcointalk.org/index.php?topic=181168.msg1977971#msg1977971

17 Gavin Andresen, "A Scalability Roadmap", Bitcoin Foundation, October 6, 2014, https://web.archive.org/web/20150130122517/https://blog.bitcoinfoundation.org/a-scalability-roadmap/

15. Fighting Back

1 Matt Corallo, "Block Size Increase", Bitcoin-development mailing list, May 6, 2015, https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-May/007869.html

2 Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008, https://www.bitcoin.com/bitcoin.pdf

3 Maria Bustillos, Inside the Fight Over Bitcoin's Future, The New Yorker, August 25, 2015, https://www.newyorker.com/business/currency/inside-the-fight-over-bitcoins-future

4 Mike Hearn, “The resolution of the Bitcoin experiment”, Medium, January 14, 2016, https://blog.plan99.net/the-resolution-of-the-bitcoin-experiment-dabb30201f7

5 Pieter Wuille, “Bitcoin Core and hard forks”, Bitcoin-dev mailing list, July 22, 2015, https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-July/009515.html

6 Stephen Pair, Peter Smith, Jeremy Allaire, Sean Neville, Sam Cole, Charles, Cascarilla, John McDonnell, Wences Casares and Mike Belshe, “Our community stands at a crossroads.”, August 24, 2015, https://web.archive.org/web/20150905190229/ https://blog.blockchain.com/wp-content/uploads/2015/08/Industry-Block-Size-letter-All-Signed.pdf

7 Joseph Young, “7 Leading Bitcoin Companies Pledge Support for BIP101 and Bigger Blocks”, Bitcoin Magazine, August 24, 2015, https://bitcoinmagazine.com/technical/7-leading-bitcoin-companies-pledge-support-bip101-bigger-blocks-1440450931

8 F2Pool, Mining Pool Technical Meeting – Blocksize Increases, June 12, 2015, https://imgur.com/a/LlDRr

9 Mike Hearn, “Why is Bitcoin forking?”, Medium, August 15, 2015, https://medium.com/faith-and-future/why-is-bitcoin-forking-d647312d22c1

16. Blocking the Exit

1 “Bitcoin.org Hard Fork Policy”, Bitcoin, June 16, 2015, https://cloud.githubusercontent.com/assets/61096/8162837/d2c9b502-134d-11e5-9a8b-27c65c0e0356.png

2 Harding, “Blog: Bitcoin.org Position On Hard Forks #894”, Github, June 16, 2015, https://github.com/bitcoin-dot-org/bitcoin.org/pull/894#issuecomment-112121007 - double check

3 Harding, “Blog: Bitcoin.org Position On Hard Forks #894”, Github, June 16, 2015, https://github.com/bitcoin-dot-

org/bitcoin.org/pull/894#issuecomment-112123722

4 Tiraspol, “These Mods need to be changed. Up-Vote if you agree”, Reddit, August 16, 2015, https://archive.ph/rum9c

5 Theymos, “It’s time for a break: About the recent mess & temporary new rules”, Reddit, August 17, 2015, https://www.reddit.com/r/Bitcoin/comments/3h9cq4/its_time_for_a_break_about_the_recent_mess/

6 “Theymos: “I know how moderation affects people.” (Bitcoin censorship)”, Reddit, September 16, 2015, https://www.reddit.com/r/bitcoin_uncensored/comments/3l6oni/theymos_i_know_how_moderation_affects_people/

7 John Ratcliff, “Confessions of an r/Bitcoin Moderator”, Let’s Talk Bitcoin, August 19, 2015, https://archive.ph/6loqD

8 “So long, and thanks for all the fish.”, Reddit, August 30, 2015, https://www.reddit.com/r/bitcoin_uncensored/comments/3iwzmk/so_long_and_thanks_for_all_the_fish/cuonqqu/?utm_source=share&utm_medium=web2x

9 Tom Simonite, “Allegations of Dirty Tricks as Effort to “Rescue” Bitcoin Falters”, MIT Technology Review, September 8, 2015, https://www.technologyreview.com/2015/09/08/166310/allegations-of-dirty-tricks-as-effort-to-rescue-bitcoin-falters/

