An Enlightened Island:
Original Vision, Community Politics, and the Failure of Bitcoin

Marjorie Murphy & Robert Weinberg
HIST091: Senior Research Seminar
16 December 2016
Abstract

One of the first paradoxes of Bitcoin was how the community would uphold Satoshi’s original vision and founding principles after its creation. Despite much recent scholarly discussion on the idea of Bitcoin, intellectual history of money, and optimistic, progressive historiography, little has been written to answer the question of whether Bitcoin has succeeded in its original vision. The article argues that Bitcoin has failed to remain civil libertarian, radically democratic, and equal and open due to community politics and an ensuing civil war over the block size debate and the future of the blockchain. In addition to drawing from two historicizations, Yap stone money and the Enlightenment, the article sources online social archives to support the thesis that various actions by the Bitcoin community during the civil war overturned and failed the original vision.

Introduction

On July 9, 2016, an island of the Internet was happily abuzz for a peculiar idea and the community it had fostered over time—Bitcoin. One redditor posted in the official r/Bitcoin subreddit a link to a collage of LEGO figures to tell the story of Bitcoin and commemorate the second halving of the young cryptocurrency. Elsewhere in the subreddit, people offered congratulations and noted their participation in what they considered a world-historical event. The Bitcoin community’s sentiment on that day was festive and exuberant.

Yet I argue that Bitcoin had already failed in its original vision by summer 2016. The historical question is how to write a history of Bitcoin. The first wave of Bitcoin scholars quibbled over the history of monetary thought and Bitcoin’s place within that intellectual history. There were vexing debates after the early period of 2008 to 2012 on whether Bitcoin is money. But a recent second wave of historiography tends to be optimistic. Vigna and Casey argue that Bitcoin and cryptocurrencies will transform the world through competition with the traditional economic order. Popper focuses on a top-down history, telling the stories of prominent and
colorful characters largely outside the Internet community, including startup entrepreneurs, angel investors, institutional capitalists, and millionaire enthusiasts, aiming to reinvent money while making a tidy profit. Both historiographies seem like linear narratives of progress. But I will incorporate everyday individuals who participate in and maintain the community to retell the story of Bitcoin’s intellectual failure and argue against that optimistic, progressive historiography.

The failure of Bitcoin transpired a mere seven years after Bitcoin the idea was created. In October 2008 Bitcoin’s creator Satoshi Nakamoto published the original white paper. At its essence, Bitcoin is a protocol or free and open source software code that has electronic cash as its first and most important application so far. Bitcoin is the first peer-to-peer, decentralized, borderless, and permissionless digital currency; it is also the first successful cryptocurrency, a currency that uses cryptography to secure transactions and regulate supply. Satoshi released Bitcoin the protocol, free and open source software written in C++, to the public on January 3, 2009. Created in the depths of the worst global economic crisis since the Great Depression, Bitcoin embodied hopes for a new world order. In 2008 Lehman Brothers filed for the largest bankruptcy in history; the S&P 500 lost over 40 percent of its value that year. The global economy teetered into the nadir of crisis, as banks, firms, and nations failed, were bailed out, and remained troubled. There could not have been a more auspicious time to introduce a new monetary system to the world.

**Original Vision and Historicization**

The mysterious, pseudonymous Satoshi Nakamoto created Bitcoin during the darkest days of the 21st century, when many people were questioning the very idea of banks and money.
After a disappearance in 2010, he or she remains an influential enigma, a historical figure enshrined in public memory. Today Satoshi's wisdom is preserved in an archive accessible to all. Because Satoshi was the godhead who literally created Bitcoin from nothing, an appeal to original vision is persuasive on both visceral and rational grounds. Compared to originalist arguments in constitutional law and political economy, Bitcoin originalism is even more powerful because Satoshi not only created the code but also welcomed and inspired a community and then voluntarily relinquished power. So what was the original vision?

Satoshi had envisioned a new money based not on social trust but cryptographic proof. Bitcoin would be civil libertarian, with ironclad privacy protections thanks to futureproof technologies like elliptic curve cryptography to secure digital signatures and pseudonymous addresses derived from hashes of private keys. It would also be radically democratic, since anyone could become a miner node and vote with their computing power to validate the blockchain or history of transactions. Finally, it would be egalitarian and open, because of decentralized leadership and the mathematical fact that no one person or entity can change the code without the supermajority consensus of the community. Non-mining participants, merchants, consumers, and enthusiasts would be able to voice their thoughts and concerns in online forums and safe spaces. Anyone in the world, no matter their race, class, geography, or language, would be able to participate as a user and community member. In essence, Bitcoin's original vision was a new, more perfect money—libertarian, democratic, and open—a revolutionary idea to subvert the corrupt interests of states and banks and return financial control back to the people.

Bitcoin can be historicized in order to better understand its commonalities with past phenomena and its unique challenges with respect to original vision. A popular way to
historicize Bitcoin is through an analogy with the Yap stone money. Until the early twentieth century, the people of the Yap islands used giant limestone disks as their money: “large, solid, thick, stone wheels, ranging in diameter from a foot to twelve feet, having in the centre a hole varying in size.” The stones were quarried and cut on an island four hundred miles away, and expeditioners transported them to Yap via ship. The value of the stone money was determined by size and quality. But the curious aspect of Yap stone money is that in general it was not physically possessed by people. Instead, wealth and transactions were recorded in the public memory, akin to Bitcoin’s blockchain. Physically burdensome to steal, the stone money was safe and secure, as Bitcoin’s cryptographic elements attempt to achieve. Like Yap, Bitcoin originally started as an island in virtual space—and then cultivated contact with the concrete world and connections to fiat money.

