Bitcoin Policy Institute

Sanctions and Sanctions-Resistant Money

Joshua R. Hendrickson
Craig Warmke

Bitcoin Policy Institute

Sanctions and Sanctions-Resistant Money

About the author(s)

Dr. Joshua R. Hendrickson is a professor of economics and chair of the Economics Department at the University of Mississippi. He is a senior fellow at the American Institute for Economic Research's Sound Money Project, a senior affiliate scholar at the Mercatus Center at George Mason University, and serves on the board of the Mississippi Council on Economic Education.

Dr. Hendrickson's research focuses on the intersection of monetary theory and political economy. He has written extensively on the political economy of bitcoin. He has published articles in scholarly journals such as the Journal of Money, Credit and Banking, the Journal of Economic Dynamics and Control, the Journal of Economic Behavior and Organization, Macroeconomic Dynamics, the Journal of Macroeconomics, Economic Inquiry, Economics and Politics, and Contemporary Economic Policy.

Dr. Craig Warmke is an Associate Professor of Philosophy at Northern Illinois University and a Senior Fellow at the Bitcoin Policy Institute. His research covers money, and especially bitcoin, at the intersection of philosophy, politics, and economics. Craig is a co-author of Resistance Money: A Philosophical Case for Bitcoin (2024) and regularly engages with scholars, technologists, and policymakers on the implications of emerging monetary technologies.

About the Bitcoin Policy Institute

The Bitcoin Policy Institute (BPI) is a non-partisan, non-profit think tank. It is dedicated to educating policymakers and the public on Bitcoin and disruptive digital technologies, providing research-based insights to inform sound policy in the United States.

The BPI team comprises experts in economics, law, philosophy, energy, and environmental science, working together to explore the impacts of new technology on existing US public policy interests. The views expressed in this publication do not necessarily reflect the views of all Bitcoin Policy Institute management or its affiliated scholars.

Bitcoin Policy Institute

Sanctions and Sanctions-Resistant Money

Joshua R. Hendrickson,
Department of Economics, The University of Mississippi

Craig Warmke,
Department of Philosophy, Northern Illinois University

Sanctions and Sanctions-Resistant Money

1 Introduction

Payments require both an asset, such as the dollar, and payment rails over which the asset travels, such as Fedwire.[1] The dollar dominates global payments,[2] and dollar payment rails help the U.S. dominate the globe.[3] Global demand for dollars over dollar rails provides the U.S. considerable leverage over the rest of the world. The U.S. exploits this leverage through international economic sanctions.

Economic sanctions remain potent partly because sovereign nations can coerce trusted parties within the financial system. Compliant trusted parties bar sanctioned entities, seize their assets, and block their transactions. Economic sanctions, then, involve various kinds of financial censorship.

Monetary technologies both old and new permit the custody and transfer of value without trusted parties. Unlike the dollar units slung through electronic payment processors, gold and cash require no trusted parties for custody or transfer. They are physical bearer assets. With cryptocurrency technology, bearer assets have entered the digital sphere. Along various dimensions and to varying degrees,[4] cryptocurrencies minimize the trust required of central authorities to custody and transfer funds. And because cryptocurrencies lack mass, they can traverse distances more quickly than traditional bearer assets. By pairing the speed of electronic money with the trust-minimization of physical cash, cryptocurrencies

[1]Benson et al. [2017].
[2]Bertaut et al. [2023].
[3]McDowell [2023, 19-36] discuss the geopolitical implications of dollar payment rails. [4]Bailey et al. [2024, 4-11] explains how bitcoin eschews three kinds of trusted parties: makers, managers, and mediators.

pose new challenges for law enforcement generally and international sanctions, in particular.

Among cryptocurrencies, bitcoin lacks trusted parties to a higher degree than any other.[5] The bitcoin network settles transactions not through trusted intermediaries but through the globally-dispersed, permissionless, and highly competitive market of bitcoin mining. Because bitcoin miners imbue the bitcoin network with such a high degree of censorship-resistance, they have begun to attract attention from policymakers and regulators keen on preserving the power of economic sanctions.[6] As a new institutional technology with geopolitical ramifications,[7] we should expect nothing less.

Although bitcoin miners do not serve as trusted parties in the traditional sense, U.S.-domiciled miners may provide avenues for efficacious sanctions. In what follows, we explain two mining-centric proposals for censoring sanctioned entities and evaluate their feasibility.[8] As bitcoin matures and settles more cross-border payment volume, these proposals will likely gain in popularity due to their *prima facie* plausibility. However, although sanctions may often limit harm, these specific proposals are likely to do more harm than good—or simply no good at all. A more pragmatic orientation towards bitcoin opens up a more realistic array of compliance and enforcement strategies.

2 The Sanctions Status Quo

Although the dollar's share in foreign currency reserves has steadily declined over the last twenty years, it continues to dominate foreign currency exchange and global payments.[9] On the international scene, about half of all currency exchange and trade involves dollars. The dollar also dominates international banking, accounting for nearly two-thirds of international and foreign currency liabilities and claims.[10] In short, the dollar enjoys the world's strongest monetary network effect.

The dollar's network effect gives the U.S. a strategic advantage in financial statecraft.[11] The Clearing House Interbank Payments System (CHIPS) processes

[5]Luther and Smith [2020] discuss bitcoin's distributed network, while Bailey and Warmke [2023] highlight its uniqueness.

[6]Luther [2022] examines additional motivations for government regulation, such as consumer protection and macroeconomic policy. Furthermore, Alston et al. [2022] discuss external forces that drive competition and development in institutional technologies.

[7]Davidson et al. [2018].

[8]Hendrickson and Luther [2017] discuss the implications of outright bitcoin bans, which are distinct from the proposals examined here.

[9]Maronoti [2022].

[10]Bertaut et al. [2023] provide detailed statistics on these points.

[11]On the notion of financial statecraft, see Steil and Litan [2006].

around 95 percent of large-value domestic and international dollar payments. CHIPS, in turn, routes transactions through branch offices located within U.S. borders. Consequently, a large fraction of international trade falls within the jurisdiction of the U.S.[12]

The U.S. leverages its power over global dollar payments to levy economic sanctions against entities large and small. A special agency within the U.S. Treasury, The Office of Foreign Assets Control (OFAC), blacklists entities by placing them on the Specially Designated Nationals and Blocked Persons List. Entities on this so-called "SDN list" suffer frozen assets, blocked transactions, and, overall, excommunication from the global dollar financial system.

In addition to the direct power exerted over its own financial plumbing, the U.S. exerts indirect power over other routes through the global monetary system.[13] Since 9/11, the U.S. regularly collects payments data from institutions around the globe, especially SWIFT, a global financial messaging system headquartered in Belgium.[14] With this data in hand, the U.S. Treasury identifies and penalizes foreign counterparties of sanctioned entities.

A potent blacklist theoretically serves at least two important purposes. First, it strangles the flow of money for disfavored and harmful activities. Second, the threat of financial strangulation deters both potential bad actors and those financial institutions otherwise disposed to serve them. Through both financial strangulation and deterrence, sanctions aim to curtail human rights abuse, terrorism, narcotics trafficking, and so on.

The aforementioned SDN list is, on a recent tally, 2905 pages long.[15] Although reasonable people may disagree about whether various entities belong on the list, several cases would certainly garner popular support. The Central Bank of the Democratic Republic of Korea is on the list—page 545. As is Kim Jong Un—page 1248. Or consider ISIS—page 1019, under the 'Islamic State of Iraq and the Levant'—or any number of child exploitation rings or drug cartels.

Scholars disagree about both the effectiveness and the ethics of economic sanctions.[16] We will not wade into these debates. Apart from whether or not punitive economic measures are generally effective or ethical, questions about the feasibility and efficacy of particular measures remain. When we assess particular proposals, we may find that some would prove too costly or insufficiently beneficial.

Economic sanctions, in part, aim to censor certain kinds of financial activity.

[12]McDowell [2021].

[13]McDowell [2023, 28 ff.] discusses these so-called "secondary sanctions."

[14]See Mohsin [2024] on the recent expansion of U.S. financial surveillance.

[15]Available at https://www.treasury.gov/ofac/downloads/sdnlist.pdf.

[16]On their effectiveness, see Hufbauer et al. [1990], Tsebelis [1990], Dashti-Gibson et al. [1997], Pape [1997], Pape [1998], Elliott [1998], Marinov [2005], and Peksen [2019b]. On their morality, see, for example, Gordon [1999], Pattison [2005], and Peksen [2019a].

As censorship-resistant money, bitcoin does not fit squarely within traditional sanctions programs. Some strategies tailor-made for the flow of dollars might prove a poor fit for the flow of bitcoin. Moreover, bitcoin's novelty and complexity may cover weak and broken proposals with a veneer of plausibility. We will soon assess two particular proposals for stemming bitcoin flows. But, first, let's review those aspects of bitcoin relevant to the proposals.

3 Bitcoin Pressure Points

Suppose you work for OFAC and hear rumors that a new adversary has adopted bitcoin to evade potential sanctions. What should you do?[17]

To start, you might place the user on the SDN list like any other sanctioned entity. You might even include one or more of their bitcoin addresses, an already common practice that began in 2018.[18] Given the legal framework of U.S. sanctions, merely listing an entity *softly censors* them by discouraging others from transacting with them. For any U.S. person who transacts with the sanctioned entity bears strict liability—those who transact unwittingly with them nevertheless face potentially severe penalties.[19] Given the wide reach of the U.S. sanctions regime, non-U.S. persons also face pressure to avoid dealings with sanctioned entities. Therefore, by placing a bitcoin address on the SDN list, you discourage others from sending bitcoin to that address and using funds received from it.[20]

In the traditional financial system, funds flow through trusted parties. Even if a sanctioned entity finds an eager counterparty for a transaction, both parties require a willing intermediary unless the parties transact directly, which is often either inconvenient or impossible, depending on the preferred mode of payment. And, in the legal framework of economic sanctions, trusted parties face severe penalties for serving sanctioned entities. In 2015, a French bank paid $8.9 billion in a settlement after facilitating transactions for sanctioned entities in Cuba, Iran, and Sudan.[21] For the obvious reason, then, few trusted parties willingly challenge the U.S. sanctions regime. Economic sanctions have therefore traditionally involved an additional layer of censorship—*strong censorship*. Whereas soft censorship deters others from transacting *with* you, strong censorship deters financial institutions from transacting *for* you.

[17] Wahrstätter et al. [2023] provides a starting point for understanding such scenarios.

[18] Office of Foreign Assets Control [2021c, 15] documents this practice.

[19] Office of Foreign Assets Control [2021c].

[20] Technically, bitcoin transactions have no "from" address, but, at a suitable layer of abstraction, this phrasing is acceptable. See Antonopoulos and Harding [2023, 18ff.]. As we explain in Section 5.1, the bitcoin network operates a "push" rather than "pull" payments system. It is cost-prohibitive for the average user with a known bitcoin address to deny funds from anyone.

[21] Raymond [2015].

