SoK: MEV Countermeasures: Theory and Practice

Sen Yang*, Fan Zhang*, Ken Huang†, Xi Chen‡, Youwei Yang§, and Feng Zhu¶

*Department of Computer Science, Yale University
†DistributedApps
‡Stern School of Business, New York University
§Bit Mining Limited
¶Harvard Business School

Abstract—Blockchains offer strong security guarantees, but they cannot protect the ordering of transactions. Powerful players, such as miners, sequencers, and sophisticated bots, can reap significant profits by selectively including, excluding, or re-ordering user transactions. Such profits are called Miner/Maximal Extractable Value or MEV. MEV bears profound implications for blockchain security and decentralization. While numerous countermeasures have been proposed, there is no agreement on the best solution. Moreover, solutions developed in academic literature differ quite drastically from what is widely adopted by practitioners. For these reasons, this paper systematizes the knowledge of the theory and practice of MEV countermeasures. The contribution is twofold. First, we present a comprehensive taxonomy of 30 proposed MEV countermeasures, covering four different technical directions. Secondly, we empirically studied the most popular MEV-auction-based solution with rich blockchain and mempool data. We also present the Mempool Guru system, a public service system that collects, persists, and analyzes the Ethereum mempool data for research. In addition to gaining insights into MEV auction platforms' real-world operations, our study shed light on the prevalent censorship by MEV auction platforms as a result of the recent OFAC sanction, and its implication on blockchain properties.

1. Introduction

Smart contracts are autonomous programs running on top of a blockchain. They achieve strong security properties (integrity, transparency, censorship-resistance, etc) that centralized systems cannot offer and have cultivated a trillion-dollar ecosystem spanning finance products (e.g., stablecoins, lending), markets and exchanges (e.g., automated market makers), digital assets (e.g., NFTs) and more.

However, blockchains cannot protect the *ordering of transactions* [1]. The ability to manipulate transaction ordering is immense power. For instance, if Alice can execute her trades before Bob's *ex-post* (i.e., after having observed Bob's trades), she can frontrun [2] Bob and reap a profit. Daian et al. [1] coined the term Miner/Maximal Extractable Value (MEV) to denote the profits that powerful players (with miners being the most powerful) can gain (or *extract*) from selectively including, excluding, or re-ordering user transactions.

MEV bears profound implications for the security and decentralization of blockchain systems. Some MEV is at the expense of regular users (e.g., sandwich attacks), which should be prevented. Some MEV is benign (e.g., arbitrage profits provide incentives for price discovery and price synchronization cross exchanges), but uncoordinated extraction of it can cause network congestion and high transaction fees [1]. Moreover, when MEV dominates block rewards (which they already do quite often in Ethereum), blockchain consensus could be destabilized [3]. Last but not least, MEV can lead to centralization because finding sophisticated MEV opportunities require significant resources (money and talent) only big players can afford [4].

Academia and the industry have attempted countermeasures from several different directions. At the highest level of abstraction, two schools of ideas were explored: 1) to facilitate MEV extraction so that the process is efficient, decentralized and transparent [5]–[7], and 2) to stop MEV extraction by ordering transactions in a way that renders order manipulation infeasible (e.g., [8]–[10]). As readers can notice, the two directions aim to lead to different and even possibly incompatible futures. There is currently no consensus on the best countermeasures. Moreover, while the second approach is better explored by academics, it is the first approach that is widely adopted in practice thus far.

Our contribution. This paper systematizes the knowledge of MEV countermeasures, covering both academically proposed solutions and the popular choice of practitioners. Thus the contribution is twofold. First, we present a comprehensive taxonomy of recently proposed MEV countermeasures, covering four different technical directions. Second, we empirically study the most popular solutions in practice, with rich blockchain and mempool data.

A taxonomy of MEV countermeasures. We selected 30 recent projects and papers that proposed representative MEV countermeasures, from the following four categories.

I: MEV auction platforms. This class of solutions builds the facility to make MEV extraction efficient, decentralized, and transparent. We call entities who actively extract MEV as *MEV searchers*. Most MEV auction platforms guarantee

the privacy and atomicity of searchers' transactions. The former protects MEV searchers from other searchers. The latter is important for MEV extraction that involves executing multiple transactions in a particular order. Atomicity ensures that either all of the transactions are executed in the desired order or none of them is, but never partially. Two guarantees together drastically reduce the risk of MEV extraction.

II: Time-based order fairness. Fundamentally, state machine replication protocols (which blockchains realize) can be extended to enforce an extended validity property that the ordering of transactions must satisfy. Different notions of *order fairness* are defined. Kelkar et al. [8], [9] proposed receive-order fairness which requires if a majority of nodes receive T_1 before T_2, then the final blockchain should respect that order. Order linearizability [11], κ-differential order-fairness [10], timed-relative fairness [12] are related notions. Enforcing order fairness on user transactions can prevent MEV caused by *ex-post* order manipulation.

III: Content-agnostic ordering. A particular (weaker) fairness property that received a lot of attention is content-agnostic ordering, which means the order of transactions is determined independently of transaction content. The high-level idea is to have users first commit to transactions, and reveal them after the ordering has been determined. Content-agnostic ordering is weaker than receive-order fairness because it permits metadata leakage (e.g., many schemes leak the sender so that a fee can be charged to prevent DoS attacks) and content-agnostic frontrunning (e.g., when the attacker just wants to place her transaction before others). While weaker, content-agnostic ordering is popular for its simplicity and multiple implementations have been proposed [13]–[20].

