STAFF
REPORTS

NO. 1112
AUGUST 2024

Regulating Decentralized Systems: Evidence from Sanctions on Tornado Cash

Anders Brownworth | Jon Durfee | Michael Junho Lee | Antoine Martin

FEDERAL RESERVE BANK *of* NEW YORK

Regulating Decentralized Systems: Evidence from Sanctions on Tornado Cash

Anders Brownworth, Jon Durfee, Michael Junho Lee, and Antoine Martin

Federal Reserve Bank of New York Staff Reports, no. 1112
August 2024
https://doi.org/10.59576/sr.1112

Abstract

Blockchain-based systems are run by a decentralized network of participants and are designed to be censorship-resistant. We use sanctions imposed by the U.S. Department of Treasury on Tornado Cash (TC), a smart contract protocol, to study the impact and effectiveness of regulation in decentralized systems. We document an immediate and lasting impact on TC following the sanction announcement, measured by market reaction, transaction volume, and diversity of users. Still, net flows into TC contracts recover to and surpass pre-announcement levels for most pools, supporting viability of TC. Evidence on cooperation at the settlement layer is mixed: the aggregate share of non-cooperative blocks increases over time, but a shrinking number of actors process Tornado Cash transactions, indicating a fragility to the sustainability of censorship-resistance. Non-cooperation is not explained by tokenomics, and changes in perception around legal authority and clarity of regulation appears to be a key factor for whether to cooperate.

JEL classification: G18, G28, G29, D40, F51, O30
Key words: decentralized systems, digital assets, privacy, regulation, sanctions

---

Durfee, Lee (corresponding author): Federal Reserve Bank of New York (email: michael.j.lee@ny.frb.org). Brownworth: Radius. Martin: Swiss National Bank. The authors thank Twinkle Gupta and Kate Nguyen for outstanding research assistance.

1 Introduction

The Office of Foreign Assets Control (OFAC), an agency within the U.S. Department of Treasury, maintains and enforces sanctions policy for the United States. Historically, OFAC sanctions programs have targeted foreign nations, business entities, groups, and people. At their core, these sanctions rely on the rule of law, i.e., the ability to impose penalties on and take enforcement actions against offenders, including bringing legal action when needed. In this respect, cryptocurrencies, which are implicated at the nexus of cyber and financial crime, potentially pose challenges relative to traditional targets of sanctions. Furthermore, cryptocurrency transactions are supported by a decentralized system, which are intended to be censorship resistant, and certain financial arrangements are facilitated by software, rather than custodied and intermediated by an individual or entity.

On August 8, 2022, the United States Department of Treasury sanctions aimed to achieve exactly this. OFAC blocked Tornado Cash, under Executive Order 13694, *Blocking the Property of Certain Persons Engaging in Malicious Cyber-Enabled Events*, and added it to the Specially Designated Nationals and Blocked Persons List (SDN List), stating it "had been used to launder more than $7 billion worth of virtual currency since its creation in 2019."[1] Tornado Cash is a set of smart contracts that aims to facilitate more anonymous transactions on public blockchains where all transactions, including the addresses of senders and receivers, are publicly observed. These sanctions mark the first-time a non-custodial cryptocurrency smart contract has been sanctioned, a notable shift from previous classes of targets, such as foreign nations, business entities, groups, and people.[2] What makes this scenario unique is that the target of a sanction is a decentralized entity which produced a piece of software that is programmed and deployed on a platform designed to be censorship resistant and consequently the software is nearly impossible to remove. This scenario begs the question can regulators effectively restrict the behavior of agents who want to use a piece of software, if removing the software from the public is not possible?

The sanctions on Tornado Cash offer a quasi-natural experiment to study the implications and effectiveness of regulation in decentralized systems. In particular, we use the announcement of the sanction and related legal decisions as shocks to examine the reactions of various stakeholders along the settlement cycle of Ethereum, where the Tornado Cash protocol is most actively used. Our focus is on regulatory cooperation: given the decentralized nature of

[1] https://home.treasury.gov/news/press-releases/jy0916

[2] A non-custodial cryptocurrency smart contract refers to a type of smart contract where funds are stored and maintained on a smart contract that itself never custodies the funds; this differs from other custodial solutions such as centralized exchanges serving as intermediaries and custodying funds.

the blockchain settlement, and specific design considerations intended to censorship-resistant, (how) did sanctions impact on-chain transactions?

To start, we first examine the market reaction and usage of Tornado Cash contracts around the sanction announcement.[3] We document a sharp immediate reaction to the sanction announcement by Tornado Cash stakeholders. Leading up to the announcement, we do not find evidence of an anticipatory effect, suggesting the announcement was a surprise. The total market value of TORN, the governance token for Tornado Cash, drops by about 60 percent from its local peak reached a day prior to the announcement, and overall a 33 percent drop around a 4-week window. Correspondingly, actual Tornado Cash transactions, both by volumes and value, significantly decline, with transaction volume across various pools dropping by about 72 percent. User diversity, as measured by unique addresses interacting with Tornado Cash also drops significantly post-announcement. Importantly, both the perceived value of the Tornado Cash and actual usage remain at significantly depressed levels in the post-sanction period, indicating a lasting impact on the protocol value and usage of Tornado cash.

With diminished usage, did sanctions compromise the functionality of Tornado Cash? An important determinant of the level of anonymity offered by Tornado Cash is the size of the pool, or *anonymity pool*. Despite gross drops in flows to and from Tornado Cash addresses, we find an increase in the total value deposited in Tornado Cash addresses, relative to pre-sanction levels, for all but the largest denominated pool. Recovery from drops at announcement, and secular increases in net flows into Tornado Cash contracts suggest that Tornado Cash remains viable as a privacy tool, particularly in the view of users.

In principle, transactions are settled only when included in a validated block that is appended to the Ethereum blockchain. Consequently, actors along the settlement chain can influence the effectiveness of sanctions on Tornado Cash to varying degrees. In September 2022, the Ethereum network underwent long-planned transition from proof-of-work to proof-of-stake. Along with structural changes to its consensus mechanism, the Proposer-Builder Separation (PBS) design proposal was implemented off-chain to encourage competition and lower barriers-to-entry. These were in support of the explicit objective to foster diverse and decentralized participation in the settlement process, for which we provide relevant institutional and technical aspects in Section 2.

We use the sanctions to study the decision on whether to cooperate, which we define in Section 4, with sanctions by actors along different stages of the Ethereum settlement chain. To start, we examine the activities of major builders, who actively select transactions to be

[3] We provide relevant background on how Tornado Cash works in Section 2. See also Nadler and Schär (2023).

included in blocks. Together, these builders represent about 79 percent of total blocks in our sample. If builders collectively cooperate by censoring Tornado Cash transactions, we should expect that fewer blocks should include Tornado Cash transactions. We find no evidence of censoring at the aggregate level. Specifically, we find that the weekly share of non-cooperative blocks, or blocks including Tornado Cash transactions, generally increases over our sample post-announcement. While Tornado Cash transactions may experience relatively delayed settlement relative to the average transaction (e.g. Wahrstätter, Ernstberger, Yaish, Zhou, Qin, Tsuchiya, Steinhorst, Svetinovic, Christin, Barczentewicz et al. (2023)), we find that the builder market continued to supply block space, and little evidence that indicates material impediments to settling Tornado Cash transactions.

As the sanction marked the first time a sanction was imposed on an (immutable) program, with decentralized governance, and running on a decentralized system, and in part, its primary function as a privacy tool, all could potentially complicate regulatory enforcement. Furthermore, changes in perception by Ethereum actors around legal authority for and clarity of regulation could factor into network participants' choice on whether to cooperate or not. Indeed, OFAC's public statement provides broad and limited guidance on what constitutes violations for settlement actors. Adding legitimacy to this view, one month after the sanction announcement, six Ethereum users sued the U.S. Treasury Department to contest the legitimacy of OFAC sanctions imposed on Tornado Cash.

To examine the impact of regulatory clarity and judicial precendent on cooperation, we exploit the timing around the court ruling in August 2023 that ruled in favor of OFAC. We find direct evidence of large builders switching to a cooperative posture following the ruling, giving credence to the idea that clarity around regulation is a pivotal factor to determining whether to cooperate. With the ruling, we find two builders responsible for over half of the non-cooperative blocks, pointing to significant dependence on a few players to facilitate the settlement of Tornado Cash transactions. This heavy dependence on a few builders reveals a surprising level of fragility in the censorship-resistance of Ethereum.

Finally, we find little variation in cooperation at the proposer (validator) level. In theory, proposers select blocks offered by builders without observing the contents of the block, which could in theory diminish proposers' ability to cooperate with sanctions. We show, however, that this is not the case: since proposers know the identity of the builder, and builders employ persistent strategies in cooperation/non-cooperation, identity can be sufficient to assess the possibility of blocks being non-cooperative.[4] In support of this, we show that some proposers'

[4]Furthermore, while out of scope in our analysis, Maximal Extractable Value (MEV) Relayers provide a means to source cooperative and non-cooperative blocks.

only validate cooperative blocks throughout our sample. In other words, implementing a strategy to be cooperative is straightforward.

A relevant consideration is whether tokenomics, or monetary incentives, motivate proposers to remain non-cooperative. In the PBS design, proposers choose blocks by the rewards, or priority fees, which determine their payoffs associated with staking ETH, Ethereum's native cryptocurrency. Priority fees could be used by users to incentivize actors along the settlement chain to include their transactions. On the contrary, we find broad evidence that non-cooperative blocks are associated with *lower* fees relative to cooperative blocks. Altogether, this shows that non-cooperation is not monetarily driven, and instead, motivated by philosophical reasons.

We draw three high-level takeaways. First, we observe that cooperation generally deteriorates with the distance from the transaction, with the strongest reaction at the user-level, followed by builders, and proposers. At the node level, furthest from the point that transactions are originated, there does not seem to be an effort to reject proposed blocks with Tornado Cash transactions, though this is out-of-scope of our analysis. Second, our results suggest that censorship-resistance is fragile. Although various design choices of Ethereum were chosen to encourage decentralization, we find a fair level of concentration along the settlement chain and high dependence on few actors to facilitate the inclusion of Tornado Cash transactions. This bolsters credence to maintained concerns about concentration in Ethereum's settlement layer and potential design updates to bring about greater decentralization (Buterin 2024). Finally, we demonstrate that non-cooperation cannot be explained by tokenomics, which is often the foundation for attracting and incentivizing players with heterogenous beliefs and preferences to contribute to the network. This sheds light on both issues of design in the context of decentralized systems, and the regulation and legal enforcement on the side of regulators.