Blacklisted users of bitcoin are subject to both soft and strong censorship through economic sanctions. Despite the trust-minimization available through cryptocurrency networks, trusted parties pepper the cryptocurrency landscape as custodians, payment processors, exchanges, stablecoin issuers, and so on. Law enforcement agencies routinely work with such institutions to freeze funds and catch criminals. But this provides small comfort to those seeking the assurances provided by sanctions in the world of traditional finance. Although bitcoin users *can* and often do use trusted parties, they *needn't* do so. With a digital bearer asset such as bitcoin, trusted parties are optional.

Since bitcoin requires no trusted parties, it lacks obvious pressure points for achieving the usual level of strong censorship from levying economic sanctions. Therefore, if the U.S. Treasury seeks to enforce compliance over the bitcoin network through a stronger form of censorship, it must find fulcra in the bitcoin network akin to the financial system's more traditional trusted parties.

Back to your job as an OFAC official—as a first order of business, you survey the various participants in the bitcoin network and assess their censorship capabilities.[22] With some simplification, you find that, besides the individuals who transact in bitcoin, the main participants fall into three non-exclusive categories:

- **Developers**, who maintain bitcoin's software.
- **Full nodes**, computers that run the software to validate proposed updates to the ledger and cultivate copies of the updated ledger.
- **Miners**, computers specially equipped to compete for the right to update the ledger.[23]

Since individual users rely on bitcoin software—no transaction settles without it—perhaps you could strongly censor a target indirectly through developers. You could do this by having them incorporate a transaction filter into the software. However, enforcing sanctions through the developers would fail for legal, technical, and sociological reasons. On the legal front, the courts have ruled that software is constitutionally protected free speech.[24] You cannot lawfully prevent someone from writing or publishing code that fails to censor a targeted entity. Technically, you would need a significant percentage of node operators to run OFAC-compliant software. And, sociologically, most node operators would likely refuse to do so.

Instead of coercing developers to include OFAC-compliant censorship filters, which is constitutionally dubious, you might fork bitcoin's software and include the

[22] Bailey et al. [2024, Ch. 2] cover censorship in the bitcoin ecosystem. For more on the bitcoin network, see Warmke [2021] and Antonopoulos and Harding [2023].

[23] When convenient, we will often use the same label for the people who run these computers.

[24] Collins [1997].

filters yourself. To succeed, a large portion of the network would need to run your OFAC-compliant software. Baking OFAC compliance into bitcoin's software would reintroduce the very thing bitcoin was designed to avoid—a trusted party with the power to censor. The global community of bitcoin enthusiasts would inspect the open-source proposal and find the OFAC filters etched into the software. Few, if any, nodes would run the software; doing so would undermine bitcoin's raison d'être as credibly neutral money.[25]

We've already seen a trial run of this sort of technique to change bitcoin's issuance and security features, not from a government entity, but from Greenpeace USA.[26] In a failed "Change the Code, Not the Climate" campaign funded by an executive of a cryptocurrency competitor, Greenpeace USA lobbied bitcoin developers to transition bitcoin from proof-of-work to proof-of-stake.[27] Although Greenpeace USA believed this would make bitcoin more environmentally friendly, it would, at this stage of bitcoin adoption, eat into bitcoin's credible neutrality for two reasons. First, proof-of-stake protocols rely on trusted nodes to counter the weak subjectivity problem.[28] Second, and in theory, power concentrates in proof-of-stake protocols because they pair rich-get-richer effects with wealth-is-power effects.[29] For the foreseeable future, any such campaign perceived to erode bitcoin's resistance properties is liable to fail.

As a pragmatic matter, then, sanctions enforcement must happen elsewhere, not among developers or node runners. This leaves the miners.

4 Mining and Pooling

Let's begin with a closer look at the role of mining in transaction settlement. Before full nodes append a new block of transactions to the blockchain, they first filter candidate transactions. When Bob attempts to send bitcoin to Alice, his wallet software constructs a transaction and sends it to the full nodes for validation. If the transaction passes a battery of tests, the full nodes relay the transaction to the rest of the network. The transaction then appears across several mempools, the queues of valid transactions miners draw from to create new blocks.

Mining a block of valid transactions requires two main operations.[30] The first, *block construction*, consists in bundling valid transactions with the right form, syntax, and digital accoutrements. The second, *hashing*, is a form of computation.

[25] Bailey and Warmke [2023].
[26] Kharif [2022].
[27] Ashraf and Pan [2022].
[28] Buterin [2014].
[29] Bailey et al. [2024, Ch. 10.4] examine these effects in detail.
[30] Antonopoulos and Harding [2023, Ch. 12] provide technical detail.

Before mining became industrialized, miners did both. Today, miners still hash—mining *is* hashing. But mining pools now play a larger role in block construction. This division of labor means that miners and mining pools might assume distinct roles in a sanctions regime. So let's explore block construction and hashing a bit further.[31]

Constructing a valid block requires bundling information from valid transactions into the proper format and attaching a header with the appropriate block metadata.[32] The header itself contains information about the previous block—this connects the blocks into a blockchain—as well as a cryptographic summary of the current block's transactions. It also has an empty slot for a *nonce*, a random number that resolves a hashing-involved mathematical challenge.

As a general mathematical phenomenon, hashing consists in feeding information into a function that returns an unpredictable but fixed-size string of bytes. So the hash function, as the name suggests, garbles the input. This garbling undergirds the bitcoin mining competition that recurs, on average, every ten minutes.

In the competition, full nodes set a numerical threshold every two weeks—think of this like lowering or raising the height of a bar in a game of mathematical limbo. Then, miners feed the hash function with candidate block headers. By hashing candidate headers with different nonces, miners produce trillions of random numerical outputs. This worldwide, iterative guessing game produces an output below the target every ten minutes, on average.[33] Upon finding such an output, a miner forwards the candidate block to the network so that full nodes can validate and endorse it. The winning block includes a transaction that rewards its miner with both transaction fees and newly minted bitcoin along a well-defined issuance schedule.[34]

The resource-intensive and unpredictable nature of bitcoin mining has led bitcoin miners to pool their computational resources. In exchange for a fee, mining pools enable miners to win a smaller but more consistent share of the mining rewards. When a pool participant wins a block, the pool distributes the reward to all participants proportionally to their contributed computational power. By dividing labor, miners needn't run full nodes or cultivate mempools. So whereas mining pools coordinate hashpower, distribute rewards, and often construct block

[31]The hashing-construction separation in bitcoin is analogous to the proposer-builder separation in Ethereum. For the latter, see Buterin [2021] and Heimbach et al. [2023]. Hashers in bitcoin also propose blocks, but they win the lottery to propose the next block through hashing rather than through random selection among stakers.

[32]The group of transactions could be empty.

[33]Mining is a Poisson process—we can reliably predict how often miners win blocks over time even though each block comes randomly and independently of all others. See Warren [2023, 11].

[34]The issuance schedule sets the maximum reward for each block. So a miner could voluntarily collect less, as in block 74,638, for example.

templates, miners now largely serve as hash specialists.[35]

To better differentiate miners from pools, let's consider examples of each. Consider the top three publicly traded bitcoin miners–Marathon Digital Holdings, CleanSpark, and Riot. In January 2025, Marathon, CleanSpark, and Riot produced 750 BTC, 626 BTC, and 527 BTC, respectively.[36] Marathon, the most productive bitcoin mining company, reports that they accounted for 5.1% of all bitcoin produced that month.

Yet Riot and Marathon differ in how they use mining pools. According to reports, Riot had used Braiins (formerly Slush Pool) as recently as 2022 before switching to another pool.[37] Marathon, however, uses its own pool, MaraPool. So the pool's share of the network hashrate (in hashes per second) currently boasts around the same share as the company's percentage of all bitcoin rewards. Although Marathon is one of the largest mining companies in the world, its pool pales in comparison to the world's largest. The leading mining pool, Foundry USA, has about one third of the world's hashrate and hence accounts for around one third of all bitcoin produced.[38] In second place, Antpool enjoys roughly one fifth of network hashrate. So, on average, they together account for approximately every other block. For reasons to be explained shortly, these two pools alone boast enough computing power in theory to gatekeep bitcoin's blockchain. They would simply need to coordinate.[39]

After examining the mining ecosystem, Treasury officials might view bitcoin miners and mining pools domiciled in the U.S. as being powerful enough to enforce sanctions—akin to the trusted intermediaries of traditional finance. Some proposals to use miners as tools of state-sponsored censorship might therefore appear attractive. In what follows, we look at two proposals in particular. These proposals deserve closer scrutiny because they have, in fact, been proposed.

[35]This particular arrangement may change in the future. New mining protocols such as Stratum V2 return the power of block construction back to the miners, giving them optionality in whether and how to include certain transactions in a candidate block. For documentation, see https://stratumprotocol.org/docs/. But in the absence of protocols such as Stratum V2, miners seem content to rely on mining pools for block templates in exchange for the benefits of pooling hashrate.

[36]MARA Holdings, Inc. [2025], CleanSpark, Inc. [2025], and Riot Platforms, Inc. [2025].

[37]Ashraf [2022].

[38]See https://mempool.space/graphs/mining/pools and https://insights.braiins.com/en.

[39]Antonopoulos and Harding [2023, 290] specify a 30% threshold for some mining attacks.

5 Block Compliance

In a relatively recent keynote talk at Princeton University, Carole House proposed two strategies for OFAC-compliant bitcoin mining.[40] House is the former Director for Cybersecurity and Secure Digital Innovation in the White House National Security Council, previously led cybersecurity policy efforts for the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN), and most recently served as a National Security Council Special Advisor for Cybersecurity and Critical Infrastructure Policy for the White House. During her leadership role at the National Security Council, House co-authored Biden's Executive Order 14067 titled "Ensuring Responsible Development of Digital Assets." In short, she has a keen sense for how regulators, policymakers, and the executive branch have been thinking about bitcoin's relation to sanctions compliance and enforcement. House's endorsement of these proposals provides strong reason to evaluate them as serious policy recommendations.

We will call the first proposal the *block compliance strategy*. On this strategy, the Treasury demands that U.S.-domiciled miners and pools avoid blocks with transactions involving blacklisted addresses. Those responsible for block construction would filter any transaction that either spends bitcoin from such an address or sends bitcoin to such an address.

At the time of writing, the SDN list includes 1,480 bitcoin addresses.[41] By comparison, 152 addresses appeared in the list released on April 30th, 2021.[42] This ten-fold increase over a four-year period also highlights the increased focus bitcoin has garnered from the highest levels of law enforcement. But this April 2021 list has particular interest for us. It was the most recent list available to Marathon Digital Holdings when they announced their first "clean" block.[43] In the preceding months, they had signaled their intention to adopt an OFAC-compliant strategy through their mining pool.[44] However, things didn't go as planned.

The received wisdom among bitcoin enthusiasts says that Marathon's failure reveals inherent challenges with implementing a block-compliance strategy.[45] However, while block-compliance may serve poorly as a means for state-sponsored censorship of sanctioned entities, its implementation is, in fact, trivial. So we must separate two questions: (1) whether block compliance is *feasibly* implementable, and (2) whether, once implemented, block compliance would *effectively* censor

[40] House [2023].

[41] By contrast, blacklisted addresses totaled 330 on Ethereum, 8 on Monero, 5 on Zcash, and 1 on Ripple.