IV: MEV-aware application design. So far the three classes of solutions are generic, but effective mitigation is possible for specific applications. Particularly interesting is the design of exchanges that are resistant to frontrunning and sandwich attacks by construction. For instance, one approach is batch auctions [21], [22] (initially proposed as a countermeasure to high-frequency trading) where orders are executed in batches so that the ordering within a batch does not make a difference.

In general, miners' tendency to maximize profits implies an adversary model that is stronger than the honest/malicious model and the passively rational model [23]. E.g., hashed timelock contract (HTLC) is widely used in payment channels and atomic swaps, but HTLC is only secure assuming honest miners because rational miners can be *bribed* to break the contract [24]. Bribery is explicit MEV created by attackers to induce desired behaviors of miners. In [23], [25], authors further showed MEV-extracting miners themselves can mount bribery attacks or collude with other participants to break the countermeasure in [24], and proposed countermeasures.

In Section 3, we deep dive into the technical details of each proposed scheme and compare their goals, technical solutions, and trust assumptions. Then, we discuss how each category of ideas approaches the MEV problem and note that not all of them addressed all aspects of it.

Empirical study on MEV auction platforms. Among the four categories above, MEV auction platforms are the most popular MEV countermeasure in practice. At the time of writing, more than 90% of Ethereum blocks are produced by MEV auction platforms. While the working of MEV auction platforms is not complex, their real-world operation is not well understood. In Section 4, we use rich blockchain and mempool data to empirically understand the ecosystem of MEV auction platforms.

Our empirical study aims to first understand the basic structure of the MEV auction platform ecosystem (e.g., what are the market shares of various MEV auction platforms in terms of searcher usage and miner participation?). Further, we ask if MEV auction platforms always uphold the privacy and atomicity promises. Finally, we want to understand a unique aspect of current MEV auction platforms, namely their roles in enforcing regulations. Recently, the Office of Foreign Assets Control (OFAC) of the US Treasury Department placed a sanction against Torando Cash [26]. To be OFAC compliant, several MEV auction platforms refuse to process blocks containing transactions interacting with sanctioned addresses, effectively censoring them. MEV auction platforms' involvement in enforcing US government regulation provoked heated discussion. While the legal discussion is out of the scope of this paper, we want to understand, from a technological point of view, to what extent are MEV auction platforms enforcing regulations, and the measurable implications of implementing a sanction on a blockchain.

Our study reveals interesting findings. For example, we find that MEV auction platforms do not always uphold privacy guarantees, and even supposedly private transactions fall victim to MEV attacks. This may be due to uncle blocks [27], which highlights a tension between full privacy and short confirmation time (which is also relevant in content-agnostic ordering protocols). Moreover, MEV auction platforms that claim to be compliant with OFAC regulation in fact are not strictly compliant, the evidence of which is publicly available on-chain (Section 4.2.3). We also quantify the sanction's implication on user transactions. Since not all MEV auction platforms are enforcing the sanction, it is not likely to cause transactions to be excluded. Rather, sanctioned transactions will incur a longer confirmation latency (or *waiting time* [28]). Using the mempool data we collected with a distributed system, we measure that sanctioned transactions on average wait for about 68% longer than regular transactions before they can be included in a block.

Roadmap. In Section 2, we review the common types of MEV and the security implications. In Section 3, we present the taxonomy of 30 proposed MEV countermeasures and the comparison of them. In Section 4, we report on an empirical study of the MEV auction platform ecosystem. In Section 5, we discuss related works. Finally, we end the paper with a discussion on the legal aspects of MEV and future research

directions.

2. Background: MEV and its security implications

2.1. MEV

The term Miner/Maximal Extractable Value was first introduced by Daian et al. [1] to refer to the value that can be extracted by a miner from manipulating the order of transactions, as an upper bound on the extractable value. In practice, MEV extracting is a growing and lucrative industry. Purpose-built *searchers* monitor pending transactions for *victims* and craft MEV extraction transactions. Crucial to the success of MEV extraction is the searcher's ability to ensure proper ordering of her transactions relative to the victim. This can be done by setting appropriate fees or through one of the MEV auction platforms (which we discuss in depth in Section 3 and Section 4).

While being a relatively new topic, there is already substantial literature on understanding, quantifying, and mitigating MEVs [23], [29]–[38]. We will defer a systematic review of MEV countermeasures to Section 3. Below we briefly review common MEV sources and their security implications.

2.1.1. Common types of MEV in finance applications.
MEV may arise in various finance applications, but essentially, extracting MEV involves precisely placing MEV-extracting transactions before, after, or around the victim.

Frontrunning. Two common forms of frontrunning attacks are observed in practice. The first form involves paying high transaction fees so that the attacker's transaction is executed before anyone else, to, e.g., take a rare market opportunity. For example, an NFT named CryptoPunk 3860 was mistakenly listed for sale at an unusually low price. The frontrunner snatched up this valuable NFT [1] by paying 22 ETH to the miner[2].

The other form of frontrunning attack involves placing the attacker's transactions right before the victim, usually in conjunction with a subsequent backrunning to form a sandwich attack as we will discuss shortly.

Backrunning. Backrunning involves placing the attacker's transaction immediately after the victim, to profit from the market dynamic created by the victim before others.

For example, when a transaction significantly (say) increases the price of a given asset in some exchange X, it creates an arbitrage opportunity. A backrunner can buy from another exchange X' at a lower price and sell back to X, pocketing the difference. Note that in this case the backrunning transaction does not inflict any loss on the user, and it helps synchronize the prices between X and X'.

