

Funding Bitcoin's Future

Paying for Security as the Block Subsidy Fades

October 2026

Cambridge
Centre
for Alternative
Finance



UNIVERSITY OF
CAMBRIDGE
Judge Business School

In collaboration with



Financial
Innovation for
Impact



Suggested Citation

CCAF and Fii (2026) ***Funding Bitcoin's Future: Paying for Security as the Block Subsidy Fades***, Cambridge Centre for Alternative Finance (CCAF), Cambridge Judge Business School, University of Cambridge; Financial Innovation for Impact (Fii)

Contents

	Foreword	4
	Executive Summary	5
	Research Team and Acknowledgements	6
Part I:	Introduction to Bitcoin's Security Model	7
	The Bitcoin System	8
	Security Dynamics	11
Part II:	The Fee Market Challenge	16
	Fee Market Dynamics and Volatility	17
	Mining Economics and Profitability	21
	Subsidy Income and Fee Revenue	23
Part III:	Attack Economics and Security Risks	25
	Attack Cost Economics	26
	Fee-Based Instabilities	28
	Empirical Evidence: Theory vs Reality	30
	Mining Centralization Risks	31
	Lessons from Other Chains	33
Part IV:	Options Under Debate and Their Trade-offs	35
	Market-Based Approaches	36
	Protocol Changes	40
	Industry Adaptation	42
Part V:	Looking Forward	47
	Spillover Risks to Traditional Finance	48
	Synthesis of Evidence	48
	Future Directions	52
	Appendix A. Measurement Methods	58
	Endnotes	60

Foreword

For nearly two decades, Bitcoin has sustained an open monetary network absent of gatekeepers, allowing anyone to participate without seeking permission from a central authority. Through a synthesis of cryptographic verification and economic incentives, the protocol aligns self-interest to ensure that actors who do not trust one another can ultimately agree on a single truth. The network's durability depends upon confidence in these rules and the continued financial motivation for miners to secure the shared transaction history.

A predictable issuance schedule and a fixed supply limit are central to this confidence, yet the block subsidy awarded to miners falls with each halving. As new issuance recedes, the eventual necessity of relying on transaction fees brings the long-term implications of this economic incentive structure into sharper focus. Rather than dictating an immediate crisis, this programmed reduction naturally highlights the importance of examining how a system capped at 21 million coins will fund its own protection.

Although the subsidy follows a predetermined path, the economic conditions surrounding it continue to fluctuate. Transaction fees, asset price, operating costs, and technological advancements all influence miner behaviour, while user choices shape the demand for block space. Historical precedent demonstrates a considerable capacity to adapt to these shifts. Understanding how that resilience extends to a future defined by negligible subsidies requires a careful examination of the mechanisms that discourage attacks and sustain honest participation.

The security budget therefore connects individual economic decisions with shared expectations of reliable settlement and resistance to censorship. It also raises fundamental questions regarding how participants with competing interests can respond to changing conditions while preserving the monetary commitments that underpin the entire ecosystem.

Since launching the Cambridge Bitcoin Electricity Consumption Index in 2019, the Cambridge Centre for Alternative Finance has worked to strengthen public understanding through transparent measurement and analysis. We bring that same commitment to this report, synthesising academic research, on-chain data, and industry perspectives to clarify the evidence and uncertainties shaping the security budget debate.

The Security Budget Health Indicator framework introduced in this report gives that inquiry a practical starting point. It offers a structured method for observing the evolving economics of network security and identifying trends that warrant closer investigation. Its utility will undoubtedly grow through scrutiny and application, as researchers and practitioners test its assumptions and refine its measures.

We present this work as a foundation for a continuing conversation regarding how the protocol can sustain the incentives that secure it. We invite the wider community to engage with these findings as the network evolves, halving by halving.

Alexander Neumueller

Research Lead, Digital Assets Energy and Climate Impact
Cambridge Centre for Alternative Finance

Douglas Arner

Associate Director – Research Programmes
Cambridge Centre for Alternative Finance

Executive Summary

Bitcoin pays miners through block subsidies and transaction fees. The BTC subsidy halves approximately every four years and eventually reaches zero. This report examines the income available to miners, the economic conditions behind attack strategies and the options for maintaining network security.

Subsidy reductions and dollar income follow different paths. The next four halvings reduce the subsidy per block by 93.75%; dollar income also depends on Bitcoin's price and transaction demand. Miners can assess equipment, power and revenue-diversification choices under these conditions, disclosing the assumptions that shape their costs and returns.

Fee income remains small and variable. Fees account for 0.67% of miner revenue over 90 days, and daily fee changes are 11.7 times as volatile as price changes over that window. Developers can improve transaction handling and fee adjustment, while the aggregate revenue effect depends on demand. Changes to issuance face additional consensus requirements.

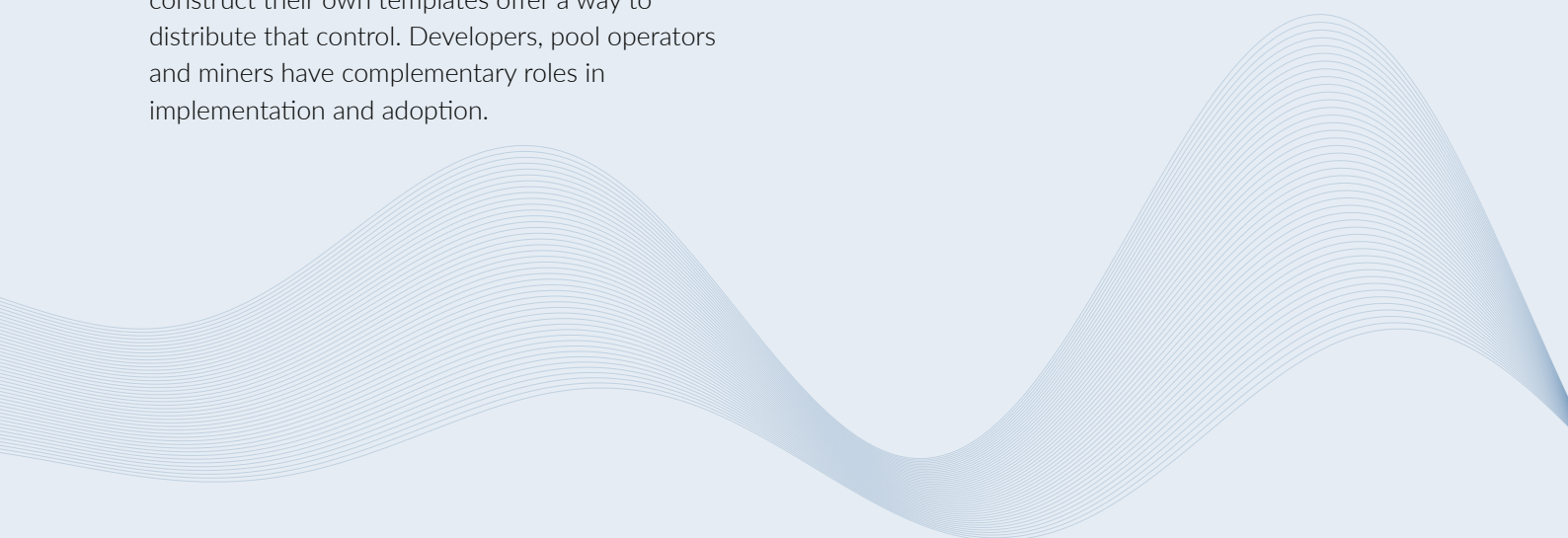
Template control matters alongside pool shares. The top three pools account for 60.8% of blocks in the one-month snapshot; proxy pooling can concentrate template selection further. Protocols that let miners construct their own templates offer a way to distribute that control. Developers, pool operators and miners have complementary roles in implementation and adoption.

Attack incentives depend on resources and feasible payoffs. The cited empirical studies have not identified the modelled fee-based instabilities on Bitcoin mainnet. Acquisition-cost estimates depend on the capacity route and costs included; derivatives-linked incentives depend on positions an attacker can build and settle. Regulators and exchanges can examine these channels through their respective supervision and surveillance roles.

Financial integration extends exposure beyond mining. ETFs, corporate treasuries and Bitcoin-backed loans connect network disruption to regulated markets. Issuers and supervisors can build on existing mining-risk disclosures to improve comparability. Investors can evaluate mining-related exposures, support independent research and prepare for custody or settlement interruptions.

Monitoring needs transparent inputs and methods. The Security Budget Health Indicator tracks five raw indicators alongside fixed reference scales, with calculations in Appendix A. Developers, academic institutions, data providers and industry can use these definitions to build monitoring tools and compare observations over time.

Market and on-chain data are reported through 4 October 2026.



Research Team and Acknowledgements

Research Team

Wenbin Wu (Principal Researcher, CCAF), **Alexander Neumueller** (Research Lead, Digital Assets Energy and Climate Impact, CCAF), and **Colin Wang** (Research Affiliate, CCAF).

Acknowledgements

We are grateful to the following reviewers, whose comments and corrections substantially improved this report (in alphabetical order). Their acknowledgement does not imply endorsement of the report's findings, and any remaining errors are our own.

- Daniel Batten – Managing Partner, CH4 Capital
- Hugo Coelho – Director of Policy and Advisory, Financial Innovation for Impact
- Shaen Corbet – Professor of Finance, Dublin City University
- Alex de Vries-Gao – Founder, Digiconomist; Vrije Universiteit Amsterdam
- Anantha Divakaruni – Associate Professor, University of Bergen
- Hanna Halaburda – Associate Professor, NYU Stern School of Business
- Campbell Harvey – Professor, Duke University, Fuqua School of Business
- Andrew Lewis-Pye – Professor, London School of Economics
- Peter McBurney – Professor, King's College London
- Mason Price – MARA Holdings
- Stefan Scharnowski – University of Mannheim, Business School
- Horst Treiblmaier – Professor, Modul University Vienna
- Michele Uberti – Bitcoin Observatory, Politecnico di Torino
- Harald Uhlig – Professor, University of Chicago
- Peter Zimmerman – Federal Reserve Bank of Cleveland (in a personal capacity)

Part I

Introduction



Bitcoin pays miners through block subsidies and transaction fees. As the subsidy in BTC falls, miners' dollar income depends on Bitcoin's price and demand for block space.

On October 31, 2008, an anonymous figure using the pseudonym Satoshi Nakamoto published a nine-page paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System"¹. The paper proposed a solution to a problem that had occupied computer scientists for decades: how to create digital money that could not be copied, counterfeited, or double-spent without relying on a trusted central authority. Nearly eighteen years later, Bitcoin has grown from a cryptographic curiosity into a trillion-dollar asset class, yet the mechanism that secures it faces a question that Nakamoto's original design left unresolved.

This report examines that question: What happens when the security budget shrinks?

The answer matters far beyond the cryptocurrency community. Bitcoin now serves as collateral for regulated financial products, a reserve asset for publicly traded companies, and a monetary alternative for citizens of countries with unstable currencies. If its security model proves unsustainable, the consequences would ripple through global financial markets. Conversely, if Bitcoin successfully transitions to fee-based security, it would validate a new paradigm for decentralized infrastructure funding.

The Bitcoin System

Bitcoin as a Financial Innovation

Bitcoin represents the first successful implementation of a decentralized digital currency. Unlike traditional payment systems that rely on banks, clearinghouses, or payment processors to validate transactions, Bitcoin uses a distributed network of computers, called nodes, to maintain a shared ledger of all transactions ever made. This ledger, the blockchain, is secured not by institutional trust but by mathematics and economic incentives.

The innovation was not any single component but their combination. Cryptographic signatures had

existed for decades. Distributed databases were well understood. Even the concept of digital cash had been explored by researchers like David Chaum in the 1980s and Wei Dai's b-money proposal in 1998. What Nakamoto achieved was synthesizing these elements into a system where participants who do not know or trust each other can nonetheless agree on a single, immutable transaction history².

This achievement required solving what computer scientists call the Byzantine Generals Problem³, which concerns how to reach consensus in a network where some participants may be malicious or unreliable. The problem, first formalized by Lamport, Shostak, and Pease in 1982, imagines a group of Byzantine generals who must coordinate an attack on a city. Some generals may be traitors who send conflicting messages. The challenge is designing a protocol that allows loyal generals to reach agreement despite the traitors' interference.

Traditional solutions to the Byzantine Generals Problem required knowing the identities of all participants and assumed a fixed, known set of actors. Nakamoto's breakthrough was creating a solution that works in an open, permissionless network where anyone can join or leave at any time, and where participants are pseudonymous. The mechanism that makes this possible is proof-of-work.

Bitcoin's design reflects several key properties that distinguish it from previous digital currency attempts:

Decentralization: Anyone can run a Bitcoin node and verify transactions without a central administrator. Open participation does not guarantee independent ownership of nodes or mining capacity. Nakamoto's security analysis assumes that honest miners collectively control more hashpower than a cooperating group of attackers⁴.

Transparency: Every transaction is recorded on a public ledger that anyone can audit. While users are identified by pseudonymous addresses rather than real names, the flow of funds is completely visible.

Immutability: Bitcoin provides probabilistic settlement: in Nakamoto's model, the chance that an attacker with less hashpower than honest miners reverses a payment falls as confirmations accumulate. This protection depends on the distribution of hashpower and network conditions¹.

Scarcity: Bitcoin's supply is capped at 21 million coins, with issuance following a predetermined schedule. This contrasts with fiat currencies, where central banks can create money at will.

Permissionlessness: Anyone can use Bitcoin without approval from any authority. Users need only generate a cryptographic key pair to send and receive funds.

These properties emerge from Bitcoin's technical architecture, but they are sustained by economic incentives. The system works because participants find it profitable to follow the rules, and this is where the security budget becomes critical.

How Proof-of-Work Creates Security

Proof-of-work is the engine that powers Bitcoin's security. To understand why Bitcoin is difficult to attack, one must first understand how new blocks are added to the blockchain and why this process is expensive.

Approximately every ten minutes, specialized computers called miners compete to solve a computational puzzle. The puzzle itself is simple to describe but expensive to solve: find a number (called a nonce) that, when combined with the block's data and hashed using the SHA-256 algorithm, produces a result below a certain target value. Because cryptographic hash functions are effectively random, meaning that small changes in input produce completely unpredictable changes in output, the only way to find a valid nonce is through brute-force trial and error. Miners compute trillions of hashes until one happens to meet the criteria.

The miner who finds a valid solution first broadcasts their block to the network. Other nodes verify that the solution is correct (which takes milliseconds, since verification is trivial even though finding the solution is hard) and that all transactions in the block are valid according to Bitcoin's consensus rules. If everything checks out, the block is added to the chain, and the

winning miner receives the block reward: newly minted bitcoin plus all transaction fees from the included transactions.

This process creates security through economic cost. An attacker seeking to reverse a confirmed transaction must build a valid competing branch that accumulates more proof of work than the branch being replaced. With Bitcoin's network operating at approximately 943 EH/s (0.9 ZH/s) as of 4 October 2026, the energy and hardware required to outpace honest miners represents a high barrier⁴.

Every 2,016 blocks (approximately two weeks), the protocol adjusts the puzzle difficulty toward an average interval of ten minutes. If miners add hardware, difficulty rises; if miners leave, it falls. Lower difficulty allows the remaining miners to restore the target block interval. The attack barrier still depends on their combined hashrate: when honest hashrate falls, an attacker needs less hashpower to outpace it.

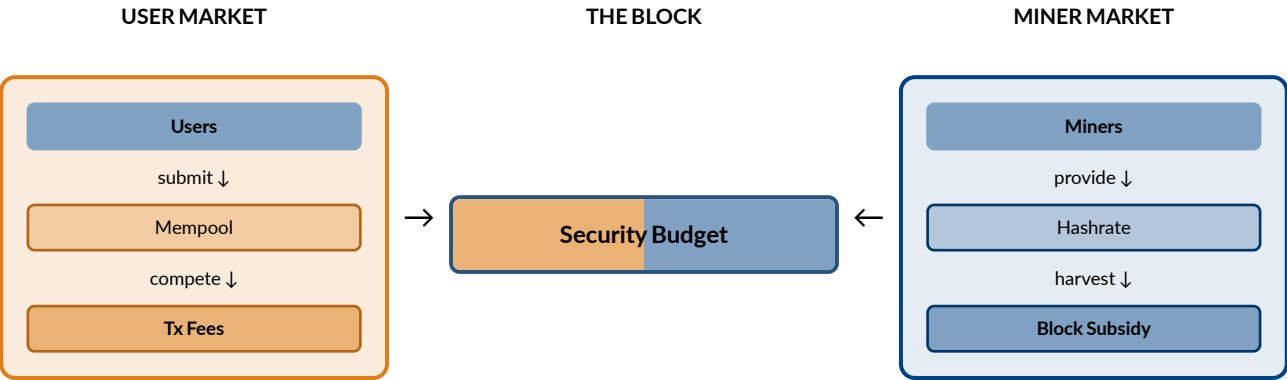
The security provided by proof-of-work can be understood through the concept of *thermodynamic security*⁵. Unlike traditional security systems that rely on secrets (passwords, encryption keys) that could theoretically be guessed or stolen, Bitcoin's security is grounded in the laws of physics. Reversing confirmed transactions requires expending real energy. There is no shortcut, no clever hack, no way to fake the work. This creates what Nick Szabo termed "unforgeable costliness", where value derives from being demonstrably difficult to produce, anchoring Bitcoin's security in physical reality through energy expenditure⁶.

Each block added after a transaction increases the work an attacker must catch up with to reverse it. Exchanges and merchants therefore wait for multiple confirmations before accepting large payments. In Nakamoto's model, the probability that a slower attacker catches up declines exponentially with the number of blocks behind¹.

However, this security comes at a price. According to the Centre's own Cambridge Bitcoin Electricity Consumption Index (CBECI), Bitcoin mining currently consumes approximately 150-180 TWh of electricity annually, comparable to the energy consumption of a medium-sized country like Argentina or Norway⁴. This energy expenditure is not waste; it is the cost of maintaining a trustless, decentralized monetary

Figure 1: Bitcoin’s Two-Market Security Model. In the User Market (left), users submit transactions to the mempool, where fee-based selection determines block inclusion, generating transaction fees. In the Miner Market (right), miners provide hashrate to produce blocks and earn the block subsidy. Both transaction fees and block subsidy flow into the Security Budget, the total resources securing the network against attack. At a fixed Bitcoin price, miners would need higher fee income to maintain the same dollar revenue as the block subsidy falls.

Bitcoin’s Security Model



system. But it must be paid for somehow, and that payment comes from the security budget.

Understanding the Security Budget

Bitcoin’s security can be understood through two interconnected markets that together determine the network’s resilience against attack. Figure 1 illustrates this “two-market model,” which provides a framework for analyzing how resources flow into network security and why the current equilibrium may be unstable.

The *User Market* generates transaction fees. When users want to transfer bitcoin, they broadcast transactions to the network’s mempool, a waiting area for unconfirmed transactions maintained by each node. Because block space is limited (capped at 4 million weight units per block under SegWit, roughly 1.5-2 MB of typical transactions, or about 2,800 of them), users compete by offering fees. Miners, acting as rational economic agents, select the highest-fee transactions to maximize their revenue. During periods of high demand, this auction mechanism can drive fees to hundreds of dollars per transaction⁷.

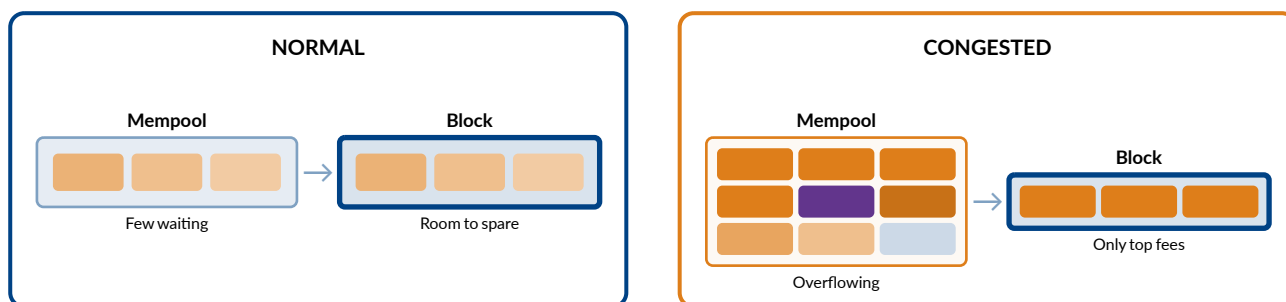
The fee market operates as a form of congestion pricing. Huberman, Leshno, and Moallemi’s analysis in the Review of Economic Studies⁷ describes Bitcoin as a “monopoly without a monopolist”: users compete to avoid confirmation delays, while no operator sets a monopoly price. Their model shows how this arrangement protects users against monopoly pricing even if Bitcoin becomes the dominant payment system. Figure 2 illustrates the role of congestion: users pay low fees when block space is available and compete for priority when demand exceeds capacity.

The *Miner Market* generates the block subsidy. Miners invest in specialized hardware (Application-Specific Integrated Circuits, or ASICs) and electricity to produce hashrate, which is computational power directed at solving proof-of-work puzzles. The protocol rewards successful miners with newly created bitcoin: currently 3.125 BTC per block following the April 2024 halving. This subsidy, paid in freshly minted coins, represents Bitcoin’s monetary inflation and has historically constituted the vast majority of miner revenue.

Together, transaction fees and block subsidies form the *security budget*, the total economic resources devoted to securing the network. This budget

Figure 2: User Competition for Block Space. Under normal conditions (left), the mempool contains few waiting transactions, and blocks have room to spare, and users pay minimal fees. During congestion (right), the mempool overflows with transactions competing for limited block space. Only the highest-fee transactions are included, while lower-fee transactions must wait or increase their bids.

User Competition for Block Space



determines how much an attacker would need to spend to compromise Bitcoin's integrity. The key point is that these two revenue streams have different characteristics:

Block subsidies are predictable and programmatic. They halve every 210,000 blocks (approximately four years) according to a schedule known since Bitcoin's inception. Every market participant can calculate exactly how many new bitcoins will be created in any future period. This predictability is a feature: it makes Bitcoin's monetary policy credible and allows long-term planning.

Transaction fees are volatile and market-driven. They depend on user demand for block space, which fluctuates with network activity, speculation, competing uses like inscriptions and tokens, and the broader cryptocurrency market cycle. Fees can spike 100x during congestion events and collapse just as quickly when demand subsides⁸.

The transition from subsidy-funded to fee-funded security is not automatic; it depends on market dynamics that remain poorly understood and largely untested. This asymmetry creates the security budget problem. As the subsidy in BTC declines, miners' dollar revenue depends on Bitcoin's price and the transaction fees users pay.

Security Dynamics

The Game Theory Behind Mining

Bitcoin's security rests on game theory: the mathematical study of strategic decision-making among rational actors. The protocol is designed so that honest behavior, following the rules and extending the longest valid chain, is more profitable than cheating. Understanding why this works, and under what conditions it might fail, requires examining the incentive structures facing miners.

