BITCOIN: UNTITLED

A Documented History of Corporate Capture

G. R. Secco

Revised Edition 2026

ramiro@duck.com

1. Introduction: The Substitution

On October 29, 2015, at the Bitcoin Investor Conference in Las Vegas, an "All-Star Panel" convened to discuss the future of cryptocurrency.[19] The participants included Nick SZABO—the creator of "bit gold" and one of the most respected cryptographers in the field—former U.S. Mint Director Edmund MOY, early Bitcoin evangelist Trace MAYER, and Dr. Craig WRIGHT, joining remotely from London.

During the discussion, WRIGHT made a technical claim: that Bitcoin's scripting language was far more capable than commonly understood—that it could support smart contracts and complex programmable functions. SZABO responded dismissively: "I have not heard that opinion before. I've never heard anybody call the bitcoin script Turing complete. I don't believe that's accurate." He called WRIGHT's view "esoteric" and suggested he "write a paper on it."

Years later, smart contracts on Bitcoin became reality. BTC eventually admitted the capability, though its artificial constraints—block size limits and slow transaction validation—render them impractical for real-world use. WRIGHT was right; the experts were wrong.

The question that no one asks: Why was WRIGHT—the man his critics would later call "Faketoshi"—invited to an All-Star Panel alongside Nick SZABO in the first place? And why did he know more about Bitcoin's technical capabilities than the assembled experts?

Six weeks after that panel, in December 2015, *Wired* and *Gizmodo* simultaneously published investigations identifying WRIGHT as Satoshi NAKAMOTO, the creator of Bitcoin. The same community that had witnessed his superior technical knowledge six weeks earlier immediately pivoted to calling him a liar.

This document examines not only who created Bitcoin, but what happened to it—and why.

The Substitution

In 2008, someone using the pseudonym Satoshi NAKAMOTO published a nine-page document titled *Bitcoin: A Peer-to-Peer Electronic Cash System*.[1] The paper described a system that could handle virtually unlimited transaction volume at near-zero cost, requiring no central authority. Today, that same name refers to a system that processes approximately three to four transactions per second on its base layer, costs dollars per transaction, and requires specialized intermediaries. The original system still exists, but it goes by a different name. This document examines how this substitution occurred.

The Core Problem

The cryptocurrency known as Bitcoin (BTC) today cannot perform the basic functions its creator designed it for. It cannot process everyday transactions at scale. It cannot serve as a practical payment system. The technology that was supposed to disrupt traditional banking now requires more intermediaries than traditional banking itself.

This is not a natural evolution. It is the result of deliberate choices made by a small group of developers who gained control of the software that most people use to run Bitcoin (the "reference implementation") and whose financial interests aligned with making Bitcoin less functional, not more.

Three Central Claims

The Technical Claim: The system called "Bitcoin" (BTC) has been deliberately constrained to process only three to four transactions per second on its base layer, despite being designed to scale to handle global payment volume. This limitation serves the business interests of companies that profit from Bitcoin's constraints. A system called Bitcoin SV (BSV) currently implements Satoshi's original architecture without these artificial limitations.

The Historical Claim: The transformation from functional payment system to deliberately constrained "digital gold" was orchestrated by developers with undisclosed conflicts of interest. The company Blockstream, founded by Bitcoin Core developers and funded by traditional financial institutions including AXA Strategic Ventures, created business models that directly profit from Bitcoin's scaling limitations.

The Identity Claim: Satoshi NAKAMOTO is Dr. Craig S. WRIGHT, an Australian computer scientist who has been systematically discredited by the same interests that benefit from Bitcoin's dysfunction. The evidence for this claim includes government testimony, contemporary documentation, and expert confirmations.

Why This Matters

If these claims are accurate, the implications extend far beyond cryptocurrency. This would represent one of the most significant intellectual property captures in technological history. A system designed to enable global financial access for billions of unbanked people has been converted into a speculative asset that serves existing financial interests.

The original inventor has been exiled from his own creation while being simultaneously acknowledged (through lawsuits predicated on his invention) and denied (through coordinated public relations campaigns). This paradox itself requires examination.

The Approach

To understand what happened to Bitcoin, we first need to understand what Bitcoin actually is. Section 2 provides the essential technical foundation—not as a comprehensive tutorial, but as the minimum context needed to evaluate the claims that follow.