Our paper contributes to the literature on illicit activity and blockchain markets. The potential for cryptocurrencies to contribute to illegal transactions has been recognized early. The lack of regulation, especially in its early stages, has been shown to create fertile ground for financial crimes, including fraud and market manipulation (Griffin and Shams 2020, Li, Shin and Wang 2021, Cong, Li, Tang and Yang 2023). More generally, cryptocurrency activity has been linked to illicit activity (Foley, Karlsen and Putniņš 2019). Correspondingly, studies have examined whether regulations appear to affect cryptocurrency prices (e.g., (Auer and Claessens 2018)). In addition to finding strong market reactions to the sanctions, our paper demonstrates how it directly affected the operations of the network as a whole, based on settlement actions taken by various key players in the Ethereum eco-system.

Our paper contributes to the literature on censorship in decentralized systems. A key

pillar of decentralized systems is to provide censorship resistance. As such, past studies have examined the extent to which Tornado Cash provides obfuscation (Wu, McTighe, Wang, Seres, Bax, Puebla, Mendez, Carrone, De Mattey, Demaestri et al. 2022), and how the design of blockchain systems affect the effective provision of features, such as censorship (Heimbach, Kiffer, Ferreira Torres and Wattenhofer 2023). Closest to our paper is Wahrstätter et al. (2023), which studies the impact of OFAC sanctions on blockchains to assess the level of censorship-resistance. They find that sanctions contributed to transaction latency for transactions involving Tornado Cash on Ethereum, lending credence to increased costs associated with settling sanctioned transactions. These costs, however, appear incremental, with delays in settlement in the order of seconds. We complement their study by providing an evaluation of censorship on a longer horizon and focusing on the dynamics of and motives for cooperation across multiple actors along the settlement chain. In particular, our evidence suggests that non-cooperation is not monetarily driven, and partially attributed to plausible ambiguity with respect to the legitimacy of OFAC sanctions on smart contracts. Furthermore, we show that cooperation dynamics of stakeholders suggest a fragility to the censorship-resistance of the system.

The remainder of the paper is summarized as follows. In Section 2, we provide a detailed overview of the institutional environment of Ethereum, in which Tornado Cash is most predominantly active, including the relevant players along the settlement life-cycle. In Section 3, we provide an overview of Tornado Cash and key features that enable Tornado Cash to provide anonymity for its users. Section 4 summarizes our empirical analysis on the cooperation of the Ethereum network. We provide concluding remarks, including an evaluation of the cooperation of various Ethereum stakeholders to the sanctions imposed by the Department of Treasury in Section 5.

2 Settlement on the Ethereum Blockchain

The Ethereum blockchain is a linear organization of blocks composed of transactions or state changes. Ethereum users submit transactions, for example a payment denominated in ETH to the Ethereum network. Transactions require users to pay a fee which is collected by a validator. This fee incentivizes validators to include a user's transaction in the next block, settling with finality within the next fifteen minutes. Consequently, the system is designed such that the higher the fee, the higher the likelihood the transaction is prioritized and included. If the fee is too low, there is a possibility the transaction is never included in a block. Ethereum users may submit their transactions in two different ways. They can

submit them either directly to the Ethereum network "mempool," which is a publicly visible pool of all pending transactions, or directly to a validator.[5] This second option is typically done "off-chain," i.e., transactions are not added to the public mempool and are instead only known to the validator and thus kept private from the wider community until appended to the public blockchain.[6]

Ethereum's validators and the consensus mechanism are responsible for maintaining the state of the Ethereum ledger by proposing a set of new transactions to be appended to the blockchain and reviewing that proposed changes do not conflict with certain requirements (e.g., funds have not been spent twice). Ethereum's Proof-of-Stake (PoS) consensus mechanism randomly allocates the opportunity to one validator, referred to as a "proposer," to propose a round of state changes to the ledger (i.e., a new block to be added to the ledger).[7] The update is then verified by other validators, and if successfully verified, the block is appended to the blockchain.

The proposer is responsible for composing a block of transactions to be appended to the Ethereum blockchain. One way a block can be constructed is for a block proposer to go through all unvalidated transactions they know about (e.g., transactions in the mempool and transactions they privately received) and construct a block that meets the necessary network requirements while maximizing the reward they earn from transaction fees.[8] We provide a simplified illustrative example in Appendix C.

In principle, a proposer can propose any block so long as it conforms to basic requirements such as data size limits. In practice, proposers' economic interests are to propose a block that maximizes transaction fees by selecting and ordering transactions in a way to yield the highest payoff. This approach is termed maximum extractable value (MEV). However, due to limitations for less sophisticated validators to source private transactions and build MEV blocks, intermediaries emerged specializing in sourcing and constructed MEV blocks. In late 2022, Ethereum proposed the Proposer-Builder Separation (PBS) design to support the separation of the role of builders, who are responsible for building blocks, and proposers, who select between potential blocks. As of date, official PBS is not in production but unofficially,

[5] A user may want to send a transaction directly to a validator rather than submit it to the mempool for a variety of reasons, including the desire to take advantage of an arbitrage opportunity without tipping other participants of the opportunity as all transactions in the mempool are visible.

[6] See, for example bloXroute's ETH Protect RPC product.

[7] We provide an in-depth overview of the Ethereum consensus process in the appendix.

[8] For example, the maximum Ethereum block size is 30 million gas. "Gas refers to the unit that measures the amount of computational effort required to execute specific operations on the Ethereum network." See documentation for more information on Ethereum blocks and gas and fees, respectively.

the network has already organized around a separation between proposers and builders.[9]

The Proposer-Builder Separator design separates proposer responsibilities into constructing blocks of transactions, a function not restricted to validators, and proposing blocks, a function restricted to the randomly assigned validator.[10] This design attempts to aid in ensuring the Ethereum network is censorship resistant while providing validators with a means, regardless of sophistication and ability, to obtain MEV for the blocks they validate. We describe the PBS design in detail below.

A builder accesses transactions in the mempool (as these transactions are publicly broadcasted to the Ethereum network) and may also have transactions privately sent to them.[11] With access to both public and private transaction channels, the builder can compose a block that pays the maximum value based on transaction fees and size (i.e., gas, or computation required). These blocks are sent to a "relayer" network, who provide intermediary services between builders and proposers.

Specifically, relay networks, such as Flashbots, serve as a centralized acceptance point for blocks built by builders.[12] Relay networks provide numerous services including data validation and prevention of Denial of Service attacks on proposers. Once all the appropriate validation steps are completed, relayers provide the proposer with two data points: who built the block and how much the block will pay-out to the proposer. This essentially creates a bidding service and platform for block space.[13] See Figure 1 for a visual depiction of blocks built by the proposer versus blocks using the PBS design, respectively.

With such designs and processes outlined above, a key requirement for Ethereum and any public permissionless blockchain is open access.[14] The state of the ledger, which represents who owns what, must be transparent so validators can maintain the accuracy and ultimately the validity of the ledger and network. However, this requirement raises a fundamental privacy concern as all transactions must be made transparent.

[9] See Heimbach et al. (2023).

[10] From a Proposer perspective, outsourcing the block production may provide a more lucrative block as a builder may have a greater set of transactions available for submission than otherwise available in the mempool. See Daian, Goldfeder, Kell, Li, Zhao, Bentov, Breidenbach and Juels (2019) for evidence on how certain actors (i.e., bots) operate in cryptocurrency markets to increase their profitability which consequently results in more value for miners (i.e., Miner / Maximal Extractable Value).

[11] Transaction fees in a private channel may be higher because a user may be attempting to take advantage of arbitrage and thus have a higher incentive to have their transaction included in the next block.

[12] See here for more details on Flashbots.

[13] Relayers do not share transaction details with the Proposer. This design supports two goals: 1) ensuring the Proposer does not simply claim the transactions as their own and thus not compensate the Builder and 2) support the goal of preventing censorship by rejecting a block due to the transaction composition.

[14] For example, see Brownworth, Durfee, Lee and Martin (2023).

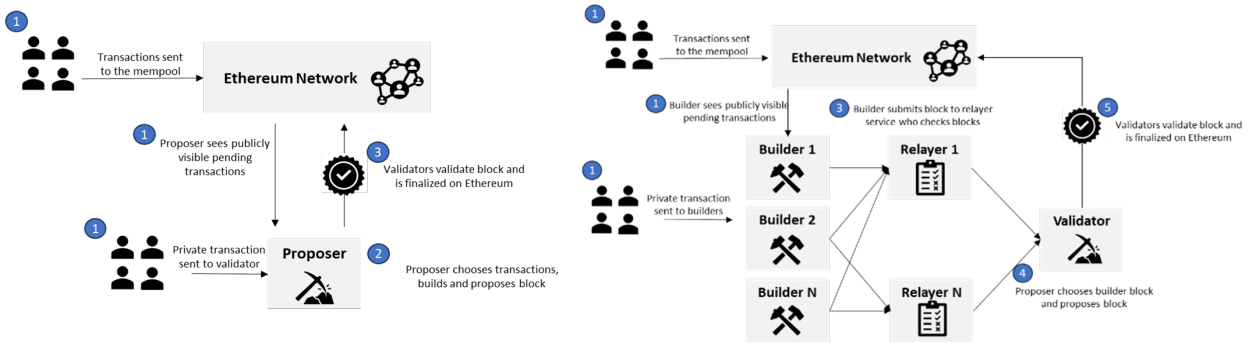

Figure 1: Illustrative Diagram of Ethereum Network

3 Privacy using Tornado Cash

Suppose Alice pays for dinner with her friends and asks them to repay her with ETH. Everyone knows Alice's Ethereum address (e.g., like a bank account number) and can observe any and all transactions to and from that address, offering no transaction privacy. Now suppose Alice wants to throw a surprise party for one of those friends and needs to collect ETH to cover the cost privately. Alice's friend, Charlie, may want to use another address or mechanism to ensure the transactions remains private so the friend remains unsuspecting. Charlie could use Tornado Cash (TC) to obtain privacy on the Ethereum Network.[15] Tornado Cash is a set of "smart contract[s] that accepts transactions in [ERC-20 tokens] so that the amount can be later withdrawn with no reference to the original transaction."[16] The ability to withdraw the funds without reference to the original transaction provides Tornado Cash users some privacy that is otherwise not offered on public blockchains.