[42] Office of Foreign Assets Control [2021b].

[43] Marathon Digital Holdings, Inc. [2021a].

[44] Marathon Digital Holdings, Inc. [2021b].

[45] For snapshots of the event's coverage, see Harper [2021] and Post [2021].

sanctioned addresses. Since it's not widely appreciated that Marathon's challenges had little to do with the implementation of block compliance, let's review the ordeal to see why.

5.1 The Feasibility of Block-Compliance

In March 2021, Marathon Digital Holdings announced that it would voluntarily adopt a block-compliant strategy through its own mining pool.[46] Then, on May 6th at 12:50 AM EST, Marathon reportedly mined block 682170, their first "clean" block.[47] On-chain sleuths soon lodged two complaints about Marathon's strategy. First, block 682170 included transactions associated with Hydra, a Russian dark web market. Second, within hours of mining block 682170, some Iranians reportedly sent bitcoin to the very address at which Marathon had received its mining reward.[48] Not long after bitcoin enthusiasts clobbered the company over social media, Marathon renounced their transaction filter.[49] A consensus soon formed that mining compliant blocks is extremely difficult and that bitcoin's design is fundamentally at odds with rules tailored for traditional finance.

That consensus was, and is, far from the truth. Marathon's compliance debacle owed more to poor public relations than falling short of its stated strategy. Before we look more closely, let's disentangle three different grades of compliance in the production of a block:

- **Grade 1**. Precludes transactions involving sanctionable entities or activity.
- **Grade 2**. Precludes transactions involving SDN-listed entities.
- **Grade 3**. Precludes transactions involving SDN-listed bitcoin addresses.

Mining blocks with no sanctionable activity—Grade 1—is unrealistic. We should not hold bitcoin miners and pools to a much higher standard than traditional financial institutions. If a mining pool has no reason to believe that a transaction involves illicit activity, partly because OFAC has not flagged any connected addresses, then we cannot realistically expect the mining pool to filter the transaction.

It's also worth remembering that in both absolute and relative terms, bitcoin arguably facilitates less criminal activity than the U.S. dollar.[50] In the last three years, the share of illicit activity in total cryptocurrency transaction volume has

[46]Marathon Digital Holdings, Inc. [2021b].
[47]Marathon Digital Holdings, Inc. [2021a]
[48]Harper [2021].
[49]Marathon Digital Holdings, Inc. [2021c].
[50]Schulp et al. [2023].

remained well below one percent. This is what we should expect: on- and off-ramps are often closely surveilled with public data trails. They also boast much less liquidity compared to dollar rails. Criminals prefer highly liquid ramps, not only for less slippage in the exchange for other assets, but also for blending into the crowd.

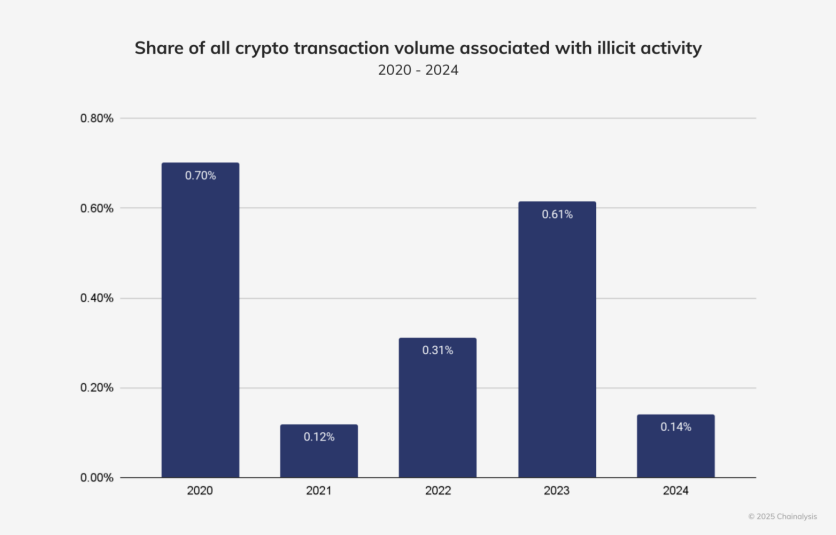

Figure 1: Transaction volume illicit activity on cryptocurrency networks. Source: Chainalysis [2025].

What's more, Figure 1 concerns illicit transaction volume for cryptocurrencies generally, not just bitcoin. According to data compiled by Chainalysis, stablecoins and assets on non-bitcoin networks account for more than three-fourths of illicit activity in each of the last several years. In 2024, for example, illicit activity on bitcoin accounted for less than .03% of its transaction volume.[51] If anything, law enforcement should encourage criminals to use bitcoin rather than alternatives so that, with the public ledger of transactions, officials may monitor networks of illicit activity more closely. So Grade 1 compliance constitutes neither a realistic nor a desirable goal.

Nor should we expect miners to filter any transactions involving SDN-listed entities and satisfy Grade 2 compliance. If OFAC places Bob on the SDN list, how would any miner know whether or not a transaction involves Bob? Bitcoin transactions involve pseudonymous addresses—not names, physical addresses, fingerprints, social security numbers, email addresses, IP addresses, or what have you. The US Treasury cannot expect miners and mining pools to conduct all their own costly fishing expeditions for any bitcoin address affiliated with any of the several

[51] Chainalysis [2025].

thousand SDN-listed entities. In the main, this due diligence falls under OFAC's purview. If OFAC wants miners to filter transactions, they should provide the relevant bitcoin addresses. And there are several places where OFAC might find them—from websites of sanctioned entities (where an entity might volunteer an address for donations or business), from centralized bitcoin exchanges (where an entity might have exchanged assets), from other law enforcement investigations, and from collaborating with data analytics firms like Chainalysis. So, overall, Grade 2 compliance is unrealistic, too.

Only Grade 3 compliance remains. Contrary to the opinion of many bitcoin enthusiasts, Grade 3 involves no insurmountable obstacles. OFAC already publishes bitcoin addresses purportedly affiliated with SDN-listed entities. Block builders can filter transactions with those addresses quite easily. And Marathon did not fail to filter transactions with those addresses—or, at least, the transactions provided as evidence for failure do no such thing. Recall the two issues with Marathon's supposedly porous filtering: the transactions involving the Hydra dark web market and those involving Marathon as the recipient of bitcoin from Iranian users. We'll consider these in reverse order.

According to blockchain explorer, oxt.me, block 682170 included a single transaction with an input from an address affiliated with Bitzlato, an exchange, and three outputs containing addresses affiliated with Hydra:[52]

Transaction ID

`wdfd26ffd3e5cd8d36a9332f847c89e7d7566d5593eb5c592e691ba6d116a80a3`

Recipient addresses tagged to Hydra	**BTC Amount**
`361iiMT9uAnz8FSm23wH8UqG5SAb9Uew6d`	0.001182
`3KCZiAzLLtdRXfwSVhdVNQ89q8BaNxMgCG`	0.002243
`3PJypYrYZaV6eEyDxa6vgNdAXYFX92xjMw`	0.004076

At the time of this transaction, in early May 2021, the most recent SDN list had been posted to the OFAC website on April 30th, 2021. That list included neither Hydra nor any of the above addresses. The Treasury did eventually sanction Hydra—almost a year later, on April 5th, 2022.[53] To this day, the Hydra-tagged addresses from Block 682170 do not appear on the SDN List. Whether those addresses genuinely belonged to Hydra or not, the point still stands: Marathon did not fall short of Grade 3 compliance, the most reasonable level of compliance to expect from a public company. In fact, it didn't even fall short of Grade 2

[52] See https://oxt.me/transaction/tiid/3475813837.

[53] For more on Hydra, see Chainalysis [2022].

compliance because OFAC hadn't yet sanctioned Hydra. Notably, Bitzlato, the purported source of bitcoin in this transaction, was later shut down around the time that the Treasury sanctioned Hydra.[54] Yet, at the time, Bitzlato wasn't sanctioned either.[55]

What, then, about the transactions from Iran? Every block has a coinbase transaction—a transaction that sends the bitcoin block reward to the block's miner or pool. A coinbase reward consists of a quantity of bitcoin equal to the sum of the subsidy (i.e., the scheduled issuance for that block) and the block's total transaction fees. Like any other bitcoin transaction, the coinbase transaction is public. In block 682170, we find both Marathon's address and the details of its total reward:[56]

Recipient Address: `3LC8dDKyBsrWPfzhXyt7aAyjXxGYkfDdHu`

Block Reward: 6.25 BTC (subsidy) + 0.05095356 BTC (fees) = 6.301 BTC

Soon after block 682170 appeared, some Iranian bitcoin users reportedly sent more bitcoin to Marathon's coinbase address.[57] For example, in block 682280, one such transaction sent 0.00008982 BTC to the Marathon address along with a Persian message in the OP_RETURN field. In English, the message reads, "Thanks for supporting our cause."[58] Unlike Hydra, Iran was already sanctioned at the time in question. And it was widely reported at the time that these supposed Iranian transactions helped undermine Marathon's compliance strategy.

This reasoning does not survive close scrutiny. Because the bitcoin network is a push rather than pull network, payers control where bitcoin goes.[59] Bitcoin also has a public ledger. As long as your address is known and all previously used addresses are known, you have virtually no say in whether your address receives bitcoin, even if it comes from a sanctioned source. Any reasonable sanctions regime must take this into account.

The U.S. Treasury largely does already. According to guidance from OFAC published in October 2021, a recipient of funds known to come from a sanctioned entity must "block" them and "deny all parties access to that virtual currency."[60]

[54]U.S. Department of Justice, Eastern District of New York [2022].

[55]Financial Crimes Enforcement Network [2023].

[56]https://mempool.space/tx/9f6f1ae55623aa320f430f9e3c6dc762c147035e713b96d72c20a58cf45fbbf.

[57]See arbedout [2021] for the most widely shared tweet and Harper [2021] and Post [2021] for reporting on the issue.

[58]See https://mempool.space/tx/c959...9cad. We used ChatGPT for translation.

[59]For more on the distinction between push and pull networks, see Benson et al. [2017, Ch. 1]. Note, however, that Benson et al. [2017] differentiate the two kinds of payment systems based on the action of an intermediary–whether it pulls funds from the sender or pushes them to the recipient. Bitcoin disrupts these definitions. It shows that push networks can exist without intermediaries.

[60]Office of Foreign Assets Control [2021a].

Doing so is trivial, given bitcoin's peculiar transaction model. Each chunk of bitcoin sent to an address appears in a uniquely identifiable sort of digital check called a UTXO (short for unspent transaction output). To comply with the blocking and denial requirements, the recipient needn't do much more than (1) keep the relevant private key(s) private so that others cannot spend it and (2) not spend the UTXO oneself.[61] OFAC's reporting requirements for having received digital currency from a sanctioned individual are also fairly trivial to follow.[62]

At the time, Marathon had little actionable evidence that sanctioned Iranians had genuinely sent bitcoin to their coinbase address. Anyone in the world can include a Persian message in a transaction's `OP_RETURN` field. Additionally, some non-Iranians would also have had reason to do so, namely anti-censorship advocates in the U.S. eager to undermine Marathon's compliance program. So Marathon had little reason to suspect that they had received bitcoin from sanctioned entities. Even if they had, they could have easily followed OFAC guidelines for blocking, denial, and reporting, given the structure of bitcoin UTXOs. Furthermore, since the addresses in question also never appeared on the SDN List, mining blocks with them would not violate Grade 3 compliance. We have little to no evidence that anyone violated the stronger but more unreasonable form of Grade 2 compliance, let alone the weaker and more reasonable level of Grade 3 compliance.