The evidence for these claims exists in public forums, code repositories, business filings, government transcripts, and technical specifications. The sources are cited throughout and compiled in the references. The interpretation of these facts is mine; the facts themselves are documented with primary sources wherever possible.

2. Technical Foundation

This section provides the technical foundation necessary to understand the claims that follow. Readers familiar with Bitcoin's basic operation may skim this material, though some commonly held assumptions about the system are incorrect.

2.1 What Bitcoin Actually Is

Bitcoin is a system for transferring control of digital assets without requiring trust in intermediaries. (A note on terminology: "control" and "ownership" are distinct legal concepts, but for simplicity, this document uses them interchangeably. What matters is that Bitcoin enables the transfer of exclusive rights over digital tokens without a central authority.)

Bitcoin accomplishes this through a distributed ledger—a record of all transactions that is maintained simultaneously by thousands of computers worldwide. The key innovation is not the ledger itself, but the mechanism that allows strangers to agree on its contents without trusting each other.

The original Bitcoin document, titled *Bitcoin: A Peer-to-Peer Electronic Cash System*, describes a system for digital payments.[1] The title itself is instructive: this was designed to be *cash*—a medium for everyday transactions—not a store of value like gold or a settlement layer for large institutional transfers.

2.2 How Bitcoin Tracks Ownership

Bitcoin uses a model that differs fundamentally from traditional banking. In traditional banking, your account has a balance that increases or decreases with each transaction. In Bitcoin, there is no "balance" in this sense. Instead, the system tracks individual coins and their chain of ownership.

Imagine each bitcoin as a unique physical coin that carries its entire history. When you "send" bitcoin, you are not transferring from one balance to another. You are signing over control of specific coins to a new owner. The ledger records this transfer, creating an unbroken chain of custody from the coin's creation to its current owner.

This design has profound implications. Unlike traditional banking, where the bank must be trusted to maintain accurate records, Bitcoin's chain of custody is publicly verifiable. Anyone can trace the ownership of any coin back to its creation.

2.3 Mining and Security

Bitcoin's security comes from a process called mining. Miners compete to process transactions by solving computational puzzles. The winner of each round gets to add the next "block" of transactions to the ledger and receives newly created bitcoins as a reward.

This process is fundamental for two reasons: it establishes the authoritative order of all transactions (preventing the same coin from being spent twice), and it does so without requiring a central authority to keep track. The puzzle-solving mechanism ensures that altering the historical record would require more computational power than the rest of the network combined.

This creates economic incentives that secure the network. To attack Bitcoin, you would need to control more computing power than the honest miners—and if you had that much power, you could make more money by mining honestly than by attacking. The system is designed so that honesty is more profitable than cheating.

Satoshi NAKAMOTO was explicit about how this would scale. In a November 2008 email, he wrote: "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."[2] The system was designed from the beginning to be maintained by professional operations, not hobbyists running software on home computers.

2.4 The Block Size Decision

Each block in Bitcoin's ledger has a size limit that determines how many transactions can be processed. Think of it like a container: a small container can only hold so many transactions before it's full, and a new container (block) must be created. The smaller the container, the fewer transactions the system can handle.

This limit was originally set as a temporary security measure when the network was small and vulnerable to certain attacks. Satoshi NAKAMOTO stated clearly that this limit should be raised as the network grew.

On October 4, 2010, Satoshi wrote: "It can be phased in, like: if (blocknumber > 115000) maxblocksize = largerlimit."[3] He anticipated that the limit would be raised before it became a constraint.

This never happened. The temporary limit became permanent, and Bitcoin's capacity was frozen at approximately three to four transactions per second while global payment systems process tens of thousands. The story of how and why this occurred is the subject of Section 3.

3. The Transformation: How Bitcoin Changed Course

This section documents the transformation of Bitcoin from its original design into its current constrained form. The evidence presented here comes from primary sources: corporate announcements, government documents, archived forum posts, and the documented statements of the participants themselves.

3.1 The Handoff (2010-2011)

In December 2010, Satoshi NAKAMOTO withdrew from public participation in Bitcoin development. He entrusted the project to Gavin ANDRESEN, an early contributor who had demonstrated technical competence and shared Satoshi's vision for Bitcoin as a payment system.

ANDRESEN made a critical error: he approached Bitcoin as a collaborative open-source project rather than as a monetary system that required stability. He gave editing rights to the core software to additional developers and introduced governance mechanisms that allowed the protocol's direction to be influenced by politics rather than economics.