10 Celean, “UDP flood DDoS attacks against XT nodes”, Reddit, August 29, 2015, https://www.reddit.com/r/bitcoinxt/comments/3iumsr/udp_flood_ddos_attacks_against_xt_nodes/

11 Sqrt7744, “PSA: If you’re running an XT node in stealth mode, now would be a great time disable that feature, DDOS attacks on nodes (other than Coinbase) seem to have stopped, it’s a great time to show support publicly.”, Reddit, December 27, 2015,

https://www.reddit.com/r/bitcoinxt/comments/3yewit/psa_if_youre_running_an_xt_node_in_stealth_mode/

12 Jasonswan, “The DDoSes are still real”, Reddit, September 3, 2015, https://www.reddit.com/r/bitcoinxt/comments/3jg2rt/the_ddoses_are_still_real/cupb74s/?utm_source=share&utm_medium=web2x

13 Oddvisions, “I support BIP101”, Reddit, September 3, 2015, https://www.reddit.com/r/Bitcoin/comments/3jgtjl/comment/cupg2wr/?utm_source=share&utm_medium=web2x&context=3

14 Aaron van Wirdum, “Coinbase CEO Brian Armstrong: BIP 101 is the Best Proposal We’ve Seen So Far”, Bitcoin Magazine, November 3, 2015, https://bitcoinmagazine.com/technical/coinbase-ceo-brian-armstrong-bip-is-the-best-proposal-we-ve-seen-so-far-1446584055

15 Desantis, “Coinbase CEO Brian Armstrong: BIP 101 is the Best Proposal We’ve Seen So Far”, Reddit, November 3, 2015, https://www.reddit.com/r/Bitcoin/comments/3rejl9/coinbase_ceo_brian_armstrong_bip_101_is_the_best/cwpglh6/

16 Brian Armstrong (@brian_armstrong), Twitter, December 26, 2015, https://archive.ph/PYwTA

17 Cobra-Bitcoin, “Remove Coinbase from the “Choose your Wallet” page #1178”, Github, December 27, 2015, https://github.com/bitcoin-dot-org/bitcoin.org/pull/1178

18 Ibid.

19 Oliver Janssens (@oliverjanss), Twitter, December 27, 2015, https://twitter.com/olivierjanss/status/681178084846993408?s=20

20 Cobra-Bitcoin, “Remove Coinbase from the ‘Choose your Wallet’ page #1178”, Github, December 27, 2015, https://github.com/bitcoin-dot-org/bitcoin.org/pull/1178

21 CrimBit, “Hackers DDoS Coinbase, website down”, Bitcoin Forum, December 28, 2015, https://bitcointalk.org/index.php?topic=1306974.0

17. Hotwired for Settlement

1 Cobra-Bitcoin, “Remove Coinbase from the “Choose your Wallet” page #1178”, Github, December 27, 2015, https://github.com/bitcoin-dot-org/bitcoin.org/pull/1178#issuecomment-167389049

2 Satoshi, “Re: [PATCH] increase block size limit”, Bitcoin Forum, October 04, 2010, https://bitcointalk.org/index.php?topic=1347.msg15366#msg15366

3 Cade Metz, “The Bitcoin Schism Shows the Genius of Open Source”, Wired, August 19, 2015, https://www.wired.com/2015/08/bitcoin-schism-shows-genius-open-source/

4 Cobra-Bitcoin, “Remove Coinbase from the “Choose your Wallet” page #1178”, Github, December 27, 2015, https://github.com/bitcoin-dot-org/bitcoin.org/pull/1178#issuecomment-167389049

5 Aaron van Wirdum, “Chinese Mining Pools Call for Consensus; Refuse Switch to Bitcoin XT”, Cointelegraph, June 24, 2015, https://cointelegraph.com/news/chinese-mining-pools-call-for-consensus-refuse-switch-to-bitcoin-xt

6 Ibid.

7 Adam Back (@adam3us), Twitter, August 26, 2015, https://twitter.com/adam3us/status/636410827969421312

8 Adam Back (@adam3us), Twitter, December 30, 2015, https://twitter.com/adam3us/status/682335248504365056

9 Mike Hearn, “AMA: Ask Mike Anything”, Reddit, April 5, 2018, https://www.reddit.com/r/btc/comments/89z483/comment/dwup253/