It is important to draw the right lessons from Marathon's compliance debacle. If mining OFAC-compliant blocks is a matter of avoiding SDN-listed bitcoin addresses, we've seen no evidence that Marathon failed. Filtering SDN-listed addresses from one's own blocks remains a trivial matter—it is comparable to blocking calls from particular phone numbers or emails from particular addresses.

The mining industry within the U.S. could plausibly implement censorship of OFAC-sanctioned addresses within their own blocks. Here's how it might work. Once daily, pools download an updated list of sanctioned bitcoin addresses. Then, within seconds, pools use the list to filter transactions during block construction. Insofar as OFAC collates and publicizes the list, compliance imposes no severe technological burden. In fact, some mining pools already filter transactions with sanctioned bitcoin addresses.[63]

So is block-compliance feasible to implement? Yes, at a reasonable level, such as Grade 3. Yet feasibility is one matter; effectiveness is another.

[61] For more on UTXOs, see Warmke [2022].

[62] For a list of OFAC's answers to frequently asked questions about digital currency, see Office of Foreign Assets Control [2018].

[63] 0xB10C [2025].

5.2 The Effectiveness of Block Compliance

Bitcoin would likely continue to settle transactions involving sanctioned addresses even if the U.S. mining industry successfully implemented the block-compliance strategy. Mining happens around the globe; anyone with the internet and a miner can use energy to produce a block. Furthermore, although U.S. mining pools recently boast about one third of the network hashrate, China effectively still retains over forty-percent of the network hashrate through mining pools.[64] This is about one hundred times the share of hashrate required for a transaction to settle within a day. It's more than enough to counter U.S. censorship through its mining pools.

This points to a key misunderstanding in House's endorsement of a block compliance strategy. Here is House in her own words:

> I'm not a lawyer but I would never want to be the person looking across an OFAC Council, the office that administers sanctions, telling them that I, the administrator of a mining pool, had been responsible for validating a block of half a billion dollars going to North Korea – that the US government had gone through the effort to very quickly attribute and tell the world publicly and add to the SDN list.
>
> This is North Korea. They stole from you. Don't let this move – they're designated. I would not want to be the ones telling them that validating that transfer that otherwise could not have occurred was not providing material support to a prohibited transaction.[65]

House seems to think that the miner or pool which includes a transaction serves as a trusted party—that the transaction "otherwise could not have occurred" without the miner's permission. Mining does not work this way. Even if an overwhelming majority of miners exclude a transaction from their blocks, the remaining miners may include it in theirs. So it simply isn't true that by including a transaction it "otherwise could not have occurred."

For perspective, over reasonable time frames, the percentage of blocks won by a miner approaches the miner's share of network hashrate.[66] So how soon a transaction will likely appear in the blockchain depends on the share of *friendly network hashrate*—the hashrate that will not censor the transaction. Given the average block interval of ten minutes, the amount of time E a transaction is expected to settle depends on the percent of friendly network hashrate, x: $E = \frac{10 \text{ minutes}}{x/100}$. The

[64] https://hashrateindex.com/hashrate/pools.
[65] House [2023] from from 27:56 - 29:14.
[66] Warren [2023, 11].

graph in Figure 2 depicts the inverse relationship between the friendly share of network hashrate and a transaction's expected settlement time:

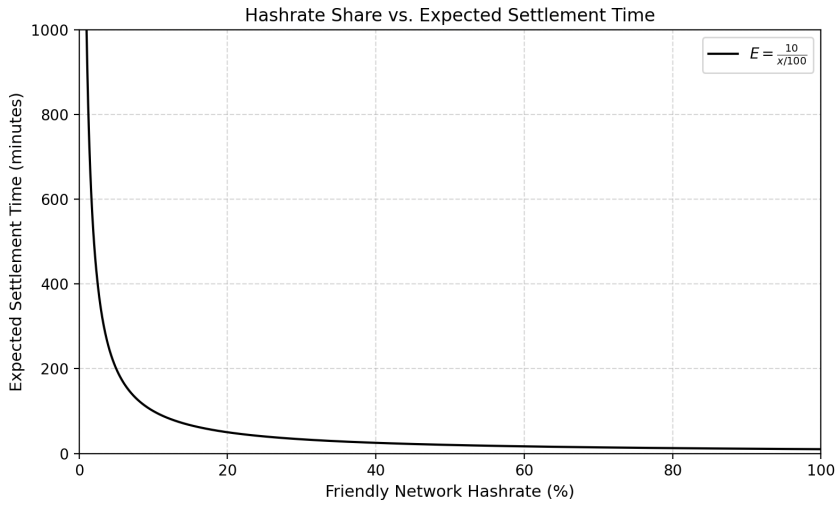

Figure 2: As a miner's share of network hashrate increases, the time expected to mine a block approaches ten minutes.

Miners with a measly 0.7% combined share of the network hashrate could reasonably expect to win a block around every 14285.71 minutes—that is, around once per day. Even if 99.3% of network hashrate belongs to unfriendly miners, the remaining hashrate would likely suffice for the transaction to settle within a day or so. And waiting a single day for final settlement still beats many alternatives for wires and cross-border payments, which can take days or weeks, especially for sanctioned entities who would otherwise meet roadblocks along more traditional rails.

Speaking on the overall effectiveness of a block-compliance strategy, the mathematician, Micah Warren, writes:

> The least effective way for a pool or collection of pools to censor is simply to decline to process a transaction. Even if the pool has a majority of the hashrate, anything less than 100% hashrate will allow the transaction on the chain.[67]

[67] Warren [2023, 90].

The block-compliance strategy would work only if everyone fully complied—everyone: publicly traded mining companies in the U.S. individual miners in emerging economies with off-grid energy sources, and any miners in sanctioned countries.

Here, we run into another problem with global compliance. Miners net transaction fees. So if several miners conspire to censor a user's transaction, the user can bump the fee to incentivize other miners to include it more quickly. The higher the fee, the more likely that some miner somewhere will eventually include it in a block. Transaction fees incentivize censorship-resistance.[68]

Given bitcoin's incentive design, as compliant hashrate share approaches one hundred percent, non-compliant transactions would require higher fees for more timely settlement. So even if block-compliant mining were to boast 99.3% of the network's hashrate, non-compliant miners would net more and higher transaction fees than they otherwise would, assuming that sanctioned entities would desire to settle their non-compliant transactions more quickly than around a day's time.

Suppose we're in such a scenario where, because of settlement preferences, non-compliant miners garner more fee revenue per block. Then, all else being equal, with more fee revenue per block, non-compliant miners could profitably deploy more hashrate compared to their compliant competitors. With such a higher share of the network's hashrate, non-compliant blocks would occur more often, not less. This follows because bitcoin's mining difficulty adjusts algorithmically to ensure that blocks continue to appear, on average, every ten minutes even as the network hashrate waxes and wanes. So when a cadre of miners gains ground in the overall share of network hashrate, they thereby gain a larger piece of the revenue pie. Since mining is zero-sum, their gain is everyone else's loss—with a lower share of network hashrate, the remaining miners collectively win blocks less frequently.[69] On the margins, then, non-compliant miners might therefore raise the price per hash just enough to run some compliant miners out of business.

Ideally, and in isolation, increasing the transaction costs of OFAC-designated entities is a good thing. But given the zero-sum nature of bitcoin mining, as compliant miners increase their share of network hashrate, the more likely that sanctioned entities would pay even higher fees for more timely settlement. And the more fees that non-compliant miners reap, the more hashrate they can deploy. Insofar as increased hashrate translates to a higher share of network hashrate, non-compliant miners would provide even faster settlement times for sanctioned entities. Hence, like a rubber band, as compliant miners approach a total monopoly on block production, non-compliant fees exert a growing restorative force, enabling non-compliant miners to deploy increased hashrate and, under reasonable assumptions, a corresponding increase in the total share of network hashrate.

[68] Voskuil [2020, 21].

[69] Cross and Bailey [2021, 2022].

Hence, the block-compliance strategy could increase transaction costs for "bad guys." But, insofar as it does, the strategy snaps back and threatens to increase the profits and network influence of non-compliant miners, who might themselves be OFAC-sanctioned entities. In such scenarios, a block-compliance regime essentially subsidizes non-compliant miners with a tax on compliant ones. Overall, as the strategy increases in effectiveness, success counterintuitively becomes less likely.

Even if House were right that those who mine blocks with transactions for designated persons "are potentially guilty of a strict liabilities sanction violation," perhaps we should simply carve out an exception for the decentralized monetary networks for which those laws might make less sense.[70] For a prohibition on mining transactions with blacklisted addresses would, first, have no discernible effect on whether the transactions appear in the blockchain and, second, at most reward non-compliant miners at the expense of compliant ones with more fee revenue.

In summary, some of the received wisdom across the bitcoin community is wrong—implementing a regime of block-compliance poses no insurmountable challenge. Implementation is not only feasible but rather trivial. Yet feasibility and efficacy can come apart. And, with block-compliance, they do. The strategy is easy to implement but practically impotent and potentially counterproductive.

Block-compliance requires universal compliance, and, in the real world, universal compliance is practically unachievable. First, Chinese mining pools already boast the greatest share of hashrate. Second, some entities not only use bitcoin precisely because they want to evade or avoid sanctions but also have the energy resources to mine blocks with their own transactions. Finally, to the extent that miners approach universal compliance, bitcoin's incentive design makes universal compliance less likely and in a way that threatens compliant mining revenue.

Let's therefore leave block-compliance behind and evaluate a more promising strategy for censoring transactions.

6 Chain Compliance

Although a block compliant strategy would inevitably fail, House also endorsed a more sophisticated strategy in her Princeton keynote:

> Wouldn't it be great if the conditions could be set where the majority of the computing power—if you garnered that kind of support among the miners...—and basically said, "how about we share a common value which is we don't like North Korea stealing this money from us and it going directly to support proliferation. *Don't validate it, and if other miners or if other people do, don't build on that.*" Also I think that

[70] House [2023], from 28:00–28:40.

> not only because you're subject to potential sanctions implications in doing it, but just also because it sucks they were stolen.[71]

With the ineffective block compliance strategy, compliant miners mind their own business. But with this more sophisticated *chain compliant* strategy, compliant miners mind others' business, too. To explain the strategy, we must wade more deeply into the mechanics of bitcoin mining.

6.1 Chain Basics

Full nodes on the bitcoin network reach agreement about the state of the ledger in the absence of trusted parties and central authorities. Instead of following a ruler, full nodes follow a rule. Specifically, they endorse whichever chain of blocks is the *heaviest*, the series of blocks whose production likely used the most computation. A chain's heaviness depends on the estimated combined computational effort to produce the winning hashes of its component blocks.