This was a fundamental misunderstanding. Money requires predictability. A monetary system whose rules can be changed by developer votes is not a monetary system—it is a technology platform subject to political capture.

3.2 The Corporate Capture (2014-2016)

In 2014, a company called Blockstream was founded by several Bitcoin Core developers, including Gregory MAXWELL, Pieter WUILLE, and Adam BACK. The company's stated purpose was to develop "sidechains"—parallel systems that would process transactions outside of Bitcoin's main network. In simple terms: if Bitcoin itself couldn't handle many transactions, Blockstream would sell you the solution.

On February 3, 2016, the *Wall Street Journal* reported: "Bitcoin Startup Blockstream Raises $55 Million in Funding Round."[4] The investors included AXA Strategic Ventures, the venture capital arm of the world's largest insurance company.

This created an extraordinary conflict of interest. The developers responsible for Bitcoin's core software were now employed by a company whose business model *required* Bitcoin to remain constrained. If Bitcoin scaled on its main chain, Blockstream's products would have no market. The same people who controlled Bitcoin's development now had direct financial incentives to prevent Bitcoin from functioning as designed.

3.3 The Blockstream Factor

The funding network reveals the institutional interests involved:

AXA Strategic Ventures led Blockstream's $55 million Series A funding. AXA is the world's largest insurance company, deeply invested in existing financial infrastructure.[4]

Digital Currency Group (DCG), led by Barry SILBERT, invested in both Blockstream and controlled Coindesk, the primary Bitcoin news outlet.[5] DCG's board included Glenn HUTCHINS, who simultaneously served on the board of the Federal Reserve Bank of New York. DCG also received investment from MasterCard.[6]

The architecture of capture is clear: traditional financial institutions funded companies whose products required Bitcoin to fail at its original purpose. The same companies controlled both the development process and the primary media outlets covering it.

3.4 The Block Size Wars (2015-2017)

When Gavin ANDRESEN proposed increasing Bitcoin's block size limit in 2015, he encountered fierce resistance from the Blockstream-affiliated developers. They argued that larger blocks would make Bitcoin more "centralized" because they would require more powerful hardware to process.

This argument was technically specious and directly contradicted Satoshi's original design, which explicitly anticipated specialized server farms. But the argument served Blockstream's business interests.

What followed was an unprecedented censorship campaign. Theymos—the pseudonymous administrator who controlled both the Bitcoin.org website and the r/bitcoin subreddit (with over 800,000 subscribers)—implemented a moderation policy that banned discussion of any scaling proposal that increased the block size limit.

In August 2015, Theymos stated: "If 90% of /r/Bitcoin users find these policies to be intolerable, then I want these 90% of /r/Bitcoin users to leave."[7] He compared scaling solutions to "hard drugs" and banned exchanges that indicated support for larger blocks.[8]

Adam BACK, Blockstream's CEO, was documented on archived social media posts discussing technical attack strategies against Bitcoin XT. Bitcoin XT was an alternative implementation created by Mike HEARN and Gavin ANDRESEN that would have increased the block size limit—effectively competing with Blockstream's sidechain business model. BACK's posts discussed sabotage tactics including: "pretend to support XT but reject XT blocks" and "bitcoin nodes could refuse connections from XT. (Or maybe teergrube them to increase their orphan rate)."[9]

The term "teergrube" (German for "tar pit") refers to a network attack technique that deliberately slows down connections—essentially sabotage by degrading the competing network's performance. In plain terms, BACK was proposing that opponents infiltrate the competing network and deliberately cause it to malfunction.

3.5 The Hong Kong Agreement Betrayal

On February 20, 2016, representatives from Bitcoin Core (the Blockstream-controlled development team) signed an agreement with major mining operations in Hong Kong. The Core developers committed to implementing a scaling solution that would increase capacity within a year.[10]

The agreement was never honored. Having secured the miners' commitment not to support competing implementations, the Core developers simply declined to implement the promised changes. When confronted, they claimed the agreement was made in personal capacities, not on behalf of Bitcoin Core.