Unlike other scholars’ work, I move beyond the comparison between Yap and Bitcoin as ideas of money. The contrast is between the demise of Yap stone money and the failure of Bitcoin; the historical focus is on how Bitcoin failed in its original vision. The people of Yap eventually stopped using stone money due to various external factors like imperial conquest and conflict between Germany and Spain, a rogue trader who introduced inflationary pressure into the monetary system, and the influx of foreign coins and bills. In Bitcoin’s early period of about 2009 to 2012, the community was largely afraid that state regulation and prohibition would destroy the nascent cryptocurrency—as it did to Yap money—but those concerns were in hindsight a sword of Damocles. The real danger was the savage civil war that emerged from the block size debate. The Winklevoss twins of Facebook fame once stated in support of Bitcoin: “We have elected to put our money and faith in a mathematical framework that is free of politics and human error.” Unfortunately, the great block size debate of 2015 demonstrated that much
politics and human error could consume Bitcoin and all but destroyed the community’s solidarity, resulting in a visionary failure from self-inflicted wounds.

Technical Overview

A brief technical overview of how Bitcoin works is necessary for understanding the block size debate. First, Bitcoin aims to be a peer-to-peer monetary system, where users can send and receive transactions without an intermediary. When one user wants to send bitcoins to another user, she uses a Bitcoin wallet, software that collects and stores private keys and lets the user access funds from her addresses. She sends a message that says she wants to send any number of BTC to a public address. The user uses her private key to sign the message and sends it to the network. The nodes in the network verify if the signature is correct. Then the nodes check if the sending address has enough funds for the transaction. Finally, the nodes update the ledger by subtracting funds from the sending address and adding them to the receiving address. The transaction process was designed to be low-cost, frictionless, and very fast.

The heart of Bitcoin is the blockchain, a public, distributed ledger that records bitcoin transactions. Users only know how much funds are associated with their private key and addresses by checking the entire blockchain. Users check the blockchain for records of ownership of funds; the blockchain itself records the history of transactions. Transactions are grouped into blocks. The blocks are recorded in order in a chain. The blockchain is an ever-growing chain of blocks. In a decentralized system, normal timestamps would not work because there is no good way to verify their authenticity without a central authority. The blockchain uses
proof-of-work to secure the history. Proof-of-work is proof that some work has been done—a problem hard to solve but easy to verify.

Essentially the blockchain is secured by the very computational power that is applied to create it. Bitcoin uses the cryptographic hash function SHA256^2, the SHA256 function applied twice, as its proof-of-work. The proof-of-work is the solution to the partial hash inversion problem. Partial hash inversion requires that the hash of a block of transactions starts with at least a certain number of zeros. A nonce is a number that solves the problem. It must be computationally guessed through brute-forcing by the network. The time it takes to solve a block is random, and the code automatically adjusts the block difficulty to target about 10 minutes between blocks. The blockchain secures the history of transactions because the proof-of-work makes it extremely difficult for attackers to commit fraud.

A valid transaction is one that enters the blockchain first. If someone wants to edit a recorded transaction, or send two different transactions attempting to spend the same funds, then she would need to perform a 51% attack. A 51% attack is where an attacker controls a hash rate, or computational power, larger than that of the rest of the network. To do so, the attacker would need to spend millions upon millions of dollars on resources including electricity. There would still be an incentive to not commit fraud in that honest mining might be the most profitable action with such a large hash power. That is how a decentralized blockchain solves the double spending problem, effectively prevents cyberattacks, deters fraud, and records an honest history of transactions.

The colloquial explanation is that bitcoins are mined into existence by computing power. Mining is a verification process that adds blocks to the blockchain. Miners are nodes in the network that actively try to solve blocks. They contribute their computational power to solve the
partial hash inversion problem. A miner rewards herself by sending the first transaction of a new block, the coinbase, to her own address. The whole process of mining can be described as following: New transactions are broadcast to the network. Miners collect new transactions into a block. Miners try to find a nonce that solves the partial hash inversion problem for their block. Upon finding a nonce that solves the problem, the miner broadcasts the proof-of-work to all nodes in the network. Receiving nodes verify the transactions of the broadcasting node and accept only if all are valid. Nodes express acceptance of the block by incorporating the hash of the block to use for working to solve the next block. Since theoretically anyone can become a miner, the network of miners functions as a democratic group that rewards market competition and honesty.

The average layperson can use Bitcoin without a deep understanding of the blockchain, being a miner, or participating in the network. Users who want to send and receive bitcoins can use a Bitcoin wallet. Unlike a physical wallet, a Bitcoin wallet can be copied digitally. A Bitcoin wallet can be stolen by attackers’ copying, but copying one’s own wallet is a good precaution against losing it. Bitcoin wallets can be distributed across several devices so that access to the funds will require cooperation among the devices. Wallets perform several tasks: interfacing with the user, querying the blockchain to inform the user of available funds, generating new addresses to receive funds, receiving change from transactions done by the wallet, generating and reading QR codes that represent addresses, allowing the user to send funds to selected addresses, tracking the confirmation status of transactions, and making and restoring a backup of the wallet.