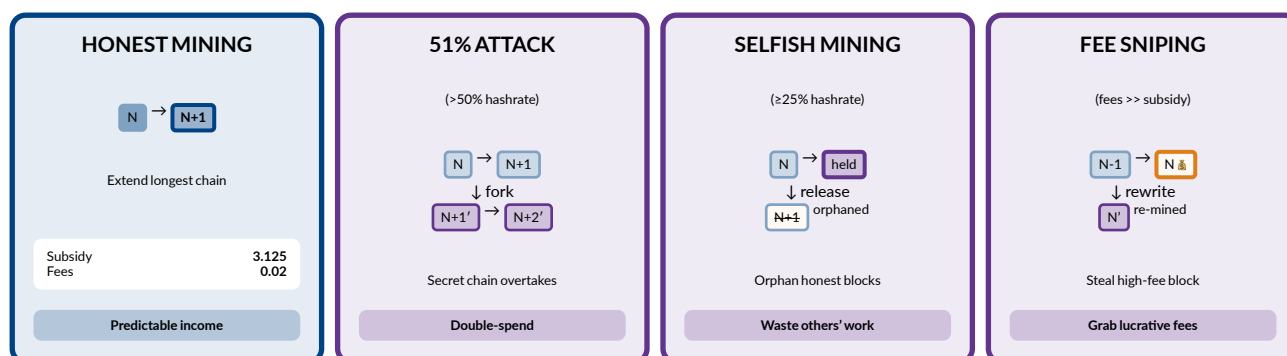
Consider a miner's strategic options. They can mine honestly, contributing hashrate to extend the blockchain and collecting rewards when they find valid blocks. Alternatively, they could attempt various attacks:

Double-spending involves paying a recipient on the public chain while mining an alternative chain containing a conflicting transaction that spends the same inputs. If the alternative chain accumulates more work and replaces the public branch, the conflicting spend invalidates the original payment, allowing the attacker to retain the purchased goods or services.

Selfish mining involves withholding discovered blocks to gain a disproportionate share of accepted rewards. In the standard fixed-reward model, this can increase

Figure 3: Miner's Strategic Options. Miners face a choice between honest mining (stable, predictable income) and various attack strategies (high risk, potential short-term gains). ASIC specialization creates “mutual assured destruction,” where attackers destroy their own hardware investment if their attack crashes Bitcoin’s value.

Miner's Strategic Options: Honest Mining vs Attack



BTC earned per day after difficulty adjusts, for miners above an assumption-dependent profitability threshold⁹. Part III explains the mechanism and how volatile fees affect it.

Fee sniping occurs when miners attempt to re-mine previous blocks to steal their transaction fees rather than extending the chain tip. This becomes attractive when a recently mined block contains unusually high fees¹⁰.

Transaction censorship involves refusing to include certain transactions in blocks, either for regulatory compliance, competitive advantage, or political reasons¹¹. Figure 3 maps these strategic options, illustrating how miners weigh stable honest income against riskier attack strategies, with ASIC specialization creating “mutual assured destruction” that deters most attacks.

For honest mining to dominate, the expected value of playing by the rules must exceed the expected value of attacking. Figure 4 depicts the underlying competitive dynamic: miners contribute hashrate to a probabilistic lottery where win probability equals their share of total network hashrate, with the winner receiving the block reward. This calculation depends on several factors: the miner’s share of total hashrate, the cost of their hardware and electricity, the value of block rewards, the potential gains from successful

attacks, and the probability of detection and retaliation.

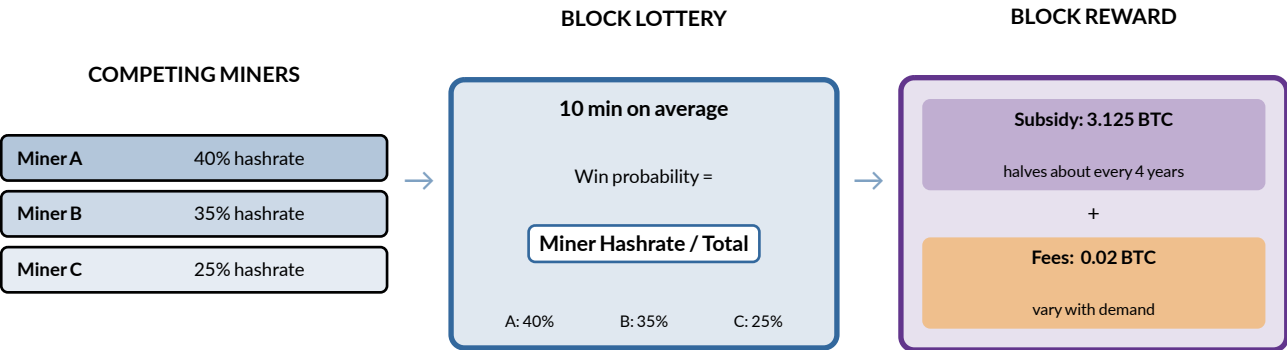
Eyal and Sirer’s 2014 paper “Majority is not Enough”⁹ demonstrated that the commonly assumed 51% threshold for attacks was too optimistic. Their analysis showed that selfish mining becomes profitable at hashrate shares as low as 25-33%, depending on network propagation characteristics. Specifically, they proved that a miner controlling more than 1/3 of hashrate can always profit from selfish mining, and with favorable network position (allowing them to hear about competing blocks quickly), the threshold drops to 1/4; in the limiting case where the attacker wins every propagation race, the threshold falls toward zero, so 25-33% is best read as the bound under propagation conditions unfavourable to the attacker.

This finding challenged the assumption that Bitcoin was secure as long as no single entity controlled a majority of hashrate. It also highlighted the importance of network topology, since miners with better connectivity have advantages that can be exploited strategically.

Subsequent research has refined and extended these results. Kwon et al.¹² introduced the Fork After Withholding (FAW) attack, which combines block withholding with selfish mining for even greater

Figure 4: Miner Competition for Block Rewards. Miners compete by contributing hashrate to a probabilistic lottery. Miners produce a block about every ten minutes on average. Win probability equals the miner's share of total network hashrate. The winner receives the block reward: currently 3.125 BTC in subsidy (which halves approximately every four years) plus transaction fees.

Miner Competition for Block Rewards



profits. Sapirshtein, Sompolinsky, and Zohar¹³ developed optimal selfish mining strategies using Markov Decision Processes. And Nayak et al.¹⁴ showed that combining selfish mining with eclipse attacks (isolating victims from the honest network) further reduces the hashrate threshold for profitable attacks.

However, the practical barriers to attacks extend beyond raw hashrate economics. An attacker must buy or rent sufficient mining hardware, a process that takes months for large quantities and would be visible to the market. They must establish the electrical infrastructure to power that hardware. And they must execute their attack before the market responds by crashing Bitcoin's price, potentially destroying the value of their own holdings and hardware investments.

Eric Budish's analysis¹⁵ formalized this as a "flow versus stock" problem. Bitcoin's security depends on ongoing "flow" payments to miners being large relative to the one-time "stock" benefits an attacker could extract. The key equation is:

$$\text{Flow} \times \text{Duration} > \text{Stock Benefit} - \text{Stock Cost}$$

Where Flow is the miner revenue rate, Duration is how long an attack takes, Stock Benefit is what the attacker gains (e.g., double-spend value), and Stock

Cost is what the attacker loses (e.g., hardware value if Bitcoin crashes).

When mining hardware is specialized and non-repurposable, as Bitcoin's ASICs are, this constraint becomes "stock versus stock": the attacker's hardware investment would be destroyed along with Bitcoin's value if an attack succeeded. This creates a form of mutual assured destruction that deters attacks even when the flow-based calculation might suggest vulnerability.

Budish's framework shows that Bitcoin's security is not just about the cost of acquiring hashrate, but about the alignment of incentives created by specialized hardware. Miners who have invested billions in ASICs that can only mine Bitcoin have strong incentives to protect the network's value. This "skin in the game" provides security beyond what the raw economics of attack costs would suggest.

The security picture becomes more complicated when we look at how mining is actually organized. Individual miners rarely work alone. Instead, they join "mining pools" that combine computational power from thousands of participants and share rewards proportionally. This pooling is economically rational: it smooths out the highly variable income from solo mining into more predictable payments. Pool operators usually select the transactions in their blocks. DATUM and pools supporting Stratum V2 Job

Declaration allow participating miners to construct their own templates (Part III).

Concentrated template selection creates coordination points for censorship or attacks. Proxy pooling can concentrate that control beyond the pool names visible in blocks¹⁶. Part III examines the pool-share data and the distinction between pool membership and template control.

Why This Matters Now

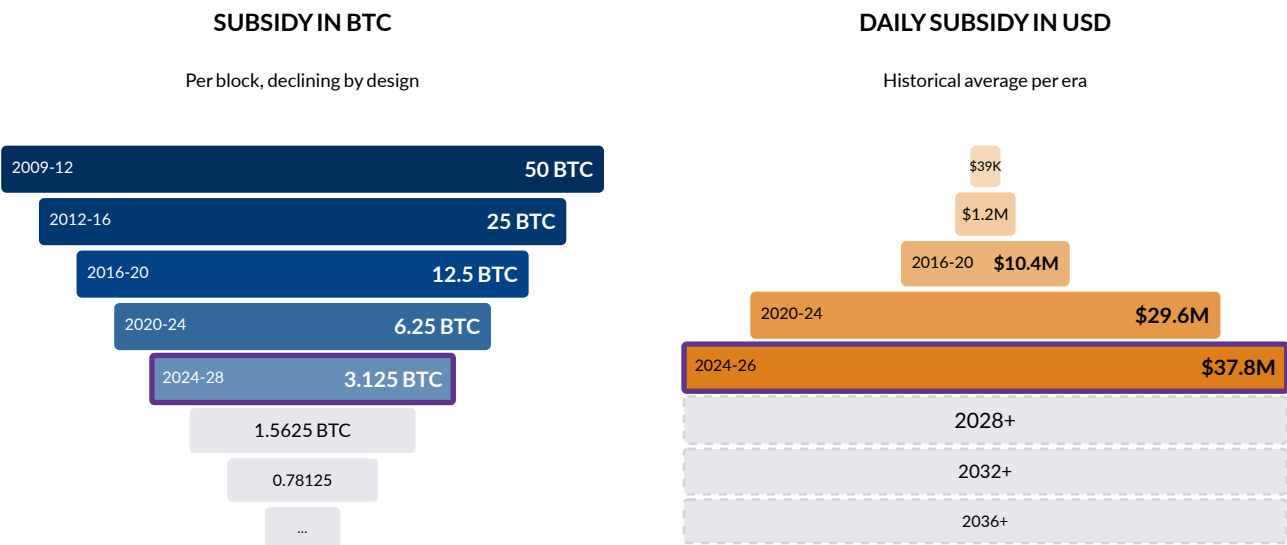
The security model described above has functioned effectively for more than a decade. Bitcoin has never suffered a successful 51% attack on its main chain. Transactions worth trillions of dollars have settled without reversal. The network has survived multiple market crashes, regulatory crackdowns, and technical challenges. By any reasonable measure, Bitcoin’s security has been robust.

Yet this track record was achieved during a period when block subsidies dominated miner revenue. When Bitcoin launched in 2009, miners received 50 BTC per block. After four halvings, that reward has fallen to 3.125 BTC, a 93.75% reduction. Subsidies still provide most miner revenue. Part II examines the fee share over time, including sustained increases during congestion.

Figure 5 shows the halving schedule, and numbers tell two very different stories depending on the unit of measurement. In BTC terms, the left pyramid shows an inexorable decline, as the protocol is doing exactly what it was designed to do. In the halving-era averages shown, daily subsidy revenue in dollar terms has *increased* nearly 1,000-fold since Bitcoin’s early days despite the 93.75% reduction in BTC per block. Price appreciation has more than compensated for each halving, so far.

Figure 5: Block Subsidies: The BTC vs USD Paradox. The left pyramid shows the programmatic decline of block subsidies in BTC terms, from 50 BTC per block in 2009 to 3.125 BTC today, a 93.75% reduction. The right pyramid multiplies the subsidy by 144 blocks per day and the mean available BTC price in each halving era. Price appreciation more than offset the subsidy reductions in these historical averages. The grey USD entries correspond to future eras. Price observations run from 17 July 2010 to 4 October 2026. Data source: Glassnode¹⁷; authors’ calculations.

Block Subsidies: The BTC vs USD Paradox



The critical question is whether this pattern can continue. The 2024 halving cut daily subsidy issuance in half; at current prices of approximately \$87,000 per bitcoin, the subsidy is worth roughly \$39 million per day, and the 2028 halving will reduce it to roughly \$19.5 million (assuming constant prices). By 2044, daily subsidies will fall below \$3 million at current prices, a few percent of today's daily miner revenue.

Nakamoto's original design assumed that "once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees"¹. This assumption, that fee revenue would naturally grow to replace declining subsidies, has not been tested at scale. Over the 90 days ending 4 October 2026, transaction fees account for 0.67% of miner revenue, alongside the higher-fee periods examined in Part II.

The Runes launch coincided with the April 2024 halving and generated a temporary surge in demand for block space¹⁸. Part II examines the fee spike and its subsequent decline.

The timing of the security budget challenge is debated. Some argue that Bitcoin has decades before fees must replace subsidies, and that market dynamics will naturally solve the problem. Others warn that the critical period is approaching faster than commonly assumed.

Bitcoin Core developer James O'Beirne has warned that "the amount of time that we have to resolve that question is not much, in the sense that two halvings from now you're going to have a pretty drastically reduced subsidy. That's seven and a half years away"¹⁹. The remark, made in April 2025, refers to the two halvings expected around 2028 and 2032. The second will reduce the subsidy to 0.78125 BTC per block, less than \$68,000 per block at current prices, or roughly \$9.7 million per day.

Fred Thiel, CEO of MARA Holdings (formerly Marathon Digital, one of the largest publicly traded Bitcoin miners), offered a starker assessment: "Bitcoin was designed with the idea that transaction fees would eventually replace the subsidy. But that hasn't happened. If bitcoin doesn't grow at 50% or more annually, the math gets very tough after 2028—and even tougher in 2032"²⁰.

The stakes extend beyond Bitcoin itself. As the first and largest cryptocurrency, Bitcoin serves as a proof

of concept for decentralized digital money. If its security model proves unsustainable, it would cast doubt on the entire category. Conversely, if Bitcoin successfully navigates the transition to fee-based security, it would demonstrate that decentralized systems can fund their own infrastructure without relying on inflationary subsidies.

This report examines whether that transition is feasible, and what happens if it is not. Part II analyzes the fee market challenge, examining whether transaction fees are growing to replace declining subsidies. Part III explores attack economics and security risks, assessing theoretical vulnerabilities and empirical evidence for whether these threats have materialized. Part IV evaluates proposed solutions and their trade-offs, from incremental protocol improvements to controversial monetary policy changes. Part V charts a path forward, synthesizing findings and outlining scenarios for Bitcoin's security future.

The question of Bitcoin's long-term security is not merely academic. It affects the hundreds of billions of dollars stored in bitcoin, the mining industry that secures the network, the Layer 2 protocols built on top of it, and the broader vision of decentralized digital money. Understanding the security budget challenge, and the range of possible outcomes, is essential for anyone with a stake in Bitcoin's future.

Part II

The Fee Market



Transaction fees contribute a small and volatile share of miner revenue.

Part I established the two-market model: miners receive a scheduled subsidy in BTC and transaction fees from users. Their dollar revenue depends on Bitcoin’s price and fee demand. This section examines fee market dynamics and miner behavior.

Fee Market Dynamics and Volatility

Transaction fees are Bitcoin’s intended long-term security funding mechanism, but their behavior raises concerns about their ability to provide stable, adequate revenue. This section examines fee market dynamics in detail, drawing on both academic research and empirical data.

The fee market operates through a first-price auction mechanism. Users attach fees to their transactions,

and miners select the highest-fee transactions to include in blocks. Figure 6 visualizes this process: the mempool sorts pending transactions by fee rate, and miners rationally select the highest-paying ones, establishing a “clearing price” below which transactions must wait. This creates a market-clearing process where fees adjust to balance supply (block space) and demand (transaction volume). During periods of high demand, fees spike as users compete for limited space; during low demand, fees fall toward the minimum⁷.

As Figure 7 shows, the fee share of miner revenue, measured over rolling 90-day windows, is usually below 5%, with sustained increases during congested periods. Bitcoin’s market capitalisation has grown across the period, while the fee share shows no comparable sustained increase. Market capitalisation and demand for block space measure different aspects of Bitcoin’s use.

Figure 6: The Fee Auction Mechanism. Bitcoin’s fee market operates as a first-price auction where transactions compete for limited block space. Left: the mempool contains pending transactions sorted by fee rate (satoshis per virtual byte). Miners rationally select the highest-paying transactions to maximize revenue. Right: only transactions above the “clearing price” are included in the next block; lower-fee transactions must wait or increase their bids. The key insight is that fee **rate** matters, not absolute fee, so a large transaction needs a proportionally higher total fee to compete.

The Fee Auction: How Transactions Compete for Block Space

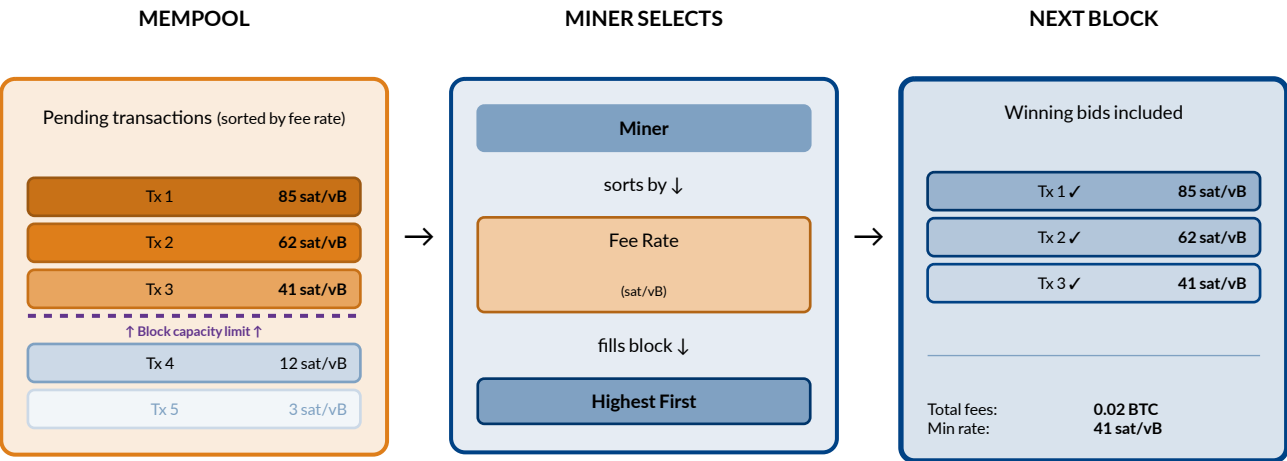
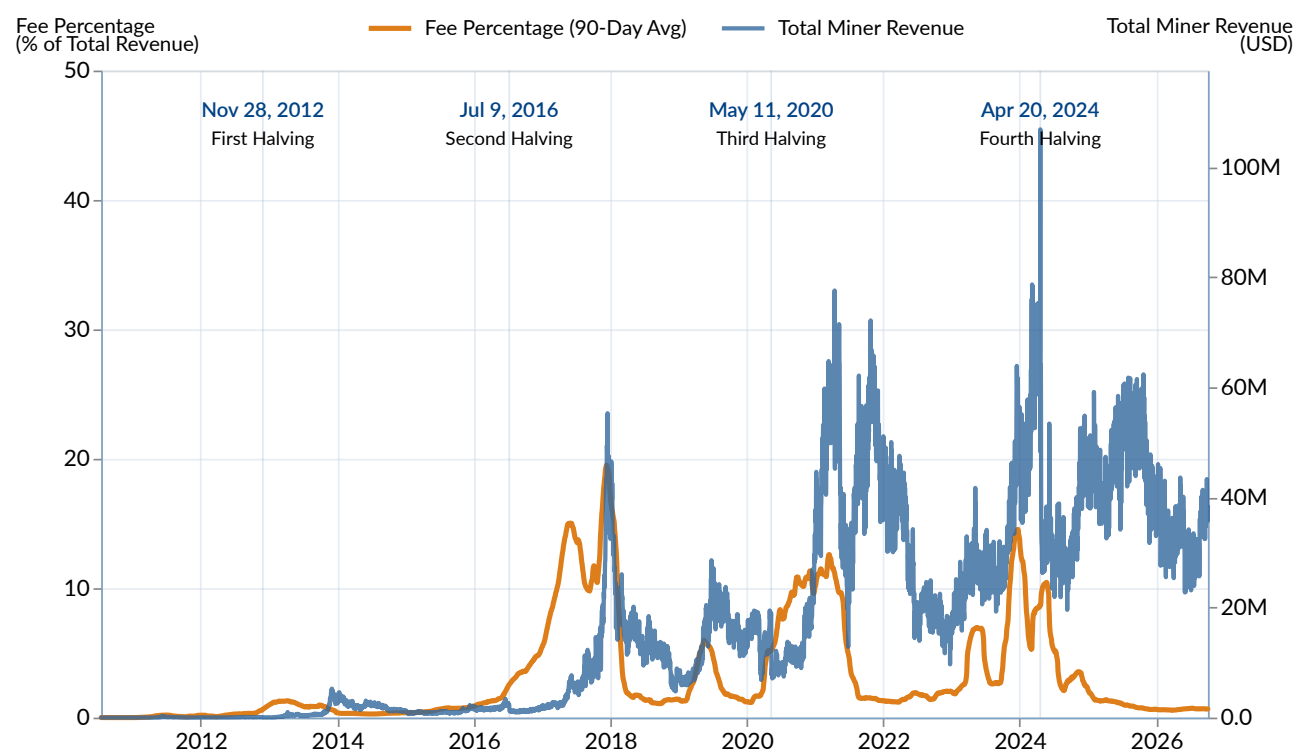


Figure 7: Transaction Fees as a Share of Miner Revenue (2010–2026). Orange shows the 90-day centred moving average of daily fee shares (left axis); blue shows daily total miner revenue (right axis). Vertical lines mark halving events. Fee shares are usually below 5%, with sustained increases during congestion. Observations through 4 October 2026. Data source: Glassnode¹⁷.

Transaction Fees as Percentage of Total Miner Revenue Over Time



Fee revenue is volatile. Figure 8 compares rolling 30-day volatility measures; at the report's data cutoff, the standard deviation of daily fee-income changes is 11.7 times that of price changes over 90 days and 10.2 times over a year²¹. Miners face variation in both fee income and Bitcoin's price.

Third, fee revenue depends on competition for block space. In Figure 9, near-full blocks coexist with widely varying fee shares. Backlogs can intensify users' competition for inclusion, but high fullness alone does not imply high fees.

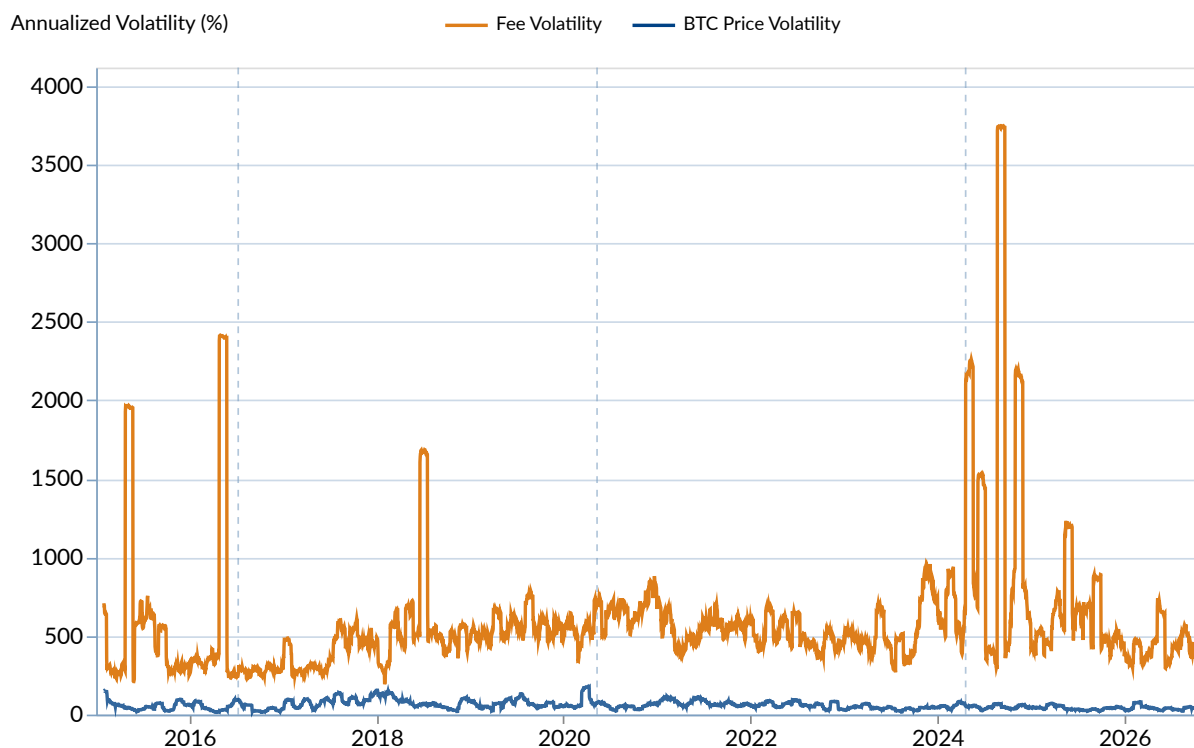
This congestion-dependence creates a problematic dynamic. For fees to provide adequate revenue, blocks must be consistently full with backlogs. But persistent backlogs degrade user experience, driving users to alternative solutions (Layer 2, other blockchains) and reducing long-term demand. The fee

market thus faces a tension between generating revenue and maintaining usability.