3.6 SegWit, Lightning, and Protocol Capture (2017)

In 2017, Bitcoin Core implemented Segregated Witness (SegWit), a technical change that fundamentally altered Bitcoin's architecture. SegWit separated transaction signatures from the main transaction data—a change that Satoshi NAKAMOTO had explicitly rejected in his original design because it broke the chain of digital signatures that defined Bitcoin's security model.[11]

SegWit was activated through a mechanism where non-mining nodes signaled support for protocol changes. This represented a fundamental corruption of Bitcoin's design. Nodes do not vote in Bitcoin—they enforce the protocol rules. Mining nodes, through proof-of-work, are the mechanism for consensus on the state of the ledger. Using non-mining nodes to force protocol changes inverted the security model: instead of economic actors with skin in the game determining the rules, the loudest voices on social media could claim to represent "the community."

SegWit also enabled the Lightning Network—a "second layer" system that processes transactions off the main Bitcoin blockchain. Users lock their bitcoins into Lightning channels and transact off-chain, only settling back to the main blockchain when they close their channels. This is precisely the kind of sidechain solution that Blockstream's business model required: if Bitcoin's base layer can't handle transactions, you need Blockstream's products to actually use it.

The Lightning Network has been promoted as Bitcoin's scaling solution for years. In practice, it introduces complexity, requires users to be online to receive payments, creates liquidity problems, and centralizes transaction processing through large "hub" nodes—the very intermediaries Bitcoin was designed to eliminate.

On August 1, 2017, Bitcoin split. Those who wanted to preserve larger blocks created Bitcoin Cash (BCH), rejecting the SegWit changes. The following year, Bitcoin Cash itself split over disagreements about the path forward. Bitcoin SV (BSV)—where "SV" stands for "Satoshi Vision"—emerged as the implementation that most closely follows Satoshi's original design, removing all artificial limits on block size and restoring the original scripting capabilities. The captured version continued as Bitcoin (BTC), constrained by artificial limits and dependent on Blockstream's products for any meaningful transaction capacity.

3.7 The Aftermath (2017-2024)

After the split, the constrained version retained the name "Bitcoin" and the ticker symbol "BTC." This was not because it followed the original design—it did not—but because it controlled the infrastructure: the dominant exchanges, the media outlets, and the narrative.

What followed was a rebranding exercise. Unable to function as a payment system, BTC was repositioned as "digital gold"—a store of value rather than a medium of exchange. The very limitation that crippled Bitcoin's utility became its marketing pitch: scarcity, not function, was now the point.

The price rose. Institutional investors entered. Bitcoin became a speculative asset class, disconnected from its original purpose. By 2024, BTC had reached prices above $100,000—not because it could do anything useful, but because enough people believed others would pay more for it later.

Meanwhile, the broader cryptocurrency ecosystem exploded into thousands of competing tokens, each promising to solve problems that Bitcoin was designed to solve from the beginning. The fragmentation was treated as innovation. The dysfunction was normalized.

Summary: The Capture in Brief

Between 2014 and 2017, Bitcoin was transformed from a functional payment system into a deliberately constrained speculative asset. The mechanism was straightforward: developers with financial conflicts of interest gained control of the reference implementation, blocked scaling improvements, implemented protocol changes that served their business interests, and used censorship to suppress opposition. The original inventor was systematically discredited. The result is the system we have today—one that bears Bitcoin's name but cannot perform its original function.

3.8 The Identity Question

The capture of Bitcoin required more than controlling the code—it required neutralizing its creator.

The identity of Satoshi NAKAMOTO has been one of the most contested questions in technology. The predominant narrative—that Satoshi is an unknown figure who has maintained anonymity—serves the interests of those who captured Bitcoin. A living inventor could challenge the changes made to his creation.

The evidence that Satoshi NAKAMOTO is Dr. Craig S. WRIGHT includes:

February 2014 Australian Tax Office Transcript: In a recorded meeting with tax authorities, WRIGHT stated: "I did my best to try and hide the fact that I've been running bitcoin since 2009."[12] This statement was made before any public investigation into Satoshi's identity and in a context where there was no incentive to make false claims.

December 2015 Wired/Gizmodo Investigation: Major technology publications simultaneously published investigations identifying WRIGHT as Satoshi, based on leaked documents and forensic analysis.[13][14]

Expert Confirmations: Jon MATONIS, former executive director of the Bitcoin Foundation, and Ian GRIGG, cryptographer and inventor of Ricardian Contracts, both publicly confirmed WRIGHT as Satoshi in 2016 following private demonstrations.[15] MATONIS stated he was "100 per cent convinced" after witnessing WRIGHT sign messages using keys from Bitcoin's earliest blocks.