There are five types of wallets. The first three are hot storage, connected to the Internet. Desktop wallets are on personal computers and can run on Windows, Mac OSX, and Linux
operating systems. Many are full clients that download the entire blockchain and perform full validation. Mobile, or lightweight, wallets are highly popular for practical use. There are options for Android, iOS, Windows Phone, and BlackBerry. Mobile wallets are thin, not full, clients. Most use simplified payment validation (SPV), which downloads a small part of the blockchain and uses block headers to verify transactions. SPV clients perform the block depth validity check, determining how many blocks have been mined on top of the block that included the transaction. In general, mobile wallets are less secure than desktop wallets but are easier to use. Web wallets are online wallets. They are the least secure type of wallet due to centralized validation and third-party control. Centralized validation, unlike full validation or SPV, is the practice of relying on a third party for validation, which requires trusting the third party to not hide or simulate payments. Third-party control refers to the fact that bitcoin funds in web wallets are controlled by the wallet instead of the user. Users do not truly own bitcoin funds in web wallets because the wallet holds the private keys. Nonetheless, web wallets are very popular and easy to use. Hardware and paper wallets are the most secure and least convenient options; they are only vulnerable to physical theft or loss. Hardware wallets are dedicated devices that both store private keys and sign transactions. Hardware wallets are cold storage, meaning private keys are kept inaccessible from the Internet. A hardware wallet communicates with wallet software in a computer, either a desktop or web wallet. The wallet software acts as an intermediary between the blockchain and the hardware wallet. Paper wallets are true offline wallets; they are private keys printed or written on paper. Physical bitcoins, coins that hide a private key behind a tamper-proof mechanism, are also paper wallets. Since many users have fallen victim to fraudulent and shoddy web wallets and exchanges in the past, the Bitcoin community generally advocates wallet
security by using hot and cold storage, regular wallet backup, and keeping many copies of backups in different safe places.

Intellectual Historicization and Satoshian Moment

Bitcoin can also be intellectually historicized. The blockchain and mining process show that honesty is key to the success of Bitcoin:

The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. 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. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. 16

Satoshi’s original vision harkened to radical Enlightenment ideas of equality, republicanism, and virtue. The success of the American Revolution depended on the shared values of republicanism—the idea that citizens would agree to practice virtue, commit to a community of honest production, and eschew privilege in favor of equality. 17 The same radical Enlightenment ideals permeated the original Bitcoin community, especially in the early period when community members socialized like a close family. In 1730 Richard Cantillon and in 1776 Adam Smith had concluded that capital and labor should flow freely through markets and nations should abandon the bondage of mercantilism. 18 Over two centuries later, Satoshi and the Bitcoin community dreamed of a hypermodern generation of global techno-citizens who would reject the world of traditional finance and through their own power mine a new, better species called Bitcoin. Finally, Bitcoin originally reincorporated much of the doux commerce thesis that arose from Renaissance and early Enlightenment thought—through commerce proud and haughty
individuals act gentle and cordial, their passions superseded by interest, so as to avoid censure and achieve success in market activities. Bitcoin first held the promise of a revolutionary way of trading money, goods, and services that could recapture agency from the violent sphere of corporatist banking and statist money and bring calm and peace to human lives.

Whereas other scholars might choose Satoshi’s world-historical moment to be the first block mined or the disappearance of Satoshi after December 12, 2010, my Satoshian moment occurred on December 5, 2010, in the midst of a debate on whether to donate bitcoins to WikiLeaks. In January, PayPal had suspended WikiLeaks’s fiat donation account and frozen its assets. A member posted on the official Bitcoin Forum on November 10 asking about how to message WikiLeaks to tell them that secure access to funds is an advantage of Bitcoin. Other members like Jeff Garzik rejected the idea because US Attorney General Eric Holder and the Department of Justice had begun a criminal investigation of WikiLeaks and its founder Julian Assange. On December 4, a Robert Horning posted an intensely personal message:

For myself, I’m getting to the point to say “bring it on” in regards to Wikileaks [sic]. […] It is the morally correct thing to be supporting Wikileaks, and if they’ll take a few of my bitcoins, I not only want to donate but to let the world know that they can donate to Wikileaks through Bitcoins as well. […] I can’t speak for everybody here in the Bitcoin community but I am speaking for myself on this matter, and I’m not afraid of anything that the U.S. government might do to me if I was associated with backing Wikileaks financially. If anything, it would show that I no longer live under a constitutional government any more. If the U.S. government wants to tip their hand to expose themselves in that way, so be it. If the U.S. government kills me or puts me in jail, I’ll certainly set a way for this community to find out. I really don’t think it would come to that either, but I don’t care if it did.

Still, Garzik and others fervently disagreed, arguing against the greater good and for avoiding a result that would hurt all in the Bitcoin community. The next day, Satoshi wrote: “The project needs to grow gradually so the software can be strengthened along the way. I make this appeal to WikiLeaks not to try to use Bitcoin. Bitcoin is a small beta community in its infancy. You would
not stand to get more than pocket change, and the heat you would bring would likely destroy us at this stage.\textsuperscript{22} After more discussion, everyone on the thread but Horning agreed with Satoshi’s statement. Eventually, a consensus was reached to keep a low profile temporarily and remain neutral for a while.