10 Mike Hearn, “The resolution of the Bitcoin experiment”, Medium, January 14, 2016, https://blog.plan99.net/the-resolution-of-the-bitcoin-

experiment-dabb30201f7

11 Jeff Garzik, “Bitcoin is Being Hot-Wired for Settlement”, Medium, December 29, 2015, https://medium.com/@jgarzik/bitcoin-is-being-hot-wired-for-settlement-a5beb1df223a#.850eazy81

12 “BitPay’s Bitcoin Payments Volume Grows by 328%, On Pace for $1 Billion Yearly”, BitPay, October 2, 2017, https://web.archive.org/web/20200517164537/https://bitpay.com/blog/bitpay-growth-2017/

13 Stephen Pair, “Bitcoin as a Settlement System”, Medium, January 5, 2016, https://medium.com/@spair/bitcoin-as-a-settlement-system-13f86c5622e3#.59s53nck6

14 Stephen Pair, “Miners Control Bitcoin: …and that’s a good thing”, Medium, January 4, 2016, https://medium.com/@spair/miners-control-bitcoin-eea7a8479c9c

15 “Bitcoin is not ruled by miners”, Bitcoin Wiki, August 18, 2023, https://en.bitcoin.it/wiki/Bitcoin_is_not_ruled_by_miners

16 “Bitcoin is not ruled by miners”, Bitcoin Wiki, August 18, 2023, https://en.bitcoin.it/wiki/Bitcoin_is_not_ruled_by_miners

18. From Hong Kong to New York

1 “What Happened At The Satoshi Roundtable”, Coinbase, March 4, 2016, https://blog.coinbase.com/what-happened-at-the-satoshi-roundtable-6c11a10d8cdf

2 “Consensus census”, Google Docs, https://docs.google.com/spreadsheets/d/1Cg9Qo9Vl5PdJYD4EiHnIGMV3G48pWmcWI3NFoKKfIzU/edit#gid=0

3“49% of Bitcoin mining pools support Bitcoin Classic already (as of January 15, 2016)”, Reddit, January 15, 2016,

https://www.reddit.com/r/btc/comments/414qxh/49_of_bitcoin_mining_pools_support_bitcoin/

4 Paul Vigna, “Is Bitcoin Breaking Up?”, The Wall Street Journal, January 17, 2016 https://archive.ph/lK24o#selection-4511.0-4511.263

5 “49% of Bitcoin mining pools support Bitcoin Classic already (as of January 15, 2016)”, Reddit, January 15, 2016, https://www.reddit.com/r/btc/comments/414qxh/comment/cz063na/?utm_source=share&utm_medium=web2x&context=3

6 “49% of Bitcoin mining pools support Bitcoin Classic already (as of January 15, 2016)”, Reddit, January 15, 2016, https://www.reddit.com/r/btc/comments/414qxh/comment/cz0hwzz/?utm_source=share&utm_medium=web2x&context=3

7 Bitcoin Roundtable, “Bitcoin Roundtable Consensus”, Medium, February 20, 2016, https://medium.com/@bitcoinroundtable/bitcoin-roundtable-consensus-266d475a61ff#.8vbwu3ft7

8 The Future of Bitcoin, “Dr. Peter Rizun - SegWit Coins are not Bitcoins - Arnhem 2017”, Youtube, July 7, 2017, https://www.youtube.com/watch?v=VoFb3mcxluY

9 “What Happened At The Satoshi Roundtable”, Coinbase, March 4, 2016, https://blog.coinbase.com/what-happened-at-the-satoshi-roundtable-6c11a10d8cdf

10 “Bitcoin Classic Nodes Under Heavy DDoS Attack”, Blocky, February 28, 2016, https://web.archive.org/web/20160302070655/http://www.blockcy.com/bitcoin-classic-nodes-under-ddos-attack

11 Drew Cordell, “Bitcoin Classic Targeted by DDoS Attacks”, Bitcoin.com, March 1, 2016, https://news.bitcoin.com/bitcoin-classic-targeted-by-ddos-attacks/

