Blockchain Censorship

Anton Wahrstätter
Vienna University of Economics and Business
Vienna, Austria

Jens Ernstberger
Technical University of Munich
Munich, Germany
Berkeley Center for Responsible Decentralized Intelligence (RDI)
Berkeley, United States

Aviv Yaish
The Hebrew University
Jerusalem, Israel

Liyi Zhou
Imperial College London
London, United Kingdom
Berkeley Center for Responsible Decentralized Intelligence (RDI)
Berkeley, United States

Kaihua Qin
Imperial College London
London, United Kingdom
Berkeley Center for Responsible Decentralized Intelligence (RDI)
Berkeley, United States

Taro Tsuchiya
Carnegie Mellon University
Pittsburgh, United States

Sebastian Steinhorst
Technical University of Munich
Munich, Germany

Davor Svetinovic
Khalifa University
Abu Dhabi, United Arab Emirates
Vienna University of Economics and Business
Vienna, Austria

Nicolas Christin
Carnegie Mellon University
Pittsburgh, United States

Mikolaj Barczentewicz
University of Surrey
Guildford, United Kingdom

Arthur Gervais
University College London
London, United Kingdom
Berkeley Center for Responsible Decentralized Intelligence (RDI)
Berkeley, United States

ABSTRACT

Permissionless blockchains promise resilience against censorship by a single entity. This suggests that deterministic rules, not third-party actors, decide whether a transaction is appended to the blockchain. In 2022, the U.S. Office of Foreign Assets Control (OFAC) sanctioned a Bitcoin mixer and an Ethereum application, challenging the neutrality of permissionless blockchains.

In this paper, we formalize, quantify, and analyze the security impact of blockchain censorship. We start by defining censorship, followed by a quantitative assessment of current censorship practices. We find that 46% of Ethereum blocks were made by censoring actors complying with OFAC sanctions, indicating the significant impact of OFAC sanctions on the neutrality of public blockchains.

We discover that censorship affects not only neutrality but also security. After Ethereum's transition to Proof-of-Stake (PoS), censored transactions faced an average delay of 85%, compromising their security and strengthening sandwich adversaries.

WWW '24, May 13–17, 2024, Singapore, Singapore

ACM ISBN 979-8-4007-0171-9/24/05.
https://doi.org/10.1145/3589334.3645431

CCS CONCEPTS

• **General and reference** → **Empirical studies**; **Measurement**.

KEYWORDS

Blockchain, Censorship, Ethereum, Bitcoin

ACM Reference Format:
Anton Wahrstätter, Jens Ernstberger, Aviv Yaish, Liyi Zhou, Kaihua Qin, Taro Tsuchiya, Sebastian Steinhorst, Davor Svetinovic, Nicolas Christin, Mikolaj Barczentewicz, and Arthur Gervais. 2024. Blockchain Censorship. In *Proceedings of the ACM Web Conference 2024 (WWW '24), May 13–17, 2024, Singapore, Singapore.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3589334.3645431

1 INTRODUCTION

A permissionless blockchain is a decentralized network composed of globally distributed nodes. Permissionless blockchains enable participants to transact without the need for a trusted intermediary. In theory, users operating under pseudonyms can execute transactions with immunity to external censorship. No single node or group of nodes can control the entire network, making it difficult for any one party to censor or halt transactions.

In recent years, the ability to deploy *smart contracts*, i.e., autonomous programs that run on a permissionless blockchain, led to the development of several applications that aim to establish anonymity, a stronger notion of privacy than pseudonymity [51, 67]. While these applications provide anonymity, they also raised concerns about misuse, as privacy-enhancing blockchain applications are often utilized for money laundering and other illicit purposes [9, 12, 55, 59, 73]. This misuse of privacy-preserving blockchain applications attracted the attention of governments. Recently, the U.S. Office of Foreign Assets Control (OFAC) included smart contract and user account addresses in its Specially Designated Nationals and Blocked Persons (SDN) list. Those subject to the U.S. jurisdiction are prohibited from interacting with persons and property on the SDN list. OFAC sanctioned the cryptocurrency service provider Blender.io [67] on May 5, 2022, for using its privacy-enhancing technology to facilitate criminal money laundering. This was followed by the sanctioning of Tornado Cash (TC) on August 8, 2022, for the same reason. Blender.io is a centralized service for hiding Bitcoin (BTC) money flows, requiring users to trust those managing the service. In contrast, TC is an autonomous and immutable smart contract application on Ethereum [51]. The imposition of OFAC sanctions on smart contract addresses is an unprecedented action that has led to cryptocurrency service providers limiting user access [76], effectively resulting in transaction censorship.

This paper. In this paper, we demystify censorship in permissionless blockchains. We first provide a holistic overview of blockchain censorship by extending the system model of Zhou *et al.* [86] to define blockchain censorship at different layers (§ 4). We provide definitions of blockchain censorship by focusing on censorship on the consensus layer, as validator nodes are responsible for including transactions in a block, and censorship on the application layer, as smart contracts can prevent the successful execution of transactions in a block (§ 4.3). We empirically analyze the impact of OFAC sanctions on Ethereum before (§ 5.2) and after (§ 5.3) the transition to Proof-of-Stake (PoS) ("the merge") and study the implications of censorship on blockchain security (§ 6).

We find that interactions with TC's smart contracts declined by 84.3% within two months following the sanctions. Furthermore, Ethermine, commanding 22% of Ethereum's Proof-of-Work (PoW) hash rate, excluded TC interactions from their blocks, leading to a daily reduction of 200 blocks ($\sim$ 33.4%) containing TC transactions.

For post-merge Ethereum, we find that as of February 2024, at least 56% of the total blocks were made by actors engaged in transaction censorship due to OFAC sanctions. At the application layer, we observed a spike in blocked users by 84.99% in August 2022, the month of introducing the OFAC sanctions. On Bitcoin, we find that OFAC sanctions prevented the Bitcoin mixer Blender.io from continuing to provide its centralized services (§ A).

From a security perspective, we find that censorship delays the inclusion of *both* censored and non-censored transactions by increasing their time in the memory pool (i.e., mempool) (§ 6). To the best of our knowledge, we are the first to provide an empirical overview of applied censorship measures (§ 5) and associated security implications (§ 6). Thereby, our contributions are threefold:

- We define blockchain censorship across system layers and temporal features, quantitatively analyzing censorship by block builders, proposers, relays, and smart contracts.
- We provide quantitative evidence of the historical transaction confirmation latency on Ethereum. We find that Ethereum's move to Proposer-Builder Separation (PBS) has been delaying inclusion of both, censored and non-censored transactions. E.g., the average inclusion delay for TC transactions increased from 15.8 ± 22.8 seconds in Aug. 2022 to 29.3 ± 23.9 seconds in Nov. 2022. Increased confirmation latencies exacerbate sandwich attack risks.
- We prove that no PoS (PoW) protocol can achieve *censorship-resilience* if the censoring validators (miners) make up more than 50% of the validator committee (hashing power).

2 BACKGROUND

2.1 Permissionless Blockchains

Permissionless blockchains build upon the premise of relying on a deterministic set of rules instead of trusted parties to determine the validity of a transaction. Bitcoin [43] is the first permissionless blockchain that enables any entity to create transactions and broadcast them to miners that eventually include them in a block appended to the blockchain. For the most part, Bitcoin transactions represent monetary flows between peers, though it is also possible to write arbitrary data onto the Bitcoin blockchain. Ethereum [75] goes further than Bitcoin by allowing the deployment of arbitrary code, commonly referred to as *smart contracts*, to the blockchain, which is then executed in a decentralized manner. Smart contracts gave birth to a thriving ecosystem of financial applications, Decentralized Finance (DeFi). Competitive trading on DeFi emerged along with novel attacks [86], such as sandwich attacks [85], more generally, front- and back-running [53, 54] exploiting transaction ordering for a financial gain. Bitcoin relies on PoW [4], while Ethereum switched to PoS in September 2022 during "the merge" [17].

Proposer/Builder Separation. Shortly after transitioning to PoS, PBS was introduced to Ethereum. PBS separates the functions of creating new blocks and appending blocks to the blockchain. This is a direct response to problems associated with Miner/ Maximum Extractable Value (MEV) [14, 54], and should supposedly enhance Ethereum's censorship-resistance [18]. MEV extraction can negatively affect user experience [71], and more importantly, the underlying incentive structure of the blockchain, thereby harming blockchain security [54, 81, 83]. In PBS, the role of a "validator" ("miner" in PoW) is divided between separate entities, namely "block builders" and "block proposers" (i.e., the validators themselves). In addition, "relays" were introduced to intermediate and establish the required trust between block builders and proposers. Currently, it is optional for Ethereum validators to participate in PBS, and they can do so by using software called MEV-Boost. Validators are still free not to use MEV-Boost and to build blocks independently.

Privacy-Enhancing Technologies. Asset transfers in blockchain systems such as Bitcoin and Ethereum are transparently traceable [1, 70]. For example, "mixing services" enable obfuscation of asset flows by creating shared transactions with other users or routing assets through shared addresses [24]. For Bitcoin, Blender.io is an example of an application that attempts to enhance privacy by allowing users to deposit their assets into a shared account together with other users and later withdraw them to a newly created, pseudonymous account. Unlike Blender.io, CoinJoin wallets do not require users to trust a service operator [38].

On Ethereum, TC represents the most prominent example of a privacy-enhancing application [51]. TC allows users to deposit assets into a shared account and later withdraw the assets anonymously to a newly generated address, thereby preventing observers from tracing asset flows [33]. This is achieved by relying on Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARKS) [6]. TC offers different "pools" in which users can deposit assets of a fixed denomination, such as a 0.1, 1, 10, or 100 ETH. Users who deposit funds into a given denomination's contract can later withdraw the same amount from the respective pool without revealing their deposit address. The fixed denomination aims to obscure the link between deposits and withdrawals for observers.