In retrospect, that episode revealed more than just a minor dispute among community members. Politics had entered the conversation for the first time. It was remarkable how Satoshi persuaded consensus in the face of a passionate libertarian cause. The cause was a creation of the decentralized Internet, a promise of global information and transparency that transcends the concrete world. WikiLeaks was not just any institution; it was one that Bitcoin enthusiasts would naturally support on an ideological level, as part of an information-based utopia under siege. Yet Satoshi and the community solved the problem through polite conversation, not savage vitriol—emphasizing the community’s welfare and potential. Although Satoshi vanished into public memory later that month in accordance with the decentralized, leaderless spirit of Bitcoin, the WikiLeaks debate showed a glimpse of how a community isolated in virtual space could use not savage but polite means to resolve tensions and settle disputes. It was like the block size debate in its centrality to the survival and prosperity of Bitcoin. But it sharply contrasted with the block size debate that erupted into a savage civil war.

The Block Size Debate

The block size, or scalability debate is related to the block reward and transaction fees. The original block reward as programmed in the Bitcoin protocol was 50 BTC per block. The software code regulates a block reward halving about every 4 years. The asymptotic progression
means the maximum amount of bitcoins in existence will be approximately 21 million; the last bitcoin should be mined in 2140. In theory, as the block reward lessens, miners will be increasingly reliant on transaction fees as earnings. Users who send bitcoins choose the transaction fee like a tip, from the tiny minimum fee up to the value of the transaction. In the early period, there were few transactions with fees above the minimum transaction fee, and transactions with a minimum fee were confirmed into new blocks by miners the same as transactions with a greater fee. But as time increased and the block reward decreased, miners have gained the incentive to prioritize transactions with greater fees. So as the blocks got bigger, inflation set into the transaction fees, and the original idealism was called into question.

The block size debate centered around the question of what the size of blocks should be. At genesis, Bitcoin had a block size limit of 32 megabytes (MB). Block size was not a problem in the early period because the blocks mined were tiny; for example, the Genesis block and second block were 285 and 215 bytes, respectively. On September 7, 2010, Satoshi changed the code after consulting the community so that the block size limit was 1 MB, and any block bigger than 1 MB would be invalid. The block size limit meant that Bitcoin could handle a maximum of seven transactions per second in theory. Some reasons for the change were to prevent early miners from spamming the mining of large blocks and to deter large-scale cyberattacks. Though not completely clear, Satoshi’s words surrounding the block size limit can be construed to support a block size increase. Whatever the true reasons behind the change, the origins of the block size limit and Satoshi’s original intent would flare up as points of contention during the debate.

On one side of the block size debate are those who can be called the libertarians, members against a block size limit increase. They oppose that because a limit increase would
mean greater centralization of mining. Bigger blocks earn more fees for miners, and larger miners can better afford the bandwidth and mining hardware necessary for bigger blocks. The system of voting with computing power or hash rate favors larger miners and allows the majority to enforce conditions on the minority. Also, miners’ interests can conflict with users’. Bigger blocks can compromise the security of Bitcoin, making it more difficult for full nodes to download and verify the entire blockchain. The fee market that arises will help solve the problems of transaction confirmation and acceptance. Finally, scalability issues should be fixed with sidechains that allow transactions to happen off the blockchain. Libertarians, or small blockers, prefer decentralization to efficiency.

On the other side of the block size debate are those who can be called the democrats, members for a block size limit increase. They advocate that because a limit increase would mean greater support for more users. Bigger blocks would benefit users by making transactions more inexpensive, accessible, and reliable. Scaling the network to become a global system capable of handling numerous transactions per second would make it easier for new adopters and ordinary people to use Bitcoin. Smaller blocks mean that transactions take much longer to become confirmed and have a greater risk of not being confirmed. Merchants need to accept payments within seconds in order for Bitcoin to be widely adopted. Finally, the fee market that arises from blocks reaching the limit hurts users. Fees should be as low as possible. Democrats, or big blockers, prefer efficiency to decentralization.

Although Bitcoin had survived some dark episodes before 2015, including Trendon Shavers’s 2012 Ponzi scheme, the 2013 shutdown of Silk Road by the US government, and the 2014 collapse of the premier exchange Mt. Gox, the block size debate was a more critical and fundamental crisis. It tore at the fabric of the code and community. It reflected a community
schism that arose from divergent values and incentives. The libertarians were members who supported freedom, individualism, and decentralization most. They saw themselves as pioneers against the state, using the power of Bitcoin to circumvent fiat hegemony and oppression. They were followers of core developers like Gregory Maxwell and Pieter Wuille, idealists and intellectuals. The democrats were members who supported democratization, collectiveness, and efficiency most. They saw themselves as apostles spreading the gospel of Bitcoin as a global payments system and long-term alternative investment. They were followers of core developers like Gavin Andresen and Jeff Garzik, pragmatists and techno-citizens. Both sides were self-proclaimed disciples of Satoshi. The clash of visions for Bitcoin would erupt in the block size debate.

Up until the actual outbreak of civil war in 2015, the two sides behaved curt but cordial during discussions on block size. For the sake of clarity of argument, henceforth the libertarian side will be referred to as small blockers, and the democrat side as big blockers.