The Kleiman Case: Ira KLEIMAN sued WRIGHT in U.S. federal court for a share of Satoshi's bitcoins. Ira is the brother of Dave KLEIMAN, a computer forensics expert and cryptographer who worked with WRIGHT during Bitcoin's early development and died in 2013. The entire lawsuit was predicated on WRIGHT's involvement in Bitcoin's creation—the plaintiff was not challenging that WRIGHT created Bitcoin, but claiming that Dave deserved a share of the coins for his contributions.[16]

The COPA Case: In 2024, the Crypto Open Patent Alliance (COPA)—a consortium of cryptocurrency companies including Coinbase, Block (formerly Square), and MicroStrategy—brought a case specifically to have a court declare that WRIGHT is not Satoshi. The ruling found against WRIGHT's claims.[17]

However, this case raises important questions. Why would an industry consortium spend millions in legal fees to prove someone is *not* an inventor, unless that person posed a threat to their interests? It is also notable that every major legal case involving WRIGHT's identity has been brought *against* him—by parties with significant financial interests in the current Bitcoin ecosystem.

Perhaps most peculiar is the logical structure of the COPA ruling itself: the court declared WRIGHT is not Satoshi NAKAMOTO, but did not—and arguably could not—determine who Satoshi actually is. Under common law principles, proving a negative without establishing the positive creates an unusual precedent. The ruling essentially says "this person is not the inventor" while the identity of the actual inventor remains officially unknown.

4. The Consequences

The capture documented in Section 3 has produced a cryptocurrency ecosystem that is simultaneously ubiquitous and useless. Understanding what was lost—and what myths have been constructed to obscure that loss—reveals the full scope of the damage.

4.1 The "Decentralization" Illusion

Decentralization is perhaps the most misused term in cryptocurrency discourse. The community uses it to mean that the system runs on thousands of computers simultaneously, implying that no single party can control it.

This fundamentally misrepresents Bitcoin's design. Satoshi NAKAMOTO was explicit that Bitcoin would be maintained by "specialized server farms," not by hobbyists running software on personal computers.[2] The relevant decentralization is *economic*—miners competing for profit—not *physical*—thousands of non-mining nodes running on personal computers.

A non-mining node contributes nothing to Bitcoin's security. It cannot process transactions. It cannot validate blocks for the network. It simply receives information that miners have already validated. The proliferation of non-mining nodes is not a feature—it is a consequence of artificial constraints that prevent Bitcoin from scaling to professional infrastructure.

The irony is stark: in the name of "decentralization," Bitcoin was captured by a small group of developers funded by traditional financial institutions.

4.2 The "Digital Gold" Rebranding

The "digital gold" narrative emerged after Bitcoin's transaction capacity was artificially constrained. Unable to function as a payment system, proponents reframed the limitation as a feature, arguing that Bitcoin's value lies in its scarcity rather than its utility.

This inverts the original design. Satoshi NAKAMOTO titled his paper "A Peer-to-Peer Electronic *Cash* System," not "A Digital Gold System."[1] The value of money derives from its function as a medium of exchange. A "store of value" that cannot be easily exchanged is not money—it is a speculative asset.

Gold derives its value from thousands of years of use as a medium of exchange, industrial applications, and cultural significance. Bitcoin was supposed to derive its value from utility as a payment system. Remove that utility, and what remains is a number on a screen that people hope will be worth more tomorrow.

4.3 The Lost Potential

What could Bitcoin have been? Satoshi's design described a system capable of:

Global payment infrastructure: Transaction volumes comparable to Visa's network—tens of thousands of transactions per second, at costs approaching zero.[2] Micropayments of fractions of a cent, enabling entirely new economic models: pay-per-article journalism, machine-to-machine payments, real-time streaming payments for services.

Financial inclusion: Approximately two billion people worldwide lack access to basic banking services. Bitcoin as designed would eliminate these barriers—anyone with internet access could participate in the global economy. No minimum balances, no geographic restrictions, no credit history requirements. The system that was supposed to bank the unbanked has been converted into a speculative vehicle for wealthy investors.

Programmable money: Bitcoin's scripting language, as Satoshi designed it, can implement smart contracts, automated payments, conditional transfers, and complex financial instruments—precisely what WRIGHT told the Las Vegas panel in 2015, and precisely what SZABO dismissed as "esoteric." Every

function that "DeFi" platforms claim to enable was already possible in Bitcoin's original design. Ethereum was explicitly created to provide capabilities that Bitcoin supposedly lacked—but those limitations were artificially imposed, not inherent.