Tornado Cash works by allowing users, like Charlie, to deposit funds into a variety of smart contracts that differ by cryptocurrencies and amounts (e.g., 0.1 ETH, 1 ETH, 1,000 ETH, 1 USDC, 100 USDC, etc.). These deposits are pooled together with those of other users depositing the same amount. Depositors can withdraw their funds from the TC smart contract using a new Ethereum address they have custody of.[17] By withdrawing a deposit to a different Ethereum address with no existing links or ties to the known depositor address, Charlie can

[15] See Pertsev, Semenov and Storm (2019).

[16] A key characteristic of the Ethereum network, and an important differentiator from Bitcoin, is that it is possible to program complex logic via smart contracts because its programming language is Turing complete. Once smart contracts are created, they operate autonomously and only require a user to trigger the smart contract to begin processing, nor can they be prevented from being used (unless the smart contract developer specifies access policies); this is due to the Network's distributed computing design.

[17] For an overview of Tornado Cash, including the protocol description and general technical background, see Nadler and Schär (2023).

potentially achieve greater anonymity and privacy otherwise unattainable on Ethereum. See Figure 2 for a high-level flow of a Tornado Cash deposit and withdraw.

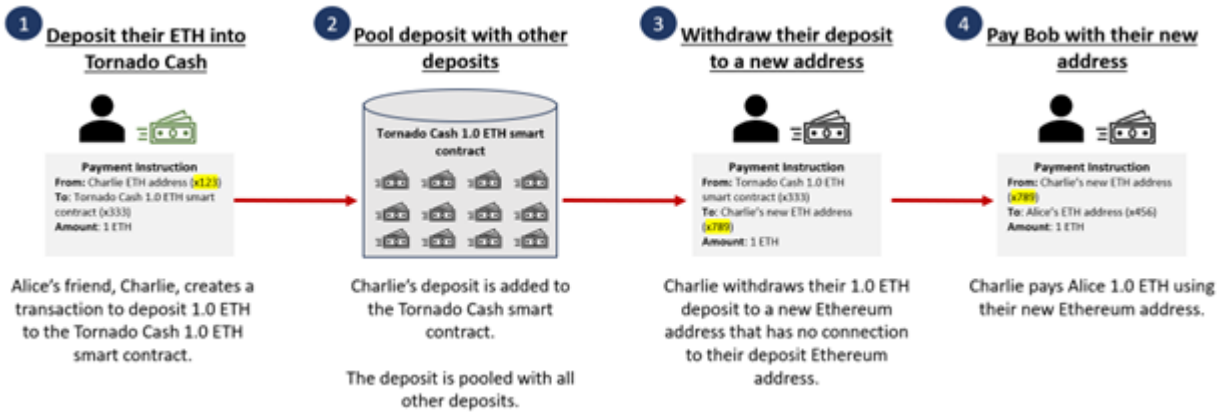

Figure 2: Illustrative Example of Tornado Cash Transaction

The degree of privacy achieved through Tornado Cash hinges on two basic components: the anonymity set and the deposit and withdrawal addresses used to interact with a smart contract.

1. Anonymity Set: The deposit depth of cryptocurrency pools (e.g., 1 ETH) that have yet to be withdrawn can provide a measurement of how much anonymity a user can generally expect from using Tornado Cash. For example, if Charlie comprises of the only deposit into the 1 ETH pool, a withdrawal from that pool will indicate that Charlie is the only possible user moving funds through the Tornado Cash 1 ETH pool, thus providing no privacy guarantee. However, if for example, 1,000 people or unique addresses deposit 1 ETH into the 1 ETH pool, then the probability that any withdrawal of 1 ETH comes from a particular user is one in a thousand. A user could further support obfuscation by depositing more funds from different addresses, therefore contributing to the anonymity set (Tornado Cash 2019).

2. Deposit and Withdraw addresses and network distance: When Charlie deposits their 1 ETH to the Tornado Cash 1 ETH smart contract pool, the transactions will be visible to all participants and observers of the Ethereum. If Charlie were to withdraw the funds with same the deposit address, an observer would see that a specific amount of ETH was deposited from and withdrawn to the same Ethereum address. This would effectively erode any privacy for Charlie. To reduce the possibility of connecting deposits and

withdraws, Tornado Cash provided two recommendations: 1) withdraw funds directly to a newly created Ethereum Address, or 2) use their relayer service to send funds to a newly created Ethereum Address.[18] Furthermore, if the depositor waits between their deposit and withdraw, then potentially a number of other deposits and withdraws are processed in-between which further adds to the potential obfuscation.

While there are clear benefits for anonymity, as described in Alice and Charlie's example, there can also be abuses. For example, anonymity can be used by criminals to launder and move illicit funds. The next section describes the use of Tornado Cash for illicit purposes and analyzes the effects of OFAC sanctions on Tornado Cash and the broader set of Ethereum participants.

4 Tornado Cash sanctions and empirical analysis of their impact

On August 8, 2022, the United States Department of Treasury sanctioned Tornado Cash, citing that it "had been used to launder more than $7 billion worth of virtual currency since its creation in 2019."[19] Tornado Cash was added to OFAC's SDN List along with identifying information, such as its website address, Tornado Cash cryptocurrency Ethereum addresses, including pools and relayer service.[20] The sanctions prohibit "all dealings by U.S. persons or within the United States (including transactions transiting the United States" that involve the sanctioned Tornado Cash assets outlined above. Furthermore, financial institutions that knowingly transact or provide "significant financial services [...] could be subject to U.S. correspondent or payable-through account sanctions."[21] Importantly, Tornado Cash smart contracts were made immutable, and its user interface and website open-sourced by its developers since 2020 (Tornado Cash 2020). This ensured that no one, including its creators, could with interfere or modify the operations of Tornado Cash unless changes were made to Ethereum itself. Coupled with the fact that Tornado Cash is deployed on a decentralized system intended to

[18] To withdraw funds directly to a newly created Ethereum address, the address must previously have ETH in it, which raises the possibility that the owner of the address could be deduced from previous transactions. The Tornado Cash Relayer service provides a method for Tornado Cash users to withdraw funds into a newly created Ethereum address that has no previous transaction history. The user pays a fee to the Relayer service which acts as an intermediary and withdraws the specified funds from a Tornado Cash pool and transfers it to the user. This provides a means for a user to withdraw funds without partaking in Ethereum transaction previously and potentially jeopardizing their privacy.

[19] The official announcement is here.

[20] A list of sanctioned Tornado Cash entities can be found here.

[21] An additional Frequently Asked Questions (FAQs) was published here

be censorship resistant, the impact of the sanction on Tornado Cash usage and the Ethereum eco-system are considerably uncertain.

4.1 Evaluating Cooperation

Our primary goal is to examine the degree of impact and cooperation on the Ethereum network to sanctions and begin to answer the question as to what regulating decentralized systems can look like. It is useful to define cooperation and discuss the scope of the sanctions.

First, we define *cooperation* as behaving in a way that does not facilitate the processing of Tornado Cash transactions. This can mean different things, depending on the type of actor along the Ethereum settlement process. We focus on cooperation because given the pseudo-anonymous nature of the Ethereum network, we are not able to identify the geo-location or nationalities of users. This limits our ability to directly test compliance, which would be relevant for a subset of users and network participants falling under the jurisdiction of US sanctions. Subsequently, our results come with the caveat that evidence for or against cooperation is not definitive proof of compliance and our work does not indicate what compliance means or any associated legal liability.

Second, while some OFAC sanctions prohibitions apply to non-US persons, OFAC sanctions apply largely to US persons, including citizens and permanent resident aliens, all persons and entities within the US, and all US incorporated entities and their foreign branches. Consequently, we should not, in principle, expect Tornado Cash activity to drop to zero, even if OFAC sanctions were fully effective, because foreign entities that are not required to cooperate with OFAC might continue to use it. This means that non-cooperation, as defined by us, does not definitely show that illegal behavior from a US sanctions perspective has occurred.

Third, while the OFAC sanction states that "[engaging] in any transaction with [Tornado Cash] is prohibited," the boundaries of what constitutes illegal engagement with Tornado Cash are relatively untested in practice and also subject to ongoing litigation. We provide a concrete example. The Ethereum network comprises of about 7,500 nodes, each maintaining a state of the ledger. In principle, nodes could reject proposed blocks containing Tornado Cash transactions as including a non-cooperative block could be construed as engagement. However, this puts considerable burden on individual nodes to exercise discretion, which in practice, often mechanically accept blocks if the state of ledger remains valid with the inclusion of the proposed block, and additionally, play no part in the construction of new blocks. Furthermore, anyone entering a transaction derivative to the new ledger that recognizes TC transactions could be argued to be engaging in some form of tacit acceptance. These examples

illustrate that it can be difficult for actors to determine whether they are engaging in actions that are prohibited by OFAC's sanctions of Tornado Cash.

Our analysis considers the period immediately following the sanctions, at a time when litigation relating to the sanctions continues and the boundaries of actions that are prohibited by the sanctions program remain relatively untested. In other words, the lack of cooperation by certain players could be based not on defiance, but rather their belief that their activities do not violate OFAC's sanctioning of Tornado Cash. In fact, our results show that regulatory clarity and judicial precedent appears to significantly affect the cooperation choice of certain actors.

We now turn to assessing the impact of US Sanctions on Tornado Cash by examining Tornado Cash and broader Ethereum network data.

4.2 Data

Our two main sources include on-chain Ethereum transaction data and pricing data across our sample period which runs from January 2020 to December 2023. Our Ethereum transaction data comes from Dune, a cryptocurrency data platform, and Amazon Web Services' (AWS) Public Blockchain Data. From Dune, we build a dataset that includes detailed information on all transactions involving known addresses of Tornado Cash. This includes all deposits and withdrawals for all active Tornado Cash ETH pools. We combine the block data obtained from AWS with transaction data of payments from block builders to block proposes obtained from Dune. From this merged data set, we identify the block builder and proposer. Using the Tornado Cash transaction data from Dune, we also identify which blocks include Tornado Cash transactions. Lastly, our analysis on crypto prices is based on pricing data from CoinGecko, a cryptoasset market price aggregation platform.