Governments believe entities like the North Korean Lazarus Group used the aforementioned privacy technologies for money laundering and evading sanctions [49].

2.2 Rationales for Censorship

While permissionless blockchains aim to resist censorship, real-world pressures can challenge this objective. Certain actors within the blockchain can obstruct user transactions or even prevent block finalization, driven by various motivations. Some reasons for obstruction are *external*, such as government or legal pressures. Others are *internal*, driven by ethical considerations or economic gain.

Endogenous and exogenous reasons are, in practice, intertwined. For example, assume that in some jurisdictions, it is unclear whether the law requires node operators to obstruct blockchain transactions involving addresses linked to a specific criminal organization. In this situation, a node operator may decide to obstruct for many reasons, including (1) lowering their risk of legal liability, (2) a genuine desire not to facilitate criminal activity, and (3) economic motives (e.g., appearing as a responsible business operator to investors). Only the first reason is exogenous, and even then, whether any operator will act on that reason will depend on their risk tolerance (an endogenous factor), especially given that the law is unclear.

Legal and Political Rationales. Blockchain transactions are sometimes used for purposes that are criminalized in most jurisdictions, like hacking, theft, or payments facilitating crimes (e.g., for Child Sexual Abuse Materials [13, 45], drugs and dark web markets [10]). Also, blockchain transactions are used for purposes prohibited for national security or humanitarian reasons, where there is less convergence across various jurisdictions. The key case of the latter is violations of economic sanctions laws. Targeting senders or addressees of such transactions may be challenging for law enforcement. Hence, imposing legal obligations to censor transactions may seem attractive from the perspective of preventing and deterring legally undesirable behavior.

The U.S. Economic Sanctions. Under U.S. sanctions law, it is prohibited to engage in transactions with sanctioned entities, their property, and their interests in property [69]. It is also prohibited to make "any contribution or provision of funds, goods, or services by, to, or for the benefit of" to sanctioned entities. [52] The U.S. OFAC maintains the Specially Designated Nationals and Blocked Persons (SDN) list, including blockchain addresses of sanctioned persons and organizations since 2018. [69] We refer to addresses included in the SDN list as "sanctioned addresses." On a technical note, Ethereum addresses (accounts) tend to prove more persistent than Bitcoin addresses (UTXO). [70]

We focus on two sanctions designations made by OFAC in 2022: Blender.io in May and Tornado Cash in August (re-designated in November) [66–68]. In both cases, blockchain addresses were added to the SDN list. Notably, in the TC case, some SDN-listed addresses refer to smart contracts without administrative functionality. This was the first time smart contract addresses were added to the SDN list. OFAC later clarified that the open-source code of TC smart contracts is not in itself sanctioned, only its instances deployed by the Tornado Cash organisation. [65]

The TC sanctions motivated blockchain node operators to censor transactions involving addresses on the SDN list (cf. Section 5). However, it is debatable whether censorship by blockchain validators, block builders, or relays is required by law [56]. Moreover, *if* those network participants are legally required to censor, it may be insufficient only to censor addresses on the SDN list without attempting to censor unlisted addresses used by sanctioned entities, as OFAC clarified that the SDN list is not exhaustive in this respect [69]. When we use the term "OFAC-compliance," we do so informally, referring to the likely rationale of the actor in question while allowing for the possibility that their actions are not legally required or insufficient for compliance with U.S. sanctions law.

3 RELATED WORK

Defining Censorship. Related contexts in which "censorship" has been defined, at least indirectly (negatively), include works on censorship-resistance (circumvention) in information systems in general [15, 31, 34, 64], and works on censorship-resistance of blockchains in particular [11, 29, 58, 61, 78, 82]. In previous works "censorship" has been understood as: *(a)* not including blocks with transactions to or from targeted entities [11, 58]; *(b)* publicly announcing an intent to exclude future transactions of targeted entities, e.g., by *feather forking* [82]; *(c)* refusing to attest to a chain that contains transactions from or to a targeted entity [58, 61].

The first kind of censorship may apply to block contents or the entity that mined or proposed the block [61]. Censorship of the second kind may also apply to the block content or the identity of the respective user. The third point is specific to PoS-based blockchains [48]. We focus on selective censorship within a network, instead of censorship of entire networks [50].

Censorship Attacks. The literature explores multiple attack vectors relevant to censorship, ranging from Denial of Service (DoS) [5], eclipse [23, 25], routing [2], to prefix hijacking [63]. Focusing on censorship on the consensus layer, Miller [40] introduced the *feather forking* attack, where attackers with a minority of the hash-rate in a PoW blockchain can censor transactions, which was later expanded upon by McCorry *et al.* [39], who propose methods to censor confirmed and unconfirmed transactions. Regarding the possibility of censorship at the network layer, Loe *et al.* [36] show that two methods to join a cryptocurrency network, DNS seeding and IP hard-coding, are vulnerable to censorship.

Censorship Examples. As part of an attack or due to legal obligations, others may ignore or even block an entity. Remote Procedure Call (RPC) endpoints can prevent users from broadcasting their transactions, e.g., in March 2022 the Ethereum RPC endpoint Infura censored OFAC-sanctioned entities [46]. In the front-end, wallet applications have been implicated in censoring transactions [46], and similarly, the web applications of DeFi projects have refused to engage with users who received funds from TC [76]. At the consensus layer, it was reported that a mining pool suppressed the inclusion of Initial Coin Offering transactions [16]. A temporal delay in the execution of a transaction may entail significant financial implications for the censored entity [85].

Preventing Censorship. Zhang *et al.* [82] propose a multi-metric evaluation framework for quantifying the attack resistance of PoW-based blockchains, including against feather-forking attacks. Kostiainen *et al.* [32] develop a censorship-resistant and confidential payment channel that can be deployed to EVM-compatible blockchains. Le and Gervais [33] construct a reward-enabled censorship-resilient mixer. Lotem *et al.* [37] present a mechanism for on-chain congestion detection which can partially defend against censorship attacks. Karakostas *et al.* [29] present a method to assess blockchain decentralization, asserting that centralization can undermine censorship resistance in permissionless protocols.

We build upon prior research to provide a quantitative overview of censorship on public and permissionless blockchains. To the best of our knowledge, we are the first to quantify censorship by different ecosystem actors and discuss its security ramifications.

4 OVERVIEW OF CENSORSHIP

We proceed to outline our system model and provide a definition of censorship on permissionless blockchains.

4.1 System Model

This paper extends the system model presented in [86], with an emphasis on the dynamics of transaction censorship within DeFi:

Network Layer (PBS extension atop [86]). Validators form a P2P network by following rules that determine the communication interface, peer discovery, and procedures for joining and exiting the network. Messages are transmitted between network participants via, e.g., gossip or dedicated communication channels. For example, in PBS, 'relays' serve as specialized communication protocols that facilitate interactions between MEV extractors, block builders, proposers, and the P2P network. Users can submit transactions by joining the P2P network through a self-operated node or by relying on intermediary services (i.e., RPC providers or relays).

Consensus Layer (PBS extension atop [86]). On the consensus layer, a fault-tolerant consensus algorithm ensures that validators in the P2P network agree on a shared state. In a blockchain, a newly proposed block is appended by the validator elected through a leader election protocol (e.g., PoW). A block consists of transactions, where the node appending the block to the blockchain decides on the order of included transactions. Nodes are incentivized through a *block reward*, paid for validating a block, and a *transaction fee*, paid by the client. Each included transaction advances the shared network state, replicated by each validator.

Application Layer (same as [86]). *Decentralized applications* (i.e., smart contracts) are smart contracts that maintain a state. A smart contract is defined by a set of functions that cause state transitions and can be invoked through a transaction. A smart contract can interact with other contracts through *internal calls.* While there is no limit on the number of contracts a contract can interact with, blockchains specify an upper limit on the number of instructions a transaction can execute (e.g., the *gas limit* in Ethereum).

Auxiliary Services (same as [86]). Auxiliary services are, e.g., browser-based cryptocurrency wallets, user interfaces of decentralized applications, and off-chain oracles.

4.2 Notation & Terminology

In this work, we assume a single blockchain $\mathcal{L}$ consisting of blocks B_i, where i corresponds to a *block identifier*, with h corresponding to the block height. We say that $B_i \in \mathcal{L}$, if a block B_i is included in the blockchain $\mathcal{L}$. The blockchain $\mathcal{L}$ is maintained by a set of n validators, which agree upon the current state of $\mathcal{L}$ through a State Machine Replication (SMR) protocol Π. The protocol Π receives as an input a set of transactions **tx**, and outputs the ordered ledger of transactions $\mathcal{L}$. Let σ be a security parameter that determines the finality of $\mathcal{L}$. Then, we denote T_Δ, a polynomial function in σ, as the *finality delay.* We define *transaction inclusion* as follows:

Definition 1 (Transaction Inclusion). A transaction tx received by a validator at time t is *included* in $\mathcal{L}$ by the SMR protocol Π, if $tx \in B_i \mid B_i \in \mathcal{L}$ at time $t' > t + T_\Delta$.

Further, we denote the address of an account maintained through $\mathcal{L}$ as a_i. We intentionally do not differentiate between externally owned accounts and smart contracts, as this abstraction is irrelevant concerning censorship. When preventing censorship, we differentiate between censorship *resistance* and censorship *resilience.* Censorship resistance describes a technology that prevents protocol participants from censoring (e.g., confidential "to" addresses). In contrast, censorship resilience describes that censorship is possible for an individual, but the respective system is resilient against it.

4.3 Definition of Censorship

Censorship is a broad term that may apply in any system layer as introduced in Section 4.1. We formally define the existing notations to clarify the notion in a blockchain context. **Consensus Layer Censorship.** Censorship on the consensus layer may either be enforced *directly* or *indirectly.* For example, a validator may enforce direct censorship by refusing to broadcast a received transaction, sign an attestation, or include a transaction in a block (cf. § 5). Alternatively, an external entity may indirectly enforce censorship by preventing the timely transmission of messages or occupying validator nodes through targeted DoS attacks. Hence, censorship on the consensus layer can also indirectly originate from the network or application layers. Therefore, we focus our definition of censorship on the consensus layer on the *intent* of a protocol participant to obstruct the inclusion of a transaction.