Automated administration: Tax collection tied directly to transactions. Automated royalty distribution. Transparent audit trails. Government services that execute automatically rather than through bureaucratic processes. These capabilities exist in Bitcoin's original design; they were disabled, not absent.

4.4 The Fragmentation

The cryptocurrency ecosystem has proliferated into thousands of different coins and chains. This proliferation has been normalized to the point where newcomers assume multiple competing chains are natural and necessary.

Consider the internet: we have one TCP/IP protocol, not thousands of competing internets. We have one HTTP standard, not a marketplace of incompatible web protocols. The entire value of a network comes from its universality. A payment system that requires you to hold dozens of different tokens, each convertible only through specific exchanges, is not an improvement over traditional banking—it is a regression.

The proliferation of altcoins serves two purposes. First, it generates trading fees for exchanges and speculation opportunities for insiders who can create and promote new tokens. Second, it normalizes fragmentation, making it seem natural that Bitcoin "can't do everything" and therefore needs to be supplemented by other chains.

One working global payment system is infinitely more valuable than thousands of incompatible speculation vehicles. Satoshi designed one protocol to handle all use cases. The fragmentation we see today is not innovation—it is the visible symptom of capture.

5. The Choice Ahead

The cryptocurrency industry, seventeen years after Satoshi's whitepaper, has produced exactly one lasting achievement: a new asset class for speculation. Thousands of coins. Hundreds of exchanges. Billions in trading volume. And not a single system that ordinary people use to buy coffee, pay rent, or send money to family abroad.

This is not a technology problem. The technology works. Bitcoin SV processes more transactions than BTC and BCH combined, at a fraction of the cost. The original design scales. The original scripting capabilities function. The infrastructure exists.

The problem is that an entire industry has been built on the assumption that the technology *doesn't* work—that we need Layer 2 solutions, sidechains, alternative chains, wrapped tokens, bridges, and an endless parade of "innovations" to solve problems that were solved in 2008.

5.1 The Comfortable Lie

It is easier to believe that thousands of smart people across hundreds of companies are building toward something real than to accept that the entire ecosystem is optimized for speculation rather than utility. It is easier to believe that "mass adoption is coming" than to notice that sixteen years of coming has produced nothing but promises.

The comfortable lie has many forms: Bitcoin is digital gold. Ethereum is the world computer. DeFi is revolutionizing finance. NFTs are transforming art. Web3 is the future of the internet. Each narrative serves to justify continued speculation while delivering nothing of practical value.

The cryptocurrency industry has become expert at one thing: creating the appearance of progress while carefully avoiding any outcome that would reduce trading volume or threaten the fee structures of entrenched players.

5.2 The Hard Truth

Building real systems requires abandoning comfortable myths.

The hard truth is that one working blockchain is sufficient. One set of rules, one ledger, one protocol that does what it was designed to do. Not because alternatives are impossible, but because network effects make fragmentation wasteful. The internet didn't need a thousand competing protocols; it needed one that worked.

The hard truth is that "decentralization" as currently preached is a distraction. A system maintained by professional operations competing for profit is more robust than a system maintained by hobbyists running nodes in their basements. Satoshi understood this. The capture of Bitcoin was accomplished by people who pretended not to.

The hard truth is that regulatory integration is necessary, not optional. The original Bitcoin was designed to work within legal systems, not to evade them. Satoshi explicitly warned against using Bitcoin for illegal activity.[18] A system that cannot comply with basic legal requirements is not a serious financial infrastructure—it is a toy for people who mistake inconvenience for revolution.

5.3 The Path Forward

The original Bitcoin still exists. Bitcoin SV implements Satoshi's design without artificial limitations. It processes transactions at scale. It supports the scripting capabilities that enable complex applications. It operates within legal frameworks rather than against them.

The technology has always worked. What remains is a question of commitment: whether enough people are ready to move past speculation and narratives, and begin the difficult work of building real infrastructure for real use.

This means abandoning the speculation mindset. A token that increases in price is not success; a system that processes useful transactions is success. A market cap is not adoption; actual usage is adoption. Trading volume is not utility; commercial deployment is utility.

This means building applications that ordinary people need. Payment systems that work. Identity verification that respects privacy while enabling compliance. Supply chain tracking that reduces fraud. Micropayment systems that enable new business models. Not whitepapers—working systems.