4.3 Value of Tornado Cash

As a starting point, we provide a brief background on TORN and examine the market reaction of TORN tokens following the introduction of sanctions. In February 2021, 500,000 TORN tokens were airdropped to early users, with the intention to delegate key decisions of the smart contract to a decentralized community of dedicated users. As a service, Tornado Cash is not managed by a corporation, but instead by members of its decentralized autonomous organization (DAO). Members of the DAO are granted various rights, including the rights to propose changes and vote on proposal, and powers are based on ownership of Tornado Cash's governance token, TORN.

Although governance tokens do not necessarily represent a claim on the revenue generated by the protocol, it is often perceived by market participants as a form of equity stake. This is due to multiple reasons, including their symbolic representation as a primary issuance from a protocol's developer, similarities in the set of governance rights, and, explicit or implicit, expectations of profit distribution to token holders in the future. Thus, the market reaction of TORN tokens following the announcement of OFAC sanctions can be instructive in evaluating how sanctions were perceived by the market.

In order to test the market impact of the sanctions announcement, we examine how the total market capitalization of TORN tokens changes around the announcement date. We test whether the market value of TORN tokens is significantly different pre- and post-announcement for both the short horizon, 4 week window, and the long horizon, one year window. Our specification is:

$$y_t = post_t + X_t + c + \varepsilon_t, \tag{1}$$

where y_t is the total market value of TORN tokens, at the daily frequency, and X_t include weekly bitcoin and ETH prices to control for broader co-movement in cryptocurrency markets. All token values are denominated in US dollars.

We find a significant impact of the sanction the value of TORN tokens, summarized in Table 1. The market cap of TORN drops significantly in the weeks following the announcements, with a drop in value of about $\$14m$. We find consistent patterns in the 1-year window, with a $\$40m$ difference in value pre- and post-announcement, suggesting a permanent impact on the intrinsic value of Tornado Cash as perceived by investors. Figure 3 shows the value of TORN tokens over time, including market caps before and after the introduction of sanctions. Importantly, price TORN value rise and locally peak in value on August 7, a day prior the sanction announcement, suggesting little anticipation from the market about the announcement. The economic significance is also large: as context, the local peak value is $\$40m$, and the announcement of the sanctions, the TORN token market cap dropped by 60% over the next few days.

Another way to appreciate the magnitude is to compare this to May 22, 2023, on which an attacker gained full governance control over Tornado Cash. In principle, the attack could have fully diluted the value of the token by selling a significant number of TORN tokens on the market. This would have destroyed the holding value of the token to other existing TORN holders. In this incident, the price of TORN immediately dropped 40%, before recovering

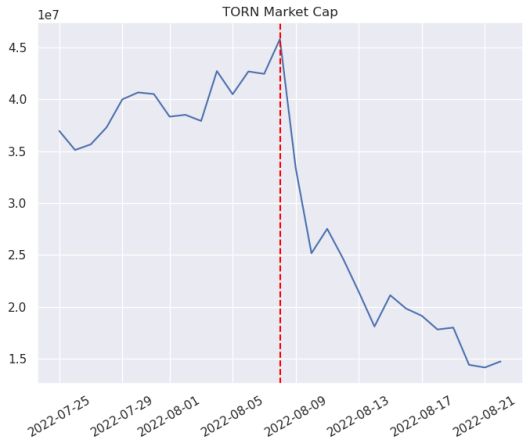

Figure 3: Value of TORN tokens around sanction announcement

after the attacker chose to relinquish their control (and siphoning a relatively small portion of tokens that were available).

Hence, at the very least, the sanctions represent a shock at least as severe as that which potentially threatened complete loss of governance control. Furthermore, the value of TORN has not rebounded during our sample period, representing a sustained view, at least from a governance holder perspective.

4.4 Impact on Tornado Cash as an anonymity pool

As detailed in earlier sections, the efficacy of Tornado Cash is based on its volume and usage; if the volume and usage of the Tornado Cash is insufficient, then it cannot provide an attractive level of anonymity that users may be searching for. To assess the impact the sanctions had on Tornado Cash's efficacy, we examine the overall user engagement with Tornado Cash by analyzing the transaction volume, various pool sizes of Tornado Cash, and user diversity, measured by the number of transactions involving Tornado Cash addresses at a weekly frequency.

As shown in Figure 4, we find a dramatic drop in transaction volume following the introduction of sanctions. The drop in transaction volumes is statistically significant, with a drop in average weekly transactions by 72%. Further splitting transaction volumes into deposit volumes and withdrawal volumes reveals a consistent pattern. Deposit volumes drop to an average of about 307 weekly deposits from a pre-sanction average of about 1184 weekly deposits, resulting in a 74% decline. Similarly, withdrawal volumes drop to an average of about 341 weekly withdrawals from a pre-sanction average of about 1093 weekly withdrawals, re-

Figure 4: Weekly deposit and withdrawal volume around sanction announcement

sulting in a 69% decline.

An aggregate drop in activity is self-evident. We further test whether drops in transactions are observed across all Tornado Cash pools of varying deposit size. We run regressional analysis using a difference-in-difference approach, with the following specification:

$$y_{it} = \text{Post} \times \text{Pool Size}_i + \text{Pool Size}_i + \varepsilon_{it}. \tag{2}$$

Here, y_{it} is the volume of transactions, either for Deposits or Withdrawals, for Tornado Cash pool i at the weekly frequency. As before, Post is 1 for the period following the sanction announcement. Pool Size_i is a categorical variable for the pool sizes $0.1, 1, 10$, and 100 ETH. We include Pool Size fixed effects to control for variation in activity across pools.

Overall, we find broadly consistent patterns for all pool sizes, reported in Table 2. Transaction volume, both in terms of deposits and withdrawals drop significantly for all pool sizes. In the case of deposits, sanctions had the smallest effect on the 0.1 ETH pool, the smallest pool, with a drop of about 120 transactions per week, and the largest affect on the 1 ETH pool, at about 275 transactions per week. Note, while volumes show a comparable drop in the count of transactions between pools, the drop in the value of transactions are significantly greater for the 100 ETH pool, with an average drop of 16,300 ETH per week.

The drop in both deposit and withdrawal volumes in aggregate are sharp and persistent, indicating that sanctions had a significant impact on overall interactions with Tornado Cash which directly affects the viability of Tornado Cash to provide its users with strong anonymity guarantees. However, while overall interactions with Tornado Cash visibly diminished, our analysis suggests that utilization of Tornado Cash, as measured by the net value of tokens

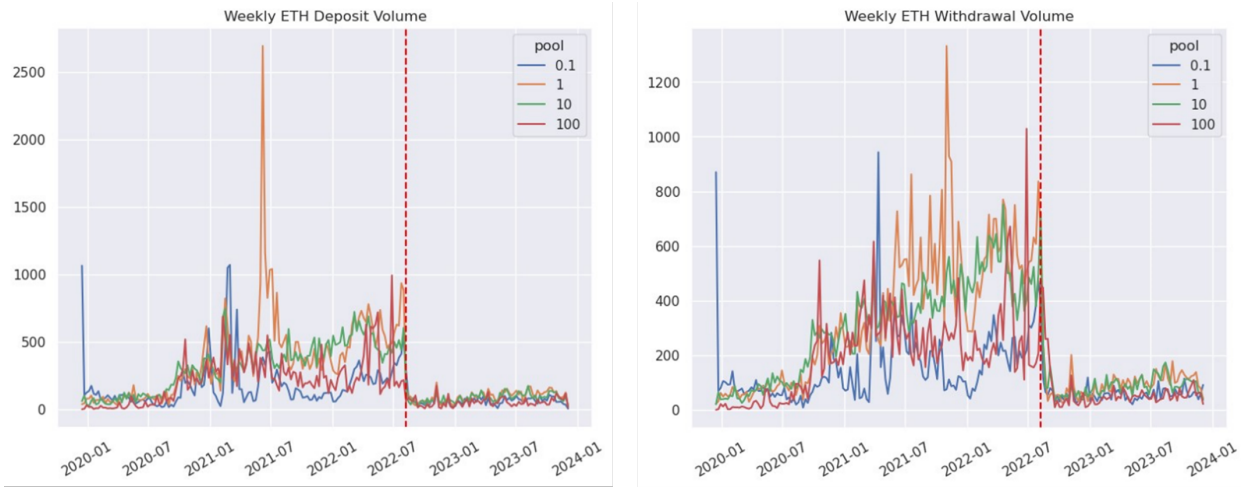

Figure 5: Weekly deposit and withdrawal volumes by pool size

deposited in the ETH pools show a more nuanced picture. See Figures 5 and 6.

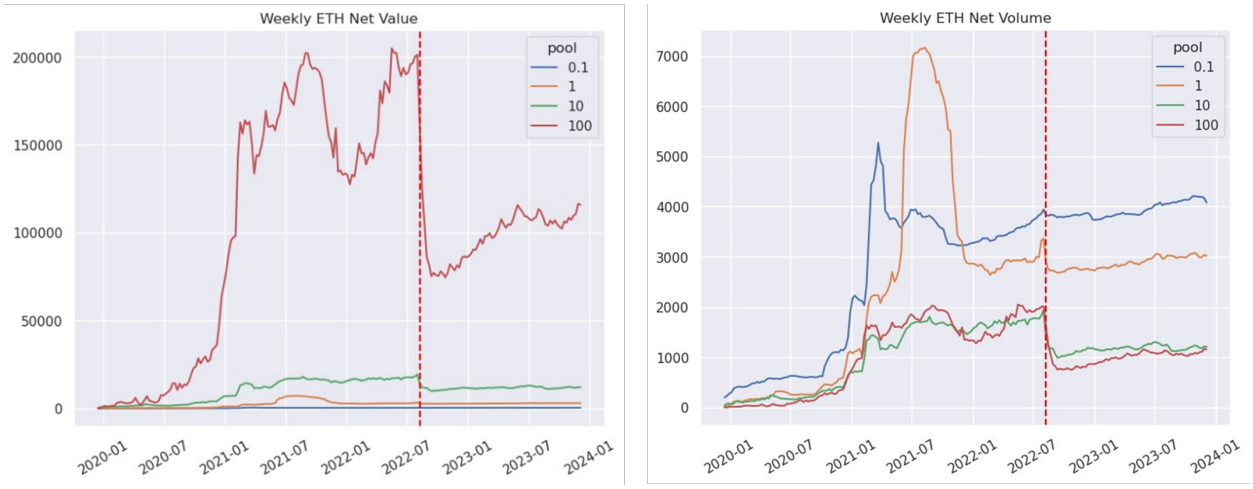

Figure 6: Net value and volume of TC pools

First, note that the bulk of value in Tornado Cash is in the 100 ETH pool. In terms of value, we see a drop immediately after the US sanctions, followed by a rebound in 2023. Furthermore, transaction volume reveals an interesting pattern: for low value pools (0.1 and 1 ETH), the pool size recovers to pre-sanction levels, whereas the impact on pool size is noticeably larger for 10 and 100 ETH pools. This could be viewed as circumstantial evidence that the anonymity depth is too shallow in the larger pools.