The origins of the block size debate can be traced to a series of posts and threads on the Forum and Reddit. The first post on August 6, 2011, was a complaint about the speed of the initial blockchain download. Other redditors helped by referring to an alternative method of downloading the blockchain via ZIP archive and verifying the blocks. The next wave of concerns surfaced throughout 2012. In January several individuals bemoaned the size of the blockchain and its slow downloading speed. One member complained that the blockchain took many hours to download when they wanted to receive a payment. In another thread in June members again complained about the time to download the blockchain, with a few noting that it took over twenty hours. A July 11 post titled “Milestone crossing for the official bitcoin client” celebrated the blockchain reaching 2 gigabytes (GB) in size. Commemoration aside, discussion
of the block size limit started in the thread. On the last day of the year, member “Kluge” posted that since his computer could not keep up with downloading the blockchain, the only option left was to switch to a SPV client.\(^\text{34}\)

On January 31, 2013, member “Jeweller” inquired about what would happen and should be done as blocks approached the 1 MB limit.\(^\text{35}\) Core developer Gavin Andresen replied on February 4 and endorsed a previous proposal to let the miners decide the optimal block size, alluding to a market equilibrium. Following commenters largely agreed with Gavin’s views. The last major discussion before the 2015 controversy was a thread posted on February 18, 2013 by developer Peter Todd titled “How a floating blocksize limit inevitably leads towards centralization.”\(^\text{36}\) Many members also predicted that in the event of a hard fork, a situation with two competing blockchains, economic incentives to avoid double spending would rapidly force a community consensus on one of the blockchains as official. It seemed that Gavin and early adopter Mike Hearn supported bigger blocks in theory.\(^\text{37}\) In a sense those Forum and Reddit threads presaged much of the block size debate civil war. But having ended in April 2013, the threads did not possess the urgency that characterized the 2015 debate. They were resolved or closed with simple solutions like using SPV clients or discussing and waiting things out. The participants knew the problem would not explode in the near future and so treated the block size question more as a thought experiment.

In early 2013, transactions needed 15 to 20 minutes to be confirmed on the blockchain, and already members worried about Bitcoin’s commercial viability.\(^\text{38}\) Fast forward to 2014 and 2015, and average users began to feel the effects of slow transaction confirmations. In September 2014, a redditor complained that their transaction had not confirmed after a day, perhaps because it included only the minimum fee.\(^\text{39}\) Commenters advised waiting more, from around 72 hours to
several weeks at worst. In May 2015, a redditor asked why their transaction was taking several hours to confirm.40 In July, two redditors complained of waiting over 12 hours for transaction confirmations.41 In the comments, some redditors criticized the existence of the block size limit and a fee market while the block reward was significant. The concerns and critiques of many members and average users would find a voice in an upcoming wave of reform proposals.

The Civil War

The civil war was ultimately sparked by a Bitcoin Improvement Proposal (BIP) from Gavin Andresen and Mike Hearn in 2015. On June 22, 2015, Gavin created BIP 101, a memo for increasing the block size limit to 8 MB by January 1, 2016 and doubling every two years until 2036, if and only if a 75 percent supermajority of the miners adopt blocks with the version number corresponding to the BIP.42 He also explained in plain English the reasons for bigger blocks. Back in May, Mike Hearn wrote a pair of articles on why the block size limit should be increased and why alternative sidechain solutions are not the answer:

I don’t believe fees will become high and stable if Bitcoin runs out of capacity. Instead, I believe Bitcoin will crash. [...] I believe there are no situations in which Bitcoin can enter an overload situation and come out with its reputation and user base intact. Both would suffer heavily and as Bitcoin is the founder of the cryptocurrency concept, the idea itself would inevitably suffer some kind of negative repercussions.43

So on August 15, Gavin and Hearn released to the public Bitcoin XT, a fork of the reference implementation that incorporated BIP 101.44 Hearn published a manifesto for XT, urging widespread adoption and calling the event a watershed that would determine the survival of Bitcoin.45 That was a historic moment, in which part of the community decided to fork the
software for a technical and political goal. A lot was at stake, for the fork meant that if XT were to become the official blockchain, people who kept mining on Bitcoin Core, the original blockchain, would find their bitcoins become worthless as exchanges and merchants stop accepting. Of course, the reputation of Bitcoin to the concrete world was also put at risk by the internal strife.

Both confusion and censorship exploded after the civil war’s start. One redditor asked for a clear explanation of what would happen in the case of a hard fork after January. Though Gavin and r/Bitcoin moderator Theymos tried to help explain, the other commenters’ answers were contentious and accused opponents of spreading misinformation and fear, uncertainty, and doubt (FUD). That became a recurring theme as the civil war dragged on, and many average users and enthusiasts found themselves caught in an uncertain situation with a dearth of quality information. The confusion and censorship reinforced and exacerbated each other, to the point of savage bitterness between the sides.

The flood of censorship began almost immediately after BIP 101’s creation. On August 9, a redditor posted an eloquent call for free and open discussion on r/Bitcoin in the wake of moderators’ banning posts that supported a hard fork:

But what warrants censorship? What can be so dangerous, even the idea of it must not spread in the bitcoin community? What is so detrimental to the community, that a call to test some code that directly relates to the foundations of Bitcoin must not be known? Sounds familiar? Except this is way, way worse than government censorship, because Bitcoin is supposed to be permissionless. […] Whatever your stance on the protocol, the code and the policies of Bitcoin, you gotta make a choice on something more fundamental: Do you believe in an open and permissionless network, or do you think Bitcoin will die because someone published some code and people are allowed to know it?