Definition 2 (Strict Censorship). A transaction is censored if a protocol participant intentionally obstructs the inclusion of a transaction, such that $tx \notin B_i \mid B_i \in \mathcal{L}$.

Furthermore, we identify a subtle variant of censorship, where transactions are included with a delay.

Definition 3 (Weak Censorship). A transaction is censored if an actor intentionally obstructs the inclusion of a transaction in the next possible block, such that a transaction tx, received at block height h, does not get included in a block B_i at block height $h' = h+1$, thus $tx \in B_i \mid B_i \in \mathcal{L}$, yet $h_{B_i} < h'_{B_i}$.

Definition 2 and Definition 3 follow related works in distinguishing *censorship* from *ordering* of transactions [3, 7, 8, 26, 54]. As transactions are only ordered once it is decided that they are included in a block, we do not treat it as "censorship" when block builders order ("re-order") transactions differently than expected by the senders of these transactions (e.g., in Ethereum, there may be an expectation of ordering only according to the fees paid by each transaction, which is the default behaviour [20]). We note, however, that intentional re-ordering may result failing transactions or in a lower economic gain for the user (e.g., due to front-running [54]).

Application Layer Censorship. As previously defined, "strict censorship" cannot be enforced directly by the application layer, i.e., smart contracts, because they cannot directly affect the inclusion or finalization of blocks and transactions at the consensus layer. However, a smart contract can indirectly influence blockchain censorship by incentivizing the inclusion or exclusion of transactions and blocks or incentivizing retroactive forking of a blockchain [39, 44, 74]. Besides indirectly influencing the consensus layer, smart contracts can enforce direct censorship by preventing the successful execution of transactions included in a block. We define *smart contract censorship* as follows.

Definition 4 (Smart Contract Censorship). A transaction tx is censored by a smart contract, if $tx \in B_i$, where $B_i \in \mathcal{L}$ is blocked by the state st_i, s.t. further state transitions $st_i \rightarrow st_{i+1}$ are blocked by the respective contract.

An example of smart contract censorship is a block list, which prevents an account with address a_i from successfully interacting with the block listing smart contract (cf. Section 5).

5 CENSORSHIP QUANTIFICATION

In the following, we provide an empirical quantification of censorship on Ethereum and Bitcoin. We distinguish pre- and post-merge Ethereum as the consensus mechanism that impacts censorship.

5.1 Data Collection

We collect data about the OFAC-sanctioned applications TC and Blender.io from the 1st of January 2021, 00:00:00 UTC, until the 17th of February 2024, 23:59:59 UTC. We elaborate on Blender.io in Appendix A.

TC Data. For collecting Ethereum application layer data, we connect to an RPC provider Infura and leverage the Etherscan API. This includes event logs broadcast by sanctioned TC contracts. The event logs indicate that a user has either deposited or withdrawn funds from a TC contract. We include all existing TC pool-contracts in all denominations (cf. Table 1). Notably, we did not include all sanctioned addresses, instead, we focus on deposits and withdrawals to the known TC pool contracts. This means that, e.g., the TC Gitcoin grant contract, contracts deployed on Layer-2 solutions such as Polygon or Arbitrum, or contracts only existing on an Ethereum testnet have been ignored. However, we capture most of the traffic from sanctioned entities because most users interact with the ETH-denominated contracts deployed to the Ethereum mainnet. Our data set has 592180 entries, each representing either a TC deposit or withdrawal, included in 483422 distinct blocks.

Ethereum Ecosystem Data. We collect data on the different ecosystem participants, such as miners, block proposers, block relays, and block builders. For information on external actors such as block builders and relay operators, we use the Relay Data API. The ProposerPayloadsDelivered API endpoint enables us to retrieve information on the parties involved in PBS. In particular, we are interested in the blocks that block builders deliver to proposers. We connect to every existing relay provider by February 2024, including Flashbots, Ultra Sound, Agnostic Gnosis, BloXroute, Blocknative, Manifold, Eden, Aestus, and Relayooor. In summary, our final data set contains 3, 721, 432 blocks, which includes every block since PBS was launched until the 17th of February 2024, 23:59:59 UTC.

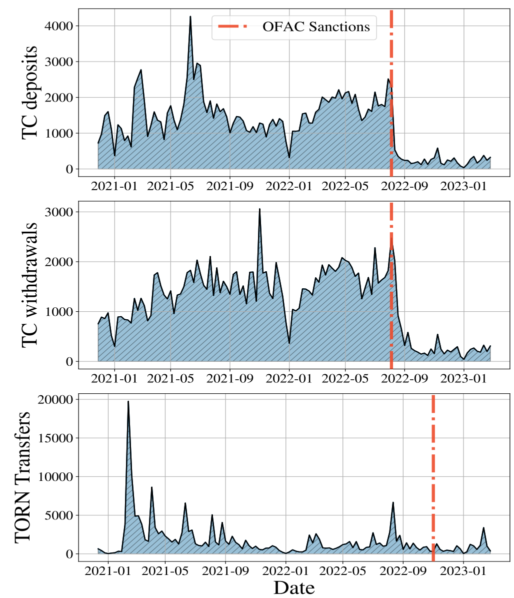

Figure 1: TC deposits and withdrawals over time, accounting for all deployed TC contracts in every denomination from the 1st of October 2021 to November 15th, 2022.

OFAC SDN List. At the time of writing, OFAC's SDN list includes 132 Ethereum addresses. 90 (68%) of the sanctioned addresses belong to the privacy tool TC.

In the following sections, we start by identifying the effects of the sanctions on the TC contracts by assessing their immediate impact on user engagement. Second, we focus on the effects of the sanctions on the individual validators. Third, we assess the impact of the sanctions on the distinct participants of the ecosystem. Thus, we distinguish between block builders, proposers, and relays.

5.2 Pre-PBS Consensus-Layer Censorship

Figure 1 shows the number of interactions with TC contracts over time through the number of weekly deposits and withdrawals. While the weekly deposits and withdrawals reached over 2000 before the sanctions, TC's activity afterward reduced by ten-fold to about 200 deposits and withdrawals per week. As of the enactment of the sanctions, we observe a decline in interactions with TC contracts. For October 2022, a total of 1630 interactions were observed, compared to 16347 interactions in July 2022. However, notably, the number of interactions has never dropped to zero.

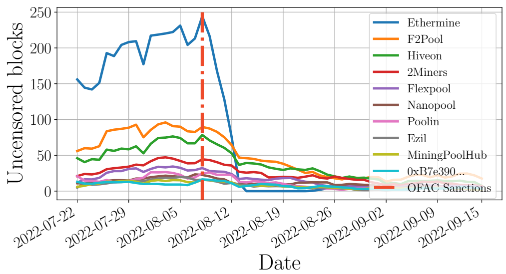

Figure 2: Blocks containing TC transactions by the top 10 miners of uncensored blocks from July 22, 2022 until the transition to PoS on September 15, 2022 (5 day average).

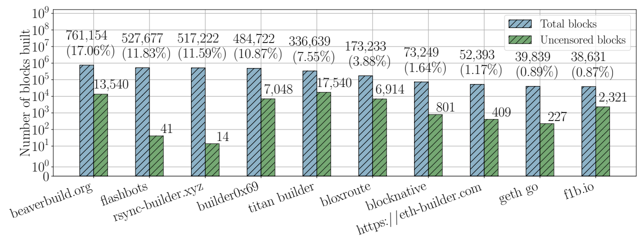

Figure 3: Block builders on the Ethereum blockchain since the activation of PBS at block height 15,537,940 (Sep-15-2022 08:33:47 AM) until block height 15,978,869 (Feb-17-2024 12:59:59 UTC). Uncensored blocks represent blocks containing interactions with TC contracts.

A decline in activity weakens TC's anonymity set, as user privacy hinges on collective participation [72]. In TC, more users amplify individual privacy due to network effects. Reduced anonymity heightens the risk of user deanonymization via side channels.

A reasonable explanation for the decrease in interactions with TC's contracts is that due to the sanctions, the TC website was promptly taken off-line [42]. Consequently, users could only interact with the respective contracts without using any interface, which may not have been feasible for most users. In addition, the open-source Github repository that hosts the TC code was temporarily taken offline, preventing users from redeploying the front end. Circle, the company issuing the USDC stablecoin, froze all USDC tokens inside the TC contracts. As a result, the owners of those assets can no longer move their funds.

How Miners React to Sanctions. Shifting the focus to the largest miners, that eventually decide upon the inclusion of TC transactions into their blocks, we visualize the number of uncensored blocks over time from July 1st, 2021 to September 15th, 2022 in Figure 2. We observe a decrease in uncensored blocks for the 10 largest miners, which is partly an expected consequence of the overall decrease in TC transactions. Nevertheless, Figure 2 indicates that the decline has been more pronounced for Ethermine compared to other miners. Before the sanctions, we observe, on average, 608 (8.5%) blocks containing uncensored daily transactions. Before the sanctions, on average, 203 uncensored blocks per day were built by Ethermine, representing ∼ 33.4% of the total number of uncensored blocks per day. After the sanctions, the number of uncensored blocks built by Ethermine decreased to ∼ 21 blocks per day, which yields a reduction of almost 90%. For the remaining miners, we observe a decrease of uncensored blocks between 50% and 65%, a significantly smaller decline, while no miner altogether ceased, including TC transactions.