Academic research has explored these dynamics in depth. Brown, Chiu, and Koepl²² used the SegWit upgrade to study fee market behavior through a calibrated model counterfactual. They found that SegWit's capacity increase reduced fee revenue by approximately 70% compared to the counterfactual without it. This suggests that capacity improvements, while beneficial for users, directly undermine the fee market's ability to generate revenue. The authors concluded that "large sustained price increases are required to keep mining rewards constant in the long run," meaning that Bitcoin must appreciate faster than capacity improvements reduce fees. This creates a dependency on perpetual price appreciation that may not be sustainable.

Figure 8: Fee Revenue Volatility vs BTC Price Volatility. Orange shows the annualised standard deviation of daily percentage changes in dollar fee revenue; blue shows the same measure for Bitcoin's price, both over rolling 30-day windows. Vertical dashed lines mark halvings. Data through 4 October 2026: Coin Metrics²¹.

Fee Revenue Volatility: The Instability Problem



Empirical Evidence from Halvings

Each halving provides a natural experiment in how the network responds to reduced subsidies. While past halvings have not caused security crises, examining them reveals important patterns and potential warning signs.

The 2012 halving occurred when Bitcoin was still a niche technology with minimal economic value at stake. Mining was done primarily by hobbyists using GPUs, and the network hashrate was a tiny fraction of current levels. The halving passed without incident, but provides little insight into how a mature network would respond.

The 2016 halving was the first to occur with significant economic stakes. Bitcoin's price was approximately \$650, giving the network a market cap of around \$10 billion. Mining had professionalized with the introduction of ASICs. The halving was

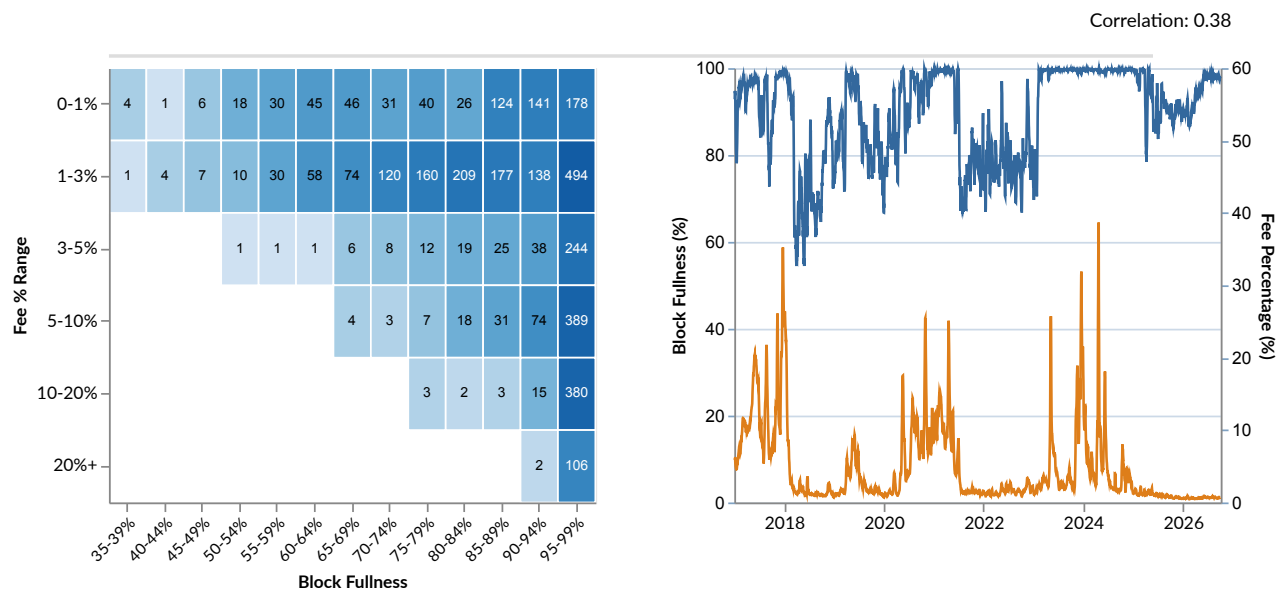
followed by a price rally that more than offset the subsidy reduction in fiat terms, and hashrate continued growing.

The 2020 halving occurred during the COVID-19 pandemic and was followed by a bull market that took Bitcoin from approximately \$9,000 to over \$60,000. Miner revenue in USD terms increased despite the halving. This experience reinforced the narrative that price appreciation would always compensate for subsidy reductions.

The 2024 halving provides the most relevant data for assessing future security budget dynamics. Unlike previous halvings, it occurred with Bitcoin already at relatively high prices (\$63,000-\$70,000 range), limiting the room for further appreciation. It also coincided with the launch of the Runes protocol, creating an unusual demand shock for block space.

Figure 9: Block Fullness vs Fee Dynamics. Fullness is daily mean block weight divided by the four-million-weight-unit limit. High fee shares cluster near capacity, but many near-full observations still have low fee shares. Daily observations from 1 January 2017 through 4 October 2026. Data source: Coin Metrics²¹.

Block Fullness vs Fee Dynamics: Congestion-Driven Revenue



Block 840,000, the April 2024 halving block, generated 37.6 BTC in fees (about \$2.4 million), or roughly 92% of its total reward. In Coin Metrics' daily observation for 20 April 2024, fees accounted for 74.8% of miner revenue and fees per recorded transaction averaged about \$124²¹. Around the launch, fees exceeded the new 3.125 BTC subsidy for 104 consecutive blocks.

This demonstrated that demand-driven fee spikes can offset subsidy reductions. For a brief period, Bitcoin operated in something approaching a fee-dominant regime, and the network continued functioning normally. No fee sniping, undercutting, or other predicted instabilities emerged.

The daily mean fee fell to about \$34 on 21 April 2024, around 73% below the preceding day's value, and to about \$4.5 by 4 May²¹.

SegWit and Runes

These two events illustrate the tensions in Bitcoin's fee market:

SegWit (2017) expanded usable block space. Brown, Chiu, and Koepl's calibrated model estimates fee revenue about 70% below its counterfactual without the upgrade²².

Runes (2024) introduced a new token protocol at the halving. The launch generated a burst of demand for block space, followed by a decline in fees as that demand subsided.

These examples show how both capacity and transaction demand influence the fees miners receive.

The Runes-driven fee spike reflected demand around the launch of a new token protocol. Ordinals inscriptions and BRC-20 use witness data, while Runes encodes its token instructions in OP_RETURN outputs²³. The 2023 inscription wave expanded this use of block space; earlier token systems, including Omni/Mastercoin and Counterparty, predate it^{24,25}. These uses generate fees when users compete for inclusion, with the duration of that demand determining their contribution to miner income.

Mining activity continued after the subsidy reduction. Coin Metrics’ daily estimate of network hashrate exceeded 1 ZH/s (1,000 EH/s) in April 2025²¹. Part IV examines operators’ responses, including efficiency investment, energy arrangements and diversification into other services.

Mining Economics and Profitability

The security budget manifests as miner profitability. If mining is profitable, miners will provide hashrate; if it becomes unprofitable, they will exit. Understanding the economics of mining, and how they change with the security budget, is essential for assessing long-term sustainability.

Hashprice measures miner revenue per unit of hashrate, typically expressed as USD per petahash per second per day (USD/PH/s/day). This metric captures the economic return to mining investment and serves as a leading indicator of miner behavior. When hashprice is high, mining is profitable and hashrate grows; when it falls, marginal miners exit, a free-entry dynamic that competes marginal mining

Figure 10: Hashprice Components: Subsidy vs Fees (2015–2026). Both axes show daily revenue per PH/s, labelled USD/PH/day; the lines use 30-day centred moving averages. The blue line (left axis) shows subsidy income per unit of hashrate, which depends on the subsidy per block, Bitcoin’s price and network hashrate. The orange line (right axis) shows fee income per unit of hashrate, which remains volatile and smaller. Data through 4 October 2026: Coin Metrics²¹.

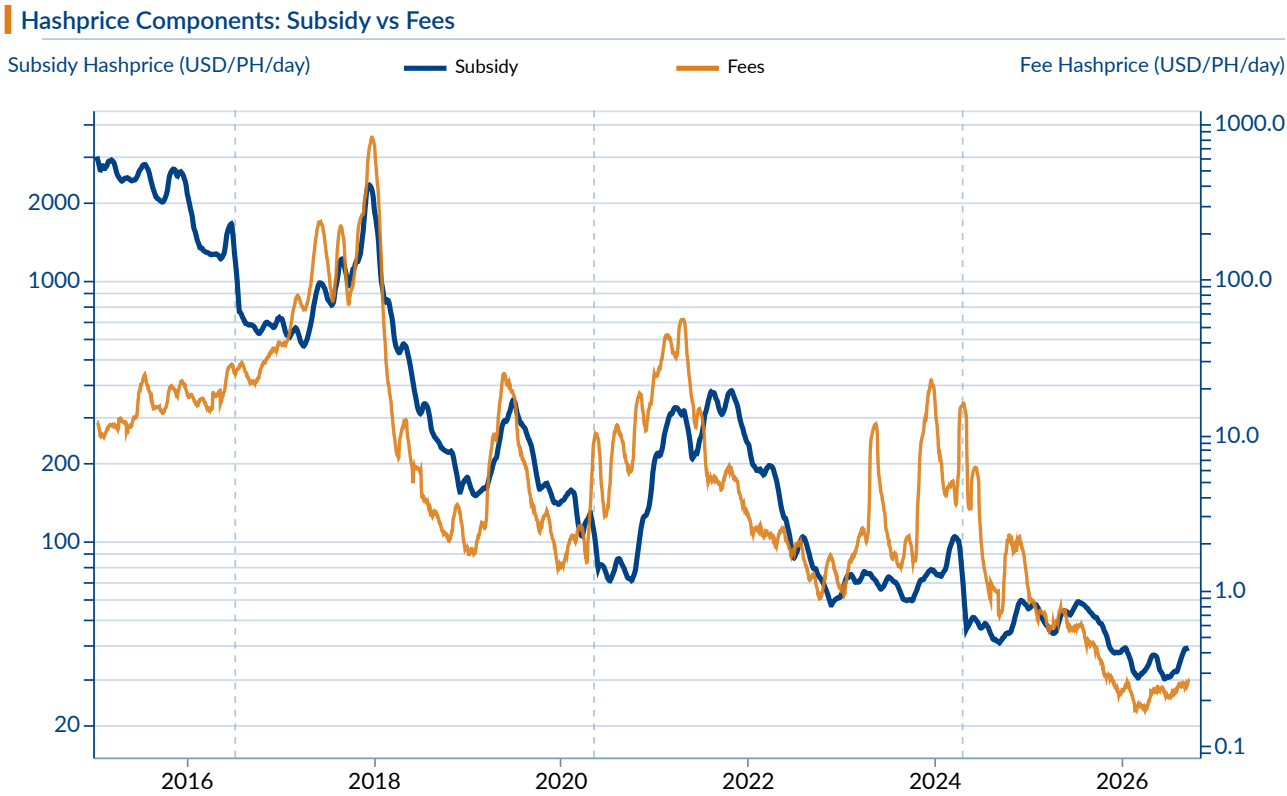
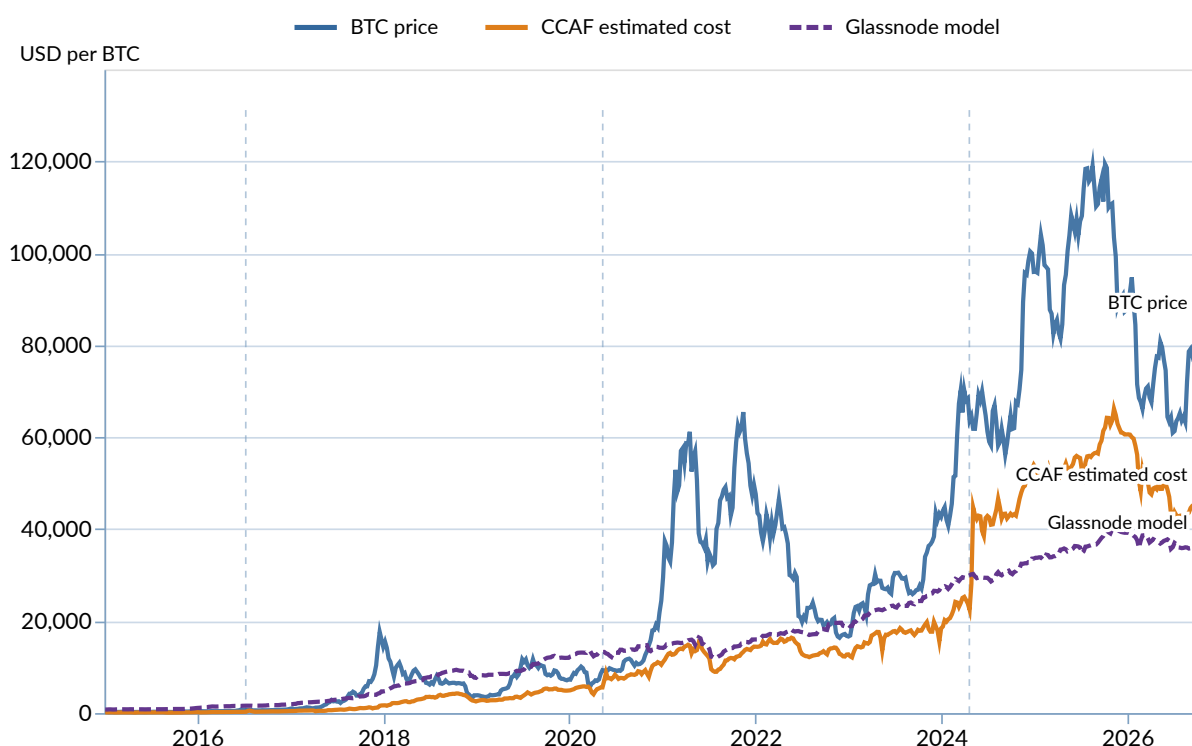


Figure 11: Bitcoin Price and Estimated Mining Costs (2015–2026). All series use USD per BTC. Blue shows BTC price; orange shows CCAF's central CBECI estimate of the cost to mine one BTC, assuming \$0.05/kWh; purple dashed shows Glassnode's Difficulty Regression Price. CCAF excludes equipment and non-electricity operating costs; Glassnode is a regression-based proxy with no itemised cost coverage. Weekly means through 4 October 2026. Sources: CCAF⁴; Glassnode²⁸; authors' implementation of Glassnode's model.

Bitcoin Price and Estimated Mining Costs



profits toward zero²⁶ (in practice, manufacturing capacity, power availability, and regulatory shocks slow this adjustment). Figure 10 separates daily income per unit of hashrate into subsidy and transaction-fee components.

The halving schedule fixes the subsidy in BTC per block. Dollar income per unit of hashrate also changes with Bitcoin's price and the amount of hashrate competing for rewards. Fee income remains volatile, with no clear upward trend in the period shown.

Miner profitability depends on revenue and the cost of hardware, electricity, cooling, facilities and labour. In CCAF's 2025 mining-industry survey, direct electricity accounted for 81.1% of cash operating expenditure, excluding non-cash expenses²⁷.

Glassnode estimates its per-BTC production-cost proxy using a log–log regression between market capitalisation and difficulty²⁸. Figure 11 compares it with CCAF's estimate and Bitcoin's price. CCAF assumes a constant \$0.05/kWh and excludes equipment and non-electricity operating costs. CCAF divides costs by seven-day average BTC rewards from subsidies and fees⁴. Neither price–cost gap represents net profit. With expenditure and block production unchanged, a halving doubles the cost per newly issued BTC.

CCAF survey respondents reported direct electricity prices of \$0.020–\$0.065/kWh, with a median of \$0.045/kWh; the median all-in cash operating cost was \$0.0555/kWh²⁷. A subsidy-only calculation using the 4 October 2026 Bitcoin price and network

hashrate gives an electricity-breakeven rate of about \$0.072/kWh for a 24 J/TH machine.^a This calculation covers electricity. Miners also pay for equipment, premises, staff and other operations.

Subsidy Income and Fee Revenue

Miners' dollar income depends on the subsidy per block, Bitcoin's price and transaction fees. Figure 12 compares historical income with subsidy income after future halvings at three price levels. We use narrow

^aInputs: Bitcoin price \$86,521; network hashrate 943 EH/s; 3.125 BTC per block; 144 blocks per day. Subsidy income is about \$0.0413/TH/day. A 24 J/TH machine uses 0.576 kWh per TH/day, giving an electricity-breakeven rate of about \$0.072/kWh.

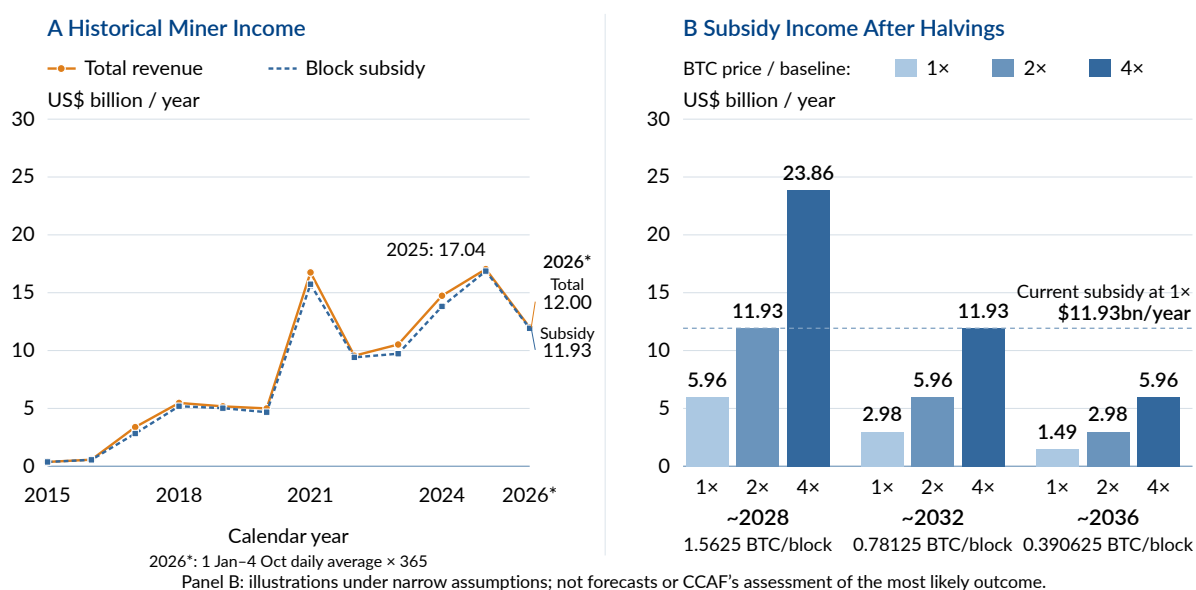
assumptions to illustrate the subsidy arithmetic. CCAF does not present these scenarios as forecasts or as its assessment of the most likely outcome.

At the 2026 average price, miners would receive approximately \$5.96 billion a year in subsidy income after the 2028 halving, \$2.98 billion after 2032 and \$1.49 billion after 2036. A price twice the baseline offsets one halving; a price four times the baseline offsets two. Across the historical halving-era averages in Figure 5, price appreciation more than offset the reductions in BTC issuance, raising dollar subsidy income.

To maintain the dollar value of the subsidy through each halving, Bitcoin's price would need to double, equivalent to about 19% annual growth over a four-year interval. If dollar subsidy income falls, miners would need more fee income to maintain the same total dollar revenue. Price appreciation and fee

Figure 12: Bitcoin Miner Income: History and Price Scenarios. Panel B contains illustrations under narrow assumptions, not forecasts or CCAF's assessment of the most likely outcome. Panel A reports mean daily revenue and subsidy income multiplied by 365; 2026* annualises observations from 1 January–4 October. Panel B halves that 2026* subsidy income for each of the next three halvings, at one, two and four times the 2026 average Bitcoin price of \$73,180. The dashed line marks the 2026* subsidy income carried forward at 3.125 BTC per block. Data source: Coin Metrics²¹; authors' calculations.

Bitcoin Miner Income: History and Price Scenarios



growth can contribute together; Table 2 sets out alternative combinations of price paths and fee shares.

Lyn Alden's fee-based security model²⁹ provides a framework for relating transaction fees and volumes to miner revenue. At \$10 per transaction with 100 million annual transactions, Bitcoin would generate approximately \$1 billion in annual fee revenue. At \$40 per transaction, approximately \$4 billion. At \$100 per transaction, approximately \$10 billion, comparable to current total miner revenue.