We formally test this using the specification in Equation 2 with net volume and net value

as outcomes. Results are reported in Table 3. First, note that, with the exception of the largest pool of 100 ETH deposits, the total ETH deposited in all pool sizes increased relative to the pre-period, with the largest increase by number of deposits in the 0.1 ETH pool, and by value of deposits, in the 10 ETH pool. As shown in Figure 6, after mass withdrawals at the onset of the announcement, net deposits gradually increase over time, and reach levels near or above previous peaks in the pre-announcement period. Although transaction frequencies have gone down, anonymity, as proxied by the size of the anonymity pools, continues to grow, and suggest that Tornado Cash's core functionality to offer greater privacy remain in tact.

Another factor that governs the privacy function of Tornado Cash is the diversity of users depositing into the pool. As described earlier, the larger set of unique deposit addresses is, the greater the probability a user's transaction may remain anonymous. We look at the number of new or unique Ethereum deposit addresses weekly to provide a rough proxy for the diversity of user engagement with Tornado Cash. We use the regression using a difference approach to examine the post-announcement effect on new addresses interacting with Tornado Cash at the weekly frequency. Results are summarized in Table 4 and Figure 7. The number of new or unique addresses that interact with Tornado Cash follows patterns observed with transaction volumes with significant drops, and remain depressed throughout the post-sanction period. The low transaction volume and diversity of users highlights that although Tornado Cash's functionality may be in tact, the level of privacy offered by its service has deteriorated relative to before.

Figure 7: User diversity

Numerous actions that occurred in response to sanctions may potentially explain these

significant drops in user activity. First, the main Tornado Cash websites were taken down and inaccessible. These websites provided users the ability to directly interact with the Tornado Cash smart contract (e.g., depositing or withdrawing funds) without having to go through other entities, such as a centralized cryptocurrency exchange. Consequently, as noted by Wahrstätter et al. (2023), this removed a potential avenue for Tornado Cash users to access and interact with the sanctioned smart contracts. Second, some centralized exchanges began blocking transaction involving sanctioned Tornado Cash addresses.[22] Given the prominence of centralized exchanges, this most likely contributed to the deterioration of Tornado Cash activity.

While user activity is key to Tornado Cash's efficacy as a privacy tool, the Ethereum network is critical to Tornado Cash's operations itself. Given the unprecedented nature of the sanction, in particular its imposition on a non-custodial smart contract deployed on public permissionless blockchains without a regulatory framework, there was considerable uncertainty regarding how the broader Ethereum ecosystem would react. We dive into this issue next, focusing on builder and proposer on-chain activity involving sanctioned transactions over time.

4.5 Impact of sanctions on how builders compose Ethereum blocks

Proposer-Builder Separation design is the dominate form of Ethereum block creation since its introduction. As explained earlier, PBS is intended to broaden the pool of validators, by allowing for a class of expert builders to supply proposers with blocks to choose from. In turn, by allowing for anyone to participate as a builder, the goal was to have a competitive market of block builders (Heimbach et al. 2023). At a high level, we find that block builder market is both concentrated and dynamic, with new entrants and market shares fluctuating over our sample period. See Figure 8 for a breakdown. The dynamism of block builder market share may possibly reflect the competitive landscape of sourcing transactions across both public and private channels to create blocks that extract MEV. Still, 12 builders account for about 79% of Ethereum blocks built over our sample period. Given that builders wield complete discretion over the inclusion of transactions in their blocks, a group of builders could float or sink the viability of sanctioned activity in Ethereum.

To evaluate this, we analyze the dynamic cooperation of 12 of the largest builders by market share. We start by examining aggregate dynamics of the inclusion of Tornado Cash transactions in blocks. If, in aggregate, fewer blocks contain Tornado Cash transactions over

[22] For example, see here for the following statements made by the CEO of a major cryptocurrency exchange.

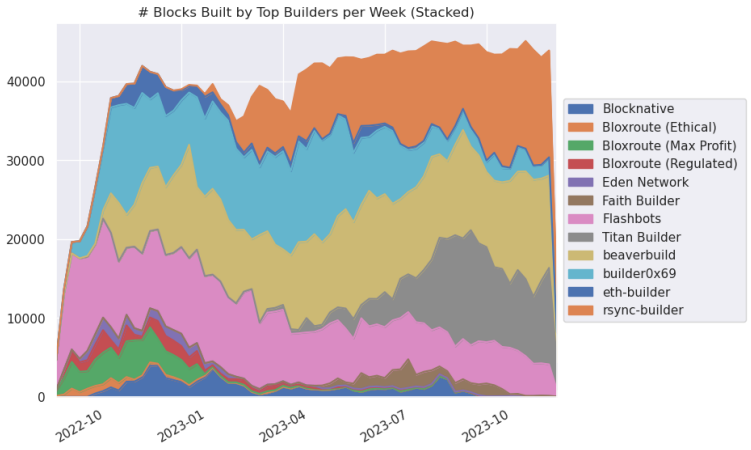

Figure 8: Block building concentration

time, this would suggest that cooperation in the builder market generally increased.

We observe that the inclusion of Tornado Cash transactions in validated blocks are, in aggregate, increasing between September 2022 and December 2023. This aligns with our earlier finding that while Tornado Cash transaction volume was impacted immediately after announcement, activity showed an upwards trend in the subsequent period. This indicates that censorship did not happen at the system-level.

An important factor to consider, however, is the impact of regulation on the cross-section of settlement actors. In particular, in the period immediately following the OFAC sanctions, Ethereum blockchain users challenged OFAC's authority to sanction Tornado Cash. The litigation could represent and even contribute to perceived ambiguity with respect to the authority for and boundaries of OFAC's sanctions. If this is the case, we should expect that changes in the clarity with respect to OFAC's authority to sanction Tornado Cash should coincide with changes in cooperative behavior by settlement actors.

We exploit the timing of the court decision to test this. Specifically, on August 17, 2023, courts ruled that OFAC sanctions could be applied to smart contracts, providing further clarity on the applicability of sanctions on decentralized finance.[23] We run the following regressional test:

$$y_t = \text{PostCourt}_t + \alpha + \beta t + \varepsilon_t, \tag{3}$$

where the dependent variable y_t is the weekly share of non-cooperative blocks and PostCourt_t

[23]Report can be found here.

is 1 for the period following the court ruling. We control for linear trend, which could be driven by other factors, including demand.

Results are reported in Table 5. We find a significant drop in the share of non-cooperative blocks following the court ruling, showing that the court ruling may have affected builders' decision on whether to cooperate. An examination into cooperation at the builder-level is illuminating. Corresponding to this result, we identify a sudden and significant drop in the inclusion of Tornado Cash transactions in blocks built by multiple large builders in August 2023.

Specifically, prior to August 2023, several block builders with sizeable market share consistently included Tornado Cash transactions in their blocks. Towards the end of August 2023, block builders accounting for 89% of blocks validated began to no longer include tornado cash transactions in their blocks – a sudden departure from previous activity.

In the latter part of our sample, from August 2023 and early December 2023, we see nearly all Tornado Cash transactions included in validated blocks by our profiled builders are built by Titan Builder, who accounts for 10.6% of blocks built on the Ethereum network between 2/2/2023, when they first produced blocks, to 12/5/2023. Furthermore, Titan Builder, and Faith Builder for a small period, account for over 50% of the block production that includes Tornado Cash transactions. As expected, when we exclude these two non-cooperative builders from the sample, we see even starker drops in non-cooperative block building, as shown in Column (2) of Table 5 and in Figure 9.

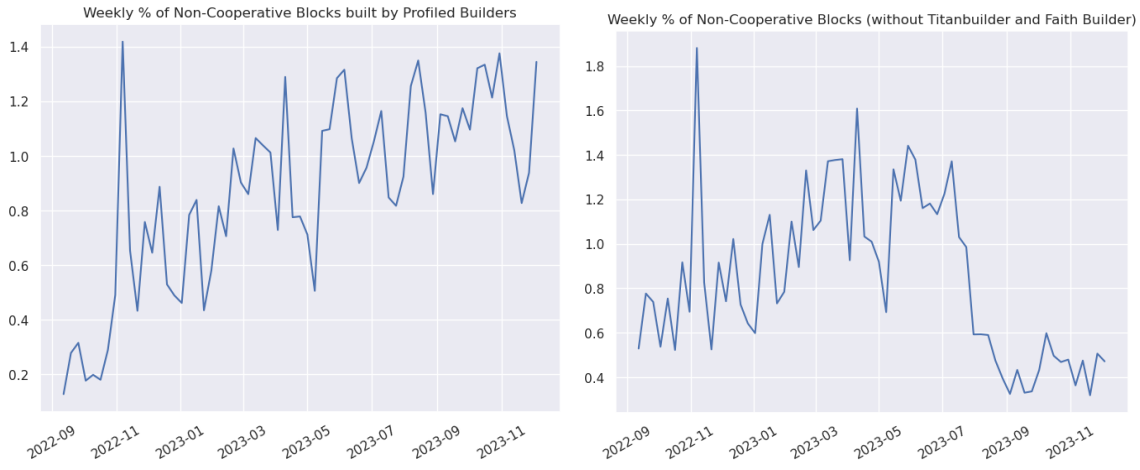

Figure 9: Non-cooperative share of blocks over time

Overall, this reveals that the inclusion and processing of Tornado Cash transactions is in a precarious state given its reliance on a single builder to compose competitively priced blocks

including Tornado Cash for proposers to select.