In the same vein, another example is to backrun oracle updates to take liquidation opportunities. We refer readers to [39] for an empirical study on liquidation.

---

1. 0xb40fd0c9a2ba2d1d5e7ee5e322f9afc5e2ec1b7e2d520b638ea83dcc9c850d02
2. 0xbc2cb18d0e58418d8d9c948cab319460bd409d7bd5f2978f3e52e445b351c522

Sandwich attacks. In a sandwich attack, an MEV searcher places a pair of transactions right before and after the victim's regular trade. The purpose of forming a sandwich is to manipulate asset prices so that the attacker benefits from the victim's loss [29].

From the attacker's point of view, mounting sandwich attacks can be risky because if the order of the three transactions is not exactly as desired, the attacker may lose money. In practice, most sandwich attacks happen through MEV auction platforms (jumping ahead, see Table 4).

2.1.2. Bribery attacks.
Attackers can create MEV explicitly to incentivize miners to take action in the interest of the attackers, in so-called *bribery* attacks. For example, a miner can be bribed to temporarily censor a transaction if the attacker sends a conflicting transaction with a higher fee [24], [40]. More sophisticated bribery attacks can be facilitated by smart contracts. The implications of bribery attacks are application-specific. In the context of payment channels and atomic swaps [23], bribery attacks are detrimental.

2.2. Security implications

2.2.1. User loss.
Some MEV extraction directly causes users to lose money. For example, predatory sandwich attackers made a profit of more than $3 million in November 2022 alone [41], at the expense of victims.

2.2.2. Inefficiency due to the lack of coordination.
Originally observed in [1], bots competing for MEV engage in on-chain bidding wars which can cause network congestion and increase transaction fees. Some MEV countermeasures can cause different forms of inefficiency. E.g., with first-come-first-served ordering, competition among MEV searchers becomes off-chain latency wars.

2.2.3. Destabilizing consensus.
Carlsten et al. [3] first showed that when transaction fees dominate block rewards, miners may deviate from honest mining and fork out high-fee blocks to attract other miners to build on the fork. MEV can be viewed as a generalized form of transaction fees paid to the miner. Having significant MEV thus exacerbates the issue. In fact, lucrative MEV extraction already dominates block rewards today [38]. Daian et al. [1] also described another attack vector exploiting MEV called Time-bandit attacks, which essentially augments reorg/51% attacks with subsidy from MEV.

2.2.4. A centralizing force.
Among many, Vitalik argued that MEV can cause centralization because there is a significant economy of scales in finding sophisticated MEV extraction opportunities [4]. We want to avoid a centralized and monopolized future because it harms transparency and decentralization. Another worry is that MEV can encourage "vertical integration" [42] of miners and traders to form closed-door systems that harm the transparency and permissionlessness of the blockchain.
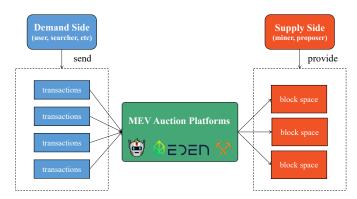
3

Figure 1: Schematic Diagram of MEV auction platforms

3. MEV Countermeasures

Recall that we defined four classes of MEV countermeasures in Section 1. In this section, we first present a taxonomy of 30 proposed schemes from the four categories in Table 1. Then, we compare how different classes of solutions address each aspect of the MEV problem as defined in Section 2.2.

3.1. MEV Auction Platforms

The core functionality of an MEV auction platform is to facilitate MEV auctions that allocate block space (sold by miners) to users (who place bids for getting their transactions included), hence the name. Figure 1 illustrates the idea. From a security standpoint, MEV auction platforms typically guarantee two key properties: transaction privacy (from anyone but the trusted parties) and atomicity (either the entire bundle is included in a block or none is, and the user pays only if the bundle is included).

Users of MEV auction platforms can be MEV searchers and regular users. Searchers use MEV auction platforms to realize their MEV-extract transactions without disclosing the transactions to other searchers and miners (otherwise they run the risk of getting frontrun by other searchers or miners). Regular users may use MEV auction platforms to hide their valuable transactions from searchers.

The recent Ethereum merge changed how MEV auction platforms are implemented, so we discuss their designs separately.

3.1.1. Pre-Merge MEV auction platforms. As the first MEV auction platform, Flashbots [43] developed a first-price sealed-bid auction mechanism between users and miners, with the Flashbots relay as the trusted auctioneer.

A typical workflow is for users to submit a set of pre-ordered transactions (referred to as *bundles*) to the Flashboys relay, specifying a promised payment. Then, the relay propagates user bundles to participating miners in direct channels. Miner picks the most profitable bundles to include in their blocks. The relay is trusted by both users and miners: users trust the relay to keep their transactions private and not

extract MEV from them; miners trust the relay to not steal profits.

Eden Network [44] is a similar MEV auction platform with a few key differences. Ethermine uses the same auction architecture as Flashbots Auction and accepts bundles compatible with a version of Flashbots. Ethermine claims [45] it allows users to submit bundles faster than going through the Flashbots relay, by providing a direct channel to their mining nodes.

3.1.2. Post-Merge MEV auction platforms. In future versions of Ethereum, MEV auctions will see native support in the form of in-protocol Proposer-Builder Separation (PBS) [56]. In-protocol PBS will change the Ethereum protocol so that block building and block proposing are done by different roles (in the proof-of-work version miners do both). The major benefit of PBS is that it opens up the competition for MEV extraction to parties other than miners.