This means accepting that most of what the cryptocurrency industry has produced is waste. Thousands of tokens that serve no purpose. Billions of dollars in "investment" that produced nothing but trading opportunities. Years of engineering talent devoted to solving problems that were already solved, or that exist only because the original solution was deliberately broken.

5.4 The Real Revolution

Bitcoin's promise was never about getting rich. It was about building infrastructure that makes financial services available to everyone, that operates transparently, that cannot be captured by special interests. That promise remains achievable—but not through speculation, not through fragmentation, and not through pretending that dysfunction is innovation.

The real revolution is not a token price. It is a merchant accepting payment without intermediary fees. It is a worker receiving wages instantly rather than waiting for bank processing. It is a family sending money across borders without losing a percentage to transfer fees. It is a creator receiving royalties automatically whenever their work is used.

And contrary to the anti-bank rhetoric that has dominated cryptocurrency discourse, this revolution does not require the elimination of banks. It requires their transformation. Banks freed from the burden of maintaining payment infrastructure can return to their essential function: the creation of capital through lending. Evaluating risk, funding entrepreneurs, financing homes and businesses—these are valuable services that require human judgment and local knowledge. A functional Bitcoin handles the plumbing; banks can focus on what they do best. The original vision was never about destroying financial institutions. It was about making them more efficient.

None of this requires new technology. It requires using the technology that already exists, as it was designed to be used.

The evidence of capture is documented. The path forward is clear. What remains is the choice: continue participating in an ecosystem designed for speculation, or start building systems designed for utility.

The interpretation is yours. The choice is yours. But the technology is ready—and has been ready since 2008.

Glossary

Block: A collection of Bitcoin transactions that are processed together and added to the ledger. New blocks are created approximately every ten minutes.

Block size limit: The maximum amount of data that can be included in a single block. This determines how many transactions can be processed. The artificial constraint on this limit is central to Bitcoin's capture.

BTC: The ticker symbol for the captured version of Bitcoin, which implements artificial constraints on transaction capacity.

BSV (Bitcoin SV): "Satoshi Vision"—the implementation of Bitcoin that follows the original protocol design without artificial limitations.

Lightning Network: A "Layer 2" system built on top of BTC that processes transactions off the main blockchain. Promoted as a scaling solution, it introduces complexity and centralizes transaction processing through hub nodes.

Mining: The process of competing to add new blocks to the Bitcoin ledger. Miners solve computational puzzles; the winner gets to process transactions and receives newly created bitcoins as reward.

Node: A computer running Bitcoin software. Mining nodes process transactions and create blocks. Non-mining nodes simply receive and relay information.

Reference implementation: The version of Bitcoin software that most users run. Control of this software determines the de facto rules of the network.

SegWit (Segregated Witness): A 2017 change to Bitcoin that separated transaction signatures from transaction data. Critics argue this fundamentally altered Bitcoin's security model.

Sidechain: A parallel system that processes transactions outside the main Bitcoin network. Blockstream's business model depends on sidechains being necessary.

Whitepaper: Satoshi NAKAMOTO's original 2008 document describing Bitcoin: "A Peer-to-Peer Electronic Cash System."

References

[1] NAKAMOTO, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." October 31, 2008. bitcoin.org/bitcoin.pdf

[2] NAKAMOTO, Satoshi. Email to cryptography mailing list. November 2, 2008. "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." Archived at satoshi.nakamotoinstitute.org

[3] NAKAMOTO, Satoshi. BitcoinTalk forum post. October 4, 2010. "It can be phased in, like: if (blocknumber > 115000) maxblocksize = largerlimit." Archived at satoshi.nakamotoinstitute.org

[4] VIGNA, Paul. "Bitcoin Startup Blockstream Raises $55 Million in Funding Round." Wall Street Journal, February 3, 2016.

[5] Digital Currency Group. "Who We Are" and "Our Portfolio." Archived at archive.is/6BLgo and archive.is/u9e3n

[6] O'CONNELL, Justin. "MasterCard Invests In Silbert's Digital Currency Group." CCN, October 2015.

[7] Theymos. "It's time for a break: About the recent mess & temporary new rules." r/Bitcoin moderation policy, August 2015. Archived at archive.is/zFqDc

[8] Theymos. "Bitstamp will switch to BIP 101 this December." Reddit comments, November 2015. Archived at archive.is/i325t

[9] BACK, Adam (@adam3us). Twitter discussion of XT sabotage strategies, August 16, 2015. Archived at archive.is/KZH33

[10] Bitcoin Roundtable. "Bitcoin Roundtable Consensus" (Hong Kong Agreement), February 20, 2016.