12 Joseph Young, “F2Pool Suffers from Series of DDoS Attacks”, Cointelegraph, March 2, 2016, https://cointelegraph.com/news/f2pool-

suffers-from-series-of-ddos-attacks

13 Coin Dance, “Bitcoin Classic Node Summary” https://coin.dance/nodes/classic, August, 2023

14 Cobra-Bitcoin, “Amendments to the Bitcoin paper #1325”, Github, July 2, 2016, https://github.com/bitcoin-dot-org/bitcoin.org/issues/1325

15 Ibid.

16 Theymos, “Policy to fight against “miners control Bitcoin” narrative #1904”, Github, November 8, 2017, https://github.com/bitcoin-dot-org/bitcoin.org/issues/1904

17 Ibid.

18C harlie Shrem (@CharlieShrem), Twitter, January 19, 2017, https://twitter.com/CharlieShrem/status/822189031954022401

19 Andrew Quentson, “Bitcoin Core Supporter Threatens Zero Day Exploit if Bitcoin Unlimited Hardforks”, CCN, March 4, 2021, https://www.ccn.com/bitcoin-core-supporter-threatens-zero-day-exploit-bitcoin-unlimited-hardforks/

20 Yuji Nakamura, “Divisive ‘Bitcoin Unlimited’ Solution Crashes After Bug Discovered”, Bloomberg Technology, March 15, 2017, https://web.archive.org/web/20170315070841/https://www.bloomberg.com/news/articles/2017-03-15/divisive-bitcoin-unlimited-solution-crashes-after-bug-exploit

21 Digital Currency Group, “Bitcoin Scaling Agreement at Consensus 2017”, Medium, May 23, 2017, https://dcgco.medium.com/bitcoin-scaling-agreement-at-consensus-2017-133521fe9a77

22 ViaBTC, “Why we don’t support SegWit”, Medium, April 19, 2017, https://viabtc.medium.com/why-we-dont-support-segwit-91d44475cc18

23 Gmaxwell, “Re: TroominCoin aka “Bitcoin_Classic” #R3KT”, Bitcoin Forum, May 13, 2016, https://bitcointalk.org/index.php?

topic=1330553.msg14835202#msg14835202

24 Mike Hearn, Hacker News, Y Combinator, March 28, 2016, https://news.ycombinator.com/item?id=11373362

19. The Mad Hatters

1 Shaolinfry, “Moving towards user activated soft fork activation”, Bitcoin-dev mailing list, February 25, 2017, https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2017-February/013643.html

2 Jordan Tuwiner, “UASF / User Activated Soft Fork: What is It?”, Buy Bitcoin Worldwide, January 3, 2023, https://www.buybitcoinworldwide.com/uasf/

3 Washington Sanchez (@drwasho), Twitter, May 17, 2017, https://twitter.com/drwasho/status/864651283050897408

4 Samson Mow (@Excellion), Twitter, March 22, 2017, https://twitter.com/excellion/status/844349077638676480

5 Adam Back (@adam3us), Twitter, October 3, 2017, https://twitter.com/adam3us/status/915232292825698305?s=20

6 Btc Drak, “A Segwit2x BIP”, Bitcoin-dev mailing list, July 8, 2017, https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2017-July/014716.html

7 AlexHM, “BTCC just started signalling NYA. They went offline briefly. That’s over 80%. Good job, everyone.”, Reddit, June 20, 2017, https://www.reddit.com/r/btc/comments/6ice15/btcc_just_started_signalling_nya_they_went/dj5dsuy/

8 Samson Mow (@Excellion), Twitter, March 29, 2017, https://twitter.com/Excellion/status/847159680556187648

9 Edmund Edgar (@edmundedgar), Twitter, March 30, 2017, https://twitter.com/edmundedgar/status/847213867503460352

10 Samson Mow (@Excellion), Twitter, March 30, 2017, https://twitter.com/excellion/status/847273464461352960

11 Adam Back (@adam3us), Twitter, April 1, 2017, https://archive.ph/WJdZj

12 Peter Todd (@peterktodd), Twitter, July 19, 2017, https://twitter.com/peterktodd/status/887656660801605633

13 Nullc, "Segwit is a 2MB block size increase, full stop.", Reddit, August 13, 2017, https://archive.ph/8d6Jm

14 Eric Lombrozo (@eric_lombrozo), Twitter, April 20, 2017, https://archive.ph/9xTbZ

15"Is SegWit a block size increase?", Segwit.org, August 29, 2017, https://archive.ph/lEpFf