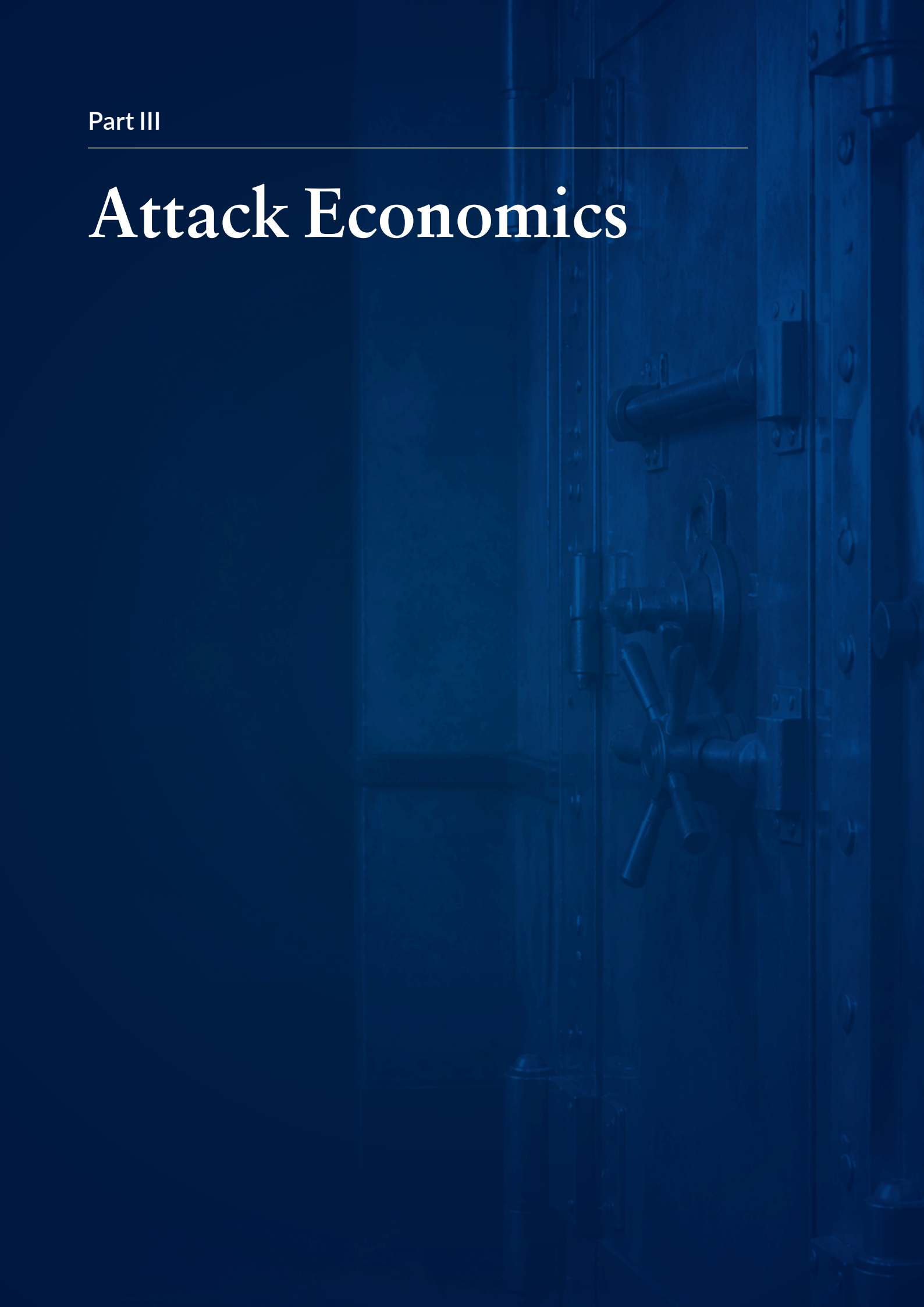
However, high per-transaction fees create their own problems. At \$100 per transaction, Bitcoin becomes economically unsuitable for transfers below approximately \$5,000-10,000 (assuming users are willing to pay 1-2% in fees). This would push smaller transactions to Layer 2 solutions or alternative blockchains, reducing demand for base layer block space and undermining the fee market.

The subsidy-replacement arithmetic illustrated by Budget.Day³⁰ depends on assumed throughput. At 3,000 transactions per block, replacing a 3.125 BTC subsidy requires an average fee of 0.00104167 BTC, or about \$76 at Figure 12's \$73,180 average price. A hypothetical 500 transactions per second, at a ten-minute average block interval, would require about \$0.76 per transaction at that price. Each calculation holds its specified volume fixed; lower volume raises the required average fee.

Users may reduce on-chain activity or move to other payment methods when fees rise. Miners' fee revenue depends on both the fee per transaction and the number of transactions they include in blocks.

Part III

Attack Economics



Attack feasibility depends on access to hashpower; profitability also depends on operating costs and rewards.

Understanding the security budget requires understanding what it protects against. As subsidies decline and the security budget potentially shrinks, various attack vectors become more economically viable. This section examines the economics of attacks, the theoretical vulnerabilities that emerge in fee-dominant regimes, and the empirical evidence for whether these threats have materialized.

Attack Cost Economics

The primary threat to Bitcoin is the 51% attack: an attacker who controls majority hashrate can rewrite transaction history, enabling double-spends and potentially destroying confidence in the network. This section examines the economics of such attacks and how they change as subsidies decline.

Coin Metrics' February 2024 "Breaking BFT" analysis³¹ introduced Total Cost to Attack (TCA), estimating \$5–20 billion under alternative ASIC acquisition and manufacturing scenarios. Its Bitcoin calculation combines equipment expenditure with one hour of electricity and considers ASIC supply constraints. The estimates describe the network conditions and cost assumptions used in that study.

Controlling existing machines and adding new machines require different capacity calculations. An attacker acquiring 51% of an existing fleet leaves 49% honest; an attacker adding capacity to an unchanged honest network needs 51/49 times that network's hashrate to reach a 51% combined share. The acquisition benchmark used in Figure 13, Figure 15 and the SBHI applies the latter case, at fixed equipment and power prices. It gives \$24.58 billion for the 4 October 2026 observation. Appendix A.1 lists the inputs and cost categories for each estimate. Harvey³² identifies a separate potential incentive: an attacker could establish short positions to profit from a price fall caused by disruption.

Gans and Halaburda³³ compare attacking with continued honest mining, accounting for operating costs, forgone profits and mining rewards collected on

the attacking chain. They show that, under conditions in their model, higher fee income can make a majority reorganisation profitable even without double-spending. The hardware and power needed to carry out the attack remain constraints on feasibility. An acquisition budget therefore differs from the net economic cost of attacking.

These estimates reveal several important dynamics:

Hardware availability constrains acquisition. Crypto51³⁴ reports a near-zero NiceHash-rentable share for Bitcoin, so that marketplace offers little capacity relative to the Bitcoin network. Acquiring or controlling a large ASIC fleet also requires access to machines, sites and power. Equipment supply, construction and deployment times affect the resources an external attacker could assemble; rental availability alone does not settle the feasibility of other routes.

Attack costs scale with hashrate, not with value protected. The cost to attack Bitcoin depends on how much hashrate honest miners provide, which in turn depends on miner revenue (the security budget). If the security budget declines, hashrate will decline, though less than proportionally: the least efficient miners exit first, and they contribute disproportionately little hashrate per revenue dollar. This creates a potential death spiral in which a lower security budget causes hashrate to decline, reducing attack costs, undermining confidence, depressing prices, and further shrinking the security budget. However, Bitcoin has shown resilience against such cascades: during China's 2021 mining ban, hashrate dropped over 50% within weeks, yet no spiral materialized. Prices recovered and hashrate was restored within months as miners relocated. This suggests the network may have stronger self-correcting properties than the theoretical spiral implies, at least under current conditions.

The derivatives market complicates but doesn't change the calculus. While Harvey notes that combining a 51% attack with large short positions could theoretically offset costs, practical barriers are high. Opening a \$20 billion+ short position would move

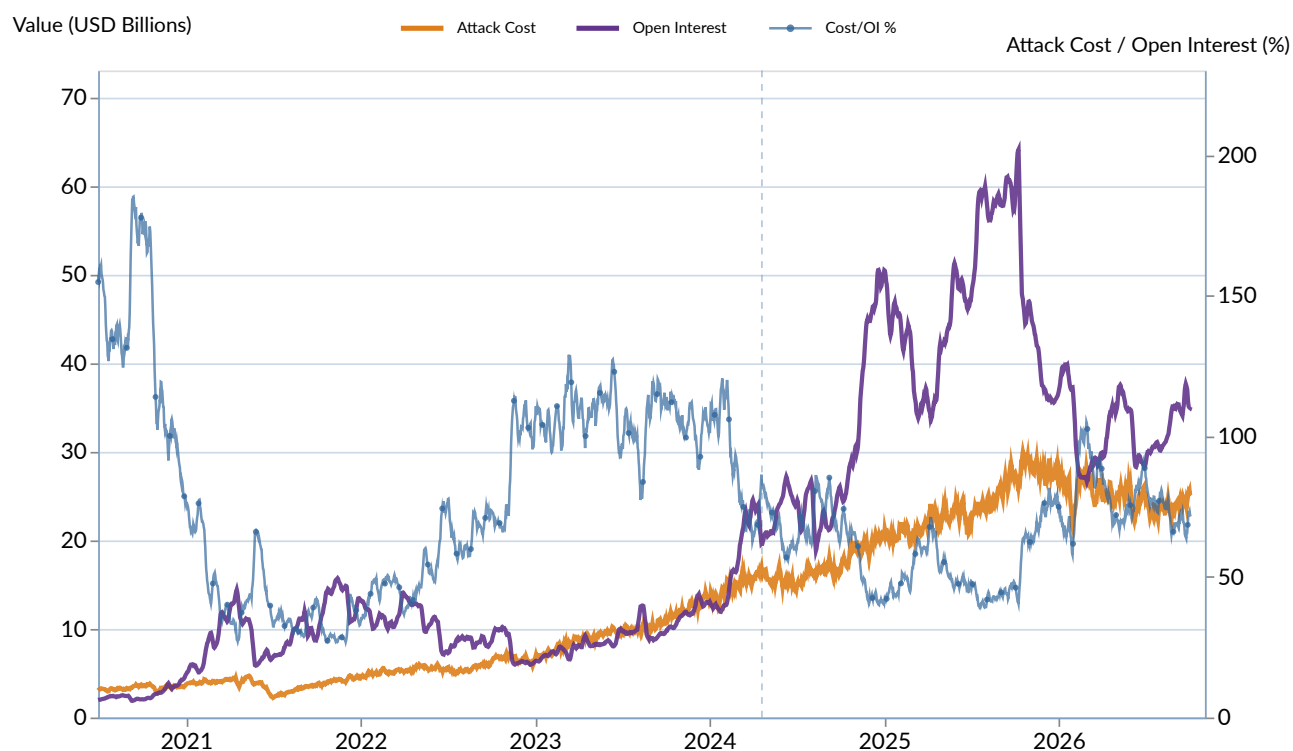
markets against the attacker before execution. Exchange surveillance systems would likely detect unusual activity. Counterparty risk means the attacker might not be able to collect on their shorts if exchanges halt trading during an attack; more fundamentally, the counterparties to a short of that size are by construction leveraged longs, many of whom would be unable to pay in precisely the state of the world where the attack succeeds. There is a further irony: the short positions themselves must be established on venues with account records, position limits, and market-abuse law, so on this attack path a system built to operate outside traditional rule of law is partially protected by it. Budish's analysis makes the mirror-image point about external legal punishment of attackers, that relying on it begs the question of what is accomplished if permissionless consensus

ultimately depends on traditional rule of law¹⁵. Attack hardware costs are also state-dependent: in a healthy market an attacker bids against constrained ASIC supply and pays a premium, while in a miner-capitulation scenario the same hardware sells at fire-sale discounts, exactly when the concerns of this report are most acute.

Figure 13 compares a fixed-unit-price acquisition benchmark with the scale of open interest. The cost/open-interest ratio varies across the period, including a low in 2021 and subsequent recovery. Open interest describes outstanding market positions; an attacker's proceeds depend on the position they can build, its entry price, funding costs and whether counterparties can settle after disruption.

Figure 13: Acquisition Benchmark and Bitcoin Perpetual-Futures Open Interest (2020–2026). Orange shows equipment and 24-hour power expenditure for new capacity sufficient to hold 51% of the combined network, using the fixed unit prices in Appendix A.1. Purple shows perpetual-futures open interest across the covered exchanges. The blue line and points (right axis) show benchmark cost as a percentage of open interest. 7-day trailing means through 4 October 2026. Data sources: Coin Metrics²¹; Glassnode³⁵.

Acquisition Benchmark and Bitcoin Perpetual Open Interest



Derivatives can add an incentive for market disruption alongside double-spending. Assessing its size requires a model of feasible attacker positions, market impact, funding costs and settlement constraints. These are priorities for the monitoring agenda in Part V.

Eric Budish's "flow versus stock" framework¹⁵, introduced in Part I, provides the analytical foundation for these dynamics: ongoing payments to miners must be large relative to one-time attack benefits, and when hardware is specialized and non-repurposable, attackers face "stock versus stock" economics in which their own investment burns with the network's value.

However, this protection weakens as the security budget declines. If mining becomes unprofitable, miners will exit, reducing the stock of hardware with aligned incentives. New entrants will be reluctant to invest in ASICs if the revenue outlook is uncertain. The result could be a smaller, more concentrated mining industry with less total capital at stake, and therefore less to lose from an attack.

Fee-Based Instabilities

Beyond 51% attacks, several other attack vectors become more relevant as subsidies decline and fees constitute a larger share of miner revenue. These "fee-based instabilities" were first identified by

Carlsten et al.¹⁰ and have been the subject of academic research. A scoping note applies throughout this section: the Carlsten et al. results hold literally when the block subsidy is zero; in the intermediate regime where fees merely dominate a small remaining subsidy, they are qualitative rather than quantitative.

Selfish Mining

Selfish mining involves strategically withholding blocks to gain disproportionate rewards. In Eyal and Sirer's fixed-reward model⁹, common tie-breaking assumptions give profitability thresholds of 25–33% of network hashrate after difficulty adjusts. Carlsten et al.¹⁰ show how fee variability changes withholding incentives in a fee-only setting. Research using reinforcement learning³⁶ finds that volatile rewards can also permit profits in the first epoch, before difficulty adjusts.

A selfish miner keeps a discovered block private and starts mining on top of it. If an honest miner finds a competing block, the selfish miner can release the private block to create a tie. After the tie, each hash attempt is independent; unsuccessful earlier attempts provide no progress toward the next block. An additional block already found in private, or honest miners choosing the attacker's branch during the tie, can provide an advantage.

Withholding can slow the growth of the accepted chain, so a larger reward share need not initially

What is a 51% attack?

A 51% attack happens when someone gains control of more than half of Bitcoin's mining power. With majority control, they can rewrite recent transaction history, letting them spend the same bitcoin twice.

The attacker pays a recipient on the public chain and privately mines a branch containing a conflicting transaction that spends the same inputs. If the private branch accumulates more work, nodes adopt it and the conflicting spend invalidates the recipient's payment.

What a 51% attacker cannot do: steal coins from other people's addresses or change Bitcoin's rules, which are enforced by every node. And an attack that destroyed confidence would crash the price, destroying the value of the attacker's own hardware, one reason concentrated hashrate has never translated into an attack in practice.

The good news: attacking Bitcoin would cost billions of dollars in specialized hardware that takes months to acquire. The bad news: as mining rewards shrink, so does the cost of attack.

What is selfish mining?

A selfish miner withholds discovered blocks and chooses when to publish them based on the private branch's lead and the blocks other miners find.

Publication can create a tied race or replace a shorter branch. Blocks excluded from the eventual main chain earn no rewards. By influencing which blocks survive, the miner seeks a larger reward share than their share of hashrate. Profitability depends on branch support, reward variability and difficulty adjustment.

increase BTC earned per day. In the fixed-reward model, a subsequent difficulty reduction can make the strategy profitable above its hashrate threshold⁷. Volatile fees change the rewards available from withholding and can permit profits before the first difficulty adjustment³⁶.

Fee Sniping

Fee sniping occurs when miners attempt to re-mine previous blocks to steal their transaction fees rather than extending the chain tip. This becomes attractive when a recently mined block contains unusually high fees¹⁰.

The attack works as follows: suppose a block is mined containing 5 BTC in transaction fees (unusually high). Instead of building on top of this block, a miner might attempt to mine a competing block at the same height, including the same high-fee transactions but with their own coinbase transaction, effectively stealing the fees from the original block finder. If successful, they would earn the block subsidy plus the high fees, rather than just the subsidy from extending the chain normally.

The incentive depends on the fees available in the competing block, the rewards from extending the tip and the probability that the fork succeeds. A block subsidy raises the opportunity cost of a failed fork; it does not make a subsidy payment guaranteed. Carlsten et al. also identify a separate incentive for “mining gaps” in a fee-only setting: miners may pause after a block clears the mempool until enough new fees accumulate to cover operating costs.

Undercutting Attacks

Undercutting attacks involve miners deliberately forking the chain while leaving high-fee transactions unclaimed, incentivizing other miners to build on their fork. This strategy can be profitable even for miners with small hashrate shares when fee variance is high³⁷.

The mechanism is subtle: a miner creates a block that excludes high-fee transactions, deliberately leaving them in the mempool. Other miners, seeing these high-fee transactions available, are incentivized to build on the undercutting miner's block rather than competing blocks, because they can claim the high fees. This gives the undercutting miner's block a better chance of being extended, even though it contains lower fees itself.

Gong et al.³⁷ analyzed the conditions under which undercutting is profitable, finding that Carlsten et al.'s original analysis “inaccurately inflated profitability.” Their refined model suggests undercutting requires >40% hashrate to be reliably profitable, and is unprofitable with 50% honest miners.

Transaction Censorship

Transaction censorship involves refusing to include certain transactions in blocks, either for regulatory compliance, competitive advantage, or political reasons¹¹. While not directly related to the security budget, censorship becomes more concerning as mining centralizes, a trend that may accelerate as margins compress and smaller miners exit.

Several incidents have demonstrated the feasibility of transaction censorship:

- MARA announced an “OFAC-compliant” mining pool in late March 2021 and began filtering transactions involving sanctioned addresses on 1

May 2021. Community backlash forced a reversal by the end of that month.

- F2Pool was discovered filtering OFAC-sanctioned transactions in late 2023, also reversing course after public exposure.

These incidents demonstrate both the feasibility of transaction censorship and the community's resistance to it. However, they also reveal that a non-trivial fraction of hashrate is controlled by entities that might comply with government mandates.

Empirical Evidence: Theory vs Reality

A critical question for the security budget debate is whether the theoretical attack vectors identified in academic literature have manifested in practice. Our analysis examines the empirical evidence for fee sniping, selfish mining, and other predicted instabilities.

Fee Sniping Evidence

For *fee sniping* (defined above), detection would involve observing miners building on blocks other than the chain tip when the previous block contained unusually high fees.

No fee-sniping incidents have been reported on Bitcoin mainnet, and our review of periods of high fee variance from 2016-2025 found no chain reorganizations suggestive of sniping attempts. Two limitations apply to any such analysis: orphaned blocks are not recorded in canonical chain data, so stale-rate signatures are only observable through network monitoring, and the difficulty adjustment absorbs modest changes in mining behavior, limiting the statistical power of block-timing tests.

This null result is consistent with multiple explanations:

- Current subsidy levels still dominate, making sniping unprofitable
- Anti-fee-sniping protections (nLockTime) deter attempts
- Miners are not purely rational profit-maximizers

- The theoretical models overestimate sniping profitability

Distinguishing between these explanations is difficult with observational data. The absence of sniping does not prove it won't occur as subsidies decline further.

Selfish Mining Evidence

Selfish mining involves strategically withholding blocks to gain disproportionate rewards. Li et al.³⁸ developed statistical methods to detect selfish mining from blockchain data. Their analysis found evidence of selfish mining on Monacoin and Bitcoin Cash, but *not on Bitcoin mainnet or Litecoin*.

This finding suggests that Bitcoin's larger hashrate and more professional mining industry may provide protection beyond what theoretical models predict. However, it also means we lack empirical data on how Bitcoin would behave under conditions where selfish mining becomes more attractive.

Undercutting Evidence

We find no evidence of undercutting attacks on Bitcoin mainnet. Gong et al.'s theoretical refinements (discussed above) suggest the attack is less practical than originally feared, at least under current conditions.

Mining Gaps Evidence

Mining gaps, periods where miners pause after blocks are found waiting for fees to accumulate, were predicted by Carlsten et al. as a consequence of fee-dominant mining. A Manifold prediction market specifically tracked whether mining gaps would appear within one month of the April 2024 halving; it resolved "NO."

Our analysis of inter-block times around the 2024 halving finds no evidence of systematic mining gaps: block times remained consistent with the expected Poisson distribution. This test has limited power, since the difficulty adjustment re-anchors average block times each epoch, but the 104-block fee-dominant window itself, the only such regime yet observed, produced no visible timing anomalies, and miners continued operating normally despite the subsidy reduction.

Table 1: Economic conditions and evidence for the attack mechanisms reviewed in Part III.

Attack Vector	Economic Preconditions	Basis Discussed in Part III	Potential Effect
51% double-spend	Majority control and attack benefits exceeding costs	Acquisition models and attacks on smaller PoW chains	Payment reversals
Derivatives-amplified attack	A position that can be built and settled profitably	Financial-incentive analysis ³²	Trading losses and price disruption
Fee sniping	A recent block with a sufficiently large fee prize	Fee-based reward models ¹⁰	Chain reorganisations
Selfish mining	Hashrate above a strategy-dependent profitability threshold	Fixed-reward and volatile-fee models ^{9,36}	Reward redistribution
Transaction censorship	Template control and incentives to filter transactions	Pool-filtering episodes described in the text	Exclusion or delay of transactions
Mining gaps	Expected rewards below marginal running costs	Fee-only reward models ¹⁰	Confirmation delays

Summary of Attack Evidence

Despite nearly a decade since Carlsten et al.'s paper, none of the predicted fee-based instabilities have been observed on Bitcoin mainnet. This could mean the models are wrong, that current subsidy levels still provide adequate protection, or that miners behave differently than the models assume. The lack of empirical evidence is reassuring but does not guarantee future safety.

Table 1 summarises the economic preconditions, evidence and potential effects of the attack mechanisms reviewed in this section.

Template control is central to censorship, while derivatives-linked incentives depend on feasible positions and settlement. Monitoring mining structure alongside financial-market exposure helps distinguish these mechanisms.

Mining Centralization Risks

The security budget problem intersects with concerns about mining centralization. Even if the total security budget remains adequate, its effectiveness depends on hashrate being distributed across many independent actors. Concentrated mining creates potential coordination points for attacks or censorship.

Figure 14 shows historical pool shares from 2020 to 2026. Over the 30 days ending 4 October 2026, Foundry USA accounts for 25.3% of blocks, AntPool for 20.3% and F2Pool for 15.2%. Together the top three account for 60.8%, and the top six for 83%³⁹.

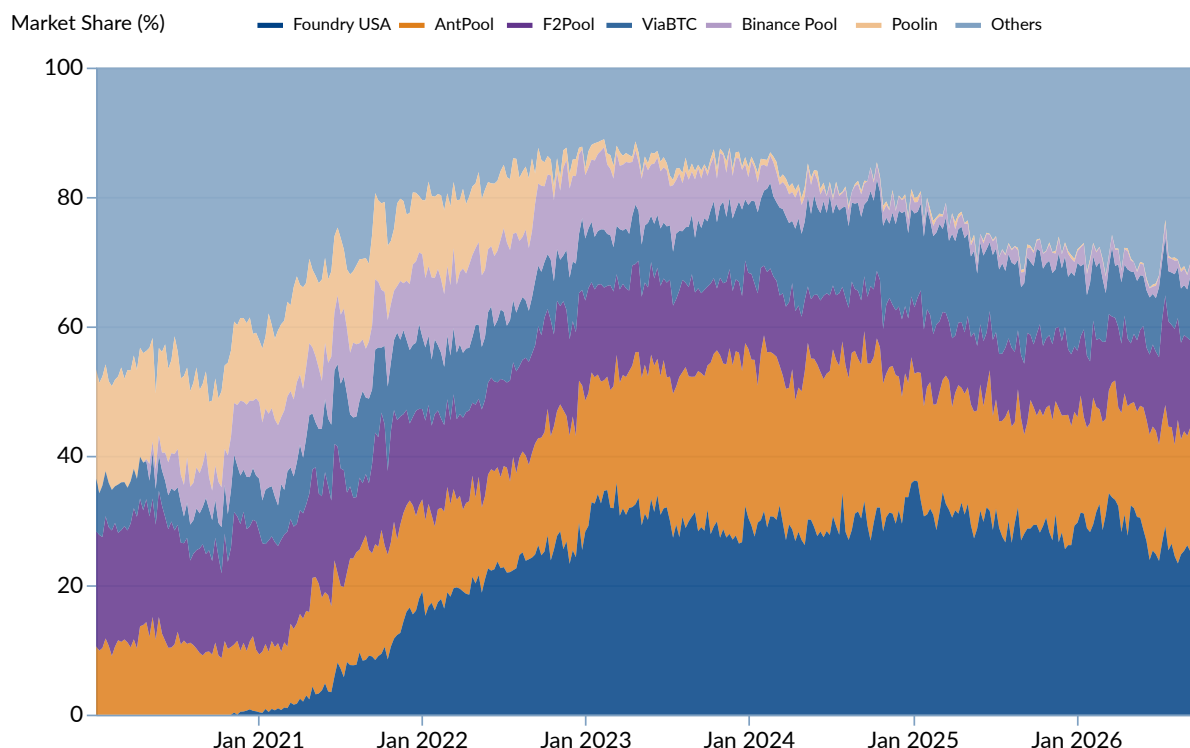
b10c's proxy-pooling analysis documents pools sharing block templates, so coinbase tags can overstate the number of independent template producers¹⁶. Acting across several entities requires coordination; selfish-mining profitability thresholds apply to a coordinated strategy rather than the sum of independent pool shares.