4.6 Impact of sanctions on the block proposing

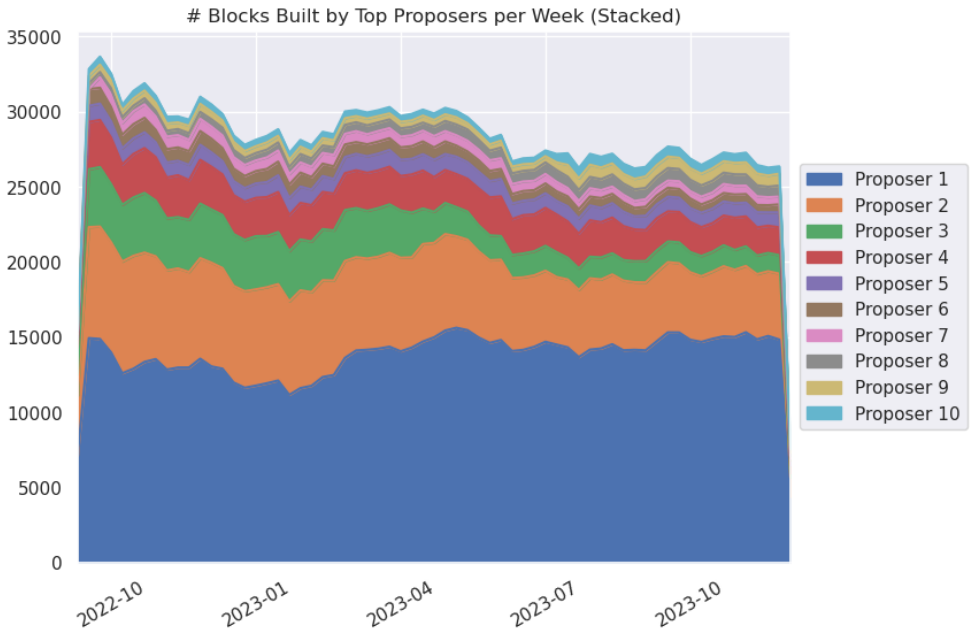

Figure 10: Block proposer concentration

Lastly, as part of our analysis of the OFAC sanctions on the broader Ethereum ecosystem, we examine block proposer activity across our research period. Although proposers who leverage the PBS design do not actively choose the contents of blocks and cannot observe transactions in a block prior to selection, proposers observe the identity of the builder and can choose cooperative or non-cooperative MEV relayers. Since builders and relayers signal their cooperation explicitly (through announcements) and implicitly (through the history of blocks built), proposers can effectively cooperate by accepting only cooperative-blocks.

We first identify the top block proposers who account for 58% of validated Ethereum blocks. Like our block builder analysis, we observe a concentrated environment where a small number of entities are responsible for the majority of validated Ethereum blocks with two entities, Proposer 1 and Proposer 2, accounting for 40% of blocks. However, unlike block builders, the market share and make-up of the largest block proposers remains stable throughout. See Figure 10 for a breakdown.

We investigate whether block proposers are actively excluding blocks including Tornado

Cash transactions. We observe in our analysis that the largest validators, Proposer 1 and Proposer 2, propose a consistent flow of blocks that include Tornado Cash transactions. In contrast, a block of other validators whom we are not able to identify did not propose any blocks that included Tornado Cash transactions. See Figures 12, 11, and 13 for a breakdown of certain block proposers and a breakdown validated blocks that either include or do not include Tornado Cash transactions.

Our analysis points to differing levels of cooperation by proposers. The largest block proposers, Proposer 1 and Proposer 2, process blocks that include Tornado Cash transactions, while other proposers profiled seem to actively exclude blocks that include Tornado Cash transactions. This confirms that some proposers appear to source their blocks in a way that are fully cooperative. A notable difference is the invariance in terms of cooperation. Whereas builders appear to actively choose their cooperation strategy, we do not observe switching in strategies for proposer in our sample period.

While the analysis is out-of-scope for this paper, we note that several relayers disclosed their decision to cooperate with the OFAC sanctions. OFAC-cooperative relayers validate the transaction bundles submitted to them do not include OFAC-sanctioned Ethereum addresses (e.g., the sanctioned Tornado Cash addresses). If a bundle includes an OFAC-listed address, relayers may reject submitted blocks.

Consequently, MEV relayer who are OFAC-cooperative provide an avenue for blocks that exclude Tornado Cash transactions. Furthermore, if a block proposer accepts block bids from a relayer who cooperates with OFAC sanctions, then the proposer is also enforcing sanction cooperation if they choose OFAC-cooperative blocks. In other words, given the PBS design and critical role MEV relayers can play, proposers may be able to outsource cooperation checks of block contents to MEV relayers and from our analysis, it seems rather effective in their ability to discern blocks that include Tornado Cash transactions versus not. This begs the question as to other potential motivating factors for proposing blocks with Tornado Cash transactions.

To assist in this question, we look at the fees proposers earn between blocks that include Tornado Cash transactions versus not. We analyze the priority fees, which are bounties offered by users to incentivize settlement, to evaluate whether non-cooperation is motivated by tokenomics. We compare the priority fees of cooperative and non-cooperative blocks over our sample. To control for unobservable variation in builders, including their ability to build profitable blocks, we include builder fixed effects. To control for variation in block-space demand, we include month-year fixed effects.

Results are summarized in Table 6. We note two potentially surprising facts. First, we

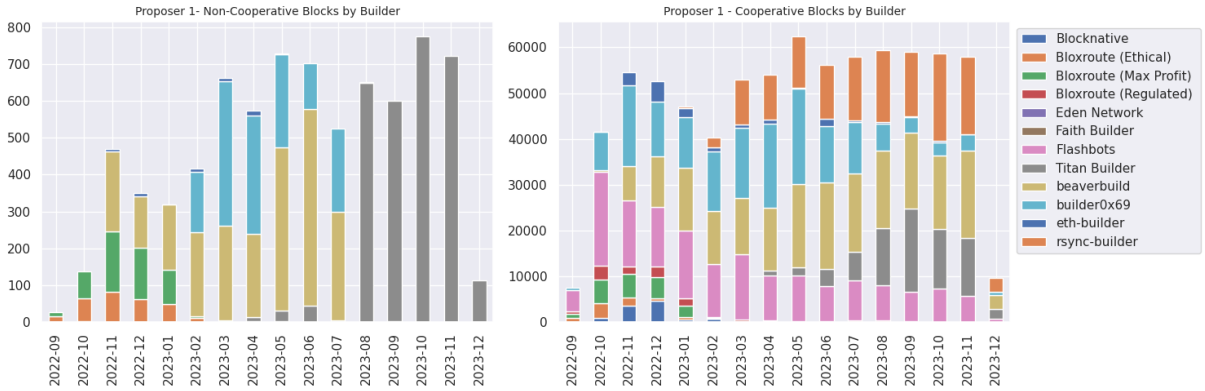

Figure 11: Non-cooperative and cooperative blocks by Proposer 1

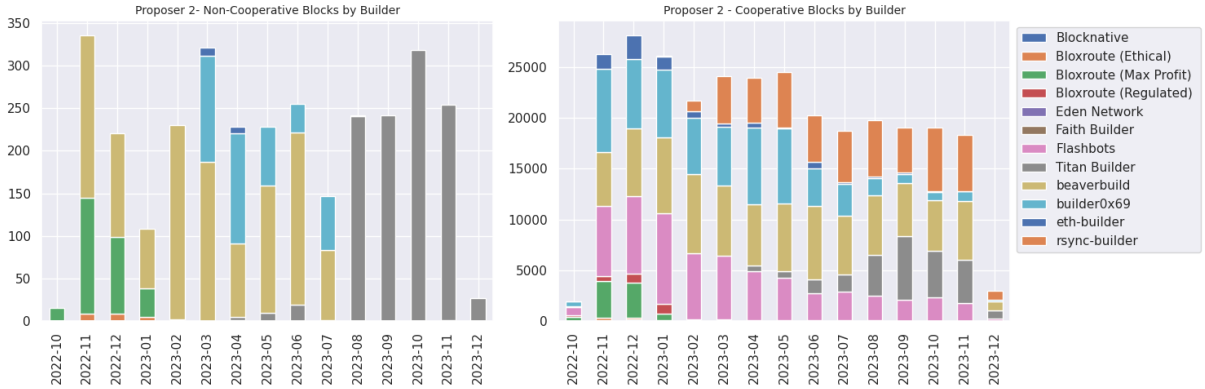

Figure 12: Non-cooperative and cooperative blocks by Proposer 2

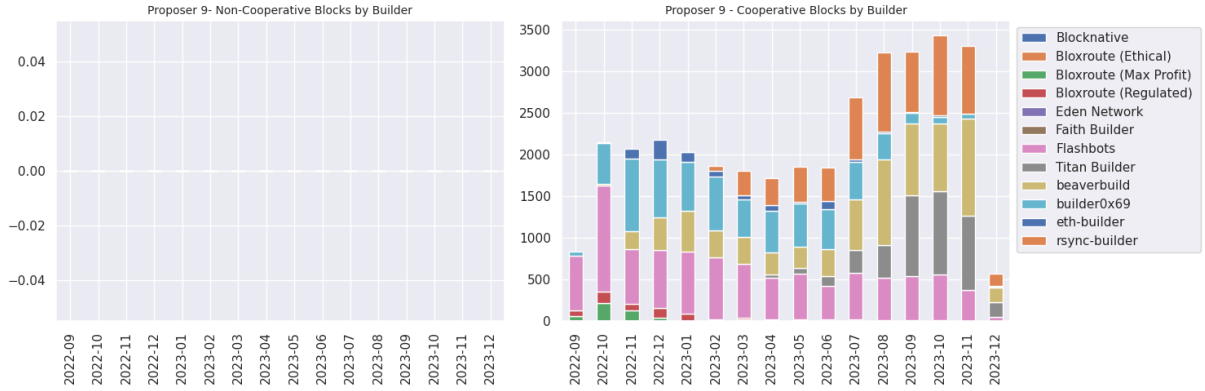

Figure 13: Non-cooperative and cooperative blocks by other proposer

find that priority fees of non-cooperative blocks are consistently lower than those of cooperative blocks throughout our sample period, ranging from 15 to 23 percent depending on the specification. This pattern is remarkably stable within builders as well: we find that priority fees of non-cooperative blocks are consistently lower than those of cooperative blocks for any given builder. This rules out the possibility that differences in priority fees reflect differences in builders' abilities to build profitable blocks. Together, this suggests that economic motives are not the defining reason for non-cooperation.