16"Delist NYA participants from bitcoin.org #1753", Github, August 18, 2017, https://github.com/bitcoin-dot-org/bitcoin.org/issues/1753#issuecomment-332300306

17 Cobra-Bitcoin, "Add Segwit2x Safety Alert #1824 ", Github, October 11, 2017, https://github.com/bitcoin-dot-org/bitcoin.org/pull/1824

18 "Bitcoin.org to denounce "Segwit2x"", Bitcoin.org, October 5, 2017, https://web.archive.org/web/20171028193101/https://bitcoin.org/en/posts/denounce-segwit2x

19 "Bitcoin.org Plans to "Denounce" Almost All Bitcoin Businesses and Miners", Trustnodes, October 6, 2017, https://www.trustnodes.com/2017/10/06/bitcoin-org-plans-denounce-almost-bitcoin-businesses-miners

20 "SegWit2x Blocks (historical) Summary", Coin Dance, August 18, 2023, https://web.archive.org/web/20171006030014/https://coin.dance/blocks/segwit2xhistorical

21 Eric Lombrozo, “Bitcoin Cash’s mandatory replay protection - an example for B2X”, Bitcoin-segwit2x mailing list, August 22, 2017, https://lists.linuxfoundation.org/pipermail/bitcoin-segwit2x/2017-August/000259.html

22M att Corallo, “Subject: File No. SR-NYSEArca-2017-06”, September 11, 2017, https://www.sec.gov/comments/sr-nysearca-2017-06/nysearca201706-161046.htm

23 Samson Mow (@Excellion), Twitter, October 7, 2017, https://twitter.com/Excellion/status/916491407270879232

24 Samson Mow (@Excellion), Twitter, October 7, 2017, https://twitter.com/Excellion/status/916492211700690945

25 Microbit, “Removal of BTC.com wallet? #1660”, Github, July 3, 2017, https://github.com/bitcoin-dot-org/bitcoin.org/issues/1660#issuecomment-312738631

26 Kokou Adzo, “Best Programming Homework Help Websites for You to Choose”, Startup.info, June 8, 2023, https://techburst.io/segwit2x-youre-fucked-if-you-do-you-re-fucked-if-you-don-t-6655a853d8e7

27 “Statement Regarding Upcoming Segwit2x Hard Fork”, Bitfinex, October 6, 2017, https://www.bitfinex.com/posts/223

28 Stephen Pair, “Segwit2x Should Be Canceled”, Medium, November 8, 2017, https://medium.com/@spair/segwit2x-should-be-canceled-b7399c767d34

29 Mike Belshe, “Final Steps”, Bitcoin-segwit2x mailing list, November 8, 2017, https://lists.linuxfoundation.org/pipermail/bitcoin-segwit2x/2017-November/000685.html

30 Gavin Andresen (@gavinandresen), Twitter, November 11, 2017, https://twitter.com/gavinandresen/status/929377620000681984

20. Challenger for the Title

1 Vitalik.eth (@VitalikButerin), Twitter, November 14, 2017, https://mobile.twitter.com/vitalikbuterin/status/930276246671450112

2 Van der Laan, "The widening gyre", Laanwj's blog, January 21 2021, https://laanwj.github.io/2021/01/21/decentralize.html

3 MortuusBestia, "BTC--->BCH has been the most popular trade on ShapeShift.io for some time", Reddit, https://www.reddit.com/r/CryptoCurrency/comments/8e3eon/comment/dxs2puh/

4 BitcoinIsTehFuture, "It's called "Bitcoin Cash". The term "Bcash" is a social attack run by r/bitcoin." Reddit, August 2, 2017, https://www.reddit.com/r/btc/comments/6r4no6/its_called_bitcoin_cash_the_term_bcash_is_a/