Geographic concentration adds another dimension of risk⁴⁰. The Cambridge Mining Map estimated the US share at 37.8% in January 2022⁴¹. Physical mining location, pool incorporation and regulatory jurisdiction measure different exposures. A government can impose requirements on miners and pool operators within its jurisdiction, including transaction-filtering rules.

The security budget problem exacerbates centralization risks. As margins compress, smaller miners exit, and the industry consolidates around the most efficient operators. These tend to be large, well-capitalized companies with significant regulatory exposure. Figure 15 tracks the network security ratio over time: miner revenue relative to market capitalization has stepped down with each halving era, while the attack-cost ratio has fluctuated without a clear trend and currently sits near the upper end of

Figure 14: Bitcoin Mining Pool Market Share (2020–2026). The stacked areas show weekly shares of blocks attributed to major pools through 4 October 2026. Shares vary over time, with Foundry USA becoming the largest labelled pool in the series. Pool membership and control of block templates are distinct, as discussed in the text. Data source: Mempool.space³⁹.

Bitcoin Mining Pool Market Share



its historical range. The result could be a mining industry that is both smaller (less total hashrate) and

more concentrated (fewer independent actors), a worst-case scenario for network security.

What was the Great Mining Migration?

In May 2021, China banned Bitcoin mining. Overnight, more than half of the world's mining capacity had to find a new home.

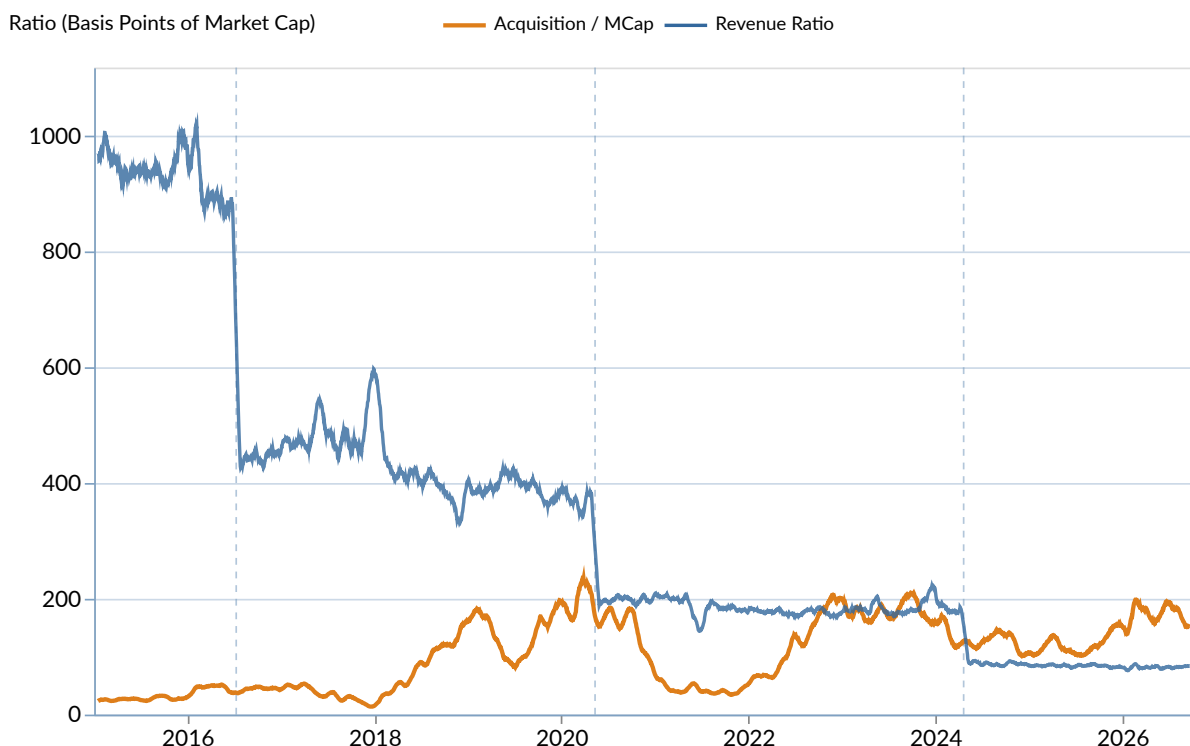
Miners scrambled to relocate equipment. Shipping containers full of ASICs crossed oceans to the United States, Kazakhstan, Russia, and beyond. Some operations moved within weeks; others took months to rebuild.

The result was a fundamental reshaping of Bitcoin's geography. The US went from hosting about 4% of global hashrate to nearly 40%. Kazakhstan briefly surged to 18% before its own grid and regulatory problems pushed miners out again.

The migration proved Bitcoin's resilience, as hashrate recovered within months, but also revealed how quickly the mining landscape can change when governments act.

Figure 15: Acquisition and Revenue Ratios to Market Capitalisation (2015–2026). Orange shows the external-capacity acquisition benchmark from Appendix A.1 divided by market capitalisation. Blue shows annualised daily miner revenue divided by market capitalisation. Both series use 30-day centred moving averages and express ratios in basis points. Data through 4 October 2026: Coin Metrics²¹.

Acquisition and Revenue Ratios to Market Capitalisation



Protocols that let miners construct their own block templates can distribute transaction selection even when reward pooling remains concentrated. Stratum V2's Job Declaration component and OCEAN's DATUM provide examples^{42,43}. Deploying Stratum V2's transport layer alone does not transfer template selection to miners; the pool and miner must support the relevant template-selection functions. Adoption therefore depends on implementation, pool support and miners' ability to operate the necessary software.

Lessons from Other Chains

Examining other proof-of-work blockchains provides context for Bitcoin's security budget dynamics. While no chain has successfully transitioned to fee-dominant security, several have experienced attacks

that illuminate the risks of inadequate security budgets.

Ethereum Classic

Ethereum Classic suffered multiple 51% attacks in 2019–2020, with attackers stealing approximately \$9 million across several incidents. The attacks were enabled by ETC's low hashrate relative to rental markets, as approximately 98% of ETC's hashrate was available on NiceHash, allowing attackers to rent majority hashrate for hours at minimal cost.

The ETC attacks demonstrate what happens when the security budget is inadequate relative to the value at stake. Attack costs of approximately \$200,000 yielded returns of \$5.6 million, a 2,800% ROI. This economic imbalance made attacks inevitable.

Bitcoin's situation differs in important ways. Available rental capacity limits that attack route, while the external-acquisition benchmarks discussed here run to billions of dollars. The ETC experience illustrates how access to hashpower and potential attack proceeds can affect incentives.

Bitcoin Gold and Verge

Bitcoin Gold and *Verge* experienced similar attacks, with losses totaling tens of millions of dollars. These chains shared ETC's vulnerability: low hashrate, rentable algorithms, and insufficient exchange confirmation requirements.

Litecoin

Litecoin provides a more relevant comparison as a major PoW chain that has not been successfully attacked. Litecoin's security comes from being the dominant Scrypt chain (similar to Bitcoin's dominance of SHA-256) and having sufficient hashrate to make attacks expensive. However, Litecoin's fee market is even less developed than Bitcoin's, suggesting it faces similar long-term challenges.

Monero's Tail Emission

Monero's tail emission provides one example of permanent issuance in a PoW chain. Since June 2022, Monero has maintained a base subsidy of 0.6 XMR per block. Dogecoin also has permanent issuance, at 10,000 DOGE per block⁴⁴. The record is no longer unblemished, however: in August 2025 the Qubic pool briefly attracted a majority of Monero's hashrate by paying miners in an external token, producing a six-block reorganisation. Tail emission did not prevent the episode, and its mechanism, auxiliary revenue outbidding native rewards, is the same channel this report discusses under merged mining in Part IV.

Monero's experience suggests that a guaranteed revenue floor keeps miners engaged but does not by itself prevent majority-hashrate events. And Monero's community culture differs from Bitcoin's, with regular hard forks and greater willingness to modify protocol parameters. Whether Bitcoin's community could achieve similar consensus for monetary policy changes remains doubtful.

Dogecoin

Dogecoin combines a permanent subsidy of 10,000 DOGE per block with merged mining alongside Litecoin, which it adopted in 2014^{44,45}. Bitcoin, as the dominant SHA-256 chain, has no larger network to merge into; the escape route that saved Dogecoin is structurally unavailable to it.

Part IV

Options Under Debate and Their Trade-offs



There are ideas to fix this, from changing Bitcoin’s code to letting markets adapt. Each comes with trade-offs.

The security budget challenge has not gone unnoticed. Researchers, developers, and industry participants have proposed various solutions, ranging from incremental protocol improvements to fundamental changes in Bitcoin’s monetary policy. This section evaluates these proposals, assessing their technical feasibility, economic implications, and political viability within Bitcoin’s conservative governance culture.

The solutions can be broadly categorized into four groups: fee market optimizations that aim to increase revenue from existing demand; Layer 2 solutions that may either help or hurt base layer fees; protocol-level changes that would modify Bitcoin’s fundamental parameters; and market-based solutions that rely on external mechanisms to provide security. Each category involves distinct trade-offs and faces different adoption barriers.

Market-Based Approaches

Fee Market Optimizations

Fee-market improvements can make transaction relay, fee adjustment and block assembly more efficient. Their effect on total fee income depends on user demand and bidding behaviour.

Replace-by-Fee (RBF) allows users to increase fees on unconfirmed transactions, enabling more efficient price discovery in the fee market. BIP 125 introduced opt-in RBF in 2016, allowing transactions that explicitly signaled replaceability to be bumped. Bitcoin Core v28.0 (October 2024) made full RBF the default policy, allowing any transaction to be replaced regardless of signaling, and v29.0 (April 2025) removed the option to disable it.

Figure 16: Security-budget Options: Mechanisms and Feasibility. Filled dots indicate the authors’ qualitative assessment: three for high feasibility, two for moderate and one for low. Technical assessments reflect implementation maturity; adoption assessments reflect coordination and consensus requirements discussed in Part IV. The revenue column identifies each mechanism, while the last column distinguishes deployed options from changes requiring further adoption or consensus.

Security-budget Options: Mechanisms and Feasibility

OPTION	Technical Feasibility	Adoption / Consensus	Revenue Channel	Implementation
Fee Market Optimizations (RBF, CPFP, Cluster Mempool)	●●●	●●●	Fee selection	Deployed
Layer 2 (Lightning) (Channel settlement)	●●●	●●●	Demand-dependent	Deployed
Merged Mining (RSK and other auxiliary chains)	●●●	●●○	Auxiliary rewards	Project-specific
Block Size Increase (Contentious history)	●●●	●○○	Block-space demand	Consensus change
Tail Emission (Perpetual fixed reward)	●●○	●○○	Added issuance	Consensus change
Demurrage (Charge on holdings)	●●○	●○○	Holding charge	Consensus change

Full RBF lets users adjust their bids as conditions change. During congestion they can raise fees to seek faster confirmation; during quiet periods they can start with lower bids. The aggregate revenue effect depends on how users change those bids and on congestion.

Child Pays for Parent (CPFP) allows users to accelerate confirmation of stuck transactions by creating child transactions with high fees. Miners are incentivized to include both the parent (stuck) and child (high-fee) transactions because the combined fee rate makes the package attractive. This mechanism has been available since Bitcoin's early days but was formalized and improved in recent protocol updates.^b

Package Relay (BIP 331) extends CPFP by allowing nodes to relay and evaluate transactions as packages rather than individually. This is particularly important for Layer 2 protocols like Lightning Network, where pre-signed transactions may have fees that become inadequate by the time they need to be broadcast. Package relay enables fee bumping of these transactions without requiring protocol changes to Lightning itself.

TRUC Transactions (BIP 431), also known as “v3 transactions,” provide anti-pinning protections for Layer 2 protocols. Transaction pinning occurs when an attacker creates low-fee child transactions that prevent legitimate fee bumps from propagating. TRUC transactions limit the size and structure of transaction packages to prevent pinning attacks, making Lightning Network channels safer and more efficient.

Cluster Mempool groups related transactions for evaluation and block assembly. It shipped in Bitcoin Core 31.0 on 19 April 2026⁴⁶, replacing the earlier ancestor/descendant-limit design.

These changes improve how nodes handle transactions and how miners select paying packages. Aggregate fee revenue also depends on the demand for block space and the prices users bid.

^bTwo caveats to the pure-auction picture: transaction accelerators route out-of-band payments to miners over other rails, so measured on-chain fee levels slightly understate true miner compensation; and empirical work documents miners sometimes including lower-fee transactions while higher-fee ones wait, consistent with side payments or private order flow. Fee bidding remains predominantly competitive.

The SegWit counterfactual discussed in Part II²² provides a cautionary example: capacity improvements benefit users but can undermine the fee market's ability to generate revenue.

This creates a tension in Bitcoin's development: improvements that benefit users (lower fees, faster confirmation, better UX) may harm the security budget. The community has generally prioritized user experience, but this approach may not be sustainable as subsidies decline.

Covenant Proposals and New Block Space Demand

A less-discussed development is the family of “covenant” proposals, protocol upgrades that would enable new types of smart contracts on Bitcoin. Proposals such as OP_CTV (BIP 119), OP_VAULT, and OP_CAT would allow users to place conditions on how their bitcoin can be spent in future transactions, enabling use cases that are currently impossible or impractical.

From a security budget perspective, covenants matter because they could create entirely new categories of on-chain demand. Payment pools would allow hundreds of users to share a single UTXO, with on-chain transactions needed to enter, exit, or rebalance, generating sustained fee revenue. Vaults would create time-locked security mechanisms for large holdings, requiring on-chain transactions for both setup and withdrawal. Congestion control transactions would allow users to commit to future on-chain settlements, creating predictable demand for block space.

The potential impact on fees is uncertain. Covenants could increase total block space demand by enabling use cases that currently migrate to other chains or don't exist at all. However, some covenant designs (like payment pools) also enable more efficient use of block space, which could reduce per-transaction fees even as total demand grows, echoing the SegWit paradox.

No covenant proposal has yet achieved the community consensus needed for activation. The debate around OP_CTV has been contentious, with concerns about unintended consequences and governance process. However, the active

What is the Lightning Network?

Lightning is a “Layer 2” system built on top of Bitcoin. It lets people make instant, nearly-free payments without waiting for blockchain confirmations.

Here’s how it works: two people lock some bitcoin in a shared account on the blockchain (opening a “channel”). They can then send payments back and forth instantly, just by updating their private records of who owns what. When they’re done, they close the channel and settle the final balance on the blockchain.

Payments can route through several channels, so users do not need a direct channel with every counterparty. Ordinary Lightning payments settle off-chain; miners earn on-chain fees from transactions that open and close channels. The net fee effect depends on congestion and other demand for block space.

development community around these proposals suggests that Bitcoin’s protocol is not as frozen as it sometimes appears, and future upgrades could meaningfully affect fee market dynamics.

Layer 2: Lightning and Base-Layer Fees

The Lightning Network enables fast, low-fee payments through bidirectional payment channels. Its effect on miner fees depends on channel activity, the payments users move off-chain and the demand for available block space.

Lightning works by moving transactions off the main blockchain. Users open payment channels by locking bitcoin in on-chain transactions, then conduct unlimited off-chain payments within those channels, and finally close channels with on-chain settlement transactions. This increases throughput by orders of magnitude: while Bitcoin’s base layer processes roughly 4-7 transactions per second depending on transaction complexity, Lightning can theoretically handle millions.

The December 2025 snapshot records public channel capacity of 5,637 BTC across roughly 48,678 channels and approximately 14,940 publicly visible nodes^{47,48}. River’s estimate of at least 6.6 million publicly routed payments and an average payment size near \$12 refers to August 2023⁴⁹.

The Lightning Network’s impact on base layer fee revenue is debated. Two competing narratives exist:

The pessimistic view holds that Lightning reduces base layer fee revenue by moving transactions off-chain. Academic research supports this concern. Divakaruni

and Zimmerman’s peer-reviewed study⁵⁰ found a “significant association between LN adoption and reduced blockchain congestion.” Their counterfactual analysis suggested that if Lightning had existed during the 2017 congestion at its scale at the end of their sample (September 2019), the mempool count would have been 84% lower and mempool fees 76% lower.

Lightning allows many payments to share on-chain channel operations. River reports a node-level ratio of 252 payments facilitated per attributed on-chain transaction when including channels opened by its peers⁴⁹. Figure 17 illustrates the mechanism with ten payments in one channel, one opening transaction and one closing transaction. Fees depend on transaction sizes, bids and the competing demand for block space.

The optimistic view holds that Lightning increases total Bitcoin economic activity, some of which spills over to the base layer. Channel opens and closes require on-chain transactions, creating anchor demand. Large-value transfers remain on-chain because Lightning’s liquidity constraints make it unsuitable for very large payments. And Lightning’s improved user experience may attract new users who eventually need base layer transactions.

Guasoni, Huberman, and Shikhelman’s analysis in *Management Science*⁵¹ provides theoretical support for the pessimistic view. They mathematically demonstrated that as payment frequency increases, on-chain transaction frequency decreases due to netting benefits. The relationship is sublinear: doubling Lightning payments does not double channel operations.

The empirical evidence is mixed. Lightning’s growth has coincided with periods of both high and low base layer fees, making causal attribution difficult; causality also runs in reverse, since high on-chain fees are themselves a motive to adopt off-chain netting. The association between Lightning adoption and reduced congestion found by Divakaruni and Zimmerman is suggestive but not definitive, as other factors (SegWit adoption, market cycles, competing blockchains) also affect congestion.

A further consideration, raised in correspondence with one of this report’s reviewers, sharpens the picture. Peter Zimmerman points out that, when block-building is competitive, the displacement effect is regime-dependent: when blocks are not full, the marginal fee for inclusion is close to zero, so the payments Lightning removes carried minimal fee revenue in the first place; when blocks are persistently full, the transactions cleared through Lightning are likely to be disproportionately low-fee payments that would not have won block space anyway. As Bitcoin matures toward persistent

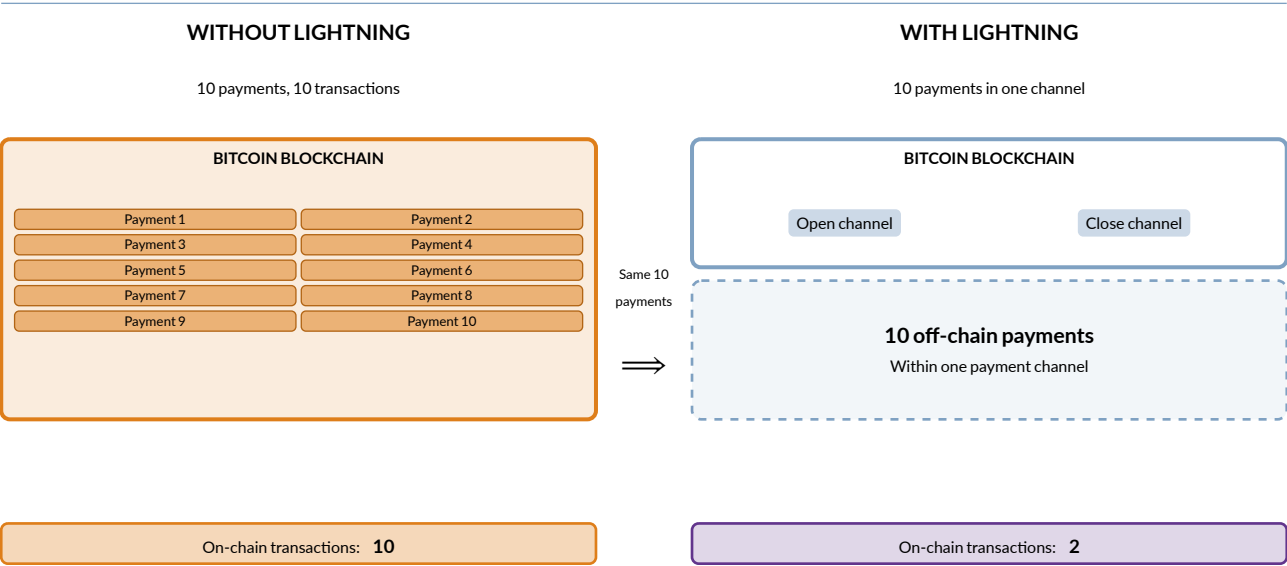
congestion, the negative effect of Lightning on fee revenue therefore weakens.

What is clear is that Lightning creates a genuine tradeoff with the security budget: its value proposition is low fees, while the security budget requires fee revenue. But the conflict is conditional rather than absolute. In the congested regime, displaced payments are those that would have paid the least anyway, and channel operations themselves anchor on-chain demand. The scenario in which Lightning meaningfully starves the base layer is one of weak overall demand for Bitcoin transactions, in which fees would be low with or without it.

Some argue this is acceptable: Bitcoin’s base layer should be a settlement layer for large transactions and Layer 2 anchoring, not a retail payment system. Under this view, a smaller number of high-value, high-fee transactions can provide adequate security; Alden’s fee model discussed in Part II²⁹ implies roughly \$10 billion in annual fee revenue at \$100 per transaction, comparable to current total miner revenue.

Figure 17: Lightning Payments and On-chain Settlement. Authors’ illustration of ten payments: the left case assumes one on-chain transaction per payment; the right assumes one channel opening, ten off-chain payments and one channel closing. Ordinary Lightning payments appear outside the blockchain outline. The diagram counts transactions; fee revenue depends on transaction sizes, fee rates and the demand occupying block space.

Lightning Payments and On-chain Settlement



If a user limits fees to 1–2% of the transferred value, a \$100 fee implies a minimum transfer of \$5,000–10,000. This is a willingness-to-pay assumption.

Lightning changes how users buy block space. Channel operations create on-chain demand, while some payments move off-chain. Congestion and the demand filling released capacity determine the effect on miner fees.

Protocol Changes

Protocol-Level Changes

More aggressive solutions would modify Bitcoin's protocol to address the security budget directly. These proposals range from adjustments to block parameters to fundamental changes in monetary policy.

Block size increases would expand the supply of block space, potentially increasing total fee revenue even if per-transaction fees decline. The logic is that lower fees would attract more transactions, and the volume increase would offset the price decrease. This argument was central to the 2015-2017 “block size wars” that ultimately resulted in the SegWit compromise.

However, the block size debate revealed deep divisions in the Bitcoin community. Opponents

argued that larger blocks would increase node operation costs, centralizing the network. They also questioned whether demand for block space was sufficiently elastic, since if users are unwilling to pay current fees, would they pay lower fees in sufficient volume to increase total revenue?

Brown, Chiu and Koepl's calibrated SegWit model estimates lower fee revenue than its counterfactual without the capacity increase²². The revenue effect of additional block space depends on how transaction demand responds to lower fees.

Tail emission would replace the halving schedule with a fixed, perpetual block reward. Instead of subsidies declining to zero, they would stabilize at some minimum level, providing permanent baseline security funding regardless of fee market conditions.

Peter Todd's 2022 analysis³² provides the strongest case for tail emission. He proved mathematically that a fixed emission rate does not lead to unlimited supply growth. With a coin loss rate λ (coins lost to deaths, forgotten passwords, accidents) and fixed emission rate k , supply converges to:

$$N(\infty) = \frac{k}{\lambda}$$

If approximately 1% of coins are lost annually and emission is set at 1% of current supply, the long-term supply stabilizes rather than growing indefinitely. Todd argues this makes tail emission “not inflationary” in any meaningful sense, since new coins merely

What is tail emission and why does it matter?