Before in-protocol PBS is implemented, MEV-Boost [6] is an intermediate realization of PBS. The shortcoming is that MEV-Boost still relies on trusted relays, though there are multiple of them now and in principle, anyone can become a relay.

In MEV-Boost, a builder assembles blocks with transactions it receives from users, the public mempool, as well as the ones it inserts to extract MEV. Assembled blocks are submitted to one or more relays, with promised payments to block proposers (previously known as miners). A relay propagates received blocks to listening proposers, who finally pick the most profitable one to propose. In this process, the relay and the proposer execute a commit-then-reveal protocol so that the proposer's decision only relies on the bids and other metadata associated with a built block. not the block content. Users pick a builder to use (or become a builder) and fully trust it, including the relay it chooses.

Among previously mentioned MEV auction platforms, Flashbots and Eden now run both builders and relays, and Ethermine exits the market. New entities, such as BloXroute, joined the ecosystem as builders and relays.

3.1.3. Private channels. For users who only want to ensure the privacy of their transactions but not the ordering, most MEV auction platforms provide a service called *private channels*. This service can be accessed via PRC endpoints, which enjoys ease of use because users can add RPC endpoints to their wallets using existing software. Examples include Flashbots Protect [46], Ethermine RPC [45] (which stopped operation after the merge [57]), Eden Network PRC [47], and bloXroute Fast Protect [48]. Currently, the service is fully trusted for privacy.

3.1.4. MEV redistribution. The idea of MEV redistribution aims to foster a more equitable distribution of MEV, granting users the ability to capture the MEV created by their own transactions. To attain kickback, users first submit transactions to an intermediate service provided by MEV auction platforms and selectively disclose transaction information to searchers. Searchers then propose transactions for bundling

TABLE 1: Comparison of specific systems/schemes to solve the problems caused by MEV, in four categories: **I: MEV auction platforms, II: Time-based ordering properties, III: Content-agnostic ordering, and IV: MEV-aware application design**.

Projects/Papers	Goal and summary of the solution	Trusted parties and assumptions
I: MEV auction platforms		
Flashbots [43], Eden Network [44], Ethermine [45] (prior MEV-Boost)	Flashbots aims to make MEV extraction easy and efficient by: 1) allowing users to specify preferred ordering and only pay if the specified ordering is satisfied, 2) Protecting the privacy of user transactions (from anyone but the trusted relay) until included on-chain, and 3) Running block space auction off-chain.	A single relay is trusted for privacy and respecting user-specified ordering.
MEV-Boost [6]	The goal is the same as above. The solution is similar but the centralized relay is replaced by multiple relays and builders.	Users choose a builder and fully trust it (including the relay it uses).
Flashbots Protect [46], Ethermine RPC [45], Eden Network PRC [47], bloXroute Fast Protect [48]	To protect the privacy of user transactions (from anyone but the service itself) until included on-chain.	The service is fully trusted for privacy.
MEV Share [49], Back-RunMe [50]	Empower users to capture MEV from their transactions via a service that matches user transactions and searcher bundles using selectively disclosed information from users.	The service is fully trusted for privacy and transaction matching.
II: Enforcing ordering properties (Notation: suppose the committee has n nodes and up to f are malicious)		
Aequitas [8]	block-receive-order fairness: if at least $n\gamma$ nodes receive T before T' for some $\frac{1}{2} < \gamma$, then T should be ordered no later than T'.	$n \geq \frac{2f+1}{2\gamma-1}$ (sync) or $n \geq \frac{4f+1}{2\gamma-1}$ (async)
Themis [9]	Same as above	$n \geq \frac{4f+1}{2\gamma-1}$
Pompē [11]	Ordering linearizability: if the highest timestamp of T from all correct nodes is lower than the lowest timestamp of T' from all correct nodes, then T is ordered before T'.	$n \geq 3f+1$
Quick-Fairness [10]	κ-differential order-fairness: if the number of correct nodes who broadcast T before T' exceeds the number of nodes who broadcast T' before T by more than $2f + \kappa$, then T' cannot be delivered before T for some $\kappa \geq 0$.	$n \geq 3f + \kappa + 1$
Hashgraph [51]	Fair transaction order based on the timestamps: the fair timestamp of T is the median of the times that each node claims it first received it.	$n \geq 3f+1$
Wendy [12]	Timed-relative fairness: if there is a time t such that all honest nodes saw (according to their local clock) T before time t and T' after time t, then T is scheduled before T'.	$n \geq 3f+1$
III: Content-agnostic ordering		
TEX [13]	Users encrypt transactions using timelock puzzles. Timelock puzzles ensure that all transactions are revealed. A similar idea is mentioned in Veedo [14].	The attacker cannot solve timelock puzzles much faster than honest users.
Tesseract [15]	Users encrypt transactions using keys generated in TEEs.	Integrity and confidentiality of TEEs
F3B [16]	Users encrypt their transactions and store the associated secret key with the secret-management committee of n trustees.	$n \geq 2f + 1$ for the secret-management committee
Sikka [17], Osmosis [18], Shutter Network [19]	Users threshold-encrypted transactions under a key generated by a committee of n nodes. Ciphertexts are ordered using a certain policy, after which the committee threshold-decrypt and executes the transactions.	Typically $n \geq 3f+1$
Fino [20]	Fino efficiently integrates threshold encryption and secret sharing to DAG-based BFT protocol.	Less than f malicious nodes where $n \geq 3f+1$ (n is the number of all nodes.)
IV: MEV-aware application design		
CoWSwap [52]	Execute transactions in frequent batch auctions. Settlement is outsourced to solvers who compete to provide the best settlement surplus.	We omit application-specific trust assumptions unless they are unique to MEV protection.
FairTraDEX [22]	Frequent batch auctions realized with zero-knowledge proofs and value commitment.	-
A^2MM [53]	Atomically route user trades across AMMs to avoid sandwich and arbitrage opportunities.	-
P2DEX [54]	Order matching using secure multiparty computation (MPC).	-
Optimal slippage for eliminating sandwich [55]	Algorithmically set the slippage to balance the cost of transaction failure and that of MEV attacks.	-
He-HTLC [23] and Rapidash [25]	Hashed Time-Lock Contract (HTLCs) schemes that are secure against MEV-extracting miners. Setting incentives properly so that miners are incentivized to penalize deviating players, yet not to deviate by themselves.	-