5 "bashco at least we got a warning right? Cobra I got a concrete head ups, I warned users to check signatures, it's that simple", https://imgur.com/a/wwVSXZW

6 Jonald Fyookball, "Why Some People Call Bitcoin Cash 'bcash'. This Will Be Shocking to New Readers.", Medium, September 18, 2017, https://medium.com/@jonaldfyookball/why-some-people-call-bitcoin-cash-bcash-this-will-be-shocking-to-new-readers-956558da12fb

21. Bad Objections

1 Ammous, The Bitcoin Standard, p. 229

2 "Latest Bitcoin Blocks by Mining Pool (last 7 days) Summary", Coin Dance, August 18, 2023, https://coin.dance/blocks/thisweek

3 Mike Hearn, "Re: More BitCoin questions", Bitcoin.com, January 10, 2011, https://www.bitcoin.com/satoshi-archive/emails/mike-hearn/12/

4 Awemany, "600 Microseconds: A perspective from the Bitcoin Cash and Bitcoin Unlimited developer who discovered CVE-2018–17144", Bitcoin

Unlimited, September 22, 2018, https://medium.com/@awemany/600-microseconds-b70f87b0b2a6

22. Free to Innovate

1 Mengerian, "The Story of OP_CHECKDATASIG", Medium, December 15, 2018, https://mengerian.medium.com/the-story-of-op-checkdatasig-c2b1b38e801a

2 Kudelski Security, "CashFusion Security Audit", CashFusion, July 29, 2020, https://electroncash.org/fusionaudit.pdf

3 "191457 Fusions since 28/11/2019", Bitcoin Privacy Stats, August 18, 2023, https://stats.sploit.cash/#/fusion

4 Jamie Redman, "Gigablock Testnet Researchers Mine the World's First 1GB Block", Bitcoin.com, October 16, 2017, https://news.bitcoin.com/gigablock-testnet-researchers-mine-the-worlds-first-1gb-block/

5 "I have previously stated that the latest RPi4 can process Scalenet's 256MB blocks in just under ten minutes. I was wrong.", Reddit, July 8, 2022, https://np.reddit.com/r/btc/comments/vuiqwm/im_terribly_sorry_as_the_noob_that_i_am_i_have/

23. Still Forking Around

1 Gavin Andresen, "Satoshi", Gavin Andresen, May 2, 2016, http://gavinandresen.ninja/satoshi

2 Jiang Zhuoer, "Infrastructure Funding Plan for Bitcoin Cash", Medium, January 22, 2020, https://medium.com/@jiangzhuoer/infrastructure-funding-plan-for-bitcoin-cash-131fdcd2412e

3 Amaury Sechet, "Bitcoin ABC's plan for the November 2020 upgrade", Medium, August 6, 2020, https://amaurysechet.medium.com/bitcoin-abcs-plan-for-the-november-2020-upgrade-65fb84c4348f

4 Peter R. Rizun (@PeterRizun), Twitter, February 15, 2020, https://twitter.com/PeterRizun/status/1228787028734574592

5 MemoryDealers, “Even if Amaury and ABC are the best developers in the world, that doesn’t mean they deserve 8% of the block reward.”, Reddit, October 18, 2020, https://www.reddit.com/r/btc/comments/jdft5s/comment/g98y9l3/

24. Conclusion

1 Turner Wright, “Coinone will stop withdrawals to unverified external wallets”, Cointelegraph, December 29, 2021, https://cointelegraph.com/news/coinone-will-stop-withdrawals-to-unverified-external-wallets

2 Mike_Hearn, “AMA: Ask Mike Anything”, Reddit, April 5, 2018, https://www.reddit.com/r/btc/comments/89z483/ama_ask_mike_anything/

About the Author

Roger Ver is the world's first investor in Bitcoin startups and has been a prominent figure in the cryptocurrency industry since it began. His investments include Bitcoin.com, Blockchain.com, Bitpay, Ripple, Shapeshift, Kraken, and many others. As a tech entrepreneur, Roger immediately knew that Bitcoin was going to change the world after discovering it in 2011. Since then, he has devoted his full attention to Bitcoin and other blockchains.