In the highly upvoted and thrice-gilded thread, commenters largely agreed that censorship of XT support and the regulatory powers of the r/Bitcoin and Forum moderators were
 unacceptable and anathema to Bitcoin’s original values. On August 14, another post called for the moderators to cease deletion of posts supporting XT. One of the moderators, BashCo, answered the August 9 post by labeling XT an altcoin and arguing that XT, like other altcoins, did not belong in r/Bitcoin. Downvoted to negative eighty, the baffling reply was unpopular and attracted numerous opposing replies.

But on August 17, moderator Theymos struck back and wrote a post titled “It’s time for a break: About the recent mess & temporary new rules.” He justified continuing censorship:

There’s a substantial difference between discussion of a proposed Bitcoin hardfork (which was previously always allowed here, even though I strongly disagree with many things posted) 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. [...] Do not violate our rules just because you disagree with them. This will get you banned from /r/Bitcoin, and evading this ban will get you (and maybe your IP) banned from Reddit entirely. 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. I do not want these people to make threads breaking the rules, demanding change, asking for upvotes, making personal attacks against moderators, etc. Without some real argument, you’re not going to convince anyone with any brains—you’re just wasting your time and ours. The temporary rules against blocksize and moderation discussion are in part designed to encourage people who should leave /r/Bitcoin to actually do so so that /r/Bitcoin can get back to the business of discussing Bitcoin news in peace. The purpose of moderation is to make the community a good one, which sometimes includes causing people to leave.

The controversial post garnered immense attention and over a thousand comments. Commenters called for Theymos and other moderators to resign and unsuccessfully reported him to the Reddit administrators. Others railed against the authoritarian nature of Theymos’s message, the wave of censorship, and the ironclad obstruction of developers. Revolutionary sentiment brewed. Although big blockers were unable to leverage Reddit administrators to stop Theymos and r/Bitcoin censorship, they did successfully popularize r/btc, a subreddit for dissent and heterodox opinion. So a new, competing safe space arose from the blaze of censorship.
In September a moderator, SeansOutpost, came out against censorship: “I don’t understand/agree with why we can’t talk about this like adults. I’m not sure why we can’t openly discuss all options. Open discussion would seem to be in the spirit of what Satoshi wanted.”51 Then he was removed as a moderator by r/Bitcoin’s moderators. In November, Theymos published another apology for censorship: “You can promote BIP 101 as an idea. You can’t promote (on /r/Bitcoin) the actual usage of BIP 101. When the idea has consensus, then it can be rolled out. Bitcoin is not a democracy. Not of miners, and not of nodes. [...] One of the great things about Bitcoin is its lack of democracy.”52 The next day, Theymos threatened to blacklist the premier exchange Coinbase after its chief executive Brian Armstrong voiced support for BIP 101: “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.”53 Redditors downvoted his comment to negative 744, showing that they passionately disagreed with Theymos.

Unfortunately, Theymos and other moderators kept their promise to blacklist Coinbase and further discussion of XT and hard forks.54 A redditor alarmingly posted the news that Coinbase had been removed from bitcoin.org’s list of wallets.55 On December 28, a r/Bitcoin moderator publicized an email conversation between other moderators on censoring Coinbase.56 Hours later, the whistleblower’s moderator status was purportedly revoked. In January, redditors discussed the moderator’s ignoring a request to restore Coinbase’s position with supermajority support.57 The top comments expressed shame that the moderators persisted in blacklisting and mistreating the most popular and functional exchange and web wallet to exist.

Finally, on March 8, a post showed that r/Bitcoin moderators had deleted a post of Satoshi’s quotes because they could be construed to support bigger blocks.58 The censorship had
come full circle. The libertarian small blocker moderators, after censoring dissent, mention of XT, and Coinbase, had censored the wisdom of Bitcoin's creator who advocated free and open dialogue even with opponents in disagreements. The irony of the situation was not lost to witnesses, who remarked that the moderators' extraordinary and arbitrary rule perverted Bitcoin's vision. Various instances of censorship continued through autumn. But the March episode was more than another example of the destruction of free discourse and similar principles articulated, ironically, by Theymos in the past. It was a moment that confirmed the vast disconnect between supposedly libertarian small blockers and the original vision of radical equality and democracy.

In addition to blatant and unrepentant censorship by the small blockers, a series of distributed denial-of-service (DDOS) attacks were launched against nodes that ran XT. A DDOS attack is a cyberattack where the perpetrator uses multiple IP addresses to barrage the target with superfluous requests in order to overload systems and disrupt services. A form of cyberwarfare and criminal sabotage, DDOS attacks are contrary to civil libertarian principles of privacy, property rights, and free enterprise, precluding doux commerce and peaceful competition.

At the end of August 2015, the first anecdotes about being DDOS attacked were posted. One redditor reported the start of an extreme form of DDOS attacks on XT nodes and identified the perpetrator as a Ukrainian IP address routed to Russia:

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. Not the silly bloom filter CPU exhaustion thing, but actual UDP flood attacks [...] Every connection of this type is from a single IP, namely 185.93.185.249, which appeared to be an Ukrainian IP belonging to the ISP Ukrmirkom Ltd.
Many commenters corroborated the account, writing that their computers and networks too had been subject to attacks.