5.3 Post-PBS Consensus-Layer Censorship

On September 15th, 2022, 38 days after the TC sanctions, Ethereum transitioned to PoS and partially adopted PBS, adding new intermediaries to the ecosystem. Block builders, proposers, and relays have distinct responsibilities and methods to censor the Ethereum blockchain. In PBS, block proposers may propose blocks they construct independently but can also source blocks from builders who specialize in constructing high-profit blocks. Relays prevent proposers from copying the contents of blocks without paying the builders who constructed them by acting as trusted intermediaries who validate blocks to ensure that proposers can profit from them while only revealing their headers to proposers. By November 15, 2022, with growing PBS adoption, third-party block builders constructed 90% of all blocks. We divide the next section by participant and analyze censorship for each separately.

Block Builder Censorship. External block builders take bundles of transactions, construct blocks, and pass them to block proposers. We display the ten largest block builders and their total number of blocks proposed in Figure 3. We add the total number of uncensored blocks to reveal potential censorship practices.

Figure 3 shows that Beaverbuild is the most successful, as measured by the number of blocks they created. Beaverbuild builders are responsible for ∼ 17.06% of all blocks created between the PoS transition and the 17^{th} of February 2024. This culminates to 761154 blocks in that timeframe. The builders of Flashbots are the second most successful with a total of 527677 (∼ 11.83%) blocks, followed by Rsync-builder, accounting for 517222 (∼ 11.95%) blocks, and Builder0x69 with 484722 (∼ 10.87%) blocks.

Since the Merge, Tornado Cash transactions occurred in 1.89% of the blocks. Our results show the statistical significance that the four largest block builders of the Ethereum network engage in censoring by not including deposits *to* and withdrawals *from* the TC contracts. The same applies to one of the BloXroute builders, accounting for 3.88% of the total number of blocks built, as well as theBlocknative builder, responsible for 1.64% of the total number of blocks.

Among the most successful builders in Figure 3, only two don't have significantly low numbers of TC deposits and withdrawals in their blocks. The non-censoring ones are Titan Builder and F1B.

Block Proposer Censorship. We visualize the most successful block proposers in Figure 4. The staking pool Lido is the most successful group of block proposers between the launch of PBS and the 17^{th} of February 2024, proposing 1163861 (∼ 30.96%) valid blocks. The 2^{nd}, 3^{rd} and 4^{th} most successful block proposers are the exchanges Coinbase, Binance, and Kraken with a total of 561458, 196886 and 187633 blocks respectively. Additionally, we identify staking pools such as Staked.us, Figment, Rocketpool, Bitcoin Suisse, and Stakefish as among the most successful block proposers.

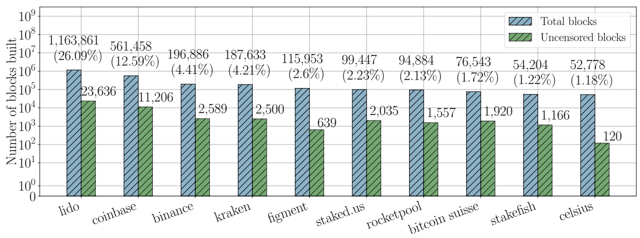

Figure 4: Ethereum block proposers from PBS activation at block 15,537,940 (Sep-15-2022 08:33:47 AM) to block 15,978,869 (Feb-157-2024 12:59:59 UTC). Uncensored blocks contain transactions interacting with TC contracts.

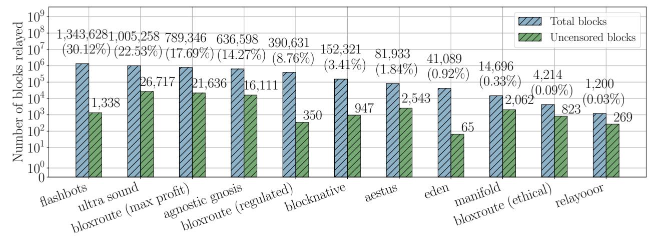

Figure 5: Ethereum block relays from PBS activation at block 15,537,940 (Sep-15-2022 08:33:47 AM) to block 15,978,869 (Nov-15-2022 12:59:59 UTC). Uncensored blocks contain interactions with TC contracts.

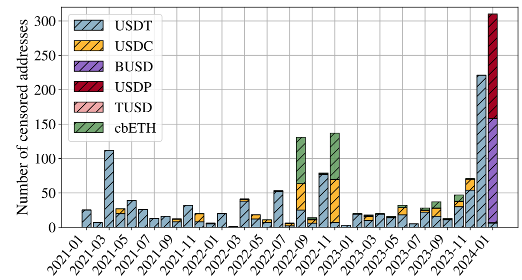

Figure 6: Censored application layer accounts per month.

Focusing on the number of uncensored blocks, we find that among the ten block proposers displayed, Binance, Kraken Figment, Rocketpool, and Celsius include a significantly low number of deposits and withdrawals to TC's contracts within the analyzed period. These proposers account for almost 17% of the total number of blocks proposed since the Merge. We can probabilistically infer that those entities engage in censoring by excluding TC transactions from their blocks. Note that block proposers adopting PBS with MEV-Boost largely depend on blocks from external block builders.

Block Relay Censorship. Third, we analyze block relays that intermediate between block builders and block proposers. In Figure 5, we visualize the existing block relays and the number of blocks forwarded to block proposers that were eventually added to the blockchain. Relays simulate blocks received from builders, censoring the network by only forwarding blocks that do not include interactions with SDN addresses to block proposers.

At the time of writing, around 90% of blocks pass one of the depicted relays. On Ethereum, there are 8 active relay services, two of which are operated by BloXroute. Flashbots relayed 30% MEV-Boost of blocks since the Merge. Ultra Sound's relay comes second with a market share of 22.53% since the Merge. The remaining relays have a market share between 17.69% and 0.3%. As of February 2024, BloXroute's ethical relay and the Blocknative and the Relayooor relays are no longer active. Since PBS activation, Flashbots relayed ~ 1343628 blocks. By looking at all blocks relayed since the Merge, we find statistical evidence ($p \leq 0.01$) that 4 out of 11 relays engaged in censorship by including significantly less TC transactions in their blocks than expected under a binomial distribution and a probability of a block with sanctioned content of 1.89%.

Concluding, we find that PBS impacts censorship on Ethereum. Block builders and block relays impose censorship on proposers who are using MEV-Boost. PBS enables block proposers to boost their profits by capturing the MEV in the proposed blocks. As the most successful block builders and block relays censor TC transactions, block proposers must decide whether to adopt censorship or exclusively connect to a non-censoring relay.

While the censoring block proposers Bitcoin Suisse and Figment both use MEV-Boost, for Bitcoin Suisse we find that only 0.28% of their 9271 blocks were built by external PBS block builders. Blocks proposed by Bitcoin Suisse were relayed by Blocknative, BloXroute ("max profit"), BloXroute ("regulated"), and Eden. Notably, while BloXroute ("max profit") does not censor TC transactions, there were no TC transactions in the blocks relayed by BloXroute ("max profit") and eventually proposed by Bitcoin Suisse. For Figment, 96.8% of the 8400 blocks were built by third-party block builders from censoring relays (i.e., Flashbots and BloXroute ("regulated")).

5.4 Application Layer Censorship

To quantify censorship at the application level (censorship by smart contract), we focus on a set of smart contracts that include functions to lock or freeze assets (cf. Figure 6). These contracts were deployed to the Ethereum blockchain but are controlled by the entity that deployed them, introducing trust requirements. Figure 6 shows per month the number of newly censored addresses by these contracts. In the analysed time frame, the USDT contract blocked 1006 accounts. This exceeds the 211 blocked accounts at USDC. For cbETH, we find that a total of 164 accounts have been blocked since its deployment in February 2022. Among the accounts blocked from interacting with the cbETH contract, we identify TC's contracts and other OFAC-sanctioned entities.

In August 2022, with sanctions on TC, blocked addresses hit 131, marking an 84.99% rise from the monthly average between July 2021 and August 2022.

Censorship at the smart contract level can utilize third-party contracts. However, its effectiveness is debatable, as sanctioned entities might transfer assets and use alternative accounts atomically.

6 CENSORSHIP, LATENCY, AND SECURITY

In the following, we explore how censorship affects security. We find that censorship slows down transaction confirmation latency,

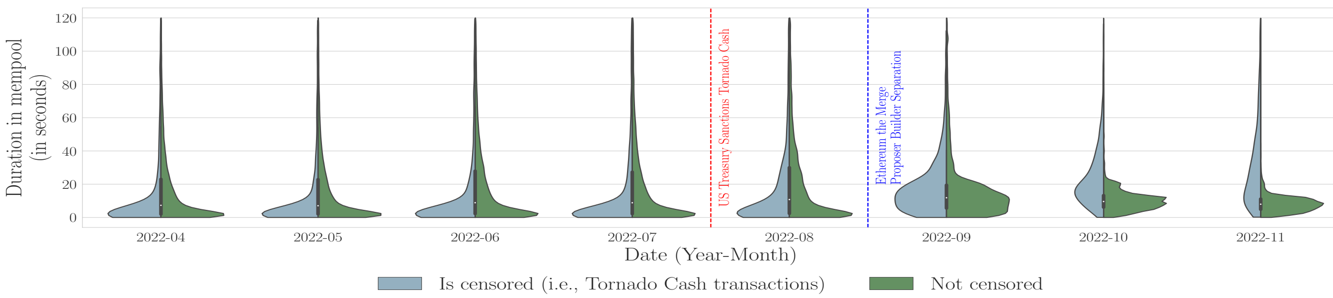

Figure 7: Transaction inclusion times before and after the merge ($15th$ **September 2022), PBS (**$15th$ **September 2022), and sanctions (8th August 2022). These events notably impacted inclusion delays; e.g., average delay for TC transactions rose from** 15.8 ± 22.8 **seconds in August** 2022 **to** 29.3 ± 23.9 **seconds in November** 2022**.**

which was shown to affect double-spending resilience [30]. In Appendix E, we show that no PoS protocol can attain censorship resilience when $> 50\%$ of the validator committee is censoring.