Tail emission is a proposed change to Bitcoin's monetary policy that would create a small, fixed block reward that continues forever, instead of rewards eventually dropping to zero.

The idea is simple: if miners always receive some baseline payment, they'll always have an incentive to secure the network, regardless of how much users pay in transaction fees.

Monero introduced a permanent base subsidy of 0.6 XMR per block in June 2022. This provides ongoing miner revenue; the majority-hashrate episode discussed in Part III illustrates the separate issue of control over mining capacity.

The catch? Implementing this in Bitcoin would require changing the 21 million coin limit, widely considered Bitcoin's most sacred property. Most Bitcoiners view this as a non-starter, making tail emission unlikely under current community sentiment, though communities can shift under changing conditions, as the SegWit adoption process demonstrated.

What's the difference between a hard fork and a soft fork?

When Bitcoin's rules need to change, there are two ways to do it, and the difference matters.

A *soft fork* tightens the rules. Old software still accepts new blocks, even if it doesn't understand the new features. It's backward-compatible, so the network doesn't split. SegWit in 2017 was a soft fork.

A *hard fork* loosens the rules or changes them fundamentally. Old software rejects new blocks as invalid. Unless everyone upgrades, the network splits into two chains. This is why hard forks are contentious: they require near-universal agreement.

Changing Bitcoin's 21 million cap would require a hard fork. Anyone who didn't upgrade would be on a different Bitcoin.

replace lost ones. The equilibrium depends on the loss rate, which is unobservable and unlikely to be constant: if custody practice improves and losses fall, the implied long-run supply rises.

However, implementing tail emission in Bitcoin would face steep obstacles:

Technical barrier: Tail emission requires a hard fork, "an incompatible rule change that existing Bitcoin nodes would reject as invalid"⁵². Unlike soft forks that tighten rules (and are backward-compatible), hard forks loosen rules and require universal adoption. Nodes that don't upgrade would see the new chain as invalid and fork off.

Social barrier: The 21 million supply cap is widely considered Bitcoin's most fundamental property, more important than any other parameter. Changing it would, in the view of many, create "an entirely new and distinct asset" rather than modifying Bitcoin. The community reaction to BlackRock's December 2024 disclaimer noting the cap "might" change, widely dismissed as "FUD," illustrates the intensity of opposition.

Coordination barrier: Even if a majority of the community supported tail emission, coordinating the transition would be difficult. The 2017 SegWit2x episode demonstrated that even changes with apparent majority support can fail if a determined minority refuses to adopt them.

Bitcoin Core developer James O'Beirne, while warning about the security budget problem, has argued that introducing a tail emission or changing the supply schedule would "totally undermine the

premise of Bitcoin"⁵³. Peter Todd himself noted: "There is a good chance the issue isn't fixed, and it leads to permanent mining centralization."

Demurrage is an even more radical proposal: a tax on unspent bitcoin that would fund mining. Under demurrage, bitcoin holdings would slowly decay over time, with the "lost" value redirected to miners. This would create a cost to holding bitcoin, incentivizing spending and providing permanent security funding.

Demurrage faces even stronger opposition than tail emission. It would alter Bitcoin's properties as a store of value, transforming it from an asset that appreciates through scarcity to one that depreciates through taxation. This is antithetical to the "digital gold" narrative that dominates current Bitcoin discourse.

Demurrage would require agreement on a holding charge and a change to Bitcoin's monetary rules. Those adoption requirements accompany its potential to transfer revenue from holders to miners.

No Bitcoin Improvement Proposal (BIP) explicitly targets the security budget as its primary goal. However, multiple BIPs indirectly address components of the problem: fee market improvements (BIP 125 for RBF, BIP 331 for package relay, BIP 431 for TRUC transactions), capacity enhancements (SegWit, Taproot), and proposed covenant opcodes that could unlock new sources of block space demand. The Bitcoin development community's approach is characteristically incremental, addressing the fee market through many small improvements rather than a single grand proposal. No BIP proposes monetary

policy changes, reflecting the community's current consensus that the 21 million supply cap is inviolable.

Merged Mining and Auxiliary Revenue

Merged mining allows miners to secure multiple blockchains simultaneously using the same proof-of-work. Bitcoin miners can earn additional rewards from chains such as RSK (Rootstock) without duplicating the hashing work. This could supplement mining revenue without requiring changes to Bitcoin itself.

The theoretical appeal is straightforward: if miners can earn fees from multiple chains while contributing the same hashrate to Bitcoin, total miner revenue increases. The additional revenue comes from other ecosystems, not from Bitcoin users, avoiding the tension between fees and usability.

RSK (Rootstock) is the most established merged-mined sidechain. It provides Ethereum-compatible smart contracts secured by Bitcoin's hashrate, with miners receiving approximately 80% of RSK transaction fees. However, RSK's total value locked remains under \$500 million, generating minimal additional revenue for Bitcoin miners.

Stacks takes a different approach, using a "proof of transfer" mechanism where Stacks miners commit Bitcoin to earn STX rewards. This creates demand for Bitcoin transactions (the commitments) rather than direct merged mining revenue. The impact on Bitcoin's fee market is positive but small.

Drivechain proposals (BIP 300/301) would enable sidechains with two-way pegs to Bitcoin. Proponents argue this could create large fee-generating ecosystems that supplement miner revenue. Critics worry about security implications, since sidechains could be used to extract value from Bitcoin or introduce new attack vectors.

The fundamental limitation of merged mining is that auxiliary chain revenue depends on those chains' success. If sidechains fail to attract significant economic activity, they provide negligible additional revenue. And if they succeed, they might compete with Bitcoin rather than complement it. Auxiliary revenue is also double-edged as a security instrument: the Monero episode of August 2025 (Part III) shows that revenue from outside the chain's native

reward can be the very tool that attracts hashrate away from honest mining.

Current merged mining revenue is negligible compared to Bitcoin's security budget. RSK, Stacks, and other auxiliary chains collectively contribute less than 1% of miner revenue. For merged mining to meaningfully address the security budget problem, auxiliary chain ecosystems would need to grow by orders of magnitude, an outcome that cannot be assumed.

Industry Adaptation

New Business Models for Mining

Bitcoin miners are diversifying beyond pure block reward revenue, developing business models that could sustain operations even if the security budget declines.

Demand response and grid services can provide miners with compensation for reducing electricity use under power contracts. In an NBER working paper, Halaburda and Yermack⁵³ study publicly traded miners with North American facilities. Their model shows how low electricity prices during renewable oversupply, curtailment payments and fixed-price contracts with power-resale options can support profitability despite periodic shutdowns. The gains depend on electricity prices and contractual terms; firm profitability need not imply continuous mining.

Grid-service payments and heat sales can supplement block rewards or reduce miners' net operating costs. Their contribution to honest hashrate depends on how much mining capacity they support and when that equipment operates. The revenue measures in this report count on-chain subsidy and fees; ancillary income can also influence miners' decisions to remain active.

Flexible-load operation also changes the shape of the security budget over time. If a growing share of hashrate curtails when electricity is expensive, effective network security becomes time-varying, and an attacker with insulated power costs could time an attempt to coincide with curtailment troughs. The demand-response business model, in other words,

trades average-cost efficiency for predictable windows of reduced hashrate.

Heat reuse captures waste heat from mining operations for productive purposes. Mining generates heat that is typically vented to the atmosphere. Some operations have found ways to use this heat for district heating, greenhouses, aquaculture, or industrial processes.

Heat reuse can improve mining economics by creating a revenue stream or reducing heating costs for co-located facilities. Its contribution depends on nearby heat demand, operating hours, transport losses and the cost of connecting users. Expanding these benefits across the network requires suitable heat customers and infrastructure at mining sites. HIVE reports heat-reuse initiatives at its Canadian data centres and, in June 2026, described exploratory work with Boden Municipality and RISE on recovering heat for community use in Sweden⁵⁴.

AI and high-performance computing (HPC) pivot represents the most significant strategic shift in the mining industry. Several major miners are converting facilities to host AI workloads, which command higher prices than Bitcoin mining.

Core Scientific signed an \$8.7 billion HPC contract with CoreWeave and is converting most facilities to support AI workloads, though shareholders rejected a \$9 billion acquisition by CoreWeave in October 2025, preferring to remain independent⁵⁵. MARA Holdings and Riot Platforms are investing in HPC infrastructure. The logic is straightforward: AI computing pays better than Bitcoin mining, and miners have the power infrastructure and cooling capabilities that AI workloads require. The binding constraint is powered land and grid connections, for which AI now outbids mining.

This trend has implications for Bitcoin's security. If mining becomes less profitable than alternative uses of the same infrastructure, miners will rationally redirect resources away from Bitcoin. The result could be declining hashrate even as the broader data center industry grows.

MARA Holdings describes its expansion as vertical integration, with mining remaining central to strategy: mining monetizes powered land while preserving the flexibility to shift capacity to AI and HPC as opportunities arise. Such investment choices reflect

relative returns and infrastructure opportunities; their effect on Bitcoin depends on the capacity firms retain for mining.

Game-Theoretic Backstops

Some analysts argue that Bitcoin's security will be maintained through game-theoretic mechanisms even without explicit protocol changes or new revenue sources.

Holder-funded mining is a possible backstop: institutions, nation-states or individuals with substantial bitcoin exposure could subsidise mining to protect their holdings, even if mining revenues did not cover its costs.

In this hypothetical backstop, a holder would compare the expected losses avoided with the cost of supporting additional honest hashrate. Participation would depend on the holder's exposure, the contribution of that capacity to deterrence, and the availability of equipment and power.

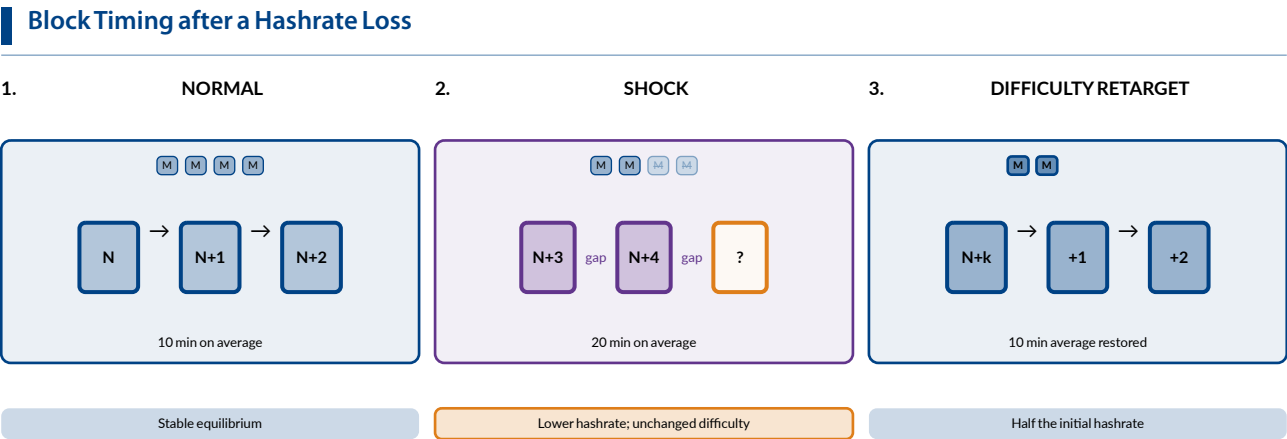
However, the miner of last resort theory faces several challenges:

Coordination problem: Who decides when intervention is needed? How do potential "miners of last resort" coordinate to avoid free-riding (letting others bear the cost while benefiting from the security)? Two considerations soften this objection. Large incumbent miners have a defensive motive to coordinate: protecting a profitable business is a private incentive that arises without altruism, and coordination costs fall as the industry concentrates. And coordination can be imposed from outside: a government whose institutions hold bitcoin, or whose jurisdiction hosts substantial hashrate, could compel domestic miners to act in concert, a mechanism that cuts both ways, serving as backstop or as attack vector depending on the government.

Threshold uncertainty: At what security budget level does intervention become necessary? The relationship between security budget and attack risk is not well understood, making it difficult to know when to act.

Commitment problem: Potential miners of last resort cannot credibly commit to future intervention.

Figure 18: Block Timing after a Hashrate Loss. Authors’ illustration: two of four equal-hashrate miners leave at the start of a difficulty period, and the remaining capacity stays constant. The expected block interval doubles from ten to twenty minutes. After the retarget, the two remaining miners restore an average ten-minute interval while total honest hashrate remains half its initial level.



Attackers might calculate that holders will not actually follow through, undermining the deterrent effect.

Scale mismatch: The security budget is currently approximately \$12 billion annually. Even large holders might balk at subsidizing mining at this scale indefinitely.

Pierre Rochard⁵⁶ describes a separate fee-response mechanism: slower confirmations can increase users’ bids for block space and make mining more attractive.

“Bitcoin’s budget for finality is NOT a fixed paycheck; it’s a market price that rises when needed. When miners shut off post-halving, blocks slow, difficulty adjusts, and fees rise as users compete for limited space. Fee spikes during stress, miners maximizing fee inclusion, and rapid reversion to normal once backlogs clear.”

Figure 18 illustrates the recovery of block timing through difficulty adjustment. A return of departed mining capacity requires incentives to operate that equipment, including expected rewards relative to power and other costs. Users bidding for confirmation during congestion can increase fee income and make mining more attractive.

The Runes launch in April 2024 illustrates a demand-driven fee response. The episode described in Part II

arose from demand for block space, rather than the miner-exit sequence in the illustration.

However, these spikes were temporary and driven by speculative activity rather than security concerns. The fee market has not demonstrated the ability to consistently replace declining subsidies. And the self-correcting mechanism assumes users will pay whatever fees are necessary, an assumption that may not hold if alternatives (Layer 2, other blockchains) are available.

Lessons from Ethereum and Alternative Approaches

Ethereum’s evolution provides instructive contrasts with Bitcoin’s approach to network security funding.

The Merge (September 2022) transitioned Ethereum from proof-of-work to proof-of-stake, changing its security model. Daily issuance dropped from approximately 13,000 ETH to roughly 1,700 ETH, a reduction of about 87%. Security now comes from staked capital rather than energy expenditure, with approximately 34 million ETH (\$100+ billion) locked as collateral.

EIP-1559 (August 2021) reformed Ethereum’s fee market by introducing a base fee that is burned rather than paid to validators⁵⁷. Over 4.4 million ETH has

been burned since implementation (as of early 2026), creating periods of net deflation when burn exceeds issuance. The mechanism improves fee predictability for users while reducing the effective supply of ETH.

Ethereum's approach demonstrates that alternative security models can work. The network has operated securely since the Merge. Attacking it is costly in a different way than attacking Bitcoin: an attacker must first acquire a large share of staked ETH, driving the price against themselves as they buy; only the attacker's own stake is subject to slashing; and the unstaking queue makes rapid exit impossible, so the capital cannot be withdrawn ahead of the value destruction the attack itself would cause. Validator yields of 3-4% APY have attracted sufficient staking participation.

However, Ethereum's solutions are largely inapplicable to Bitcoin:

Proof-of-stake transition would require abandoning proof-of-work entirely, a "cultural non-starter" that contradicts Bitcoin's core identity. PoW is not merely a technical choice but a philosophical commitment to anchoring security in physical reality. The Bitcoin community views PoS as inferior, citing concerns about centralization (large holders accumulate more stake), "nothing at stake" problems, and the lack of objective chain selection criteria.

Budish, Lewis-Pye, and Roughgarden's formal analysis⁵⁸ proves that the additional economic security that slashing provides is unavailable to protocols in the "dynamically available" setting, the class of fully permissionless, longest-chain protocols that Bitcoin occupies. The result is best read not as an engineering bar but as a statement of price: to gain slashing-based security, Bitcoin would have to move to a different permissionlessness class (as Ethereum did), a change that carries its own costs and trade-offs.

Fee burning would reduce rather than enhance Bitcoin's security budget. Unlike Ethereum, which has ongoing issuance to offset burns, Bitcoin's fixed supply makes burning permanently deflationary. More critically, burning fees removes revenue that miners need to cover operational costs. In a PoW system where miners expend real resources (electricity, hardware), burning fees directly undermines security.

Ethereum's post-Merge experience also contains a direct parallel to the Lightning paradox. Following the EIP-4844 upgrade of March 2024, which sharply cut the cost of posting rollup data, activity migrated to layer-two networks, L1 fee revenue fell steeply, and ETH turned intermittently inflationary as burn fell below issuance. The response came at the protocol level: the EIP-7918 blob fee floor, activated in the December 2025 Fusaka upgrade, ties the minimum price of rollup data to L1 execution fees. Layer-2 fee displacement, in other words, has now been observed on another chain, with a sharp activation date and an explicit mechanism-design remedy. Fee-floor mechanisms provide another approach to block-space pricing, although their applicability to Bitcoin would depend on design choices and the consensus processes discussed below.

The relevant lesson from Ethereum is therefore double-edged: radical protocol changes can re-fund security, and even then the fee-displacement problem recurs and demands active management. Bitcoin's challenge is finding a path that works within its more constrained design philosophy.

Tim Roughgarden's academic analysis of EIP-1559⁵⁹ concludes: "No transaction fee mechanism, EIP-1559 or otherwise, is likely to substantially decrease average transaction fees; persistently high transaction fees is a scalability problem, not a mechanism design problem." Formal results bound the design space from the other side as well: Chung and Shi⁶⁰ and Chung, Roughgarden, and Shi⁶¹ prove that no non-trivial fee mechanism can simultaneously satisfy user incentive compatibility, miner incentive compatibility, and collusion-proofness, so fee-market optimisation alone has provable limits.

This insight applies to Bitcoin as well. The security budget problem is about demand for block space, not about how fees are collected or distributed. No clever mechanism design can create demand that doesn't exist. If users are unwilling to pay high fees for base layer transactions, the security budget will decline regardless of protocol optimizations.

The Governance Challenge

Perhaps the greatest barrier to addressing the security budget problem is Bitcoin's governance structure, or lack thereof.

Bitcoin has no formal governance mechanism. Changes to the protocol require “rough consensus” among developers, miners, node operators, and users. This decentralized governance is a feature, not a bug: it prevents any single entity from controlling Bitcoin and makes the protocol resistant to capture. But it also makes coordinated responses to challenges difficult.

The 2015-2017 block size debate illustrated these dynamics. Despite years of discussion and apparent majority support for larger blocks, the community could not reach consensus. The result was a compromise (SegWit) that satisfied few and a contentious fork (Bitcoin Cash) that split the community. The episode demonstrated that even modest changes face deep resistance.

Monetary policy changes would face far greater opposition. The 21 million supply cap is considered sacrosanct, more fundamental than any other parameter. Proposals to modify it, even slightly, are dismissed as attacks on Bitcoin’s core value proposition. The community’s reaction to BlackRock’s disclaimer about potential supply cap changes, widespread mockery and accusations of “FUD,” illustrates the intensity of this commitment.

This governance structure creates a paradox: Bitcoin’s resistance to change protects it from capture but may also prevent necessary adaptations. If the security budget problem becomes acute, the community may be unable to respond in time. The very decentralization that makes Bitcoin valuable could become a liability.

Anthony Towns’ “Bitcoin Forking Guide” (December 2025) outlines the process for protocol changes, emphasizing the need for a “cooperative environment” and broad stakeholder buy-in. For controversial changes like tail emission, achieving such consensus seems nearly impossible under current conditions.

Protocol changes require time for technical development and agreement among participants. A response developed after a disruption would face those same coordination requirements. Research, monitoring and discussion of trade-offs can inform decisions before participants need to choose a response.

Part V

Looking Forward



Stakeholders can track miner revenue, attack costs and mining concentration as block subsidies decline.

Attack costs depend on how an attacker obtains control: acquiring existing machines, adding capacity and renting hashrate require different arrangements. ASIC supply, hosting and power access constrain external acquisition, while limited marketplace capacity constrains rental. Appendix A.1 separates these routes and identifies the assumptions behind the estimates used in the report.

Fees account for 0.67% of miner revenue over the 90 days ending 4 October 2026. Their future contribution depends on demand for block space, including settlement from other layers. Proposed changes to issuance face social consensus barriers, as the 21 million supply cap is considered “constitutive, not merely descriptive” of Bitcoin⁶. This final section brings together the evidence, the monitoring framework and considerations for stakeholders.

Spillover Risks to Traditional Finance

Bitcoin is no longer an isolated system. Its integration into traditional finance means that security budget risks are no longer confined to the cryptocurrency ecosystem; they have potential spillover effects for regulated financial institutions and markets.

Exchange-traded funds (ETFs). US spot Bitcoin ETF net assets passed \$100 billion in November 2024⁶². These products provide Bitcoin exposure through regulated exchanges. Network disruption can affect valuation, trading and settlement for fund holders. Existing disclosures address these risks: the iShares Bitcoin Trust ETF prospectus dated 31 July 2025 describes the halving schedule and warns that reduced mining incentives could jeopardise network security⁶³.

Corporate treasury holdings. Publicly traded companies hold Bitcoin on their balance sheets. Strategy, formerly MicroStrategy, reported 601,550 BTC on 14 July 2025⁶⁴. A security failure could trigger write-downs, margin calls on Bitcoin-backed debt and effects on equity valuations.

Collateralized lending. Bitcoin and other crypto-assets support lending across centralised and decentralised markets. Galaxy estimates the broader crypto-collateralised lending market at \$69.55 billion at the end of 2025, including CeFi loans, DeFi borrowing and crypto-backed collateral-debt-position stablecoins⁶⁵. A Bitcoin confidence shock could trigger margin calls on Bitcoin-backed loans and transmit losses through shared lenders and collateral markets.

Custodial infrastructure. Regulated custodians (Coinbase Custody, Fidelity Digital Assets, BitGo) hold hundreds of billions in Bitcoin on behalf of institutional clients. These custodians rely on Bitcoin’s consensus mechanism functioning correctly. A prolonged chain reorganization could create conflicting views of account balances and complicate settlement.

The magnitude of these spillover channels has grown since the security budget debate began. When Carlsten et al. published their 2016 paper, Bitcoin’s market cap was approximately \$10 billion, with negligible institutional exposure. Today, with a market capitalisation around \$1.7 trillion and deep integration into regulated finance, the stakes are qualitatively different. Budish’s analysis makes the implication formal: the more economically important a chain becomes, the greater the incentive to attack it¹⁵, so integration into regulated finance raises exposure and attack incentive together. This makes the security budget question relevant not only for the Bitcoin community but for financial regulators and stability boards worldwide.

Synthesis of Evidence

Before proposing solutions, we articulate what the evidence reveals. Our analysis across Parts I-IV yields several key conclusions that frame the path forward.

The subsidy decline follows the protocol. Bitcoin’s block subsidy will fall from 3.125 BTC per block today to 0.78125 BTC after the halving expected around 2032 and 0.1953125 BTC after the halving around 2040,

Table 2: Illustrative price paths and fee shares in total miner revenue across future subsidy halvings.

Scenario	BTC Price Trajectory	Fee Revenue (% of Miner Income)
Price stagnation	Flat (current price)	Stays below 5%
Moderate growth	+10%/year	Grows to 10-15%
Fee market maturation	Any	Grows to 30%+
Structural demand shock (e.g. Ordinals-scale adoption)	Any	Periodic spikes to 50%+

reaching zero around 2140. The next four halvings reduce BTC issuance per block by 93.75%. Price appreciation and fee growth can offset lower issuance in miners’ dollar income.

Fee income varies with congestion. Over the 90 days ending 4 October 2026, fees account for 0.67% of miner revenue, and the volatility of daily percentage changes in dollar fees is 11.7× that of Bitcoin’s dollar price²¹. Part II documents sustained higher-fee episodes as well as quieter periods. In the congestion-pricing model, users pay for priority when demand exceeds available block space⁷.