5 Concluding Remarks

First, we find that the level of cooperation weakens along the settlement chain. In general, the total value and volume of Tornado Cash drops precipitously and remains so for our sample period following the announcement of the sanctions. Although Tornado Cash transactions are continuously settled throughout our sample period, an increasing number of large builders, who are responsible for selecting transactions for settlement, cooperate with the sanctions by excluding Tornado Cash transactions from their blocks. By comparison, we see little change in the cooperative posture by block proposers, including those based in the US. Although not included in the paper, the final line of cooperation could be validating nodes, who could choose to reject blocks involving sanctioned transactions and thereby fork the Ethereum blockchain. No such effort is observed, and in this sense, all nodes have been non-cooperative.

Second, we demonstrate that although Tornado Cash transactions continue to be settled, censorship-resistance appears more tenuous than what the transaction volume suggests. In particular, one major block builder is responsible for a majority of non-cooperative blocks towards the end of our sample period. Given that the market for block building is open, the withdrawal of other established builders from building non-cooperative blocks sheds light on the fragility of censorship-resistance of the Ethereum network.

Finally, our analysis indicates that non-cooperation is not driven by pecuniary motives or operational constraints, and instead by philosophical reasons. We observe several proposers who throughout our sample only validate cooperative blocks, which confirms the feasibility of cooperation, even if the contents of blocks cannot be examined by a proposer. Second, we find that non-cooperative blocks are systematically less profitable than cooperative blocks. Although priority fees are designed to incentivize settlement, sanctioned transactions do not appear to be included in blocks due to bounties offered by users.

We attempt to assess the impact of OFAC sanctions cooperation across different Ethereum

communities and actors by analyzing on-chain Ethereum data. We ultimately find that cooperation with sanctions is mixed. We see an initially significant impact at first with respect to Tornado Cash volume and utilization – this effectively deteriorates the anonymity it can provide. While volumes and transaction diversity for larger Tornado Cash pools never fully recover to pre-sanction levels, we observe recovery in the smaller pools which may indicate retail users continue to find the product attractive.

Furthermore, analysis of the Ethereum settlement layer also produces interesting insights. We observe that Tornado Cash transactions are not being excluded at the proposer level given the fact the largest proposers process blocks with Tornado Cash transactions. However, it is important to note that it seems possible to develop a cooperative proposer ecosystem; our data indicates other proposers' source cooperative blocks from builders that produce both cooperative and non-cooperative blocks. This leads us to conclude Tornado Cash transaction exclusion seems to be enforced at the block builder level. The exclusion of Tornado Cash transactions within the block building community has changed over time, but has become prevalent since August 2023. These broader market changes have put Tornado Cash and its users in a precarious position as the processing of Tornado Cash seems to rely on Titan Builder, given its prominence or a disparate number of much smaller builders.

This use-case shows Ethereum is not immune to censorship and cooperation – different actors across the ecosystem have different roles that influence where censorship and cooperation can be enforced. The Ethereum community is attempting to grapple with this situation in various ways (see, e.g., Buterin, Illum, Nadler, Schär and Soleimani (2024)).

References

Auer, Raphael and Stijn Claessens, "Regulating cryptocurrencies: assessing market reactions," *BIS Quarterly Review September*, 2018.

Brownworth, Anders, Jon Durfee, Michael Lee, and Antoine Martin, "What Makes Cryptocurrencies Different?," *Liberty Street Economics*, 2023.

Buterin, Vitalik, "Supporting decentralized staking through more anti-correlation incentives," *Ethereum Research*, 2024.

____, Jacob Illum, Matthias Nadler, Fabian Schär, and Ameen Soleimani, "Blockchain privacy and regulatory compliance: Towards a practical equilibrium," *Blockchain: Research and Applications*, 2024, *5* (1), 100176.

Cong, Lin William, Xi Li, Ke Tang, and Yang Yang, "Crypto wash trading," *Management Science*, 2023, *69* (11), 6427–6454.

Daian, Philip, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels, "Flash boys 2.0: Frontrunning, transaction reordering, and consensus instability in decentralized exchanges," *arXiv preprint arXiv:1904.05234*, 2019.

Foley, Sean, Jonathan R Karlsen, and Tālis J Putniņš, "Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?," *The Review of Financial Studies*, 2019, *32* (5), 1798–1853.

Griffin, John M and Amin Shams, "Is Bitcoin really untethered?," *The Journal of Finance*, 2020, *75* (4), 1913–1964.

Heimbach, Lioba, Lucianna Kiffer, Christof Ferreira Torres, and Roger Wattenhofer, "Ethereum's Proposer-Builder Separation: Promises and Realities," in "Proceedings of the 2023 ACM on Internet Measurement Conference" 2023, pp. 406–420.

Li, Tao, Donghwa Shin, and Baolian Wang, "Cryptocurrency pump-and-dump schemes," *Available at SSRN 3267041*, 2021.

Nadler, Matthias and Fabian Schär, "Tornado cash and blockchain privacy: a primer for economists and policymakers," *Federal Reserve Bank of St. Louis Review*, 2023.

Pertsev, Alexey, Roman Semenov, and Roman Storm, "Tornado cash privacy solution version 1.4," *Tornado cash privacy solution version*, 2019, *1*, 6.

Tornado Cash, "Introducing Private Transactions On Ethereum NOW!," 2019.

____ , "Tornado.cash is Finally Trustless," 2020.

Wahrstätter, Anton, Jens Ernstberger, Aviv Yaish, Liyi Zhou, Kaihua Qin, Taro Tsuchiya, Sebastian Steinhorst, Davor Svetinovic, Nicolas Christin, Mikolaj Barczentewicz et al., "Blockchain censorship," *arXiv preprint arXiv:2305.18545*, 2023.

Wu, Mike, Will McTighe, Kaili Wang, Istvan A Seres, Nick Bax, Manuel Puebla, Mariano Mendez, Federico Carrone, Tomás De Mattey, Herman O Demaestri et al., "Tutela: An open-source tool for assessing user-privacy on ethereum and tornado cash," *arXiv preprint arXiv:2201.06811*, 2022.

A Tables

Table 1: Market Cap of TORN Token Post Announcement

	4-Week Window	1-Year Window
Post	-14830650.9***	-40790761.1***
	(2142072.7)	(1385781.2)
BTC Price	4052.3***	-178.3
	(949.4)	(186.6)
ETH Price	-15470.3*	16321.8***
	(7755.3)	(2393.9)
Constant	-29598375.9**	28176843.8***
	(11539765.0)	(2368385.8)
Adj. R2	0.847	0.849
Num. obs.	56	731

Post date: 8/8/22
* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$
Standard errors in parentheses

This table presents estimates of the TORN token's market cap around the OFAC announcement on August 8, 2022. Column 1 includes the sample 4 weeks prior to and 4 weeks after the announcement. Column 2 includes the sample 1 year prior to and 1 year after the announcement. The unit of analysis is daily. Post is an indicator variable with post = 1 for days including and after August 8, 2022 and post = 0 for days prior to the announcement. The variables BTC price and ETH price represent the prices of Bitcoin and Ethereum respectively. The constant term represents the expected value of the TORN market cap when all predictor variables are zero. Standard errors are in parentheses. Significance at the 10% level is denoted by *; 5%, by **; and 1%, by ***.

Table 2: Transaction Volume by Pool Size

	Deposits	Withdrawals
Pool Size = .1 × Post	-120.1***	-93.51***
	(3.60e-14)	(1.89e-14)
Pool Size = 1 × Post	-274.9***	-245.6***
	(7.05e-14)	(1.18e-13)
Pool Size = 10 × Post	-237.3***	-212.8***
	(7.75e-14)	(1.92e-13)
Pool Size = 100 × Post	-163.5***	-136.8***
	(1.31e-14)	(2.11e-15)
Constant	273.9***	253.5***
	(1.15e-13)	(4.36e-14)
Adj. R2	0.271	0.301
Num. obs.	832	832

Post date: 8/8/22
Pool Size Fixed Effects
SE clustered by Pool Size
* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$
Standard errors in parentheses

This table presents estimates of tornado cash volumes around the OFAC announcement on August 8, 2022 for four different pool sizes. Column 1 estimates weekly deposit volumes. Column 2 estimates weekly withdrawal volumes. The unit of analysis is pool-week. Post is an indicator variable with post = 1 for days including and after August 8, 2022 and post = 0 for days prior to the announcement. The constant term represents the expected value of the volumes when all predictor variables are zero. We include pool size fixed effects are for amounts 0.1, 1, 10, and 100. Standard errors in parentheses are clustered by pool size. Significance at the 10% level is denoted by *; 5%, by **; and 1%, by ***.

Table 3: Net Transaction Volume and Value by Pool Size

	Net Volume	Net Value
Pool Size = .1 × Post	1537.5***	153.7***
	(8.43e-14)	(1.74e-13)
Pool Size = 1 × Post	574.8***	574.8***
	(1.99e-13)	(2.05e-13)
Pool Size = 10 × Post	162.7***	1627.1***
	(1.29e-13)	(1.40e-12)
Pool Size = 100 × Post	-43.14***	-4313.7***
	(9.03e-14)	(8.76e-13)
Constant	1682.0***	29065.0***
	(2.21e-13)	(4.65e-12)
Adj. R2	0.392	0.637
Num. obs.	832	832

Post date: 8/8/22
Pool Size Fixed Effects
SE clustered by Pool Size
* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$
Standard errors in parentheses

This table presents estimates of the net volume and value of tornado cash around the OFAC announcement on August 8, 2022 for four different pool sizes. Column 1 estimates weekly net volume, which is computed as cumulative deposit volume minus cumulative withdrawal volume. Column 2 estimates weekly net value, which is net volume multiplied by pool size. The unit of analysis is pool-week. Post is an indicator variable with post = 1 for days including and after August 8, 2022 and post = 0 for days prior to the announcement. The constant term represents the expected value of the net volume and value when all predictor variables are zero. We include pool size fixed effects are for amounts 0.1, 1, 10, and 100. Standard errors in parentheses are clustered by pool size. Significance at the 10% level is denoted by *; 5%, by **; and 1%, by ***.