Transaction Latency and Security. Research indicates that extended mempool presence facilitates double-spending of zero confirmation transactions [30]. Increased confirmation latencies raise the success rate for sandwich attackers targeting trades [85]. Moreover, price shifts in automated market makers can trigger transaction failures if transactions confirm "slowly" [84]. Finally, systematically increased transaction latencies bear the risk of congesting the mempool, increasing the likelihood of transaction re-transmission and P2P network congestion. Congestion slows down block and transaction propagation, deteriorating blockchain security [23, 35].

Transaction Issuance Time. We adapt geth [84, 85], Ethereum's predominant execution client [19], to log all P2P transactions from April to November 2022. A node's observed transactions scale with peer connections, bandwidth, and computing power. Our geth runs on an Ubuntu 20.04.2 LTS, AMD Ryzen Threadripper 3990X (64-core, 2.9GHz), 256 GB RAM, and NVMe SSDs, with a cap of $1,000$ peer connections, up from the standard 50. Located in Europe, it recorded 316.5 million transactions during this period. We rely on the timestamp data in the block header to estimate the transaction confirmation time. It should be noted that this is a rough estimate of the confirmation time because miners may decide not to report the precise timestamp when the blocks are generated [80].

Results. After gathering the timestamps when a transaction emerges on the P2P network and the time the transaction is included on-chain, we can identify the relative time it takes for a transaction's inclusion. Further, we distinguish between transactions that are and are not subject to censorship (i.e., TC and non-TC transactions). To ensure a fair comparison, we only consider uncensored transactions mined in the same blocks as TC transactions at a similar gas price (i.e., $\pm 10\%$). Two insights emerge. First, censored transactions linger longer in the mempool and confirm more slowly on-chain than non-censored ones. By November 2022, the average inclusion delay was 8.7 ± 8.3 seconds for non-censored transactions, compared to 29.3 ± 23.9 seconds for TC transactions. Second, since Ethereum's transition to PoS and adoption of PBS, transaction inclusion latency increased. For instance, the average delay for TC transactions rose from 15.8 ± 22.8 seconds in August 2022 to 29.3 ± 23.9 seconds in November 2022. To eliminate the impact of the node's location, we repeat the same experiment with the US node (for two weeks) and confirm that TC transactions stay longer than non-TC transactions.

7 DISCUSSION

Our analysis indicates that distinguishing individual actors is non-trivial, as the behavior of one can influence others' practices. Block proposers utilizing MEV-Boost rely on block builders and relays for payload delivery. Consequently, these proposers, who by default use a profit-maximizing strategy to choose payloads, often accept assigned blocks without assessing potential contributions to censorship. By building blocks locally (as was the standard before PBS) or by exclusively connecting to non-censoring relays, block proposers can ensure to not partake in censorship. Furthermore, proposers can use the *min-bid* flag offered by the MEV-Boost software that enables them to automatically fall back to uncensored block building ("vanilla" building) if the payments offered by blocks constructed by builders are not above a certain threshold [27].

8 CONCLUSION

In this paper, we investigate the impact of censorship in blockchains. We present a systematization of blockchain censorship through formal definitions and quantification of the effect of OFAC sanctions on censorship in Ethereum and Bitcoin. After transitioning to PoS, we find that 46% of Ethereum blocks were made by censoring actors intending to comply with OFAC sanctions. Additionally, we reason about the impact of censorship on blockchain security. We find that censorship prolongs the time until a transaction is confirmed. Increased transaction confirmation latency not only compromises the integrity and trustworthiness of the blockchain but also opens avenues for various security vulnerabilities, including double-spending and network congestion.

Our results show that censorship on blockchains is not a mere hypothetical threat: it already degrades the security of existing blockchains and the quality of service for users. Our work sheds light on a dilemma anticipated for a decade: will the promise of a permissionless, secure append-only ledger withstand if regulators intervene? We hope that this work draws attention to the significance of censorship in permissionless blockchains and engenders future work on addressing the mentioned security issues.

REFERENCES

[1] Elli Androulaki, Ghassan O. Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Capkun. 2013. Evaluating User Privacy in Bitcoin. In *Financial Cryptography and Data Security*, Ahmad-Reza Sadeghi (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 34–51.

[2] Maria Apostolaki, Aviv Zohar, and Laurent Vanbever. 2017. Hijacking bitcoin: Routing attacks on cryptocurrencies. In *2017 IEEE symposium on security and privacy (SP)*. IEEE, 375–392.

[3] Raphael Auer, Jon Frost, Jose María Vidal Pastor, et al. 2022. *Miners as intermediaries: extractable value and market manipulation in crypto and DeFi.* Technical Report. Bank for International Settlements.

[4] Shehar Bano, Alberto Sonnino, Mustafa Al-Bassam, Sarah Azouvi, Patrick McCorry, Sarah Meiklejohn, and George Danezis. 2019. SoK: Consensus in the Age of Blockchains. In *Proceedings of the 1st ACM Conference on Advances in Financial Technologies* (Zurich, Switzerland) *(AFT '19)*. Association for Computing Machinery, New York, NY, USA, 183–198. https://doi.org/10.1145/3318041.3355458

[5] Alex Biryukov and Ivan Pustogarov. 2015. Bitcoin over Tor isn't a good idea. In *2015 IEEE Symposium on Security and Privacy*. IEEE, 122–134.

[6] Nir Bitansky, Ran Canetti, Alessandro Chiesa, and Eran Tromer. 2012. From Extractable Collision Resistance to Succinct Non-Interactive Arguments of Knowledge, and Back Again. In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference* (Cambridge, Massachusetts) *(ITCS '12)*. Association for Computing Machinery, New York, NY, USA, 326–349. https://doi.org/10.1145/2090236.2090263

[7] Vitalik Buterin. 2021. State of research: Increasing censorship resistance of transactions under proposer/builder separation (PBS). https://notes.ethereum.org/@vbuterin/pbs_censorship_resistance

[8] Tarun Chitra and Kshitij Kulkarni. 2022. Improving Proof of Stake Economic Security via MEV Redistribution. In *Proceedings of the 2022 ACM CCS Workshop on Decentralized Finance and Security*. 1–7.

[9] Nicolas Christin. 2013. Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace. In *Proceedings of the 22nd International Conference on World Wide Web* (Rio de Janeiro, Brazil) *(WWW '13)*. Association for Computing Machinery, New York, NY, USA, 213–224. https://doi.org/10.1145/2488388.2488408

[10] Nicolas Christin. 2022. *Measuring And Analyzing Online Anonymous ('DARKNET') Marketplaces*. Technical Report. CARNEGIE-MELLON UNIV PITTSBURGH PA.

[11] Tyler Crain, Christopher Natoli, and Vincent Gramoli. 2021. Red belly: a secure, fair and scalable open blockchain. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 466–483.

[12] Jesse Crawford and Yong Guan. 2020. Knowing your Bitcoin Customer: Money Laundering in the Bitcoin Economy. In *2020 13th International Conference on Systematic Approaches to Digital Forensic Engineering (SADFE)*. 38–45. https://doi.org/10.1109/SADFE51007.2020.00013

[13] Kirsten Cremona, Donald Tabone, and Clifford De Raffaele. 2019. Cybersecurity and the Blockchain: Preventing the Insertion of Child Pornography Images. In *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*. 197–204. https://doi.org/10.1109/CyberC.2019.00042

[14] Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels. 2020. Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability. In *2020 IEEE Symposium on Security and Privacy, SP 2020, San Francisco, CA, USA, May 18-21, 2020*. IEEE, San Francisco, CA, USA, 910–927. https://doi.org/10.1109/SP40000.2020.00040

[15] George Danezis and Ross Anderson. 2004. The economics of censorship resistance. *Proceedings of the 3rd Annual Workship on Economics and Information Security (WEIS04)(May 2004)* (2004).

[16] Shayan Eskandari, Seyedehmahsa Moosavi, and Jeremy Clark. 2019. SoK: Transparent Dishonesty: front-running attacks on Blockchain. https://doi.org/10.1007/978-3-030-43725-1_13 arXiv:1902.05164 [cs.CR]

[17] Ethereum. 2022. The Merge. https://ethereum.org/en/upgrades/merge/

[18] Ethereum. 2023. Proposer-builder separation. https://github.com/ethereum/ethereum-org-website/blob/1729448/src/content/roadmap/pbs/index.md

[19] Ethernodes. 2022. The popularity of Ethereum clients. https://ethernodes.org/ethernodes.org.

[20] Yotam Gafni and Aviv Yaish. 2022. Greedy Transaction Fee Mechanisms for (Non-)myopic Miners. https://doi.org/10.48550/ARXIV.2210.07793

[21] Yingzi Gao, Yuan Lu, Zhenliang Lu, Qiang Tang, Jing Xu, and Zhenfeng Zhang. 2022. Dumbo-ng: Fast asynchronous bft consensus with throughput-oblivious latency. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*. 1187–1201.

[22] Juan Garay, Aggelos Kiayias, and Nikos Leonardos. 2015. The Bitcoin Backbone Protocol: Analysis and Applications. In *Advances in Cryptology - EUROCRYPT 2015*, Elisabeth Oswald and Marc Fischlin (Eds.). Springer, Berlin, Heidelberg, 281–310.

[23] Arthur Gervais, Hubert Ritzdorf, Ghassan O Karame, and Srdjan Capkun. 2015. Tampering with the delivery of blocks and transactions in bitcoin. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. 692–705.

[24] Noemi Glaeser, Matteo Maffei, Giulio Malavolta, Pedro Moreno-Sanchez, Erkan Tairi, and Sri Aravinda Krishnan Thyagarajan. 2022. Foundations of Coin Mixing Services. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* (Los Angeles, CA, USA) *(CCS '22)*. Association for Computing Machinery, New York, NY, USA, 1259–1273. https://doi.org/10.1145/3548606.3560637

[25] Ethan Heilman, Alison Kendler, Aviv Zohar, and Sharon Goldberg. 2015. Eclipse attacks on Bitcoin's peer-to-peer network. In *24th USENIX Security Symposium (USENIX Security 15)*. 129–144.