with user transactions through the intermediate service. The service will optimize MEV by matching user transactions with searcher bundles, allowing users to receive a return of the MEV. Examples include MEV Share [49] and BloXroute BackRunMe [50]. Presently, the service is fully trusted for privacy and transaction matching.

3.2. Time-based ordering properties

Drastically different from MEV auction platforms, the second category of solutions in Table 1 prevents order manipulation by clearly defining the properties that transaction ordering must satisfy. A number of papers explore the notion of time-based ordering properties, which we review below. In the next section, we review a weaker ordering property called content-agnostic ordering.

3.2.1. Receive-order fairness. Receive-order fairness is first proposed by Kelkar et al. in [8]. Basically, receive-order fairness captures the intuition of first-come-first-served ordering: if at least γ-fraction nodes receive a transaction T before another transaction T', then T should be ordered no later than T'. Themis [9] achieves the same fairness as Aequitas [8], but with stronger liveness and less communication complexity. κ-differential-order-fairness achieved by Quick-Fairness [10] can also be treated as a reparameterization of batch-order-fairness as claimed in [9]. Table 1 presents the technical definitions more precisely.

Chainlink Fair Sequencing Service (FSS) [58] plans to use a receive-order fairness protocol such as Aequitas [8].

Trust assumptions. Above protocols assume a committee of n nodes with up to f of them malicious. Aequitas requires $n \geq \frac{2f+1}{2\gamma-1}$ in the synchronous setting and $n \geq \frac{4f+1}{2\gamma-1}$ in the asynchronous setting. Themis requires $n \geq \frac{4f+1}{2\gamma-1}$ and Quick-Fairness requires $n \geq 3f + \kappa + 1$.

3.2.2. Relative fairness. Receive-order fairness is defined with respect to the relative ordering of transactions. Another set of fairness definitions involves using absolute time.

Wendy [12] (also known as Vega [59]) proposes relative fairness: if there is a time t such that all honest validators saw transaction T before t and another transaction T' after t, then T must be scheduled before T'. Pompē [11] proposes a similar notion called ordering-linearizability Indeed, [9] show that both definitions can be consolidated into a single property called fair separability.

A key difference is that Pompē relaxes the requirement so that the definition is only required if both transactions are output. In other words, it is acceptable if T' is output and T is not, even if all honest parties receive T before T'. While this relaxation achieves better liveness (T' cannot be held by T in case of network congestion), it also permits censorship.

Hashgraph [51] assigns every transaction a fair timestamp, which is the median of the time each node claims to have first received it. However, [8] gave an attack showing that median-time-based ordering is subjective to adversary manipulation by a single attacker.

Trust assumptions. Similar to receive-order fairness protocols, Wendy, Pompē, and Hashgraph all require a committee of $n \geq 3f + 1$ nodes.

3.3. Content-agnostic ordering

Content-agnostic ordering (also known as blind-order-fairness [34] and casual ordering [60]) is somewhat of a catch-all term because it does not correspond to a specific way of determining the ordering, as long as it is determined independent of transaction content. In practice, content-agnostic ordering is commonly realized with a commit-and-reveal protocol. Instead of sending transactions in plaintext, users send commitments along with some metadata (e.g., the transaction fee). The miner determines an ordering based on the commitments (by hiding, they do not leak information about the transaction content), then the protocol opens the commitment, and the transactions are executed.

The commit-and-reveal step can be instantiated with different primitives, such as threshold encryption, timelock encryption, and trusted execution environments (TEEs), etc.

3.3.1. Threshold encryption. The general setup is a key management committee of n nodes with an honest majority (or super-majority). Users encrypt transactions under the public key of the committee, which determines the ordering of user transactions in a protocol-specific way. Then the committee threshold-decrypts the transactions and executes them.

Sikka [17], Osmosis [18], and Shutter Network [19] are systems that integrate threshold encryption to Ethereum (and potentially other blockchains). Meanwhile, Fino [20] proposes a way to efficiently integrate threshold encryption and secret sharing with DAG-based BFT protocol. F3B [16] uses a secret-management committee to store encryption keys so that when the transaction has been committed by the underlying consensus layer, its content will be later revealed by a decentralized secret-management committee.

We use (a simplified description of) Shutter Network [19] to illustrate the end-to-end transaction flow. In Shutter Network, a group of nodes (called keypers) infrequently executes a distributed key generation (DKG) protocol to generate the main public key with the corresponding secret key secret-shared across keypers. To send a transaction T, the user first obtains the main public key, picks a future epoch e when the transaction will be decrypted, derives the epoch-e public key PK_e, and encrypts T under PK_e. The ciphertext C is sent to a smart contract for ordering. When epoch e arrives, keypers derive the epoch-e secret key and decrypt C off-chain and send the plaintext to an execution smart contract for execution.