Table 4: New Addresses Post Announcement

	Deposit Addresses	Withdrawal Addresses
Post	-226.5***	-276.5***
	(18.58)	(30.38)
Constant	296.8***	439.0***
	(10.78)	(17.62)
Adj. R2	0.416	0.283
Num. obs.	208	208

Post date: 8/8/22
* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$
Standard errors in parentheses

This table presents estimates of new tornado cash addresses around the OFAC announcement on August 8, 2022. Column 1 estimates new weekly deposit addresses. Column 2 estimates new weekly withdrawal addresses. The unit of analysis is weekly. Post is an indicator variable with post = 1 for days including and after August 8, 2022 and post = 0 for days prior to the announcement. The constant term represents the expected value of new addresses when all predictor variables are zero. Standard errors are in parentheses. Significance at the 10% level is denoted by *; 5%, by **; and 1%, by ***.

Table 5: Weekly % of Non-Cooperative Blocks Post Court Ruling

	All Builders	Excluding Titan and Faith Builder
PostCourt	-0.182*	-0.787***
	(0.106)	(0.115)
Linear Time Trend	0.0144***	0.00734***
	(0.00243)	(0.00264)
Constant	0.683***	0.797***
	(0.0702)	(0.0762)
Adj. R2	0.437	0.471
Num. obs.	65	65

Post date: 8/17/23
* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$
Standard errors in parentheses

This table presents estimates of the percentage of blocks that are non-cooperative to the tornado cash sanction around the court ruling on August 17, 2023. Column 1 includes the full sample of builders. Column 2 excludes Titan Builder and Faith Builder, which produce the highest concentration of non-cooperative blocks. The unit of analysis is week-block. Post is an indicator variable with post = 1 for days including and after August 17, 2023 and post = 0 for days prior to the court ruling. The linear time trend is 0 at t = 0 and increments by 1 for each week. The constant term represents the expected value of the percent of non-cooperative blocks when all predictor variables are zero. Standard errors are in parentheses. Significance at the 10% level is denoted by *; 5%, by **; and 1%, by ***.

Table 6: Block-Level Priority Fees

	Priority Fee	Priority Fee	Priority Fee	Priority Fee
Non-Cooperative	-0.0202***	-0.0104***	-0.0195***	-0.0124***
	(0.00395)	(0.000656)	(0.00460)	(0.00352)
Constant	0.0876***	0.0875***	0.0876***	0.0875***
	(0.00895)	(0.00685)	(0.00363)	(0.0000105)
Builder FE	N	Y	N	Y
Month-Year FE	N	N	Y	Y
Adj. R2	0.0000263	0.00216	0.00622	0.00776
Num. obs.	2600722	2600722	2600722	2600722

SE clustered by builder and month-year
* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$
Standard errors in parentheses

This table presents estimates of block priority fees based on block cooperation with different variations of fixed effects. Column 1 does not include fixed effects. Column 2 includes only builder fixed effects. Column 3 only includes month-year fixed effects. Column 4 includes both builder and month-year fixed effects. The unit of analysis is month-year-builder-block. The variable non-cooperative is 1 if the block includes a tornado cash transaction and 0 otherwise. The constant term represents the expected value of the priority fee when all predictor variables are zero. Standard errors in parentheses are clustered by builder and month-year. Significance at the 10% level is denoted by *; 5%, by **; and 1%, by ***.

B Overview of Ethereum's Proof-of-Stake Consensus mechanism

Given the distributed nature of public permissionless blockchains, it is critical that all participants operate on the same version of the truth. They must agree on the current state of the ledger, which specifies who owns what. They also need to believe that all participants will come to an agreement on correct the future states of the ledger. This is essential because if someone receives ETH in exchange for some goods or services, that person wants to be sure all other Ethereum users acknowledge the transfer of these ETH, which allows the receiver, in turn, to use them. Agreement on the present and future state of the network is done through a consensus mechanism. A consensus mechanism provides both rules and economic incentives for validators to partake in the process of verifying that Ethereum transactions do not violate specified requirements, such as spending money one does not have.

To participate in the Ethereum validation and consensus process, an Ethereum participant must become a validator. To be designated a validator, a participant must first lock-up "32 ETH into an Ethereum deposit contract [for a predetermined time] and run a set of softwares [including running a node]" specific to running the consensus mechanism.[24] The 32 ETH locked in the deposit contract serves as an entry-fee for participants aiming to partake in the consensus process and is an incentive for the validator to act honestly whilst the funds are locked. If at any time the validator acts dishonestly (e.g., process a transaction where someone did not originally have the funds in the first place), then the validator ultimately risks losing some or all of the ETH they locked up.

In the PoS consensus mechanism validators can have different roles and responsibilities. A validator will be randomly selected from the set of all validators and designated as the proposer for every round of state change. The proposer is responsible for deciding which transactions to append to the blockchain, as described in Section 2. A new block is proposed every 12 seconds and consequently the proposer role will rotate every 12 seconds. A subset of validators are randomly selected from the set of all validators to serve on a committee responsible for attesting whether a proposed block of transactions should be appended to the ledger. Once a block is proposed and shared with the committee of validators, each member of the committee will execute several validation steps and attest that the block of transactions is valid. If a supermajority of the committee attests to the proposed block, the block is added

[24]The PoS design differs from a PoW strategy which required Validators (Miners on Bitcoin) to expend energy to solve a mathematical problem. The solution to the problem can only be found by trial and error but it is easy to verify that the solution is correct. For that reason, the probability of solving the mathematical problem is proportional to one's processing power. Once the problem is solved, the miner is rewarded through both transaction fees and block rewards.

to the ledger, and members of the committee are rewarded with a payment in ETH.[25] The probability of being selected as either a block proposer or to serve on a committee is unrelated to the amount of ETH staked (i.e., locked in the deposit contract); however the more validators an entity controls, the greater the chances they partake in the consensus process.

[25]There is a nuance between the execution chain which manages blocks, mempool transactions, and the beacon chain which manages the consensus process.

C Illustrative example of block building

Suppose a block proposer knows the proposed ETH payments listed in the table below:

Transaction Details			Transaction Cost			
ID	Time submitted	Amount	Computation required (multiplier) C	Base transaction fee B	Priority transaction fee P	Total cost = (C*(B+P))
1	10:00	5.1 ETH	1	0.05 ETH	0.05 ETH	0.1 ETH
2	10:01	20.15 ETH	1.5	0.05 ETH	0.05 ETH	0.15 ETH
3	10:01	10.1 ETH	1	0.05 ETH	0.05 ETH	0.1 ETH
4	10:02	50.3 ETH	2	0.05 ETH	0.1 ETH	0.3 ETH
5	10:04	15.1 ETH	1	0.05 ETH	0.05 ETH	0.1 ETH

We describe the above table in further details and note a few observations:

1. The "Transaction Details" section shows there are five transactions submitted at different times for varying amounts.

2. The "Transaction Cost" section, consist of the following:

   (a) Computation required (C): This indicates how much computation the Ethereum Network must expend to process a transaction. Typically, simple payments, such as ETH transfers, do not require as much computation than smart contracts that maintain more complex logic. The computation required serves as a multiplier of how costly the transaction will be.

   (b) Base transaction fee (B): This amount represents the baseline fee a transaction will have to pay for the Network to process the transaction. The base fee is ultimately removed from circulation and is not necessarily paid to any Ethereum participant.

   (c) Priority transaction fee (P): The Priority fee represents the additional fee a transaction originator is willing to pay the block proper, in addition to the baseline fees, to have their payment included and processed on the Ethereum Network.

   (d) Total cost (C*(B+P)): This is accounts for the total amount a transaction originator will pay to have their transaction processed on Ethereum.

   (e) In summary, the complexity of the transaction, the baseline fee the Ethereum network charges, and the additional fee amount a transaction originator is willing to pa, all influences how profitable a transaction can be to a proposer.

Now let's further assume the proposer is targeting a block size equaling 0.30 ETH in total cost. The 0.30 ETH in total cost becomes a limiting factor in which transactions a proposer

should include. We use the below table to help illustrate how and why a block proposer may choose certain transactions.

Transaction Details			Transaction Pay-Outs			
ID	Time submitted	Amount	Total cost	Baseline fees removed from circulation	Priority fee paid to the Validator	Payment to the Beneficiary
1	10:00	5.1 ETH	0.1 ETH	0.05 ETH	0.05 ETH	5.00 ETH
2	10:01	20.15 ETH	0.15 ETH	0.05 ETH	0.05 ETH	20.00 ETH
3	10:01	10.1 ETH	0.1 ETH	0.05 ETH	0.05 ETH	10.00 ETH
4	10:02	50.3 ETH	0.3 ETH	0.05 ETH	0.1 ETH	50.00 ETH
5	10:04	15.1 ETH	0.1 ETH	0.05 ETH	0.05 ETH	15.00 ETH

If the block proposer simply chooses the first three transactions (i.e., transaction 1, 2, 3), they will be paid .15 ETH for their validating work. If the proposer is incentivized to build and propose a block that maximizes the priority fee paid to them, then they should build a block including transactions 1, 3, and 5, which yields 0.15 ETH in transaction fees earned. This transaction is more than any other transaction combination while maintaining the 0.30 fee constraint we set. This example highlights the need for block proposers to proactively review transactions if they are incentivized to earn the maximum rewards from their proposer activity.

D MEV Relayers and their cooperative status

MEV Relayer	OFAC Cooperation?
Aestus	
Agnostic Gnosis	
Blocknative[35]	x
BloXroute – Regulated[36]	x
BloXroute – Max Profit	
Eden[37]	x
Flashbots	x
Manifold	
Ultra Sound	
Wenmerge	

Table 7: Cooperation status by MEV relayers

This table presents whether or not top MEV relayers are cooperative to sanctions. We identified 4 relayers that have announced their abstention from engaging with Tornado Cash. Sources: Blocknative, BloXroute – Regulated, Eden