[26] Lioba Heimbach and Roger Wattenhofer. 2022. SoK: Preventing Transaction Reordering Manipulations in Decentralized Finance. arXiv:https://doi.org/10.48550/arXiv.2203.11520 https://arxiv.org/abs/2203.11520

[27] Alejo; Hasu Hu, Elaine; Salles. 2022. The Cost of Resilience. https://web.archive.org/web/20230325222151/https://writings.flashbots.net/the-cost-of-resilience

[28] Hideaki Ishii, Yuan Wang, and Shuai Feng. 2022. An overview on multi-agent consensus under adversarial attacks. *Annual Reviews in Control* 53 (2022), 252–272.

[29] Dimitris Karakostas, Aggelos Kiayias, and Christina Ovezik. 2022. SoK: A Stratified Approach to Blockchain Decentralization.

[30] Ghassan O Karame, Elli Androulaki, Marc Roeschlin, Arthur Gervais, and Srdjan Čapkun. 2015. Misbehavior in bitcoin: A study of double-spending and accountability. *ACM Transactions on Information and System Security (TISSEC)* 18, 1 (2015), 1–32.

[31] Sheharbano Khattak, Tariq Elahi, Laurent Simon, Colleen M Swanson, Steven J Murdoch, and Ian Goldberg. 2016. SOK: Making sense of censorship resistance systems. *Proceedings on Privacy Enhancing Technologies* 2016, 4 (2016), 37–61.

[32] Kari Kostiainen, Sven Gnap, and Ghassan Karame. 2022. Censorship-Resilient and Confidential Collateralized Second-Layer Payments. Cryptology ePrint Archive, Paper 2022/1520. https://eprint.iacr.org/2022/1520 https://eprint.iacr.org/2022/1520.

[33] Duc V. Le and Arthur Gervais. 2021. *AMR: Autonomous Coin Mixer with Privacy Preserving Reward Distribution.* Association for Computing Machinery, New York, NY, USA, 142–155. https://doi.org/10.1145/3479722.3480800

[34] Christopher S Leberknight, Mung Chiang, Harold Vincent Poor, and Felix Wong. 2010. A taxonomy of Internet censorship and anti-censorship. In *Fifth International Conference on Fun with Algorithms*. 52–64.

[35] Yulin Liu, Yuxuan Lu, Kartik Nayak, Fan Zhang, Luyao Zhang, and Yinhong Zhao. 2022. Empirical Analysis of EIP-1559: Transaction Fees, Waiting Times, and Consensus Security. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* (Los Angeles, CA, USA) *(CCS '22)*. Association for Computing Machinery, New York, NY, USA, 2099–2113. https://doi.org/10.1145/3548606.3559341

[36] Angelique Faye Loe and Elizabeth Anne Quaglia. 2019. You Shall Not Join: A Measurement Study of Cryptocurrency Peer-to-Peer Bootstrapping Techniques. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (London, United Kingdom) *(CCS '19)*. Association for Computing Machinery, New York, NY, USA, 2231–2247. https://doi.org/10.1145/3319535.3345649

[37] Ayelet Lotem, Sarah Azouvi, Patrick McCorry, and Aviv Zohar. 2022. Sliding Window Challenge Process for Congestion Detection. https://doi.org/10.48550/ARXIV.2201.09009

[38] Felix Konstantin Maurer, Till Neudecker, and Martin Florian. 2017. Anonymous CoinJoin transactions with arbitrary values. In *2017 IEEE Trustcom/BigDataSE/ICESS*. IEEE, 522–529.

[39] Patrick McCorry, Alexander Hicks, and Sarah Meiklejohn. 2018. Smart Contracts for Bribing Miners. In *Financial Cryptography and Data Security: FC 2018 International Workshops, BITCOIN, VOTING, and WTSC, Nieuwpoort, Curaçao, March 2, 2018, Revised Selected Papers* (Nieuwpoort, Curaçao). Springer-Verlag, Berlin, Heidelberg, 3–18. https://doi.org/10.1007/978-3-662-58820-8_1

[40] Andrew Miller. 2013. Feather-forks: enforcing a blacklist with sub-50% hash power. https://web.archive.org/web/20221101152114/https://bitcointalk.org/index.php?topic=312668.0

[41] Andrew Miller, Yu Xia, Kyle Croman, Elaine Shi, and Dawn Song. 2016. The honey badger of BFT protocols. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*. 31–42.

[42] Immanual John Milton. 2022. Crypto Mixer Tornado Cash's Accounts Are Disabled After US Sanctions. https://www.bloomberg.com/news/articles/2022-08-08/crypto-mixer-tornado-s-accounts-are-disabled-after-us-sanctions

[43] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. https://web.archive.org/web/20100704213649/https://bitcoin.org/bitcoin.pdf

[44] Gleb Naumenko. 2022. TxWithhold Smart Contracts. https://web.archive.org/web/20220628075911/https://thelab31.xyz/blog/txwithhold

[45] Malaw Ndiaye and Pr Karim Konate. 2021. Cryptocurrency Crime: Behaviors of Malicious Smart Contracts in Blockchain. In *2021 International Symposium on*