Subsequent posts served as further evidence that XT nodes were being targeted for running XT. The largest mining pool, SlushPool, was reportedly attacked on September 1 after becoming the first pool to publicly support XT. On September 3 a redditor claimed that one of their hosting customers reported a DDOS attack after switching their node from Core to XT. More and more evidence throughout the year pointed to a massive concerted effort to target and sabotage XT nodes. Though there was no airtight evidence that the DDOS attacks were supported by small blockers, the pattern and concentration pointed to a systematic effort by one or several perpetrators to hinder and undermine the growth of XT.

One solution for nodes running XT was to enter stealth mode, an update from September that allowed nodes to appear to be running Core but disabled some upgrades as a tradeoff. By year’s end the DDOS attacks had let up, and a redditor encouraged others running XT nodes to disable stealth mode. On that thread claims surfaced that DDOS attacks crashed one third of XT nodes and large-scale DDOS attacks took out entire Internet Service Providers (ISP) in rural areas. Coinbase, having been a specific victim of the widespread DDOS attacks, went back online.

Finally, in January small blockers attempted gaslighting in their denial of DDOS attacks focused on XT nodes, with developer Luke Jr brushing aside a condemnation of small blocker Core supporters for implicitly encouraging the cybercrime. The gaslighting continued into 2016, with core developer Gregory Maxwell claiming that the DDOS anecdotes were actually lies fabricated by fake accounts. But with the virtual violence ossified in the community’s memory,
the real damage was done. The supposedly libertarian small blockers had abandoned libertarian principles for political gain.

The final element that made the block size controversy surpass a heated debate and become a civil war that overturned Bitcoin’s founding principles was the nature of the criticism levied by both sides against each other. Bitter contention over both normative economics—the truth—and positive economics—what would happen in the future—added a twist of personal weight. Ad hominem attacks and insults that attempted to discredit the leaders of the small and big blockers escalated the savageness of the debate into a flame war.

Many small blockers personally attacked Mike Hearn after the release of XT. They primarily tried to characterize him as the vessel for a vast banking conspiracy against Bitcoin. First, they searched his history of involvement in Bitcoin for support. A particular piece of evidence was an incident in 2013 where Hearn proposed a policy of “redlisting” certain bitcoins used in illegal activity during his tenure at the controversial nonprofit Bitcoin Foundation as Chair of Law and Policy. He had wanted to combat Bitcoin’s growing association with crime while adding legal legitimacy. Since his proposal would have hurt Bitcoin’s fundamental characteristics of anonymity and fungibility, the community reasonably rejected it. Some prominent libertarians had criticized Hearn’s proposal and called him an apologist for censorship and surveillance. In 2016 the small blockers wanted to remind the community of what Hearn had done and allude that XT was an extension of the “redlisting” proposal and its authoritarian connotations. Second, they focused on Hearn’s decision in November to join R3, a fintech consortium that has partnered with big banks. After Hearn made an infamous blog post in January in the wake of XT’s projected failure that announced his departure and the death of Bitcoin, many small blockers concocted and disseminated an elaborate conspiracy theory about
how Hearn worked with R3 and the media to publicize the failure of Bitcoin and crash the price so as to force the core developers to implement big blocks and how the ultimate goal was to convert Bitcoin into an instrument of private banks.\textsuperscript{74} The charges became so fiery and widespread that Hearn replied and refuted them in a final blog post.\textsuperscript{75} Regardless of any degree of truth in the charges, the fact that so many small blockers supported and propagated the conspiracy allegations to help win a civil war demonstrates that some community members did not see virtue in helping Bitcoin succeed, instead viewing political victory as the end goal.

On the other hand, many big blockers attacked core developers who supported small blocks as being dictators and tyrants. In summer 2015, Mike Hearn blasted Gregory Maxwell for “attempt[ing] to bullshit,” “getting really crazy,” and fantasizing about creating a so-called GregCoin.\textsuperscript{76} After XT’s failure, Hearn called out core developer and small blocker Gregory Maxwell as a terrible leader and decision maker and Bitcoin’s main problem.\textsuperscript{77} In another instance, Hearn accused the small blockers of “character assassination attacks” and being a “sufficiently aggressive minority [that would] end up taking over Bitcoin through social means.”\textsuperscript{78} Other big blockers created a blacklist of individuals who support small blocks, calling them enemies of Bitcoin who had engaged in spreading FUD, misinformation, and doublespeak.\textsuperscript{79} Finally, big blockers performed a similar character assassination against Gregory Maxwell for his involvement in the fintech firm he cofounded named Blockstream, calling him arrogant, toxic, and horrible.\textsuperscript{80} They also sifted through his employment history to support the argument that he had a record of being destructive to group projects. Although not as egregious and publicized as the personal attacks by the small blockers, the actions taken by big blockers also demonstrate a disruption of the community solidarity and republican virtue that had emerged from the early days of Satoshi and friends who felt like family.
Conclusion

The historicizations bring everything full circle. To return to Yap is to return to the old parallelism. Yap stone money met its end around the turn-of-the-century, a time when Irish-American David Dean O'Keefe artificially increased the supply of stones to bolster his trading venture and German imperial authorities devised a clever plan to paint the massive stones with German letters to signify state ownership. Subsequent inheritance by conquest and treaty to the Japanese Empire after the First World War and the United States after World War Two all but obliterated the traditional practice of using stones as money. The Japanese imperial forces made stones into construction tools and anchors and forced natives to labor on defense works in order to avoid having stones broken. The postwar infusion of US aid dollars further tied Yap to fiat money and the whims of Congress. The story of Yap stone money illustrates a series of external state forces that destroyed a unique money and way of life.