Trust assumptions. Using threshold cryptography assumes that a threshold of nodes is honest.

3.3.2. Time-lock encryption. Another option to hide the content of transactions is using timelock encryption, which allows decrypting a message once a certain time has passed.

TEX [13], a front-running resilient exchange, uses time-lock puzzles to automatically decrypt transactions in case users fail to open the commitment. A similar idea also appears in Veedo documents [14].

Trust assumptions. In order to use time-lock in commit-and-reveal schemes, we need to assume that 1) one can set the time-lock parameters relatively accurately so that reveal happens roughly at the desired time, and that 2) the attacker cannot solve time-lock puzzles much faster than honest users.

3.3.3. Trusted Execution Environments (TEEs).
TEEs are hardware-protected isolated execution environments. TEE protects the confidentiality and integrity of the data and program inside. The state-of-the-art implementation is Intel SGX [61], and upcoming (and potentially better) implementations include Keystone [62], and Nvidia H100 GPU [63]. TEEs also support remote attestations so that a remote user can obtain hardware-generated proofs of the code running inside.

At a high level, TEEs can take the role of key management committees in the above solutions, by generating a pair of keys inside a TEE and publishing the public key. TEE can be programmed so that it releases the decryption key for epoch e only if the ordering of epoch e has been committed to. However, a caveat is that TEEs do not guarantee availability. Care must be taken to ensure the liveness of TEE-based protocols.

Tesseract [15] is a real-time cryptocurrency exchange built on TEEs. Tesseract relies on TEE and TLS to form secure channels between users and the exchange, so user transactions are hidden from frontrunners. Although Tesseract is an off-chain exchange, the idea can be generalized to implement content-agnostic ordering for smart contracts.

Trust assumptions. TEE implementation achieves confidentiality and integrity.

3.4. MEV-aware application design

In this section, we review application-level mitigation. We focus on decentralized exchanges (DEX) because they are currently a significant source of MEV opportunities.

Batch auction. Frequent Batch Auctions (FBAs) [21] was proposed as a response to high-frequency trading arm races. The idea essentially is to batch execution trades in discrete time intervals. Trades in the same batch are executed at the same price, thus eliminating the advantage of manipulating the ordering within a batch.

Although proposed for traditional markets, FBAs have been applied to DEX as well. CowSwap [52] and FairTraDEX [22] are two examples. One idea new in CowSwap is they outsource the task of settling a batch to third-party solvers, who compete for submitting the best settlement that optimizes trade surplus, avoiding the reliance on a trusted third party required in the initial FBA mechanism. FairTraDEX uses cryptography (zero-knowledge protocols in particular) and incentives to perform the settlement.

Publicly verifiable multi-party computation. P2DEX [54] proposes a decentralized exchange construction using publicly verifiable multi-party computation where orders are matched privately via MPC servers, and misbehavior can be identified by publicly verifiable proofs and punished.

Atomic routing. As previous work shows that sandwich attacks are not profitable if the victim's input amount remains below the minimum profitable victim input (MVI) [29], by combining multiple AMMs, A^2MM [53] can aggregate the MVI thresholds among the underlying liquidity pools to reduce the risks of sandwich attacks. Moreover, atomic routing can reduce price disparity among AMMs (in a way, the arbitrage surplus is given back to the user) and thus the overhead caused by backrunning flooding as a result of the competition to extract arbitrage.

Optimal slippage setting. To use AMMs, users set a slippage to tolerate unexpected price movements. Using a low slippage run the risk of transaction failures, but setting a high slippage attracts attackers to reap the difference between the slippage and the actual price (e.g., through sandwich attacks). [55] proposes an algorithm to calculate the optimal slippage that balances the cost of transaction failures and sandwich attacks.

3.5. Comparison of different approaches

In Section 2, we defined four problems that MEV may cause. Table 2 summarizes how different approaches address each problem. In the interest of space, we will refer readers to the self-explanatory table.

4. An Empirical Study on MEV Auction Platforms

Practical implementation of MEV auction platforms changed significantly with the Merge [57] (i.e., Ethereum's transition to the Proof-of-Work based consensus protocol), but MEV auction platforms remain the de facto most popular MEV mitigation in both eras. Prior to Merge, the largest MEV auction platform, Flashbots, is adopted by more than 99.9% of Ethereum hashrate [64]. Post merge, more than 90% of blocks are produced by MEV-Boost [65].

Our study covers both the pre-Merge MEV auction platform ecosystem (Flashbots, Eden Network, Ethermine, etc) in Section 4.1, and the MEV-Boost ecosystem post-Merge in Section 4.2.

4.1. MEV auction platforms before Merge

As introduced in Section 3, the basic functionality of a MEV auction platform is to allow users (MEV searchers and regular users) to buy block space from miners (also known as block proposers in PoS Ethereum) in an efficient and trustworthy way. In other words, a MEV auction platform can be viewed as a two-sided marketplace, with the miners supplying block space and the users demanding it. In this section, we are interested in understanding the dynamics

TABLE 2: Comparison of different approaches to the problems caused by MEV.