In a feat of elegant engineering, nodes on the bitcoin network need only inspect one feature of blocks to find competing ledgers and estimate the combined computational effort of each. This feature is the block's winning hash. For it reveals both the preceding block and the computational effort likely used to produce the hash.[72] The bitcoin protocol requires that a block's winning hash appears in the next block's header—a title page of sorts that also includes a cryptographic summary of a block's transactions, the variable difficulty threshold, and a random number. Simplifying a bit, mining involves varying the random numbers in potential block headers and feeding them into the hash function until an output satisfies the network's current difficulty threshold. Since each block in the ledger has a header with the previous block's winning hash, the winning hashes order blocks into a series.

Those same hashes also serve as self-referencing measures on the probable amount of work required for their production. Every two weeks, the bitcoin network algorithmically sets a numerical threshold under which any winning hash must fall. Lower thresholds shrink the space of acceptable outputs. Since hash outputs are unpredictable, and miners hash through trial-and-error, numerically lower hash outputs generally involve more computation. Nodes observe candidate chains of blocks strung together by their hashes and endorse the chain whose hashes, in aggregate, likely required the most computation. No central authority required.

Yet in the absence of a central authority, the heaviest chain rule exposes bitcoin to reorganizations of the blockchain (or, "reorgs"). Although each block can

[71] House [2023].
[72] Warmke [2021].

have but one predecessor, any block could temporarily have multiple successors. Sometimes, two equally valid blocks propagate at around the same time, and different miners begin to build on top of each. As the chain branches into two, full nodes eventually endorse the heavier chain. Although this happens as a matter of course when miners find winning hashes at approximately the same time, it can also happen intentionally. For example, someone may attempt to overtake the heaviest chain with an alternative that rewrites one or more of the most recent blocks. Because 51% of the network's hashrate suffices to produce the heaviest chain, this is often called a 51% attack.[73]

Rewriting blocks enables double-spending where bitcoin spent in an orphaned block gets spent again in a newly written block. Or, instead of double-spending, one might overtake the heaviest chain to produce empty blocks and render bitcoin unusable. Or, instead of censoring all transactions with empty blocks, one might overtake the heaviest chain to exclude particular transactions indefinitely. Whatever the reason, any rewritten blocks prove costly to their original miners. In a reorg, the mining rewards within a rewritten block disappear along with it. Since the cost to produce a block approaches the block reward's dollar value, a lost reward is quite costly, indeed.

6.2 Incentivizing Compliance

As House suggests, the chain compliance strategy does not merely demand that miners or pools exclude certain transactions in their own blocks. Instead, it manipulates incentives by increasing the costs to include them. Suppose OFAC-compliant miners form a coalition and sincerely announce their intention not to build directly on top of a non-compliant bitcoin block. When a non-compliant block first appears, the coalition will not immediately endorse it. The coalition will instead try to mine a compliant block in the hope that it will replace the non-compliant block in the heaviest chain. To succeed, the compliant coalition must produce two consecutive blocks.

Even if the U.S. has a small minority of global hashrate, the announcement alone upsets the expected value of mining on top of non-compliant blocks. Suppose the U.S. has as little as, say, ten percent of global hashrate. The U.S then has a 1% chance of producing two blocks in a row. As a result, any new non-compliant block has a 1% chance of being reorg-ed. So an independent but economically rational miner accordingly discounts by 1% the expected value of producing a non-compliant block.

Without assurances that the transaction fees of non-compliant transactions will swamp the discount, economically rational miners will also build on top of

[73] See fn. 39.

compliant blocks and mine compliant blocks themselves, which effectuates a discount cascade for the expected value of mining non-compliant blocks. In bitcoin discussion forums, this attack is known as *feather forking*.[74]

In a feather fork, the discount on non-compliant block production increases quadratically with the compliant coalition's share of hashrate. That is, when a coalition of miners with a percent of network hashrate, n, credibly announces the intention to censor, rational non-coalition miners discount the value of mining a non-compliant block by n^2.[75]

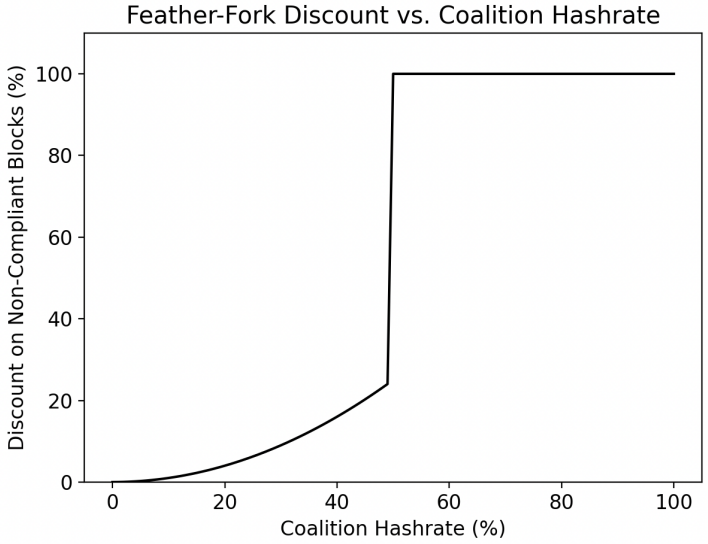

Figure 3: The discount on non-compliant block production scales with the share of compliant hashrate until it nears 51%.

Note that a coalition with majority hashrate can effectively censor transactions indefinitely. At that point, the discount for non-compliant mining jumps to 100%. In such a scenario, non-compliant miners must increase their share of hashrate to produce any blocks at all. To do so, one might increase one's raw hashrate or, whether through incentives or sabotage, reduce the hashrate of compliant miners. In any case, the success of the chain compliant strategy depends on the hashrate share of compliant miners, the fee premium from non-compliant transactors, and the penalties, if any, non-compliant miners expect to pay.

These complexities call for a model.

[74]Miller [2013].

[75]Maxwell [2013], Bonneau et al. [2015].

7 Strategic Behavior and Effectiveness

To examine how miners would behave in the presence of censorship, we develop a model of the strategic behavior of miners. For simplification, we partition miners into two groups. One group only cares about the expected profit from mining compliant transactions and mines blocks with those transactions alone, i.e., compliant blocks. Their expected profit depends partly on the other group's share of hashrate.

This second group also maximizes expected mining profits but its miners are willing to mine blocks with non-compliant transactions—i.e., non-compliant blocks. This group faces additional costs. One such cost is the likelihood that the compliant group re-writes non-compliant blocks with compliant ones. Another potential cost involves penalties for detection. We assume that the entity imposing censorship rules can identify the miner of a non-compliant block with some positive probability and impose some sort of punishment. The expected punishment cost then factors into the willingness of these miners to participate in the mining competition.

The choice of hashrate for each group is strategic because the probability of mining a block depends on the hashrate of the other group. Since we assume that the groups decide on their hashrates simultaneously, each group must set its hashrate based on its expectations of the other's choice. The resulting choice of hashrate for each group represents a Nash equilibrium. Our framework enables us to solve for any existing Nash equilibrium and check whether such an equilibrium is incentive-feasible for each group.

Classifying all miners into two groups oversimplifies matters, as we will discuss below. Nonetheless, since our primary focus is whether or not miners would produce non-compliant blocks, this setup reveals the success conditions of censorship more precisely.

7.1 The Model

We assume that miners broadly fit into one of two groups of type $i \in \{1, 2\}$, in which Group 1 is willing to mine non-compliant blocks and Group 2 is only willing to produce compliant ones. Since the members of each group face the same incentives, we will assume that decisions occur at the group level. When we later discuss the broader implications and comparative statics of the model, we will note the implications for disparate members in each group. As previously mentioned, the model assumes that each group makes a once-and-for-all decision about the hashrate committed to their strategy.[76]

[76] Alternatively, we could assume that each group makes investment decisions about hashrate. However, if we are interested in the long-run outcome, a steady state equilibrium investment

The following is the optimization problem for non-compliant Group 1:

$$\max_{h_1} \gamma_1(h_1, h_2)(pb + t) - c_1(h_1) - \gamma_2(h_1, h_2)\theta(p'b' + t') - qF$$

where γ_1 is the probability that Group 1 mines a block as a function of each group's hashrate, p is the price of bitcoin, b is the block reward, t is the block's transaction fee, $c_1(\cdot)$ is the cost of mining as a function of the group's hashrate and $\frac{\partial c_1}{\partial h_1}, \frac{\partial^2 c_1}{\partial h_1^2} > 0$, q is the probability that the group is detected as non-compliant, and F is the penalty for non-compliance. The third term, $\gamma_2(h_1, h_2)\theta(p'b' + t')$, is the expected loss from losing a block reward from the previous period, $(p'b' + t')$, after the second group re-writes the last block (with probability θ) and replaces it with a compliant block. We can interpret $\theta \in (0, 1)$ as the fraction of Group 2 miners who attempt to re-write a new non-compliant block with a compliant one. So the policy levers here include both θ, reorg aggressiveness, and qF, the expected penalty.

In Group 2's optimization problem:

$$\max_{h_2} \gamma_2(h_1, h_2)(pb + t) - c_2(h_2)$$

γ_2 is the probability that Group 2 mines a block and $c_2(\cdot)$ is the cost of mining as a function of hashrate and $\frac{\partial c_2}{\partial h_2}, \frac{\partial^2 c_2}{\partial h_2^2} > 0$. Note that since there are only two groups, it must be true that $\gamma_1 + \gamma_2 = 1$.

The first-order conditions for each group yield reaction functions that specify the choice of hashrate as a function of the other group's choice of hashrate. These first-order conditions are given for Group 1 and Group 2, respectively, as

$$\frac{\partial \gamma_1}{\partial h_1}(pb + t) = \frac{\partial c_1}{\partial h_1} + \frac{\partial \gamma_2}{\partial h_1}\theta(p'b' + t')$$

$$\frac{\partial \gamma_2}{\partial h_2}(pb + t) = \frac{\partial c_2}{\partial h_2}$$

Note that the reaction functions show that each group chooses to increase its hashrate up to the point where the expected marginal benefit of additional hashrate equals the marginal cost of increasing hashrate. But only Group 1 factors in the expected marginal cost from a rewritten block.

Let us now specify the functional forms of γ_i and c_i, for $i = 1, 2$. Suppose that $\gamma_1 = \frac{h_1}{h_1 + h_2}$. This implies $\gamma_2 = \frac{h_2}{h_1 + h_2}$. In addition, suppose that $c_1(h_1) = \frac{\phi_1}{2}h_1^2$ and $c_2(h_2) = \frac{\phi_2}{2}h_2^2$. Furthermore, to simplify some of the notation, let $a := pb + t$

choice is independent of time as is the resulting "stock" of hashpower. Thus, it wouldn't change the model's implications.

and assume that $a' = \psi a$ where $\psi > 0$. Thus, ψ is a measure of the value of an orphaned block relative to the current block. As a result, the reaction functions can be re-written as

$$\frac{h_2}{(h_1 + h_2)^2}\left[(1 + \theta\psi)a\right] = \phi_1 h_1 \tag{1}$$

$$\frac{h_1}{(h_1 + h_2)^2}a = \phi_2 h_2 \tag{2}$$

The equilibrium choices of these two groups satisfy these two equations with two unknowns. In addition, it must be the case that the expected benefit of each group is greater than the total expected cost, including the cost punishment. It must be the case that,

$$\left[\frac{h_1^*}{h_1^* + h_2^*} - \frac{h_2^*}{h_1^* + h_2^*}\theta\psi\right]a - \frac{\phi_1}{2}(h_1^*)^2 - qF \geq 0 \tag{3}$$

$$\gamma_2(h_1^*, h_2^*)a - \frac{\phi_2}{2}(h_2^*)^2 \geq 0 \tag{4}$$

where h_1^* and h_2^* are the optimal choices of hashrate for each group from equations (1) and (2).