The external-capacity benchmark reaches \$24.58 billion at the 4 October 2026 observation, using the fixed equipment and power prices in Appendix A.1. Coin Metrics’ \$5–20 billion range describes its February 2024 study scenarios³¹. Hardware

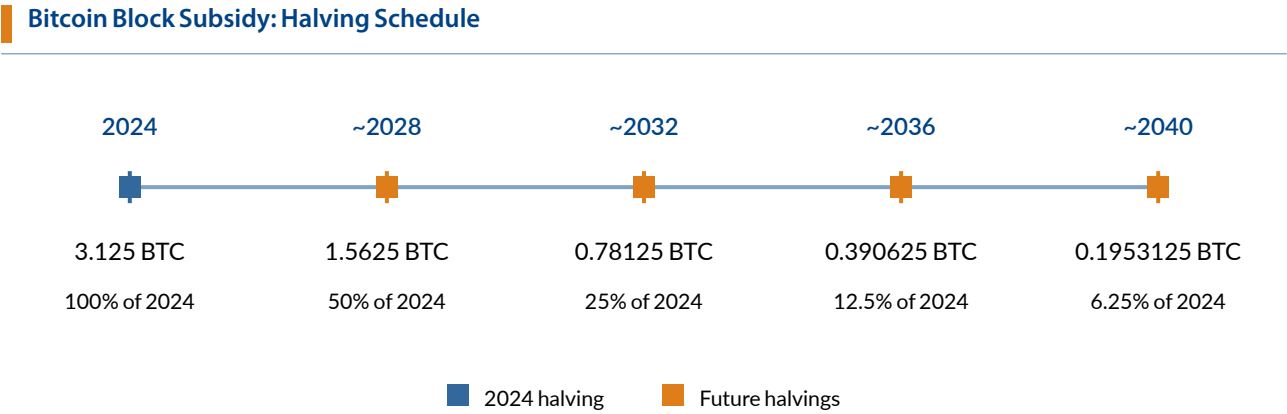
availability and deployment requirements also shape what an attacker could acquire.

Table 2 sets out combinations of Bitcoin price paths and transaction-fee shares that shape miner revenue as block subsidies decline:

Figure 19 shows the subsidy per block through the halving expected around 2040.

Theoretical attacks have not materialized. The gap between academic predictions and observed reality is wide. Carlsten et al.’s 2016 paper predicted fee sniping, undercutting attacks, and mining gaps would emerge as fees became more significant relative to subsidies¹⁰. Nearly a decade later, with fees occasionally exceeding subsidies during congestion events, none of these attacks have been observed on Bitcoin mainnet.

Figure 19: Bitcoin Block Subsidy Halvings. The protocol halves the subsidy every 210,000 blocks, approximately every four years. Labels show the subsidy in BTC per block and its share of the 2024 level. The four halvings expected between 2028 and 2040 reduce the subsidy from 3.125 to 0.1953125 BTC per block. Authors’ illustration.



Statistical analysis by Li et al.³⁸ detected evidence of selfish mining on Monacoin and Bitcoin Cash, but *not on Bitcoin mainnet or Litecoin*. This null result admits multiple interpretations. Optimists argue it demonstrates that theoretical models overestimate risks; pessimists counter that current subsidy levels still provide adequate protection. The honest answer is that we do not know which interpretation is correct.

Solutions face tight constraints. The solution space is narrow. Protocol-level changes that might address the security budget, such as tail emission, demurrage, and increased block size, face high social consensus barriers. No Bitcoin Improvement Proposal (BIP) directly addresses the security budget. Peter Todd's mathematical proof that tail emission is "not inflationary"⁵² has not changed community sentiment. The 2015-2017 block size wars demonstrated that even modest changes face deep resistance.

Lightning compresses payments into fewer on-chain operations; its revenue effect depends on congestion and other demand for block space^{50,51}. Transaction-handling improvements affect bidding and block assembly. Heat reuse and grid services can support mining economics, while HPC hosting may replace mining at some sites. Assessing these options requires both their effects on operating hashrate and the coordination needed for adoption.

The Strongest Counterarguments

The security budget concern has vocal critics who argue that the problem is overblown or will resolve itself through market mechanisms. These counterarguments deserve careful evaluation.

The self-correcting mechanism thesis. Rochard's fee-response argument, discussed in Part IV, links scarce confirmations to higher user bids and incentives for honest miners⁵⁶. Full nodes enforce transaction and supply rules, while mining determines which valid history accumulates work. These functions protect different properties. Congestion episodes demonstrate users' willingness to pay for scarce block space; the Runes launch does not establish that miner exit, difficulty adjustment and renewed capacity followed the sequence in Figure 18.

The price appreciation thesis. Dan Held⁶⁶ and others argue that Bitcoin's price will continue appreciating,

offsetting subsidy reductions in fiat terms. Historical evidence supports this: despite four 50% reductions in the BTC subsidy, total miner revenue in USD has generally trended upward due to price appreciation.

The argument has intuitive appeal. If Bitcoin's price doubles with each halving (roughly 19% annual compound growth), the subsidy's fiat value remains constant. Given Bitcoin's historical growth rates, this seems achievable. Theory counsels caution, however. Schilling and Uhlig⁶⁷ show that in equilibrium the Bitcoin price should behave as a risk-adjusted martingale: under risk neutrality, the expected future price equals today's, making persistent appreciation an anomaly rather than a baseline. The qualifier "risk-adjusted" carries weight in the other direction: realized compound returns of 40-85% per year over the past decade far exceed the roughly 19% the halving arithmetic requires, consistent with a persistent risk premium that may continue to overcompensate for halvings. Nothing in the theory guarantees that it will.

The aligned incentives thesis. ASIC investment creates aligned incentives, since attacking Bitcoin destroys the value of billions in specialized hardware that has no alternative use. Miners who have invested heavily in Bitcoin-specific equipment have strong incentives to protect the network. This "skin in the game" provides security beyond what raw cost calculations suggest.

Evaluation of counterarguments. Price appreciation has offset past halving impacts, and ASIC owners have an incentive to protect the value of their equipment, a deterrent identified in Federal Reserve staff analysis⁶⁸. Kubal and Kristoufek⁶⁹ find that price changes help predict hashrate changes with a one-to-six-week lag in their sample. These mechanisms connect network value with mining incentives.

Their contribution in a sustained fee-dominant regime remains an open question. Fee responses depend on demand for confirmation, while capacity decisions depend on expected mining returns and equipment and power costs. The monitoring framework below tracks these conditions.

A Security Budget Health Indicator Framework

We propose a Security Budget Health Indicator (SBHI) with five components: fee reliance, attack-cost exposure, security expenditure, fee volatility and mining concentration. The framework draws on Alden's security-spend analysis²⁹ and Coin Metrics' attack-cost framework³¹. Appendix A specifies the calculations, observation windows and fixed reference intervals used to display the components on a 0–100 scale.

Component 1: Fee Revenue Ratio (FRR). The Fee Revenue Ratio measures the share of miner revenue paid through transaction fees:

$$\text{FRR} = \frac{\text{Transaction Fees}}{\text{Total Block Reward}}$$

As of 4 October 2026, fees account for 0.67% of total miner revenue over 90 days and 0.64% over 30 days. Each ratio divides aggregate fees by aggregate revenue over the stated window. Higher fee income or lower subsidy income can raise the fee share. Comparing this measure across halving cycles helps track miners' reliance on user-paid fees.

Component 2: Attack Cost Ratio (ACR). The Attack Cost Ratio compares the external-capacity acquisition benchmark with market capitalisation:

$$\text{ACR} = \frac{\text{Acquisition Benchmark}}{\text{Network Market Cap}}$$

The benchmark prices enough new capacity to hold 51% of the combined network while the observed network remains honest. It includes equipment at \$25/TH and 24 hours of electricity at \$0.05/kWh, using 25 J/TH hardware. At the data cutoff, this requires 981.9 EH/s and costs \$24.58 billion, giving an ACR of 141.4 basis points (1.41%). Appendix A.1 defines the cost categories and distinguishes this benchmark from the Coin Metrics scenarios. Market capitalisation provides a common denominator for comparison over time; attacker proceeds depend on the transactions and financial positions exposed to the attack.

Component 3: Security Spend to Market Cap (SSMC). This metric compares annualised miner revenue with market capitalisation:

$$\text{SSMC} = \frac{\text{Annualised Miner Revenue}}{\text{Market Cap}}$$

The current SSMC is 0.69%, using the trailing 90-day mean of daily miner revenue multiplied by 365. ACR measures an acquisition benchmark; SSMC measures an income flow. Alden²⁹ suggests an approximate security-spend range of 0.5–1.5% of market capitalisation when modelling fee-funded security. The current SSMC falls within that proposed range.

Component 4: Fee Volatility Index (FVI). The Fee Volatility Index compares the variability of daily percentage changes in dollar fee income with those in Bitcoin's dollar price:

$$\text{FVI} = \frac{\sigma_{\text{fee changes}}}{\sigma_{\text{price changes}}}$$

The ratio is 11.7× over 90 days and 10.2× over the trailing year²¹. A value of one indicates equal standard deviations; higher values indicate more variable fee income relative to price. The current reading shows that miners face substantial variation in fees as well as in Bitcoin's price.

Component 5: Hashrate Concentration Index (HCI). Using the Herfindahl-Hirschman Index (HHI) methodology applied to mining pool market shares:

$$\text{HCI} = \sum_{i=1}^n s_i^2$$

where s_i is the market share of pool i expressed as a percentage.

Current value: approximately 1500 (in HHI points), calculated from recent block data. The top three pools, Foundry USA (25.3%), AntPool (20.3%), and F2Pool (15.2%), control approximately 61% of hashrate. Research from OxB10C¹⁶ reveals that AntPool and affiliates may control additional hashrate through proxy pooling arrangements, meaning actual block template producers are fewer than coinbase tags suggest.

The antitrust reference describes market concentration. For Bitcoin, miners' ability to switch pools and the sharing of block templates also matter for control over transaction selection. The dashboard's HCI scale uses fixed endpoints of 1,500 and 3,000; HHI values at or below 1,500 receive 100

What is the Herfindahl-Hirschman Index?

The HHI is a standard measure economists use to gauge market concentration. It works by squaring each company's market share and adding them up.

A market with 100 equal competitors would score 100 (very competitive). A monopoly scores 10,000 (maximum concentration). The 2023 US Merger Guidelines treat markets above 1,800 as "highly concentrated" (the earlier 2010 guidelines used 2,500).

For Bitcoin mining, we calculate HHI using pool market shares, an antitrust benchmark applied here as a heuristic: pool shares are not firm shares, since miners can switch pools freely. Over the 30 days ending 4 October 2026, Bitcoin mining's HHI is approximately 1500, below the 1,800 reference in the 2023 merger guidelines. When accounting for proxy pooling arrangements (where nominally independent pools share block templates), the effective HHI may be considerably higher.

This matters because concentrated mining creates potential vectors for censorship or coordinated attacks, even if no single pool controls 51%.

on that scale. Appendix A.2 provides the mapping and a worked example for 1500.

Reading the dashboard. We display the five components separately. A high reading on one component cannot offset a low reading on another, and some components share inputs, including the fee series used by FRR and FVI. Readers can compare each raw indicator and its normalised reading across observations using the fixed reference intervals in Appendix A.2.

In 4 October 2026, the fee share remains below 1%, and daily fee changes are 11.7 times as volatile as price changes over 90 days. The acquisition benchmark is 1.41% of market capitalisation, compared with 0.69% for annualised miner revenue. Pool shares imply an HHI of 1500 shared templates can concentrate transaction selection beyond the pool tags observed in blocks.

Developers, researchers and data providers could use these definitions to build a dashboard with historical comparisons around halvings, hashrate drawdowns and mining disruptions. Publishing the raw inputs alongside the component readings would let users track changes and examine the assumptions behind them.

Future Directions

Open Research Questions

Our analysis reveals several unresolved questions and require further academic investigation. These research gaps represent opportunities for the academic community to contribute to Bitcoin's long-term sustainability.

Will fee markets mature organically? The fundamental assumption underlying Bitcoin's design, that fees will naturally grow to replace subsidies, remains untested at scale. Current evidence is mixed: fee spikes during congestion demonstrate market responsiveness, but sustained fee revenue has not materialized despite four halvings and growth in Bitcoin's adoption and market capitalisation⁸.

Research needed: Longitudinal studies of fee market development across multiple halving cycles, with particular attention to the relationship between adoption metrics (transaction count, unique addresses, exchange volume) and fee revenue. Comparative analysis with traditional payment networks' fee structures could provide benchmarks.

What is the minimum viable security budget? No consensus exists on what level of miner revenue is "enough" to secure a trillion-dollar network. Eric Budish's theoretical framework¹³ provides bounds, but empirical validation requires observing fee-dominant

Figure 20: Security Budget Health Indicator (SBHI) dashboard showing current component values and their normalized readings. The framework comprises five components: FRR (fee reliance), ACR (attack cost), SSMC (security spend), FVI (fee stability), and HCI (hashrate concentration). Each reading follows the fixed reference interval in Appendix A.2; 100 denotes the reference endpoint mapped to the top of the scale, or a value beyond it. Data: Coin Metrics²¹ and Mempool.space³⁹ (4 October 2026).

Security Budget Health Indicator (SBHI) Dashboard

METRIC	VALUE	REFERENCE SCALE	0–100
FRR Fee Revenue Ratio	0.67%		2
ACR Attack Cost Ratio	141.4 bp		93
SSMC Security Spend / MCap	0.69%		27
FVI Fee Volatility Index	11.7×		28
HCI Hashrate Concentration	1500		100

Reference ranges and a worked example: Appendix A.2.

security in practice, something no PoW chain has achieved.

Research needed: Development of empirically-grounded security budget thresholds, potentially drawing on historical attack data from smaller chains. Game-theoretic analysis of attack profitability under various fee market conditions would inform minimum security requirements.

Why haven't theoretical attacks materialized? The gap between Carlsten et al.'s predictions¹⁰ and observed reality is notable. Understanding why fee sniping, undercutting, and mining gaps have not occurred would inform predictions about future vulnerability.

Research needed: Empirical analysis of miner behavior during high-fee periods, with particular attention to deviations from theoretical profit-maximizing strategies. Interviews with mining operators could reveal practical constraints not captured in academic models.

How do derivatives markets affect attack economics? Budish's framework¹⁵ identifies potential for short-

position amplification of attack returns. Our analysis in Part III showed open interest growing faster than attack costs; what is missing is a defensible model of attacker short capacity, the position size a single actor could actually build, hold, and collect on, given market depth, funding-rate dynamics, position limits, and counterparty haircuts.

Research needed: Analysis of derivatives market liquidity and the feasibility of establishing large short positions without market impact. Modeling of attack profitability under various derivatives market conditions would inform risk assessment.

How will Layer 2 adoption affect base layer fees? The studies reviewed in Part IV identify payment compression and lower congestion, while channel operations create on-chain demand. The net effect on miner revenue depends on the fee bids and transactions that fill the available block space.

Research needed: Modeling and measurement of both demand reduction (payments moving off-chain) and demand creation (channel operations, anchor transactions), distinguishing congested and

uncongested periods. Node-level payment-to-settlement ratios, such as River's estimate⁴⁹, describe compression at the observed node; estimating network-wide fee effects requires broader coverage and a counterfactual for displaced payments.

Can fee-based instabilities emerge gradually? Carlsten et al.'s predictions assume a sharp transition to fee dominance. In practice, the transition will be gradual. Whether instabilities emerge incrementally or only after crossing specific thresholds is unknown.

Research needed: Simulation studies of gradual transition scenarios, with attention to early warning indicators of emerging instabilities. Recent work by Sarenche et al.³⁶ using reinforcement learning found that under volatile rewards selfish mining can turn a profit in its first epoch, before any difficulty adjustment, suggesting instabilities may emerge before full fee dominance.

What would trigger community consensus for protocol changes? If security budget concerns become acute, would the Bitcoin community accept monetary policy changes? The conditions under which such consensus might form, and whether it could form quickly enough to prevent damage, remain speculative.

Research needed: Analysis of Bitcoin governance dynamics, including historical precedents for contentious protocol changes. The 2015-2017 block size wars demonstrated that even changes with apparent majority support can fail if a determined minority refuses to adopt them.

The International Regulatory Landscape

The security budget question does not exist in a vacuum. It intersects with a rapidly evolving international regulatory landscape that shapes where

Table 3: Selected Mining Policy and Investment Measures. Entries identify the scope and date of each measure or announcement; subnational rules also shape access to power and mining sites.

Jurisdiction	Scope	Dated Measure
United States	Federal support; state and local rules vary	23 January 2025 executive order supports lawful mining and validation; 6 March order establishes a Bitcoin reserve ^{70,71} .
Russia	Registration	Miner and infrastructure-operator registries from 1 November 2024; reporting obligations described by the FTS on 3 March 2026 ⁷² .
China	Prohibition	Notice of 3 September 2021, published 24 September, prohibits new mining projects and requires existing projects to exit ⁷³ .
Kazakhstan	Licensed mining	Digital Assets Law of 6 February 2023 establishes the mining-licensing framework ⁷⁴ .
Canada	Provincial electricity access	British Columbia's 20 October 2025 announcement proposes permanent exclusion of new crypto-mining grid connections, following existing restrictions ⁷⁵ .
Ethiopia	Power and investment permits	The 2024 framework requires an EEP power agreement, an investment permit and hardware-import clearance ⁷⁶ .
UAE	Project-level investment	MARA and Zero Two announced a 250 MW Abu Dhabi joint venture on 9 May 2023 ⁷⁷ .
EU	Issuer and service-provider disclosures	MiCA, adopted 31 May 2023, requires consensus-impact disclosures through Articles 6 and 66; it does not establish a mining-licensing regime ⁷⁸ .
Norway	Registration; proposed restriction	Registration from 1 January 2025. The 12 January 2026 ministerial answer describes assessment of a temporary restriction on new power-intensive crypto data centres ⁷⁹ .

mining occurs, how concentrated it becomes, and whether policymakers recognise the issue at all.

These measures connect mining economics with public-sector exposure and access to infrastructure.

Public-sector exposure. The March 2025 US executive order establishes a Strategic Bitcoin Reserve and requires agencies to account for their holdings⁷¹. Government holdings create a financial interest in network integrity, while mining and data-centre investments create separate interests in power use and infrastructure.

Power and licensing. Electricity access, planning rules and licensing affect where miners can operate. British Columbia's connection restrictions and Ethiopia's power-agreement requirements illustrate different approaches^{75,76}. Following China's 2021 restrictions, miners relocated, while the Cambridge Mining Map continued to identify activity in China in January 2022⁴¹. Physical location and regulatory jurisdiction therefore require separate assessment.

Official-sector analysis. Federal Reserve staff have examined attack incentives and mining economics^{26,68}, and Auer's BIS working paper studies fee-funded mining security and finality⁸⁰. Tracking consensus incentives alongside regulated financial exposure can extend this work to the institutions that hold Bitcoin or provide Bitcoin-linked services.

Considerations for Stakeholders

Participants face different choices about protocol development, mining operations and financial exposure. The following considerations connect those choices to the mechanisms examined in the report.

Developers, Pool Operators and Miners. Transaction-handling improvements, including package relay, TRUC transactions and cluster mempool, can improve fee adjustment and block assembly. Cluster mempool shipped in Bitcoin Core 31.0⁴⁶. Their aggregate revenue effect depends on demand and bidding, alongside their benefits for transaction reliability.

Miner-selected templates offer a way to distribute transaction selection among pool participants. Developers can provide tooling and documentation, while pools and mining companies can support

deployment of protocols that give miners this capability. Running nodes and maintaining compatible software impose operational requirements; the aim is to support the function across implementations.

Developers, academic institutions, data providers and industry can collaborate on monitoring infrastructure. Publishing input definitions, observation windows and calculation methods would let users compare indicators over time. The SBHI and Appendix A provide one set of definitions for that work.

Mining Companies. Diversification and efficiency investment can change the costs and revenues that support mining operations. MARA's energy investments, Riot's demand-response activity and Core Scientific's HPC hosting agreements are examples discussed in Part IV. Firms can evaluate these options against capital requirements, contract terms and operating conditions; the network effect depends on whether they sustain Bitcoin mining or replace it with another use of power and facilities.

Comparable disclosures can help investors assess those choices. Public miners, including MARA, Riot and CleanSpark, can specify their equipment mix, power arrangements and sensitivity to price, fees and subsidy changes, separating mining income from other business lines.

Institutional Investors and Large Holders. Mining-related investments, hashrate purchase agreements and mining funds offer different exposures to mining returns. Investors can assess their cash flows, equipment and power commitments, and contribution to operating hashrate alongside the risks of holding Bitcoin itself.

Investors, philanthropic foundations and public research funders can support work on fee demand, attack incentives and measurement. Open methods and reproducible data can improve comparison of competing claims about security economics.

Contingency planning can address custody, settlement and collateral exposures. Large holders can examine how reorganisations, delayed confirmations or interrupted withdrawals would affect their positions and operational arrangements.

Policymakers, Regulators and Product Issuers. Existing ETF prospectuses already disclose halving and mining-incentive risks, including the iShares Bitcoin

Trust ETF prospectus⁶³. Work on disclosure can build on that coverage by improving the comparability of assumptions about miner incentives, network disruption and product exposure.

Financial-stability monitoring can place miner revenue, acquisition-cost benchmarks and concentration alongside measures of exchange, custody and lending exposure. Lenders and supervisors can examine chain-disruption scenarios in collateral stress tests, including settlement delays and market liquidity.

The CFTC provides public supervision of US regulated derivatives markets, while exchanges such as CME conduct their own market surveillance. These bodies can examine unusual positioning around network disruptions, taking account of market depth, funding and settlement conditions.

Mining-policy assessments can consider grid services and effects on the location of capacity alongside energy and environmental requirements. The dated examples in Table 3 illustrate how national and subnational measures shape access to mining infrastructure.

Conclusion

Bitcoin's security model faces a long-term challenge as block subsidies decline toward zero. Fixed-reward models already permit profitable selfish mining above thresholds that depend on hashrate and tie-breaking assumptions⁹. Volatile fees can expand the profitable region and permit gains before difficulty adjusts³⁶; fee-only models also identify fee-sniping and undercutting incentives¹⁰. The empirical Bitcoin analyses reviewed in Part III have not identified these strategies on mainnet.

During the April 2024 halving, fees briefly exceeded subsidies as Runes users competed for block space. Fees fell as that demand subsided. Lightning changes on-chain demand through payment compression and channel operations; its net effect on miner fees depends on congestion and the other transactions competing for block space⁵⁰.

The strongest counterarguments merit serious consideration. ASIC investment creates aligned incentives, since attacking Bitcoin destroys the value of billions in specialized hardware³¹. Miners operate as

long-term businesses optimizing quarterly returns, not game-theoretic automata maximizing per-block profits⁵⁶. Price appreciation has historically offset halving impacts⁶⁹. And the decade-long gap between Carlsten et al.'s predictions and observed reality suggests models may overestimate risks.

Three fundamental questions remain unresolved: (1) whether organic fee market development will outpace subsidy decline, (2) whether theoretical fee-based instabilities will emerge as the subsidy diminishes, and (3) whether social consensus could ever permit monetary policy changes if needed.

The absence of tail emission proposals or security budget BIPs in active development suggests the Bitcoin community's current strategy is observational, waiting to see if problems materialize before proposing solutions that would compromise core principles. Whether this approach reflects well-founded confidence in market mechanisms or underestimation of structural challenges will become clearer over the next two halving cycles.

Bitcoin Core developer James O'Beirne's warning from April 2025 bears repeating: "two halvings from now you're going to have a pretty drastically reduced subsidy. That's seven and a half years away"¹⁹. The 2028 halving will reduce subsidies to 1.5625 BTC per block; the 2032 halving to 0.78125 BTC. The effect on miners' dollar revenue will depend on Bitcoin's price and transaction fees.