	Preventing user loss	Reducing inefficiency due to lack of coordination	Reducing consensus destabilizing risks	Reducing centralization
MEV auction platforms	Yes and No. Users can use MEV auction platforms for self-protection, but attackers can also use MEV auction platforms to attack.	Yes. Off-chain auctions can reduce network congestion caused by PGA.	No. MEV is still present in blocks.	Facilitating MEV extraction so non-miners can extract MEV too
Time-based ordering properties	Yes. Ex-post order manipulation is prevented.	Mostly. It will obsolete on-chain bidding war but some inefficiency may be lost to off-chain latency war.	Yes.	It removes the ordering privilege from miners but it introduces a permissioned committee.
Content-agnostic ordering	Mostly, but metadata leakage blind frontrunning is possible.	Mostly, but it depends on the ordering mechanism. If transactions are ordered by fees, then on-chain bidding wars are possible amongst blind front-runners.	Yes.	It removes the ordering privilege from miners, but protocol-specific trust assumptions may reduce the degree of decentralization of the blockchain
MEV-aware application design	Yes, for specific applications.	Yes, since MEV is eliminated for the given application.	Yes.	Partially, as it removes the ordering privilege from miners for specific applications.

of such markets, in particular, with the following research questions.

- What is the market share of various MEV auction platforms both in terms of usage and in terms of miner participation?
- Who uses MEV auction platforms and why?
- Do MEV auction platforms always uphold privacy and atomicity guarantees?

Approach. Our main vantage point to understanding MEV auction platforms is *the flows of private transactions*. We trace the path through which transactions land in the blockchain without appearing in the public mempool, to understand the interaction between users (the demand side) and the miners (the supply side), as well as the intermediate MEV auction platforms.

The first task is to identify private transactions and trace their flow. Below we detail the data collection process.

4.1.1. Data collection. As summarized in Table 3, our dataset consists of several parts: general blockchain information, private transactions (identified by our modified Ethereum nodes), transactions released by Flashbots and Eden Network, MEV labels as well as Etherscan label. Our data covers the block range between 15,253,306 and 15,537,393 (roughly Aug 1st, 2022 to Sept 15th, 2022).

General information. We collected block and transaction information from standard Web3 APIs.

Pending transactions. We built the Mempool Guru (https://mempool.guru/) system to collect and persist pending transactions as they enter the mempool. Mempool Guru is a modular system consisting of full Ethereum nodes across the globe that record pending transactions as they enter the mempool. Mempool Guru also polls pending transactions from managed RPC nodes from Infura and QuickNode. We identify private transactions by calculating the set difference

TABLE 3: MEV auction platform Ecosystem Dataset

Data Type	Sub-Type	Count
General Information	Blocks	284,088
	Transactions	50,217,035
User Tranactions	Private Transactions	1,222,057
	Flashbots Transactions	1,185,957
	Flashbots Protect Transactions	200,053
	Eden Network Transactions	16,416
MEV Activities	Sandwich	68,517
	Arbitrage	215,703
	Liquidation	1,378
Labels	Miner Labels	127
	MEV Bot Labels	279

between on-chain transactions and pending transactions observed by Mempool Guru. For periods of time in which our system is down (from block 15413796 to 15414005), we use private transaction labels from Zeromev [66] as a supplement.

Flashbots transactions. User transactions submitted to Flashbots are released through public APIs [67], from which we obtained 1,185,957 transaction hashes included in the block range of our study. We also query the private transaction status API [46] to get the list of 200,053 transaction hashes submitted to Flashbots Protect RPC.

Eden network transactions. Eden Network does not fully release user transactions as Flashbots, but by scraping the Eden Network Explorer [68], we managed to download all transactions submitted to Eden RPC in the block range of our study.

MEV labels. We use data from EigenPhi [69] to identify MEV activities[3]. During the block range of our study, we

---

3. queried on Dec 6th, 2022

identify 205,551 sandwich transactions (i.e., 68,517 sandwiches), 215,703 arbitrage transactions, and 1,378 liquidation transactions.

Etherscan labels. To identify different entities, we obtain miner and MEV Bot addresses and their related labels from Etherscan [70]. For entities without a label, we use their addresses as identifiers.

4.1.2. Tracing private transaction flow. Identifying which MEV auction platforms a given private transaction was submitted to is not obvious, because MEV auction platforms (other than Flashbots) do not release such data in full. With partial data that is available, we attribute private transactions to MEV auction platforms as follows. First, since Flashbots publishes all transactions it received, we can accurately attribute a private transaction to Flashbots. Eden network publishes a subset of transactions they receive, which allows us to attribute some transactions to Eden. For transactions we cannot attribute thus far, we try to attribute them to a MEV auction platform by the miner identity. If a given private transaction is not sent through Flashbots or Eden but is mined by Ethermine, then we mark it as "probably Ethermine", meaning it is highly likely that the transaction was sent to Ethermine RPC in private. Finally, for each private transaction still cannot be classified, if it is mined by a participant in the Eden Network, we mark it as "probably Eden Network", which means it is likely sent to the Eden MEV auction platform in private, but it might also be possible that the transaction was sent to *miners* in private. Otherwise, we consider it belongs to an unknown MEV auction platform. We exclude miner payout transactions using unknown platforms because they are most likely inserted by the miner itself.

Figure 2 plots the private transaction flows. Each transaction starts from the sender of the private transaction from the left (identified by public keys or labels if known), goes to one of the five possible MEV auction platforms (including unknown and uncertain), and finally ends at a miner on the right. The Sankey graph provides a panoramic view of the MEV auction platform ecosystem and we make several observations.