[11] BIP 141: Segregated Witness Specification. Bitcoin Improvement Proposals.

[12] Australian Tax Office. Interview transcript with Craig WRIGHT, February 18, 2014.

[13] Wired Magazine. "Bitcoin's Creator Satoshi Nakamoto Is Probably This Unknown Australian Genius." December 2015.

[14] Gizmodo. "This Australian Says He and His Dead Friend Invented Bitcoin." December 2015.

[15] O'HAGAN, Andrew. "The Satoshi Affair." London Review of Books, Vol. 38 No. 13, June 30, 2016.

[16] Kleiman v. Wright, Case No. 9:18-cv-80176 (S.D. Fla.)

[17] Crypto Open Patent Alliance Ltd v. Wright [2024] EWHC 1198 (Ch)

[18] NAKAMOTO, Satoshi. BitcoinTalk forum post. December 5, 2010. "WikiLeaks has kicked the hornet's nest, and the swarm is headed towards us." Archived at satoshi.nakamotoinstitute.org

[19] Bitcoin Investor Conference. "All-Star Panel: Ed Moy, Joseph Vaughn-Perling, Trace Mayer, Nick Szabo, Dr. Craig Wright." Las Vegas, NV. October 29-30, 2015. Video: youtube.com/watch?v=LdvQTwjVmrE

Bibliography

Primary Sources

NAKAMOTO, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." 2008. bitcoin.org/bitcoin.pdf

Satoshi NAKAMOTO Forum Posts and Emails. Archive: satoshi.nakamotoinstitute.org

Australian Tax Office. Interview transcript with Craig WRIGHT, February 18, 2014.

Bitcoin Roundtable. "Bitcoin Roundtable Consensus" (Hong Kong Agreement), February 20, 2016.

Bitcoin Investor Conference. "All-Star Panel: Ed Moy, Joseph Vaughn-Perling, Trace Mayer, Nick Szabo, Dr. Craig Wright." Las Vegas, NV. October 29-30, 2015. Video: youtube.com/watch?v=LdvQTwjVmrE

Corporate Documents

HILL, Austin. "Blockstream Welcomes New Investors: Adds $55 Million in Series A." Blockstream Blog, February 2, 2016.

VIGNA, Paul. "Bitcoin Startup Blockstream Raises $55 Million in Funding Round." Wall Street Journal, February 3, 2016.

Digital Currency Group. "Who We Are" and "Our Portfolio." Archived at archive.is/6BLgo and archive.is/u9e3n

O'CONNELL, Justin. "MasterCard Invests In Silbert's Digital Currency Group." CCN, October 2015.

Community Documentation

Theymos. "It's time for a break: About the recent mess & temporary new rules." r/Bitcoin moderation policy, August 2015. Archive: archive.is/zFqDc

Theymos. "Bitstamp will switch to BIP 101 this December." Reddit comments, November 2015. Archive: archive.is/i325t

BACK, Adam (@adam3us). Twitter discussion of XT sabotage strategies, August 16, 2015. Archive: archive.is/KZH33

Singularity87. "People should get the full story of r/bitcoin..." Reddit documentation of censorship campaign, 2016. Archive: archive.is/TkUus

Journalism

Wired Magazine. "Bitcoin's Creator Satoshi Nakamoto Is Probably This Unknown Australian Genius." December 2015.

Gizmodo. "This Australian Says He and His Dead Friend Invented Bitcoin." December 2015.

O'HAGAN, Andrew. "The Satoshi Affair." London Review of Books, Vol. 38 No. 13, June 30, 2016.

HEARN, Mike. "The Resolution of the Bitcoin Experiment." Blog.plan99.net, January 14, 2016.

Technical Documentation

Bitcoin SV Wiki. wiki.bitcoinsv.io

BIP 141: Segregated Witness Specification. Bitcoin Improvement Proposals.

MORGAN, Daniel. "The Great Bitcoin Scaling Debate — A Timeline." HackerNoon, December 1, 2017.

Legal Proceedings

Kleiman v. Wright, Case No. 9:18-cv-80176 (S.D. Fla.)

Crypto Open Patent Alliance Ltd v. Wright [2024] EWHC 1198 (Ch)