Solving equations (1) and (2) requires numerical methods. We calibrate the parameters of the model as follows. Since one block is mined approximately every 10 minutes, $\gamma_i(h_1, h_2)a$ is the expected reward, where γ_i is the probability of mining the next block, and a is the block reward plus the transaction fees in the next block. To simplify the calibration of the model, we will abstract from transaction fees. We will assume that the price of bitcoin is \$55,000 and the block reward is 3.125 bitcoin. Hence, $a = \$171,875$. The expected benefit is defined per block. Since a block arrives, on average, every 10 minutes, the parameters ϕ_1 and ϕ_2 can be thought of as the marginal cost per terahash.

As a benchmark, we will assume that both groups face the same electricity costs. To calibrate the electricity cost, suppose that the miners in both groups pay \$0.10 per kWh of electricity and that each group uses the Antminer S19. These machines have an efficiency of 34.2 joules per terahash. Since 32.4 joules is equal to 0.0000095 kWh, we get a cost of \$0.00000095 per terahash.[77] Given that an S19 can produce 141 terahashes per second, the same machine can produce 84,600 terahashes per 10-minute interval. The cost of running a machine is therefore approximately \$0.08 per interval. Let h_i denote the number of S19s (in millions) run during that 10-minute interval, then $\phi_1 = \phi_2 = \$80,000$. Furthermore, for the benchmark allocation, we set $\theta = qF = 0$. Finally, note that ψ is not separable from θ in terms of optimal decision-making. Thus, we normalize $\psi = 1$.

[77] $1\text{joule} = 2.78 \times 10^{-7}\text{kWh}$.

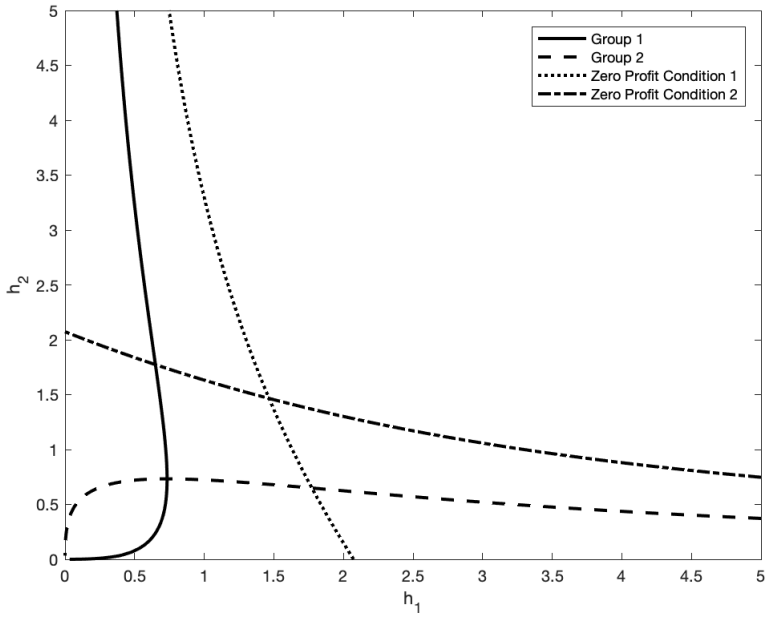

Figure 4: **Benchmark Allocation**

Figure 4 shows the reaction function for each group. The point at which the two curves intersect is the equilibrium hashrate pair that solves equations (1) and (2).[78] In addition, we have plotted zero expected profit conditions for each group. Note that any point below the zero expected profit condition curve for each group represents a positive expected profit, whereas any point above the curve is a negative expected profit. Thus, only the choices of h_1^* and h_2^* that lie within the positive expected profit regions or on the zero expected profit curve are assumed to be compatible with the incentives of miners. As shown in Figure 4, our baseline assumptions result in equilibrium choices with positive expected profits. Since the baseline calibration does not include any costs associated with detection or any lost value to Group 1 from orphaned blocks, the solution is symmetric and $h_1 = h_2 \approx 0.73$. This solution implies that each group operates approximately 730,000 S19s, which would correspond to a total hashrate of 205 million terahash per second.[79]

Our primary focus concerns whether sanctions can successfully drive the optimal choice of Group 1 to a negative expected profit. Although one could argue

[78]Note that $h_1 = 0$ and $h_2 = 0$ also solves equations (1) and (2). However, in that scenario, no one is hashing new blocks, and sanctions are irrelevant. Thus, we ignore this possible equilibrium.

[79]The observed hashrate for the Bitcoin network as of September 2024 was around 600 million terahash per second.

that those committed to censorship resistance might continue to mine with negative expected profit because they get some additional non-pecuniary benefit from doing so, this is not financially feasible long-term. Thus, we will consider any outcome in which Group 1's optimal choice would result in negative expected profit as successful censorship. To get a sense of how punishments and orphaned blocks affect the decision-making process of those willing to mine transactions targeted for sanctions, we need to consider changes in qF and θ, respectively.

Consider first the role of θ, which represents the fraction of Group 2 willing to rewrite a previous non-compliant block. Note that for Group 1, an increase in θ has both a substitution effect and an income effect. In terms of the substitution effect, a higher θ increases the costs associated with mining by lowering Group 1's expected profit, which, in turn, reduces the incentive to contribute to mining effort. However, at the same time, the higher the value of θ, the greater the incentive Group 1 has to win the next block, since the group has more at stake. Thus, the income effect implies that Group 1 should want to provide more mining effort. Whether Group 1 provides more or less mining effort will depend on which effect dominates. To demonstrate the effect of changes in θ, Figure 5 adjusts the benchmark allocation such that $\theta = 0.1$ in the left panel and $\theta = 0.9$ in the right panel.

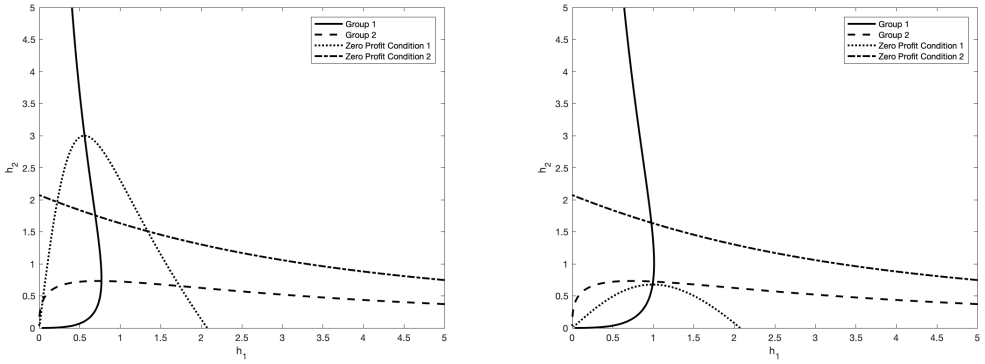

Figure 5: **The Effect of Re-Writing the Blockchain**. The figure plots the reaction functions and zero profit conditions under the assumption that $\theta = 0.1$ (left panel) and $\theta = 0.9$ (right panel).

As shown in Figure 5, a positive value for θ significantly reduces Group 1's potentially profitable allocations. When $\theta = 0.1$, although the set of profitable combinations of hashrate between the two groups is significantly smaller, the allocation of hashrate between the groups is relatively unaffected. As shown in the right panel of Figure 5, as θ increases, this increases h_1 relative to h_2. Thus, the threat of a previously mined block being re-written actually encourages Group 1

to contribute more mining effort relative to Group 2. However, as the right panel of Figure 5 shows, a sufficiently high value of θ shrinks the set of profitable opportunities to exclude Group 1 from its optimal choice. So if a sufficiently large fraction of Group 2 is willing to re-write the blockchain, then those willing to mine sanctioned transactions will find it unprofitable to do so.

Now consider the effect of the expected punishment, qF, of being caught including transactions in a mined block that have been targeted for sanctions. There are a couple of important points to note. The first is with regard to marginal decision making. As shown from equations (1) - (4), the expected punishment does not have any effect on the choice of mining effort contributed to the network by Group 1. However, the expected punishment does have an effect on the profitability of mining. Thus, a sufficiently large expected punishment could discourage Group 1 from participating in the market. Since there are no countervailing effects, it is straightforward to understand that positive expected punishment costs will result in a hump-shaped zero-profit condition for Group 1 since the expected punishment operates like a fixed cost of mining. As the expected punishment rises, the set of profitable allocations of mining effort shrinks. As a result, if the expected punishment is sufficiently large, those willing to mine transactions targeted for sanctions will be driven from the market because it is unprofitable to do so. A second important result is that what matters is the expected punishment. Those seeking to sanction transactions can increase the expected punishment by either increasing the probability of detection or by increasing the cost of the punishment once detected.

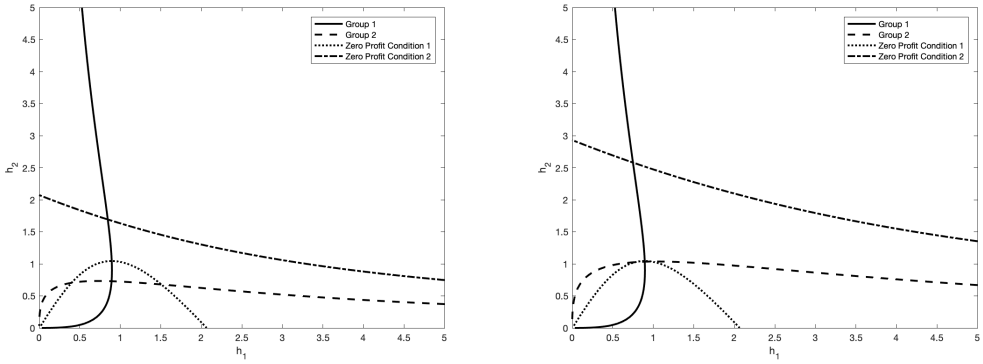

Figure 6: **The Effect of Different Energy Costs**. The figure plots the reaction functions and zero profit conditions under the assumption that $\theta = 0.5$ and $qF = \$1,000$. In the left panel, energy costs are equal for both groups. In the right panel, $\phi_2 = 0.5\phi_1$

Overall, what this analysis suggests is that censorship of transactions on the

blockchain is possible if the fraction of miners that are willing to rewrite the blockchain to exclude sanctioned transaction is sufficiently high or if the expected punishment is sufficiently large. Importantly, the thresholds for whether or not Group 1 will continue to operate depend on the relative energy costs of the two groups. In the benchmark allocation, it was assumed that both groups faced identical energy costs. However, to see how the incentives to mine non-compliant transactions changes, let's modify the benchmark allocation from $\theta = qF = 0$ to $\theta = 0.5$ and $qF = \$1,000$. This new benchmark is shown in the left panel of Figure 6. Now, suppose that $\phi_1 = \$80,000 = 2\phi_2$. Then, the marginal cost of mining for Group 2 is half that of Group 1. The effect of this difference is shown in the right panel of Figure 6. Note from the right panel that both Group 1 and Group 2 increase their mining effort. However, the equilibrium allocation is now barely profitable for Group 1. This yields the interesting result that those willing to process non-compliant transactions will contribute more mining effort when their competition faces lower energy costs, but that such effort might not be profitable depending on the relative costs, the expected punishment, and the fraction of miners willing to re-write the blockchain. All else equal, sanctions are likely to be more successful in areas with higher energy costs.