For now, the appropriate response is neither complacency nor alarm, but careful monitoring. The Security Budget Health Indicator framework proposed in this report provides a starting point for tracking security budget health across multiple dimensions. The research gaps identified require continued academic attention, since understanding fee market dynamics, attack economics, and Layer 2 impacts is essential for informed decision-making. And the stakeholder actions outlined offer constructive paths forward within existing constraints.

Bitcoin has demonstrated resilience over nearly two decades. Its security model has withstood market crashes, regulatory attacks, and technical challenges that would have destroyed lesser systems. The network's survival through four halvings, the 2021 China mining ban, and countless predictions of

imminent failure speaks to the robustness of Nakamoto's original design¹.

Whether Bitcoin can withstand the transition to fee-dominant security, a transition no proof-of-work blockchain has ever completed, remains the defining question for its second decade and beyond. Miners' incentives will depend on Bitcoin's price, fee income and the cost of providing hashrate as the block subsidy declines.

The path forward requires vigilance without panic, preparation without paralysis, and honest acknowledgment of both the challenge and the uncertainty surrounding it. Bitcoin's security budget is not a problem to be solved once and forgotten, but a dynamic system requiring ongoing attention and adaptation. The framework and recommendations in this report aim to support that ongoing effort.

As Satoshi Nakamoto wrote in the original whitepaper: "The incentive may help encourage nodes to stay honest"¹. Whether that incentive remains sufficient as block subsidies approach zero is the question that will define Bitcoin's future. The answer is not yet written, but the tools for monitoring, the research agenda for understanding, and the stakeholder actions for responding are now clearer than ever before.

Appendix A. Measurement Methods

A.1 Attack-Cost Benchmarks

We distinguish control of existing capacity from the addition of new capacity. Let H denote observed network hashrate and $q = 0.51$ the attacker’s share. Acquiring control over existing machines requires qH , leaving $(1 - q)H$ honest. Adding machines while the observed network remains honest requires:

$$H_A = \frac{q}{1 - q} H.$$

Rental estimates depend on quoted rates, available capacity and duration. Electricity-only calculations price the operation of equipment already controlled. We price the external-capacity acquisition benchmark with the following fixed inputs:

Input	Value
Target share after adding capacity	51%
Equipment reference price	\$25 per TH/s
Machine efficiency	25 J/TH
Electricity price	\$0.05/kWh
Operating period	24 hours
Included expenditure	Equipment purchase and electricity

With H_A expressed in TH/s, equipment expenditure is $25H_A$ dollars. Electricity expenditure in dollars is:

$$C_{\text{power}} = H_A \times 25 \times 24 \times \left(\frac{0.05}{1000} \right).$$

Site acquisition, facility construction, deployment and procurement premiums lie outside this fixed-unit-price benchmark. Equipment choice and supply constraints enter the broader acquisition scenarios discussed in Part III.

At 4 October 2026, observed hashrate is 943.4 EH/s. The external-capacity calculation requires 981.9 EH/s, giving \$24.55 billion for equipment and \$29.46 million for 24 hours of electricity, or \$24.58 billion combined. Dividing by market capitalisation of \$1,738.5 billion gives 141.4 basis points. Coin Metrics’ February 2024 TCA study uses different network observations, equipment acquisition or manufacturing scenarios, and a one-hour operating period³¹. Its \$5–20 billion range belongs to those study scenarios.

Figure 13 matches the fixed-input benchmark based on Coin Metrics’ hashrate with Glassnode’s perpetual-futures open interest and displays 7-day trailing means through 4 October 2026. Figure 15 applies it to Coin Metrics’ hashrate and market-capitalisation data through 4 October 2026 and displays 30-day centred means. The SBHI uses the latest observation from that same Coin Metrics archive. The benchmark-to-open-interest ratio compares two aggregate dollar amounts; modelling an attacker’s net trading proceeds requires position size, entry prices, funding costs, market impact and settlement terms.

A.2 SBHI Component Readings

The dashboard uses Coin Metrics observations through 4 October 2026 and Mempool.space block counts over the 30 days ending on that date. For each window, we include dates later than the cutoff minus the stated number of days and up to the cutoff. Calculations use unrounded inputs; displayed values are rounded.

- **FRR:** sum of dollar transaction fees divided by sum of dollar miner revenue over 90 days, reported as a percentage. The text also reports the 30-day ratio.
- **ACR:** the acquisition benchmark in A.1 divided by same-day market capitalisation, reported in basis points.
- **SSMC:** mean daily miner revenue over 90 days, multiplied by 365 and divided by cutoff-date market capitalisation, reported as a percentage.
- **FVI:** sample standard deviation of daily percentage changes in dollar fees divided by that of daily percentage changes in Bitcoin's dollar price. We report 90-day and 365-day windows; the dashboard uses 90 days.
- **HCI:** sum of squared pool shares expressed in percentage points. Pool shares use each pool's block count divided by the total over the 30-day window, including an Unknown bucket for unattributed blocks.

We use author-selected, fixed display intervals to place the five components on a common 0–100 axis. Higher fee reliance, acquisition cost and security expenditure map upward; lower fee volatility and pool concentration map upward. The endpoints define the reading shown in the dashboard and stay fixed across observations.

Component	Raw unit	Lower bound L	Upper bound U	Direction
FRR	% of miner revenue	0.5	10	Increasing
ACR	Basis points of market cap	20	150	Increasing
SSMC	% of market cap	0.2	2	Increasing
FVI	Volatility ratio	3	15	Decreasing
HCI	HHI points	1,500	3,000	Decreasing

For an increasing component, the reading is $100 \times \max(0, \min(1, \frac{x-L}{U-L}))$. For a decreasing component, it is $100 \times \max(0, \min(1, \frac{U-x}{U-L}))$. A reading of 100 denotes the endpoint mapped to the top of the scale or a raw value beyond it; the raw value remains visible alongside the scale.

For example, the 90-day FRR is 0.6715%. Its reading is $100 \times \frac{0.6715-0.5}{10-0.5} \approx 1.81$, displayed as 2 after rounding. For an HHI of 1,499.83, $100 \times \frac{3000-1499.83}{3000-1500} \approx 100.01$, which clips to 100. The 1,500 endpoint matches the unconcentrated-market boundary in the 2010 US Merger Guidelines; 3,000 is the upper display reference selected for this dashboard. The current 2023 Guidelines' 1,800 highly-concentrated-market reference is stated separately in the main text^{81.82}.

Endnotes

1. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Accessed August 18, 2026. <https://bitcoin.org/bitcoin.pdf>
2. Bonneau J, Miller A, Clark J, Narayanan A, Kroll JA, Felten EW. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In: *2015 IEEE Symposium on Security and Privacy*. 2015:104-121. doi:10.1109/SP.2015.14
3. Lamport L, Shostak R, Pease M. The Byzantine Generals Problem. In: *Concurrency: The Works of Leslie Lamport*. ACM; 2019:203-226. doi:10.1145/3335772.3335936
4. Cambridge Centre for Alternative Finance. Cambridge Bitcoin Electricity Consumption Index. 2024. Accessed October 7, 2026. <https://ccaf.io/cbnsi/cbeci>
5. Szabo N. Bit Gold. December 2008. Accessed August 17, 2026. <https://unenumerated.blogspot.com/2005/12/bit-gold.html>
6. Carter N. Don't Fear the Reaper. August 24, 2020. Accessed August 18, 2026. https://medium.com/@nic__carter/dont-fear-the-reaper-8bbb42358efb
7. Huberman G, Leshno JD, Moallemi C. Monopoly Without a Monopolist: An Economic Analysis of the Bitcoin Payment System. *The Review of Economic Studies*. 2021;88(6):3011-3040. doi:10.1093/restud/rdab014
8. Easley D, O'Hara M, Basu S. From Mining to Markets: The Evolution of Bitcoin Transaction Fees. *Journal of Financial Economics*. 2019;134(1):91-109. doi:10.1016/j.jfineco.2019.03.004
9. Eyal I, Sirer EG. Majority is not Enough: Bitcoin Mining is Vulnerable. *Communications of the ACM*. 2018;61(7):95-102. doi:10.1145/3212998
10. Carlsten M, Kalodner H, Weinberg SM, Narayanan A. On the Instability of Bitcoin Without the Block Reward. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. 2016:154-167. doi:10.1145/2976749.2978408
11. Khazzaka M. Bitcoin: Censorship Resistance Against Hash Dominance. *SSRN Electronic Journal*. Published online 2024. doi:10.2139/ssrn.4803116
12. Kwon Y, Kim D, Son Y, Vasserman E, Kim Y. Be Selfish and Avoid Dilemmas: Fork After Withholding (FAW) Attacks on Bitcoin. In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. 2017:195-209. doi:10.1145/3133956.3134019
13. Sapirshstein A, Sompolinsky Y, Zohar A. Optimal Selfish Mining Strategies in Bitcoin. In: *Financial Cryptography and Data Security*. Vol 9603. Lecture Notes in Computer Science. Springer; 2016:515-532. doi:10.1007/978-3-662-54970-4_30
14. Nayak K, Kumar S, Miller A, Shi E. Stubborn Mining: Generalizing Selfish Mining and Combining with an Eclipse Attack. In: *2016 IEEE European Symposium on Security and Privacy (EuroSP)*. 2016:305-320. doi:10.1109/EuroSP.2016.32
15. Budish E. Trust at Scale: The Economic Limits of Cryptocurrencies and Blockchains. *Quarterly Journal of Economics*. 2025;140(1):1-62. doi:10.1093/qje/qjae033
16. OxB10C. Bitcoin Mining Centralization in 2025. April 15, 2025. Accessed August 18, 2026. <https://b10c.me/blog/015-bitcoin-mining-centralization/>
17. Glassnode. Miner Revenue from Fees. 2024. Accessed October 7, 2026. <https://studio.glassnode.com/charts/mining.RevenueFromFees>
18. Rodarmor C. Runes. September 25, 2023. Accessed January 18, 2026. <https://rodarmor.com/blog/runes/>
19. O'Beirne J. What's the Problem With Bitcoin? James O'Beirne. April 22, 2025. Accessed July 17, 2026. <https://www.youtube.com/watch?v=JITvE9BwIRQ>
20. Braun H. Bitcoin Miners Must Own Power—or Die Trying Before Next Halving, MARA CEO Says. November 11, 2025. Accessed August 17, 2026. <https://www.coindesk.com/markets/2025/11/11/bitcoin-miners-must-own-power-or-die-trying-before-next-halving-mara-ceo-says>
21. Coin Metrics Inc. Coin Metrics API. 2024. Accessed October 7, 2026. <https://docs.coinmetrics.io/>
22. Brown C, Chiu J, Koeppl TV. *What Drives Bitcoin Fees? Using Segwit to Assess Bitcoin's Long-Run Sustainability*. 2022. doi:10.34989/swp-2022-2
23. Ordinals Contributors. Runes Protocol Documentation. Accessed October 5, 2026. <https://docs.ordinals.com/runes/specification.html>
24. Omni Layer. Omni Layer. Accessed October 5, 2026. <https://www.omnilayer.org/>
25. Counterparty. Counterparty: The Original DeFi and NFT Protocol on Bitcoin. Accessed October 5, 2026. <https://counterparty.io/>
26. Garratt R, Hayes R. Entry and Exit Leads to Zero Profit for Bitcoin Miners. August 28, 2015. Accessed July 20, 2026. <https://libertystreeteconomics.newyorkfed.org/2015/08/entry-and-exit-leads-to-zero-profit-for-bitcoin-miners/>
27. Neumueller A, Pieters G, Mohaddes K, Rousseau V, Zhang B. *Cambridge Digital Mining Industry Report*. 2025. Accessed October 5, 2026. <https://www.jbs.cam.ac.uk/wp-content/uploads/2025/04/2025-04-cambridge-digital-mining-industry-report.pdf>
28. Glassnode. Investigating the Production Cost of Bitcoin. March 24, 2023. Accessed October 7, 2026. <https://research.glassnode.com/investigating-the-production-cost-of-bitcoin/>
29. Alden L. Bitcoin: Fee-Based Security Modeling. March 2021. Accessed August 18, 2026. <https://www.lynalden.com/bitcoin-security-modeling/>
30. Blockchair. Bitcoin's Security Budget Issue: Problems, Solutions and Myths Debunked. 2025. Accessed August 18, 2026. <https://budget.day/>
31. Nuzzi L, Waters K, Andrade M. Breaking BFT: Quantifying the Cost to Attack Bitcoin and Ethereum. *SSRN Electronic Journal*. Published online 2024. doi:10.2139/ssrn.4727999

32. Harvey CR. *Gold and Bitcoin*. 2025. doi:10.2139/ssrn.5530719
33. Gans JS, Halaburda H. "Zero Cost" Majority Attacks on Permissionless Proof of Work Blockchains. *Management Science*. 2024;70(6):4155-4165. doi:10.1287/mnsc.2023.02426
34. Crypto51. Cost of a 51% Attack for Different Cryptocurrencies. 2024. Accessed August 17, 2026. <https://crypto51.app/>
35. Glassnode. Futures Open Interest Perpetual (Stacked). 2024. Accessed October 7, 2026. <https://studio.glassnode.com/charts/derivatives/FuturesOpenInterestPerpetualSumAll?a=BTC&e=aggregated>
36. Sarenche R, Aghabagherloo A, Nikova S, Preneel B. Bitcoin Under Volatile Block Rewards: How Mempool Statistics Can Influence Bitcoin Mining. In: *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security (CCS '25)*. 2025:903-917. doi:10.1145/3719027.3744875
37. Gong T, Minaei M, Sun W, Kate A. Towards Overcoming the Undercutting Problem. In: *Financial Cryptography and Data Security (FC 2022)*. Vol 13411. Lecture Notes in Computer Science. Springer; 2022:444-463. doi:10.1007/978-3-031-18283-9_22
38. Li SN, Campajola C, Tessone CJ. Statistical Detection of Selfish Mining in Proof-of-Work Blockchain Systems. *Scientific Reports*. 2024;14(1):6251. doi:10.1038/s41598-024-55348-3
39. Mempool Space K.K. Mempool.space REST API. 2024. Accessed October 7, 2026. <https://mempool.space/docs/api/rest>
40. Scharnowski S, Shi Y. Bitcoin blackout: Proof-of-work and the risks of mining centralization. *Journal of Financial Stability*. 2026;85:101569. doi:10.1016/j.jfs.2026.101569
41. Cambridge Centre for Alternative Finance. Cambridge Bitcoin Mining Map. 2024. Accessed November 1, 2025. https://ccaf.io/cbsi/cbeci/mining_map
42. Stratum V2 Contributors. Stratum V2 Protocol Specification. Accessed October 5, 2026. <https://github.com/stratum-mining/sv2-spec>
43. OCEAN. DATUM. Accessed October 5, 2026. <https://ocean.xyz/docs/datum>
44. Dogecoin Core Contributors. Dogecoin Core: Block Subsidy Rules. Accessed October 5, 2026. <https://github.com/dogecoin/dogecoin/blob/master/src/dogecoin.cpp>
45. Dogecoin Core Contributors. Dogecoin Core 1.8. 2014. Accessed October 5, 2026. <https://github.com/dogecoin/dogecoin/releases/tag/v1.8.0>
46. Bitcoin Core Project. Bitcoin Core 31.0 Release Notes. April 19, 2026. Accessed October 5, 2026. <https://bitcoincore.org/en/releases/31.0/>
47. Bitcoin Visuals. Bitcoin Visuals: Lightning Network Statistics. 2025. Accessed August 18, 2026. <https://bitcoinvisuals.com/lightning>
48. Amboss Technologies. Amboss: Lightning Network Explorer. 2025. Accessed August 18, 2026. <https://amboss.space/>
49. Wouters S. The Lightning Network Grew by 1212% in 2 Years. October 2023. Accessed August 18, 2026. <https://river.com/learn/files/river-lightning-report-2023.pdf>
50. Divakaruni A, Zimmerman P. The Lightning Network: Turning Bitcoin into Money. *Finance Research Letters*. 2023;52:103480. doi:10.1016/j.frl.2022.103480
51. Guasoni P, Huberman G, Shikhelman C. Lightning Network Economics: Channels. *Management Science*. 2024;70(6):3827-3840. doi:10.1287/mnsc.2022.01664
52. Todd P. Surprisingly, Tail Emission Is Not Inflationary. July 9, 2022. Accessed August 18, 2026. <https://petertodd.org/2022/surprisingly-tail-emission-is-not-inflationary>
53. Halaburda H, Yermack D. *Bitcoin Mining Meets Wall Street: A Study of Publicly Traded Crypto Mining Companies*. 2023. doi:10.3386/w30923
54. HIVE Digital Technologies. HIVE Digital Technologies to Acquire 32 MW Data Center in Boden, Deepening an Eight-Year Community Partnership in Northern Sweden. June 18, 2026. Accessed October 5, 2026. <https://www.hivedigitaltechnologies.com/news/hive-digital-technologies-to-acquire-32-mw-data-center-in-boden-deepening-an-eight-year-community-partnership-in-northern-sweden/>
55. Reuters. Core Scientific shareholders reject \$9 billion CoreWeave offer, deal terminated. October 30, 2025. Accessed January 19, 2026. <https://www.cnbc.com/2025/10/30/core-scientific-shareholders-reject-9-billion-coreweave-offer-deal-terminated.html>
56. Rochard P. Bitcoin's Security Budget Problem is Solved. August 15, 2025. Accessed August 18, 2026. <https://x.com/BitcoinPierre/status/1956151795287515230>
57. Leonardos S, Monnot B, Reijbergen D, Skoulakis S, Piliouras G. Dynamical Analysis of the EIP-1559 Ethereum Fee Market. In: *Proceedings of the 3rd ACM Conference on Advances in Financial Technologies (AFT '21)*. ACM; 2021:114-126. doi:10.1145/3479722.3480993
58. Budish E, Lewis-Pye A, Roughgarden T. The Economic Limits of Permissionless Consensus. In: *Proceedings of the 25th ACM Conference on Economics and Computation (EC '24)*. 2024:704-731. doi:10.1145/3670865.3673548
59. Roughgarden T. Transaction Fee Mechanism Design. *Journal of the ACM*. 2024;71(4):1-25. doi:10.1145/3674143
60. Chung H, Shi E. Foundations of Transaction Fee Mechanism Design. In: *Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*. SIAM; 2023:3856-3899. doi:10.1137/1.9781611977554.ch150
61. Chung H, Roughgarden T, Shi E. Collusion-Resilience in Transaction Fee Mechanism Design. In: *Proceedings of the 25th ACM Conference on Economics and Computation (EC '24)*. ACM; 2024:1045-1073. doi:10.1145/3670865.3673550
62. Adejumo O. US Bitcoin ETFs Surpass \$100 Billion, Pose Challenge to Largest Bitcoin Holders. November 22, 2024. Accessed October 5, 2026. <https://cryptoslate.com/insights/us-bitcoin-etfs-surpass-100-billion-pose-challenge-to-largest-bitcoin-holders/>
63. iShares Bitcoin Trust ETF. iShares Bitcoin Trust ETF: Prospectus. July 31, 2025. Accessed October 5, 2026. <https://>

- www.sec.gov/Archives/edgar/data/1980994/000143774925024228/bit20250731_424b3.htm
64. Strategy. Strategy Acquires 4,225 BTC and Now Holds 601,550 BTC. July 14, 2025. Accessed October 5, 2026. https://www.strategy.com/press/strategy-acquires-4225-btc-and-now-holds-601550-btc_07-14-2025
 65. Pokorny Z. *The State of Crypto Leverage: Q4 2025, Surviving a Stress Test*. 2026. Accessed October 5, 2026. <https://www.galaxy.com/insights/research/state-of-crypto-leverage-q4-2025>
 66. Held D. Bitcoin's Security is Fine. May 15, 2019. Accessed August 18, 2026. <https://medium.com/@danhedl/bitcoins-security-is-fine-93391d9b61a8>
 67. Schilling L, Uhlig H. Some Simple Bitcoin Economics. *Journal of Monetary Economics*. 2019;106:16–26. doi:10.1016/j.jmoneco.2019.07.002
 68. Garratt R, Hayes R. Bitcoin: How Likely Is a 51 Percent Attack?. November 24, 2014. Accessed July 20, 2026. <https://libertystreeteconomics.newyorkfed.org/2014/11/bitcoin-how-likely-is-a-51-percent-attack/>
 69. Kubal J, Kristoufek L. Exploring the Relationship Between Bitcoin Price and Network's Hashrate Within Endogenous System. *International Review of Financial Analysis*. 2022;84:102375. doi:10.1016/j.irfa.2022.102375
 70. The White House. Strengthening American Leadership in Digital Financial Technology. January 23, 2025. Accessed October 5, 2026. <https://www.whitehouse.gov/presidential-actions/2025/01/strengthening-american-leadership-in-digital-financial-technology/>
 71. The White House. Establishment of the Strategic Bitcoin Reserve and United States Digital Asset Stockpile. March 6, 2025. Accessed October 5, 2026. <https://www.whitehouse.gov/presidential-actions/2025/03/establishment-of-the-strategic-bitcoin-reserve-and-united-states-digital-asset-stockpile/>
 72. Federal Tax Service of Russia. How to Mine Legally: Guidance on the PRO Taxes Programme. March 3, 2026. Accessed October 5, 2026. https://www.nalog.gov.ru/rn77/news/activities_fts/16605641/
 73. National Development and Reform Commission. Notice on Rectifying Virtual-Currency Mining Activities, No. 1283. September 24, 2021. Accessed October 5, 2026. https://www.ndrc.gov.cn/xxgk/zcfb/tz/202109/t20210924_1297474.html
 74. Republic of Kazakhstan. On Digital Assets in the Republic of Kazakhstan, Law No. 193-VII. February 6, 2023. Accessed October 5, 2026. <https://adilet.zan.kz/eng/docs/Z2300000193>
 75. Government of British Columbia. New Legislation Powers Economy with Clean Energy, North Coast Transmission Line. October 20, 2025. Accessed October 5, 2026. <https://news.gov.bc.ca/releases/2025ECS0044-001032>
 76. US International Trade Administration. Ethiopia: Energy-Intensive Tech Opportunities. 2024. Accessed October 5, 2026. <https://www.trade.gov/market-intelligence/ethiopia-energy-intensive-tech-opportunities>
 77. Marathon Digital Holdings. Marathon Digital Holdings and Zero Two to Develop and Operate the First Large-Scale Immersion Bitcoin Mining Facilities in Abu Dhabi. May 9, 2023. Accessed October 5, 2026. <https://ir.mara.com/news-events/press-releases/detail/1312/marathon-digital-holdings-and-zero-two-to-develop-and-operate-the-first-large-scale-immersion-bitcoin-mining-facilities-in-abu-dhabi>
 78. European Parliament and Council of the European Union. Regulation (EU) 2023/1114 on Markets in Crypto-Assets. May 31, 2023. Accessed October 5, 2026. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1114>
 79. Norwegian Ministry of Digitalisation and Public Governance. Written Reply on Cryptocurrency Mining and Data-Centre Regulation. January 12, 2026. Accessed October 5, 2026. <https://www.stortinget.no/no/Saker-og-publikasjoner/Sporsmal/Skriftlige-sporsmal-og-svar/Skriftlig-sporsmal/?qnid=113963>
 80. Auer R. *Beyond the Doomsday Economics of "proof-of-Work" in Cryptocurrencies*. 2019. Accessed July 17, 2026. <https://www.bis.org/publ/work765.htm>
 81. US Department of Justice, Federal Trade Commission. *Horizontal Merger Guidelines*. 2010. Accessed October 5, 2026. <https://www.justice.gov/atr/file/810276/dl>
 82. US Department of Justice, Federal Trade Commission. *2023 Merger Guidelines*. 2023. Accessed October 5, 2026. <https://www.justice.gov/atr/media/1329301/dl?inline>

Cambridge
**Centre
for Alternative
Finance**



In collaboration with



**Financial
Innovation for
Impact**