However, the specter of state oppression only haunted but did not reach Bitcoin or cause its demise. Instead, the intellectual revolution that was so palpable and poignant in 2008 and 2009 became something that overthrew its very founding ideas. On returning to the Enlightenment again, as the American founding generation reviewed the young nation from the early nineteenth century, they were aghast at just how radical the democratic society and idea of equality had become. The opposite occurred with Bitcoin—the founders envisioned a radically democratic and libertarian experiment that was devastated afterwards by community political conflict and would be unrecognizable to Satoshi today.
Ultimately, the community’s politics and actions in the civil war sowed the seeds of its own destruction. Good libertarians do not censor or attack property. Good democrats do not slander, gaslight, or reject votes. Yet the community did all that and inflicted wounds on itself. The small blockers engaged in the vast majority of censorship, DDOS attacks, and savagery, eviscerating Satoshi’s original vision in the process. Perhaps their tactics, though ruthless, proved effective. Due partly to miner centralization and hesitation, the big blockers did not win, as not enough miners—about ten percent—had adopted XT by early 2016, the earliest possible switchover date. But Mike Hearn did not accept the democratic result either, instead deciding to write an obituary and secede from the community once and for all. The big block movement lives on in Bitcoin Classic, another attempted fork of the Bitcoin reference implementation released by Gavin, Garzik, and others in February that will increase the block size to 2 MB if and only if adopted after reaching consensus. But Classic has encountered the same obstacles as XT did. Thus the civil war over Bitcoin’s future continues.

In 2016 Bitcoin faced a crossroads. It was a maturing cryptocurrency, the pioneer for new digital coins. It was an indefinite peer-to-peer payments system, mostly functional yet mired in crisis. It was a trader’s instrument, strangely regulated by states as a commodity, property, and currency. It was an economic curiosity, a specimen studied by global financial institutions that desired to construct their own private blockchains in a perceptive counterrevolution. And it was an idea around which a community struggled savagely to steer its direction.

The future of Bitcoin by summer 2016 was uncertain, but it is evident that Satoshi’s original vision of a civil libertarian, radically democratic, and equal and open idea that would empower people and change lives had failed. Regardless of the outcomes of future political battles, only by returning to such founding principles can Bitcoin realize its dream of a new
money that allows all people to be their own bank and build a community that shapes their own history.

Acknowledgements

I am grateful to Professor Timothy Burke and the Swarthmore College History Department for the opportunity to spend a summer researching Bitcoin and money. I am especially grateful to Professors Marj Murphy and Bob Weinberg for their critique, advice, and support during senior research seminar. I am also grateful to the Bitcoin community for easy access to online archives.

Endnotes

6. Bitcoin is remarkable for solving the Byzantine Generals’ Problem, a classic computer science problem on agreement, in a unique way, which one can appreciate regardless of political ideology.
7. “Block #0.” Blockchain. https://blockchain.info/block/0000000000000019d6689c085ace165831e934ff763ae46a2a6c172b3f1b60a8ce26f.
15. Please refer to Pedro Franco’s *Understanding Bitcoin* and Andreas Antonopoulos’s *Mastering Bitcoin* for more information.
23. The minimum transaction fee for a transaction to be eligible to be included in a block is 0.01 millibitcoins per kilobyte.
24. “Block #1.” Blockchain. https://blockchain.info/block/00000000839a8e6886ab5951d766411475428af0c90947ec320161bfb18e6048
27. The term core developer refers to the five individuals who have commit access, or the ability to make changes to the Bitcoin Core source code. They are Gavin Andresen, Jeff Garzik, Wladimir van der Laan, Gregory Maxwell, and Pieter Wuille. Before disappearing, Satoshi bequeathed commit access to Gavin, who then shared it with the other four developers.
52. ExEnigmaticX. Reddit post, July 8, 2015. https://bitcointalk.org/r/Bitcoin/comments/3cje7y/over_12_hours_and_no_confirmation_can_any_one/
54. ExEnigmaticX. Reddit post, July 8, 2015. https://bitcointalk.org/r/Bitcoin/comments/3cje7y/over_12_hours_and_no_confirmation_can_any_one/
56. ExEnigmaticX. Reddit post, July 8, 2015. https://bitcointalk.org/r/Bitcoin/comments/3cje7y/over_12_hours_and_no_confirmation_can_any_one/
57. WellsHunter. Reddit post, July 8, 2015. https://bitcointalk.org/r/Bitcoin/comments/3cjeyp/14_hours_without_confirmation/;
58. ExEnigmaticX. Reddit post, July 8, 2015. https://bitcointalk.org/r/Bitcoin/comments/3cje7y/over_12_hours_and_no_confirmation_can_any_one/
90. Undoubtedly, the article does not conclude the story of Bitcoin. For the curious learner, a world of information is available on the Internet, in physical archives, and in books about economics, cryptography, Bitcoin, and the history of the future.

Appendix

Mike Hearn, developer and cocreator of XT

Gavin Andresen, core developer
Theymos AKA Michael Marquardt, moderator of r/Bitcoin and Bitcoin Forum

Gregory Maxwell, core developer

Jeff Garzik, core developer

Miner centralization: group of seven miners who controlled over 90 percent of hash power as of 2015

Bitcoin (BTC) symbol