Networks, Computers and Communications (ISNCC). IEEE, 1–8.
[46] Danny Nelson. 2022. Crypto Industry's Sanctions Woes on Full Display in MetaMask's Venezuela Hiccup. https://web.archive.org/web/20220516095735/https://www.coindesk.com/business/2022/03/04/crypto-industrys-sanctions-woes-on-full-display-\in-metamasks-venezuela-hiccup/
[47] Joachim Neu, Ertem Nusret Tas, and David Tse. 2022. The availability-accountability dilemma and its resolution via accountability gadgets. In *International Conference on Financial Cryptography and Data Security*. Springer, 541–559.
[48] Michael Neuder, Daniel J Moroz, Rithvik Rao, and David C Parkes. 2021. Low-cost attacks on Ethereum 2.0 by sub-1/3 stakeholders.
[49] Joshua Park. 2021. The Lazarus group: The Cybercrime Syndicate Financing the north Korea State. *Harvard International Review* 42, 2 (2021), 34–39.
[50] Ginger Perng, Michael K Reiter, and Chenxi Wang. 2005. Censorship resistance revisited. In *International Workshop on Information Hiding*. Springer, 62–76.
[51] Alexey Pertsev, Roman Semenov, and Roman Storm. 2019. Tornado Cash Privacy Solution Version 1.4.
[52] President of the United States. 2015. Executive Order 13694 of April 1, 2015. https://www.federalregister.gov/documents/2015/04/02/2015-07788/blocking-the-property-of-certain-persons-engaging-in-significant-malicious-cyber-enabled-activities.
[53] Kaihua Qin, Liyi Zhou, Pablo Gamito, Philipp Jovanovic, and Arthur Gervais. 2021. An Empirical Study of DeFi Liquidations: Incentives, Risks, and Instabilities. In *Proceedings of the 21st ACM Internet Measurement Conference* (Virtual Event) *(IMC '21)*. Association for Computing Machinery, New York, NY, USA, 336–350. https://doi.org/10.1145/3487552.3487811
[54] Kaihua Qin, Liyi Zhou, and Arthur Gervais. 2022. Quantifying Blockchain Extractable Value: How dark is the forest?. In *43rd IEEE Symposium on Security and Privacy, SP 2022, San Francisco, CA, USA, May 22-26, 2022*. IEEE, San Francisco, CA, USA, 198–214. https://doi.org/10.1109/SP46214.2022.9833734
[55] Tim Ruffing, Pedro Moreno-Sanchez, and Aniket Kate. 2014. Coinshuffle: Practical decentralized coin mixing for bitcoin. In *European Symposium on Research in Computer Security*. Springer, 345–364.
[56] Rodrigo Seira, Amy Aixi Zhang, and Dan Robinson. 2022. Base Layer Neutrality. https://www.paradigm.xyz/2022/09/base-layer-neutrality.
[57] Peiyao Sheng, Gerui Wang, Kartik Nayak, Sreeram Kannan, and Pramod Viswanath. 2021. BFT protocol forensics. In *Proceedings of the 2021 ACM SIGSAC conference on computer and communications security*. 1722–1743.
[58] Paulo Silva, David Vavricka, João Barreto, and Miguel Matos. 2020. Impact of Geo-Distribution and Mining Pools on Blockchains: A Study of Ethereum. In *2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. IEEE, San Francisco, CA, USA, 245–252. https://doi.org/10.1109/DSN48063.2020.00041
[59] Johann Stockinger, Bernhard Haslhofer, Pedro Moreno-Sanchez, and Matteo Maffei. 2021. Pinpointing and Measuring Wasabi and Samourai CoinJoins in the Bitcoin Ecosystem. arXiv:2109.10229 [cs.CR]
[60] Ertem Nusret Tas, David Tse, Fisher Yu, Sreeram Kannan, and Mohammad Ali Maddah-Ali. 2022. Bitcoin-enhanced proof-of-stake security: Possibilities and impossibilities.
[61] Wai Yan Maung Maung Thin, Naipeng Dong, Guangdong Bai, and Jin Song Dong. 2018. Formal analysis of a proof-of-stake blockchain. In *2018 23rd International Conference on Engineering of Complex Computer Systems (ICECCS)*. IEEE, 197–200.
[62] Tin Tironsakkul, Manuel Maarek, Andrea Eross, and Mike Just. 2022. The Unique Dressing of Transactions: Wasabi CoinJoin Transaction Detection. In *Proceedings of the 2022 European Interdisciplinary Cybersecurity Conference* (Barcelona, Spain) *(EICC '22)*. Association for Computing Machinery, New York, NY, USA, 21–28. https://doi.org/10.1145/3528580.3528585
[63] Muoi Tran, Inho Choi, Gi Jun Moon, Anh V Vu, and Min Suk Kang. 2020. A stealthier partitioning attack against bitcoin peer-to-peer network. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 894–909.
[64] Michael Carl Tschantz, Sadia Afroz, Vern Paxson, et al. 2016. Sok: Towards grounding censorship circumvention in empiricism. In *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, 914–933.
[65] U.S. Department of the Treasury. 2022. FAQ 1076. What is prohibited as a result of OFAC's designation of Tornado Cash? https://web.archive.org/web/20221014112946/https://home.treasury.gov/policy-issues/financial-sanctions/faqs/1076.
[66] U.S. Department of the Treasury. 2022. Treasury Designates DPRK Weapons Representatives. https://web.archive.org/web/20221126125148/https://home.treasury.gov/news/press-releases/jy1087.
[67] U.S. Department of the Treasury. 2022. U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats. https://web.archive.org/web/20221124112323/https://home.treasury.gov/news/press-releases/jy0768.
[68] U.S. Department of the Treasury. 2022. U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash. https://web.archive.org/web/20221026104007/https://home.treasury.gov/news/press-releases/jy0916.
[69] U.S. Department of the Treasury's Office of Foreign Assets Control. 2021. Sanctions Compliance Guidance for the Virtual Currency Industry. https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf.
[70] Friedhelm Victor. 2020. Address Clustering Heuristics For Ethereum. In *Financial Cryptography and Data Security: 24th International Conference, FC 2020 , Kota Kinabalu, Malaysia, February 10–14, 2020 Revised Selected Papers* (Kota Kinabalu, Malaysia). Springer-Verlag, Berlin, Heidelberg, 617–633. https://doi.org/10.1007/978-3-030-51280-4_33
[71] Ye Wang, Patrick Zuest, Yaxing Yao, Zhicong Lu, and Roger Wattenhofer. 2022. Impact and User Perception of Sandwich Attacks in the DeFi Ecosystem. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 591, 15 pages. https://doi.org/10.1145/3491102.3517585
[72] Zhipeng Wang, Stefanos Chaliasos, Kaihua Qin, Liyi Zhou, Lifeng Gao, Pascal Berrang, Benjamin Livshits, and Arthur Gervais. 2023. On How Zero-Knowledge Proof Blockchain Mixers Improve, and Worsen User Privacy. In *Proceedings of the ACM Web Conference 2023* (Austin, TX, USA) *(WWW '23)*. Association for Computing Machinery, New York, NY, USA, 2022–2032. https://doi.org/10.1145/3543507.3583217
[73] Mark Weber, Giacomo Domeniconi, Jie Chen, Daniel Karl I. Weidele, Claudio Bellei, Tom Robinson, and Charles E. Leiserson. 2019. Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for Financial Forensics. arXiv:1908.02591 http://arxiv.org/abs/1908.02591
[74] Fredrik Winzer, Benjamin Herd, and Sebastian Faust. 2019. Temporary Censorship Attacks in the Presence of Rational Miners. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE Computer Society, Los Alamitos, CA, USA, 357–366. https://doi.org/10.1109/EuroSPW.2019.00046
[75] Gavin Wood et al. 2014. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper* 151, 2014 (2014), 1–32.
[76] Liam Wright. 2022. DeFi protocols Aave, Uniswap, Balancer, ban users following OFAC sanctions on Tornado Cash. https://web.archive.org/web/20220816142409/https://cryptoslate.com/defi-protocols-aave-uniswap-balancer-ban-users-following\-ofac-sanctions-on-tornado-cash/
[77] Lei Wu, Yufeng Hu, Yajin Zhou, Haoyu Wang, Xiapu Luo, Zhi Wang, Fan Zhang, and Kui Ren. 2021. Towards Understanding and Demystifying Bitcoin Mixing Services. In *Proceedings of the Web Conference 2021* (Ljubljana, Slovenia) *(WWW '21)*. Association for Computing Machinery, New York, NY, USA, 33–44. https://doi.org/10.1145/3442381.3449880
[78] Xiangbin Xian, Yu Zhou, Yurong Guo, Zhenguo Yang, and Wenyin Liu. 2019. Improved consensus mechanisms against censorship attacks. In *2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS)*. IEEE, 718–723.
[79] Aviv Yaish, Kaihua Qin, Liyi Zhou, Aviv Zohar, and Arthur Gervais. 2023. Speculative Denial-of-Service Attacks in Ethereum. Cryptology ePrint Archive, Paper 2023/956. , 24 pages. https://ia.cr/2023/956
[80] Aviv Yaish, Gilad Stern, and Aviv Zohar. 2022. Uncle Maker: (Time)Stamping Out The Competition in Ethereum. https://ia.cr/2022/1020
[81] Aviv Yaish, Saar Tochner, and Aviv Zohar. 2022. Blockchain Stretching & Squeezing: Manipulating Time for Your Best Interest. In *Proceedings of the 23rd ACM Conference on Economics and Computation* (Boulder, CO, USA) *(EC '22)*. Association for Computing Machinery, New York, NY, USA, 65–88. https://doi.org/10.1145/3490486.3538250
[82] Ren Zhang and Bart Preneel. 2019. Lay down the common metrics: Evaluating proof-of-work consensus protocols' security. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, IEEE, San Francisco, CA, USA, 175–192. https://doi.org/10.1109/sp.2019.00086
[83] Liyi Zhou, Kaihua Qin, Antoine Cully, Benjamin Livshits, and Arthur Gervais. 2021. On the Just-In-Time Discovery of Profit-Generating Transactions in DeFi Protocols. In *42nd IEEE Symposium on Security and Privacy, SP 2021, San Francisco, CA, USA, 24-27 May 2021*. IEEE, San Francisco, CA, USA, 919–936. https://doi.org/10.1109/SP40001.2021.00113
[84] Liyi Zhou, Kaihua Qin, and Arthur Gervais. 2021. A2MM: Mitigating Frontrunning, Transaction Reordering and Consensus Instability in Decentralized Exchanges. arXiv:2106.07371 https://arxiv.org/abs/2106.07371
[85] Liyi Zhou, Kaihua Qin, Christof Ferreira Torres, Duc Viet Le, and Arthur Gervais. 2021. High-Frequency Trading on Decentralized On-Chain Exchanges. In *42nd IEEE Symposium on Security and Privacy, SP 2021, San Francisco, CA, USA, 24-27 May 2021*. IEEE, San Francisco, CA, USA, 428–445. https://doi.org/10.1109/SP40001.2021.00027
[86] Liyi Zhou, Xihan Xiong, Jens Ernstberger, Stefanos Chaliasos, Zhipeng Wang, Ye Wang, Kaihua Qin, Roger Wattenhofer, Dawn Song, and Arthur Gervais. 2022. SoK: Decentralized Finance (DeFi) Attacks. https://doi.org/10.48550/ARXIV.2208.13035

A CENSORSHIP ON BITCOIN

Blender.io Data. For data on Blender.io, we set up a local Bitcoin node and parse the raw data files. We filter for transactions from

Table 1: Tornado Cash contracts we capture in this work.

Tornado Cash Contract	Address
0.1 ETH	0x12D66f87A04A9E220743712cE6d9bB1B5616B8Fc
1 ETH	0x47CE0C6eD5B0Ce3d3A51fdb1C52DC66a7c3c2936
10 ETH	0x910Cbd523D972eb0a6f4cAe4618aD62622b39DbF
100 ETH	0xA160cdAB225685dA1d56aa342Ad8841c3b53f291
0.1k DAI	0xD4B88Df4D29F5CedD6857912842cff3b20C8Cfa3
1k DAI	0xFD8610d20aA15b7B2E3Be39B396a1bC3516c7144
10k DAI	0x07687e702b410Fa43f4cB4Af7FA097918ffD2730
100k DAI	0x23773E65ed146A459791799d01336DB287f25334
5k CDAI	0x22aaA7720ddd5388A3c0A3333430953C68f1849b
50k CDAI	0x03893a7c7463AE47D46bc7f091665f1893656003
500k CDAI	0x2717c5e28cf931547B621a5dddb772Ab6A35B701
5m CDAI	0xD21be7248e0197Ee08E0c20D4a96DEBdaC3D20Af
100 USDC	0xd96f2B1c14Db8458374d9Aca76E26c3D18364307
1k USDC	0x4736dCf1b7A3d580672CcE6E7c65cd5cc9cFBa9D
10k USDC	0xD691F27f38B395864Ea86CfC7253969B409c362d
100 USDT	0x169AD27A470D064DEDE56a2D3ff727986b15D52B
1000 USDT	0x0836222F2B2B24A3F36f98668Ed8F0B38D1a872f
10k USDT	0xF67721A2D8F736E75a49FdD7FAd2e31D8676542a
100k USDT	0x9AD122c22B14202B4490eDAf288FDb3C7cb3ff5E
0.1 WBTC	0x178169B423a011fff22B9e3F3abeA13414dDD0F1
1 WBTC	0x610B717796ad172B316836AC95a2ffad065CeaB4
10 WBTC	0xbB93e510BbCD0B7beb5A853875f9eC60275CF498
TORN	0x77777FeDdddFfC19Ff86DB637967013e6C6A116C

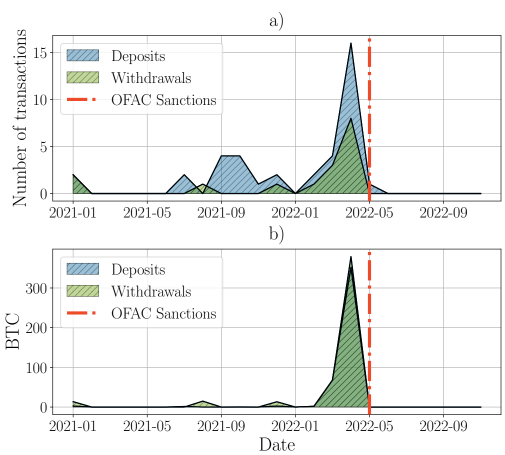

Figure 8: Interactions with the Bitcoin mixer Blender.io.

and to the sanctioned addresses of Blender.io using the addresses listed in OFAC's SDN list.