Given these conclusions, it is also useful to return to the limitations of the model. As we acknowledge, confining the groups into two categories is an oversimplification. It is therefore worthwhile to examine the types of miners that might fall into each group and what implications we can draw from the model. In reality, miners would likely fall into one of four different categories. For example, some miners are chain-compliant—they will only mine compliant blocks and attempt to re-write non-compliant blocks. A second subgroup is merely block-compliant (Section 5) and will never try to re-write non-compliant blocks. A third group of economically rational miners simply ignores sanctions and mines whatever block is profit-maximizing. The fourth and final subgroup of non-compliant miners is not only willing to mine non-compliant blocks, but might even seek out such blocks for mining.

Despite this greater complexity, our model can capture at least some of this behavior. For example, Group 1 in our model can be thought to consist of non-compliant miners and economically rational miners whereas Group 2 consists of chain compliant miners and block compliant miners. In our model, the division of Group 2 into two distinct subgroups is simply measured by the parameter θ, which can be thought of as the fraction of Group 2 that is chain compliant whereas the fraction that is merely block compliant is $1 - \theta$.

In addition, consistent with our model, sanctioning bodies would likely target only members of Group 1 for punishment—those who produce non-compliant blocks. But by varying the expected punishment, the sanctioning body might

also convince economically rational miners to quit mining non-compliant blocks. However, it is not entirely clear whether such efforts would actually be successful. For example, when the share of non-compliant hashrate declines, those wishing to get non-compliant transactions processed are likely to offer higher transaction fees to miners. It is at least theoretically possible that the transaction fees would be high enough to offset an increase in the expected punishment. However, that is beyond the scope of our model. Furthermore, it should be pointed out that the sanctioning body would not necessarily to be able to vary the expected punishment in predictable ways. For example, members of Group 1 might have an incentive to engage in behavior that makes them appear to be block compliant. Whether or not such members are able to do that would depend on the cost of hiding behavior relative to their ability to avoid detection. To the extent that Group 1 can avoid detection, this lowers q in our model. The only variable that the sanctioning body truly has at its disposal is the punishment once detected, F. Again, although modeling this process of avoiding detection is beyond the scope of our model, it is nonetheless an important determinant of q and therefore would likely affect the sanctioning body's choice of F.

7.2 Further Complications

Although the model provides a useful framework for understanding a chain-compliance strategy in the abstract, we suspect that a U.S.-led feather fork to censor non-compliant transactions would face a number of complications that the model does not explicitly capture. Those complications include:

- The amount of U.S. hashrate from harder-to-detect miners that would switch to non-compliant pools. For smaller miners—especially those with an indiscernible impact on the grid—there will be no conceivable enforcement without more authoritarian surveillance around energy use.
- The amount of hashrate that would re-locate to non-compliant jurisdictions for additional non-compliant fee revenue and/or cheaper energy.
- The amount of U.S. hashrate that may shut down in protest or in favor of a comparatively more profitable business model, especially given the energy demand for artificial intelligence training and inference.[80]

Hence, we cannot reliably ascertain ahead of time the relative share of hashrate the U.S. might cede following a feather-fork announcement. As a result, the U.S. cannot safely forecast the consequences of a feather fork by banking on the share of hashrate currently thought to reside within the borders of compliant jurisdictions.

[80]Data accessed on 3/13/2024 from `https://mempool.space/`.

In addition to that uncertainty, the U.S. could encounter a range of further unintended consequences and unforeseen costs:

- Below 51 percent hashrate, the compliant-mining coalition may require federal subsidy to continue feather-forking, with larger subsidies required the further below 51 percent the coalition goes. This could effectively nationalize the U.S. bitcoin-mining sector and ignore a public-relations firestorm—why would the U.S. make a once-profitable and growing industry unprofitable and then bridge the difference with taxpayer money?

- Much of the mining within the U.S. occurs in states like Texas, which may mount prolonged court battles. Does the federal government have the standing to block miners in Texas from building *compliant* blocks on top of non-compliant blocks?

- A feather-fork announcement could motivate other countries to bring more hashrate online. Even if the U.S. currently boasts, say, 40% of global hashrate, an announcement might inspire several countries to subsidize the capital and operational expenditures of miners within their borders to protect their own ability to transact without hindrance as a matter of national security. In other words, a feather-fork announcement could jump-start *defensive mining*.

Countries ripe for defensive mining include not only those on the SDN list but also BRICS-affiliated nations, including many resource-rich countries where cheaper energy could underwrite rapid hashrate expansion. Many of these countries have sought routes around the dollar's dominance in global payments. So an attempt by the U.S. to bend the world's most credibly neutral monetary network into conformity with U.S. interests might evoke push-back in the form of additional or subsidized hashrate—a counter that could render compliant U.S. miners *unprofitable*. We should also note that, across the top ten mining pools, pools historically affiliated with China boast more hashrate than pools run in the U.S.[81]

Much more could be said about variations on the feather-fork proposal.[82] Overall, however, even though a feather fork could conceivably succeed, its expected value to the United States is inscrutable, and it carries a reasonable chance of being counter-productive. As countries continue to recognize the strategic, geopolitical importance of neutral money for their own economic and security interests, the failure of a U.S.-led feather fork becomes more likely—not less. The looming specter of an expensive, interminable hash-war of attrition may explain why no country has yet attempted such a measure.[83]

[81]Data available at `https://insights.braiins.com/en`.

[82]See Miller [2013] and Warren [2023, 90 - 111].

[83]Morosz et al. (2020).

In summary, we do not seem to live in a world with conditions ripe for a successful OFAC-led feather fork. There are too many resource-rich countries with incentives to protect their own ability to transact over a neutral monetary network. Hence, the chain-compliance strategy—which involves feather forking—is likely not worth trying. The cost of success is incalculable. The chance of failure is high. The risks to U.S. businesses are substantial.

8 Conclusion

Although both block-compliance and chain-compliance strategies suffer from poor cost-benefit ratios, those generally supportive of U.S. sanctions need not despair.

First, the bitcoin ledger is fully public and effectively permanent. So even without any additional sanctions enforcement mechanisms, the ledger is likely an aid to U.S. sanctions enforcement through a combination of analytics and soft censorship (Section 3). Officials may not be able to stop certain transactions. But they can trace flows of money and build evidence chains extending over years or decades. Those who assist sanctions evaders must avoid slip-ups for years on end. So, too, must those who assist the assisters. By not driving miners overseas—or making domestic mining uneconomical—the United States also retains valuable visibility and subpoena leverage.

Second, bitcoin is an anti-authoritian technology that empowers whistle blowers, journalists, oppressed minorities, and "good" criminals in other countries with censorship-resistant money.[84] Supporting domestic mining helps undermine the very entities that populate the SDN list. Bitcoin exports liberal values peacefully.[85]

Third, without a majority of global hashrate, the U.S. itself is susceptible to feather forks and other ledger-rewrite attacks. A failed chain-compliance strategy may hobble domestic mining and potentially compromise national resilience. The U.S. has good reason to support miners and or at least not burden them with ineffective or costly restrictions, given its economic and geopolitical interests. In 2023, the White House proposed the Digital Asset Mining Energy (DAME) excise tax where "firms would face a tax equal to 30 percent of the cost of the electricity they use in cryptomining."[86] The proposal, motivated by environmental concerns, would have effectively killed the domestic mining industry. But given mining's role in renewable-energy build-out, grid demand-response, and methane-mitigation programs, the tax would likely have harmed rather than benefitted the environment

[84]Bailey and Warmke [2023] and Bailey et al. [2024].

[85]Pines [2021].

[86]For details, see Council of Economic Advisers [2023].

overall.[87] U.S. adversaries would also have quietly cheered: mining elsewhere would have become more profitable and made the U.S. more vulnerable to mining attacks, including feather forks.

In the years ahead, obtaining and retaining a substantial share of bitcoin hashrate stands to become a matter of geopolitical importance. Rather than try to reproduce in bitcoin the levels of censorship familiar from traditional finance, the U.S. would likely do better by planning for a hashrate arms race in which it is itself a vulnerable target.

In a not-too-distant future, hashrate treaties may be necessary to prevent an unproductive arms race. And mining facilities will also need protection against sabotage as a matter of national security—for a substantial loss in the share of hashrate here means a substantial gain in revenue and power elsewhere. Although we are not there yet, countries have little time to realize that benefitting from bitcoin's credible neutrality may require active participation.

Acknowledgments

For helpful comments, we thank Andrew Bailey, Nathan Ballantyne, Marcello Di Bello, Troy Cross, David Dunning, Zachary Glatzer, Thomas Hogan, David McElhoes, Bradley Rettler, and especially William Luther. We also thank audiences from the 2023 Mont Pelerin Society meeting in Bretton Woods and the philosophy department at Arizona State University.

Disclosures

The authors are Senior Fellows with the Bitcoin Policy Institute, a non-partisan, non-profit think tank.

References

0xB10C. Fifteen ofac-sanctioned transactions missing from blocks, 2025. URL `https://b10c.me/observations/13-missing-sanctioned-transactions-2024-12/`.

E. Alston, W. Law, I. Murtazashvili, and M. Weiss. Blockchain networks as constitutional and competitive polycentric orders. *Journal of Institutional Economics*, 18(5):707–723, 2022.

[87] See Bailey et al. [2024, Chs. 9-10].

A. M. Antonopoulos and D. Harding. *Mastering Bitcoin*. O'Reilly, Boston, 3rd edition, 2023.

arbedout. Tweet dated 2021-05-06. Twitter, 2021. URL https://twitter.com/arbedout/status/1390296943511982080. Accessed: 2025-02-13.

A. Ashraf. Bitcoin miner riot switches mining pool after falling short in november, 2022. URL https://www.coindesk.com/business/2022/12/05/bitcoin-miner-riot-switches-mining-pool-after-falling-short-in-november/.

Aoyon Ashraf and David Pan. Greenpeace, crypto billionaire lobby to change bitcoin's code. 2022. URL https://www.bloomberg.com/news/articles/2022-03-29/greenpeace-crypto-billionaire-lobby-to-change-bitcoin-s-code?embedded-checkout=true. Accessed: 2024-12-20.

A. M. Bailey and C. Warmke. Bitcoin is king. In J. Liebowitz, editor, *Cryptocurrency: Concepts, Technology, and Issues*. Taylor & Francis, 2023.

A. M. Bailey, B. Rettler, and C. Warmke. *Resistance Money: A Philosophical Case for Bitcoin*. Routledge Press, 2024.

C. C. Benson, S. Loftesness, and R. Jones. Payments systems in the us: A guide for the payments professional, 2017.

C. Bertaut, B. von Beschwitz, and S. Curcuru. The international role of the us dollar, 2023. URL https://www.federalreserve.gov/econres/notes/feds-notes/the-international-role-of-the-us-dollar-post-covid-edition-20230623.html. FEDS Notes.

J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In *2015 IEEE symposium on security and privacy*, pages 104–121, 2015.

Vitalik Buterin. Proof of stake: How i learned to love weak subjectivity, 2014. URL https://blog.ethereum.org/2014/11/25/proof-stake-learned-love-weak-subjectivity.

Vitalik Buterin. Proposer/block builder separation-friendly fee market designs, 2021. URL https://ethresear.ch/t/proposer-block-builder-separation-friendly-fee-market-designs/9725.

Chainalysis. Hydra and garantex: OFAC takes action as russia-based crypto crime grows, 2022. URL https://www.chainalysis.com/blog/hydra-garantex-ofac-sanctions-russia/. Accessed: 2025-02-13.

Chainalysis. 2025 crypto crime trends: Illicit volumes portend record year as on-chain crime becomes increasingly diverse and professionalized, January 2025. URL https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/. Accessed: 2025-02-10.

CleanSpark, Inc. Cleanspark releases january 2025 bitcoin mining update, February 2025. URL https://investors.cleanspark.com/news/news-details/2025/CleanSpark-Releases-January-2025-Bitcoin-Mining-Update/. Accessed: 2025-02-07.

J. P. Collins. Speaking in code: Bernstein v. united states department of state, 922 f. supp. 1426 (nd cal. 1996); bernstein v. united states department of state, 945 f. supp. 1279 (nd cal. 1996). *The Yale Law Journal*, 106(8):2691–2696, 1997.

Council of Economic Advisers. The DAME tax: Making cryptominers pay for costs they impose on others. White House blog post, May 2 2023. URL https://web.archive.org/web/20230503060352/https://www.whitehouse.gov/cea/written-materials/2023/05/02/cost-of-cryptomining-dame-tax/.

T. Cross and A. M. Bailey. Greening bitcoin with incentive offsets, 2021. URL https://www.resistance.money/green/.

T. Cross and A. M. Bailey. Carbon-neutral bitcoin for nation states. In *International Conference on Financial Cryptography and Data Security*, pages 55–65. Springer International Publishing, 2022.

J. Dashti-Gibson, P. Davis, and B. Radcliff. On the determinants of the success of economic sanctions: An empirical analysis. *American Journal of Political Science*, pages 608–618, 1997.

S. Davidson, P. De Filippi, and J. Potts. Blockchains and the economic institutions of capitalism. *Journal of Institutional Economics*, 14(4):639–658, 2018.

K. A. Elliott. The sanctions glass: half full or completely empty? *International Security*, 23(1):50–65, 1998.

Financial Crimes Enforcement Network. Imposition of special measure prohibiting the transmittal of funds involving Bitzlato as a primary money laundering concern, 2023. URL https://www.fincen.gov/sites/default/files/shared/Order_Bitzlato_FINAL%20508.pdf. Accessed: 2025-02-13.

J. Gordon. A peaceful, silent, deadly remedy: The ethics of economic sanctions. *Ethics & International Affairs*, 13:123–142, 1999.

C. Harper. Marathon miners have started censoring bitcoin transactions; here's what that means, 2021. URL https://www.coindesk.com/tech/2021/05/07/marathon-miners-have-started-censoring-bitcoin-transactions-heres-what-that-means/.

L. Heimbach, L. Kiffer, C. Ferreira Torres, and R. Wattenhofer. Ethereum's proposer-builder separation: Promises and realities. In *Proceedings of the 2023 ACM on Internet Measurement Conference*, pages 406–420, 2023.

J. R. Hendrickson and W. J. Luther. Banning bitcoin. *Journal of Economic Behavior & Organization*, 141:188–195, 2017.

C. House. Keynote: Decenter spring conference 2023, princeton university, 2023. URL https://vimeo.com/819245954.

G. C. Hufbauer, J. J. Schott, and K. A. Elliott. *Economic sanctions reconsidered: History and current policy*, volume 1. Peterson Institute, 1990.

Olga Kharif. Greenpeace, crypto billionaire lobby to change bitcoin's code, 2022. URL https://www.bloomberg.com/news/articles/2022-03-29/greenpeace-crypto-billionaire-lobby-to-change-bitcoin-s-code.

W. J. Luther. Regulating bitcoin—on what grounds? *Journal of New Finance*, 2 (4):4, 2022.

W. J. Luther and S. S. Smith. Is bitcoin a decentralized payment mechanism? *Journal of Institutional Economics*, 16(4):433–444, 2020.

MARA Holdings, Inc. Mara announces bitcoin production and mining operation updates for january 2025, February 2025. URL https://ir.mara.com/news-events/press-releases/detail/1386/mara-announces-bitcoin-production-and-mining-operation-updates-forjanuary-2025. Accessed: 2025-02-07.

Marathon Digital Holdings, Inc. Marathon digital holdings becomes the first north american enterprise miner to produce fully aml and ofac compliant bitcoin, May 2021a. URL https://ir.mara.com/news-events/press-releases/detail/1239/marathon-digital-holdings-becomes-the-first-north-american. Accessed: 2025-02-10.

Marathon Digital Holdings, Inc. Marathon digital holdings to launch the first north american-based bitcoin mining pool, fully compliant with u.s. regulations, March 2021b. URL https://ir.mara.com/news-events/press-releases/detail/1232/marathon-digital-holdings-to-launch-the-first-north-

american-based-bitcoin-mining-pool-fully-compliant-with-u-s-regulations. Accessed: 2025-02-10.

Marathon Digital Holdings, Inc. Marathon signals for taproot, May 2021c. URL https://ir.mara.com/news-events/press-releases/detail/1244/marathon-signals-for-taproot. Accessed: 2025-02-10.

N. Marinov. Do economic sanctions destabilize country leaders? *American Journal of Political Science*, 49(3):564–576, 2005.

B. Maronoti. Revisiting the international role of the us dollar, 2022. URL https://www.bis.org/publ/qtrpdf/r_qt2212x.htm.

G. Maxwell. Re: Feather-forks: enforcing a blacklist with sub-50 URL https://bitcointalk.org/index.php?topic=312668.msg3353100#msg3353100.

D. McDowell. Financial sanctions and political risk in the international currency system. *Review of International Political Economy*, 28(3):635–661, 2021.

D. McDowell. *Bucking the Buck: US Financial Sanctions and the International Backlash Against the Dollar*. Oxford University Press, 2023.

A. Miller. Feather-forks: enforcing a blacklist with sub-50 URL https://bitcointalk.org/index.php?topic=312668.0.

Saleha Mohsin. *Paper Soldiers: How the Weaponization of the Dollar Changed the World Order*. Penguin Random House, New York, NY, 2024.

Office of Foreign Assets Control. Questions on virtual currency, 2018. URL https://ofac.treasury.gov/faqs/topic/1626. Accessed: 2025-02-13.

Office of Foreign Assets Control. Faq 646, 2021a. URL https://ofac.treasury.gov/faqs/646. Accessed: 2025-02-13.

Office of Foreign Assets Control. Specially designated nationals and blocked persons list (sdn list), May 2021b. URL https://web.archive.org/web/20210503044548/https://www.treasury.gov/ofac/downloads/sdnlist.pdf. Accessed: 2025-02-10.

Office of Foreign Assets Control. Sanctions compliance for the virtual currency industry, 2021c. URL https://ofac.treasury.gov/media/913571/download?inline.

R. A. Pape. Why economic sanctions do not work. *International Security*, 22(2):90–136, 1997.

R. A. Pape. Why economic sanctions still do not work. *International Security*, 23 (1):66–77, 1998.

John Pattison. The ethics of economic sanctions. *Journal of Moral Philosophy*, 2 (1):123–145, 2005.

D. Peksen. Political effectiveness, negative externalities, and the ethics of economic sanctions. *Ethics & International Affairs*, 33(3):279–289, 2019a.

D. Peksen. When do imposed economic sanctions work? a critical review of the sanctions effectiveness literature. *Defence and Peace Economics*, 30(6):635–647, 2019b.

M. Pines. Bitcoin and u.s. national security: An assessment of bitcoin as a strategic opportunity for the united states, 2021. URL `https://www.btcpolicy.org/articles/bitcoin-and-us-national-security`.

K. Post. An 'ofac-compliant' bitcoin miner revives debate about transaction censorship, 2021. URL `https://www.theblock.co/post/104263/an-ofac-compliant-bitcoin-miner-revives-debate-about-transaction-censorship`.

Nate Raymond. Bnp paribas sentenced in $8.9 billion accord over sanctions violations, 2015. URL `https://www.reuters.com/article/idUSKBN0NM41J/`.

Riot Platforms, Inc. Riot announces january 2025 production and operations updates, February 2025. URL `https://www.riotplatforms.com/riot-announces-january-2025-production-and-operations-updates/`. Accessed: 2025-02-07.

J. Schulp, J. Solowey, N. Anthony, and N. Thielman. Overstating crypto crime won't lead to sound policy, 2023. URL `https://www.cato.org/blog/overstating-crypto-crime-wont-lead-sound-policy`.

Benn Steil and Robert E. Litan. *Financial Statecraft: The Role of Financial Markets in American Foreign Policy*. Yale University Press and Brookings Institution Press, New Haven, 2006.

G. Tsebelis. Are sanctions effective? a game-theoretic analysis. *Journal of Conflict Resolution*, 34(1):3–28, 1990.

U.S. Department of Justice, Eastern District of New York. Founder and majority owner of cryptocurrency exchange pleads guilty to unlicensed money transmitting, 2022. URL `https://www.justice.gov/usao-edny/pr/founder-and-majority-owner-cryptocurrency-exchange-pleads-guilty-unlicensed-money`. Accessed: 2025-02-13.

E. Voskuil. Cryptoeconomics. fundamental principles of bitcoin, 2020. URL https://voskuil.org/cryptoeconomics/cryptoeconomics.pdf.

A. Wahrstätter, J. Ernstberger, A. Yaish, L. Zhou, K. Qin, T. Tsuchiya, and et al. Steinhorst, S. Blockchain censorship. *arXiv preprint*, 2023. URL https://arxiv.org/pdf/2305.18545.pdf.

C. Warmke. What is bitcoin? *Inquiry*, pages 1–43, 2021. URL https://www.tandfonline.com/doi/abs/10.1080/0020174X.2020.1860123.

C. Warmke. Electronic coins. *Cryptoeconomic Systems*, 2(1), 2022. doi: 10.21428/58320208.eb69605e.

M. Warren. *Bitcoin: A Game-Theoretic Analysis*. Walter de Gruyter, 2023.

Bitcoin Policy Institute

www.btcpolicy.org