Several privacy-enhancing technologies exist on Bitcoin, such as centralized Bitcoin mixers and CoinJoin wallets [62, 77]. All were developed to prevent observers from tracing money flows through the ecosystem, enabling users to increase their on-chain privacy. In contrast to Ethereum, where shared addresses are used to obfuscate money flows, the UTXO-based Bitcoin blockchain relies on shared transactions among users. In the following, we exclusively focus on the centralized Bitcoin mixer Blender.io, since CoinJoin Wallets, such as Wasabi Wallet or Samurai Wallet, were not targeted by OFAC sanctions. Blender.io was sanctioned by OFAC in May 2022.

In Figure 8, we visualize the interactions with the sanctioned Blender.io over time. Figure 8 a) shows the number of transactions with Blender.io from January 2021 to November 15th, 2022. In Figure 8 b), we display the amount of BTC deposited and withdrawn for the same period. We observe that after OFAC's sanctions against Blender.io were imposed, there were no further interactions with the application. Shortly before the sanctioning, there was a spike in deposits and withdrawals from Blender.io. We find that 351 BTC and 379.06 BTC were deposited and withdrawn from addresses belonging to Blender.io the month before the sanctioning. Assuming an exchange rate of 35000 USD per BTC, around $10.5 million were deposited and withdrawn just before the sanctions took effect.

Figure 8 suggests that the sanctions entirely prevented Blender.io from continuing to provide its centralized services. We do not propose that this occurred due to censorship as defined in Definitions 2-4, as the likely cause is the removal of the Blender.io website.

B CENTRALIZATION & CENSORSHIP

Validators or miners may face legal, financial, or social incentives to engage in censorship, particularly in jurisdictions with strict regulatory frameworks. This suggests that while protocols may be designed to be censorship-resistant, real-world factors can lead to censorship being enforced in a cryptocurrency network. We highlight the importance of decentralization to avoid such consequences. Thus, there is a balance between geographical and jurisdictional decentralization, which requires additional protocol resilience to instances of censorship that may not be avoided due to validators being bound to certain jurisdictions. Intuitively, the censorship implications of centralization may be amplified by the separation of roles introduced by PBS, as dependent on the market's structure. For example, if proposers do not locally construct blocks and all parties rely on a single censoring relay, then censorship is total.

C STRICT VS. WEAK CENSORSHIP

Note that the notions defined in Definition 3 and Definition 2 can differ. In leader-based protocols, strict censorship may require that all leaders censor a given transaction, while the latter can be implemented by the potentially smaller set of leaders responsible for the targeted block height. With respect to the security implications of both notions, recent work highlighted that adversaries can use censorship to cheapen the cost of denial-of-service attacks [79]. For example, attackers can create computationally complex transactions with execution paths that cannot be easily foreseen and culminate with an interaction that should be censored; thus, validators that execute these transactions cannot be compensated.

D EXTENDED RELATED WORKS

Adversarial attacks similar to censorship in permissionless blockchains have been studied in the context of multi-agent systems. Ishii *et al.* [28] investigated the robustness of multi-agent systems against denial-of-service (DoS) attacks. The difference to censorship for distributed ledgers on the consensus layer is in the differing adversarial model. For DoS attacks in multi-agent systems, it is assumed that the adversary compromises the communication of honest agents for a specific duration at a determined frequency. In the case of censorship, the adversary is relatively weak, so messages broadcast by other agents are not forwarded. The paper does not establish whether both notions yield an equivalent outcome concerning the liveness of the overall system. We deem this intersection of research as an interesting area for further investigation in future work.

E IMPOSSIBILITY OF CENSORSHIP-RESILIENCE

In this section, we argue that previous results on liveness in PoS [21, 57, 60] constitute a lower bound for censorship-resilience on the consensus layer. Concretely, we prove that no PoS protocol can achieve *censorship resilience* if the number of censoring validators makes up more than 50% of the validator committee. In the following, we first introduce our model in reasoning about security in PoS blockchains. We outline recent results on *liveness* in PoS blockchains and further introduce the relationship of censorship-resilience to liveness. After introducing an intuition, we state our impossibility result in Theorem 7 and prove it through a sequence of worlds and an indistinguishability argument.

Security Model. Recall that $B_i \in \mathcal{L}$, if a block B_i is included in the distributed ledger $\mathcal{L}$, and that tx is included in $\mathcal{L}$ if $tx \in B_i \wedge B_i \in \mathcal{L}$ (cf. Section 4.2). Two views of ledgers $\mathcal{L}_1, \mathcal{L}_2$ are conflicting if they differ in their included transactions. We further assume that n is the total number of validators. In our model, transactions tx are input to validators by the environment $\mathcal{Z}$. Before the execution of the protocol starts, an adversary $\mathcal{A}$ corrupts a subset of validators $f < n$ and renders them *adversarial* such that they can arbitrarily deviate from the specified protocol. The remaining validators are *honest* and follow the protocol as specified. We assume that network communication is synchronous, hence messages are instantly delivered once they are sent by a network participant.

Safety & Liveness. To formally define liveness, we follow the holistic definition of Garay *et al.* [22], which states that all transactions originating from an honest client will eventually end up in an honest validators' view of a ledger; hence, an adversary cannot perform a DoS attack against honest clients. We formally define liveness in PoS:

Definition 5. A validator ensures *liveness* of a PoS protocol if it satisfies the following properties:

(1) **Propagation.** Upon reception of a transaction tx by an honest client C, the validator forwards tx to other peers in the network.

(2) **Inclusion.** A transaction tx sent by an honest client C is eventually included in the local view of an honest validator's distributed ledger $\mathcal{L}$.

(3) **Availability.** Upon query, an honest validator will report whether a transaction is included in the ledger.

Importantly, recent results highlight a trade-off between accountability and availability [47] and show the impossibility of liveness beyond $f > \frac{n}{2}$ adversarial validators [60].

Modeling Censorship. In a real-world environment, a validator censoring transactions may not be considered adversarial. For example, censorship may be considered beneficial from a legal perspective, as malicious actors are prevented from participating in the system. However, as first identified by Miller *et al.* [41], censorship-resilience is a property of liveness. We further argue that censorship is equivalent to a subset of adversarial actions defined in a PoS protocol. To formally define this finding, we say that $\mathcal{A}_C$ is a probabilistic polynomial time algorithm, where a subset $f_c < n$ of validators, which are corrupted by $\mathcal{A}_C$, arbitrarily deviates from the PoS protocol. For example, a censoring validator may, upon reception of a transaction tx by the environment $\mathcal{Z}$, refuse to *(i)* include tx in block B_i, *(ii)* propagate tx to peers *(iii)* build upon $\mathcal{L}$, where tx is included in $\mathcal{L}$, and by *(iv)* refusing to attest to B_i, where $tx \in B_i$. We define Δ-*censorship-resilience* as follows.

Definition 6. (Δ-Censorship-resilience) Suppose an honest client inputs tx to $(n - f_c)$ honest validators. Then, tx is committed to $\mathcal{L}$ within Δ, except with negligible probability.

Intuition. Let us consider a PoS protocol where $f_c > \frac{n}{2}$ of validator nodes are directly censoring transactions. We show that censoring impacts the liveness of a blockchain. Intuitively, censorship of a transaction prevents it from being included in the blockchain, as a censoring validator drops transactions that, e.g., involve sanctioned addresses. As such, censoring validators create a conflicting chain, which can be considered *adversarial* in the context of traditional BFT consensus protocols. To prove Theorem 1, we show that the threat to liveness posed by a validator corrupted by $\mathcal{A}$ is indistinguishable from the threat to liveness posed by a (censoring) validator corrupted by $\mathcal{A}_C$. We defer the proof of liveness to Tas *et al.* [60] and present Theorem 7.

Theorem 7. *Consider a PoS protocol* Π *with* n *validators in a synchronous network, where at least* $f_c > \frac{n}{2}$ *are corrupted by* $\mathcal{A}_C$*. Then,* Π *cannot provide censorship-resilience.*

Proof. Suppose the number of validators is $n \in \mathcal{Z}$, where we assume that n is even in each epoch. Further, consider there exists a protocol Π that supports *liveness* with $f < \frac{n}{2}$ corrupted validators that is further Δ-*censorship-resilient* with $f_c > \frac{n}{2} - f$ censoring validators. Then, there exists a decision function $\mathcal{D}$, which outputs a non-empty set of censoring validators. We prove Theorem 7 through a sequence of worlds and an indistinguishability argument.
(World 1.) Let P, Q and R partition n into three disjoint groups, where $|P| < \frac{n}{2}, |Q| > \frac{n}{2} - |P|$ and $R = n - |P| - |Q|$. Nodes in P are corrupted by $\mathcal{A}$, nodes in Q are corrupted by $\mathcal{A}_C$ and nodes in R are honest. Corrupted nodes are adversarial and do not communicate with honest nodes in R. Hence, upon input of randomly distributed transactions by $\mathcal{Z}$, validators in $P \cup Q$ output a diverging view of $\mathcal{L}$ as opposed to R. So the decision function outputs a non-empty set of adversarial validators $P \cup Q$.
(World 2.) Let P, Q and R partition n into three disjoint groups, where $|P| < \frac{n}{2}, |Q| > \frac{n}{2} - |P|$ and $R = n - |P| - |Q|$. Nodes in P are corrupted by $\mathcal{A}_C$, nodes in Q are corrupted by $\mathcal{A}$ and nodes in R are honest. Corrupted nodes are adversarial and do not communicate with honest nodes in R. Hence, upon input of randomly distributed transactions by $\mathcal{Z}$, validators in $P \cup Q$ output a diverging view of $\mathcal{L}$ as opposed to R. So the decision function outputs a non-empty set of adversarial validators $P \cup Q$.

However, worlds 1 and 2 are indistinguishable for $\mathcal{D}$. Thus, $\mathcal{D}$ cannot output a non-empty set of censoring validators.

We note that this lower bound for censorship-resilience also applies to Nakamoto consensus [22, 43].