Market shares of MEV auction platforms. As shown in Figure 2, Flashbots is the most popular MEV auction platform in the period of our study, both in terms of usage (63.53% private transactions are sent to Flashbots) and miner participation (56.28% of hash power participates in Flashbots). At the same time, quite a few transactions (22.37%) are sent through unknown MEV auction platforms. Despite the dominance of Flashbots, we note that users do leverage the diversity of MEV auction platforms. More than 17.6% of MEV auction platform users (including searchers and regular users) made use of more than two platforms.

For the market share of miners, Ethermine sold the most block spaces compared to other miners through Ethermine and Flashbots. We note that there are many miners selling their block space through multiple MEV auction platforms, such as Hiveon Pool and F2Pool Old. This reveals that miners are strategic and optimize for profits. Also, MEV auction

TABLE 4: MEV activities in private transactions versus the public mempool.

MEV Type	Private # (%)	Public # (%)	ALL # (%)
Sandwich attacks	64,433 (94.04)	4,084 (5.96)	68,517 (100.00)
Arbitrage	154,758 (71.75)	60,945 (28.25)	215,703 (100.00)
Liquidation	1,150 (83.45)	228 (16.55)	1,378 (100.00)

platforms make it easy for miners to interoperate potentially as a means to attract miner participation. For example, Eden Network allows miners to accept bundles from the Flashbots relay and include them in blocks. We can find that some Eden miners, such as `2Miners: PPLNS` and `Cruxpool`, sell block spaces through both Eden Network and Flashbots. Besides, a significant part of private transactions is sent through an unknown platform, which means miners may run "underground" MEV auction platforms. [64] made a similar observation and found two miners, Flexpool and F2Pool, participate in unidentified private MEV auction platforms besides Flashbots.

Reasons to use MEV auction platforms. We can use the flow of private transactions to understand who uses MEV auction platforms and why. Looking at the left side of Fig. 2, a significant portion (45.61%) of private transactions whose senders are miners and MEV searchers, which is in line with findings in the previous work [71], [72]: In addition to protecting transaction privacy and preventing frontrunning attacks, MEV auction platforms are also used for MEV extraction and redistribution of mining revenue.

To investigate how searchers use MEV auction platforms for MEV activities, we calculate the intersection between the set of private transactions and the set of MEV transactions. Table 4 shows the number of MEV extraction activities that happened through MEV auction platforms (column Private) and through public mempool (column Public). It is not surprising that MEV searchers prefer MEV auction platforms over the public mempool, thanks to the privacy and atomicity guarantees. More than 71% of arbitrage transactions and 83% of liquidation transactions are made with MEV auction platforms. For sandwich attacks, the percentage of using private transactions (both the frontrunning and backrunning transactions are private) is 94.04%, which is in line with previous work [64] that only 5.6% of sandwich attacks were carried out using the public mempool. A significantly higher percentage of sandwich attacks is conceivable: sandwich attacks require atomicity, so using a MEV auction platform is particularly important.

Self-protection. Regular users and developers may use a private channel service offered by MEV auction platforms for self-protection against frontrunning attacks. Flashbots Protect is a private channel (defined in Section 3.1.3) for that purpose. We can find that 13.39% of private transactions flow to Flashbots Protect. Although it is possible that some searchers may also use Flashbots Protect instead of the more powerful Flashbots Auction, it is conceivable that some of the transactions come from regular users. This finding shows that MEV auction platforms are not exclusively used by
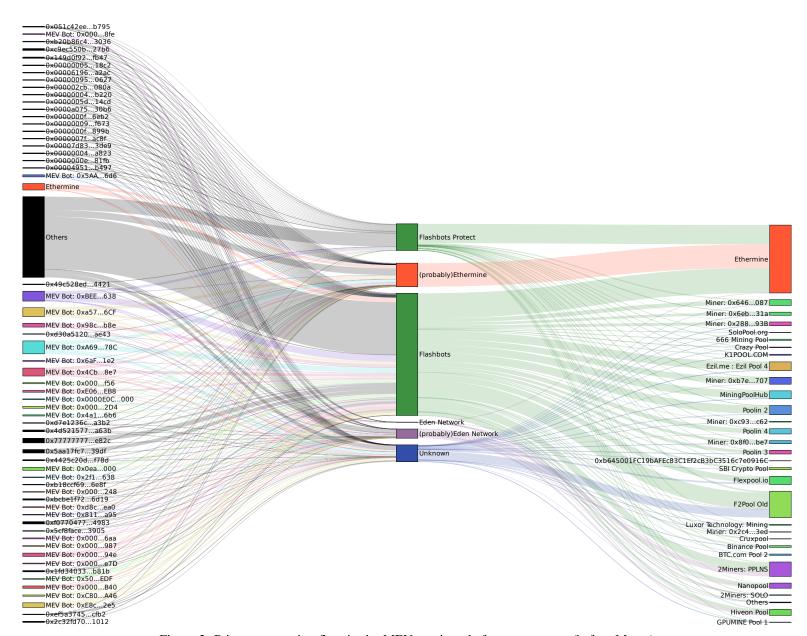
Figure 2: Private transaction flow in the MEV auction platform ecosystem (before Merge)

searchers to perform MEV extraction. Regular users also leverage it to protect transaction privacy.

Do MEV auction platforms uphold their promises? All MEV auction platforms promise that user transactions sent to their services will be private from MEV bots lurking in the public mempool. However, we observe 8 sandwich attacks whose victim transaction is a private transaction, the complete list of them is in Table 5.

We take one victim transaction [4] as an example. The searcher swapped 350,000 USDC for 197.59 Ether and paid 0.2856 ETH as the tip to the miner in this transaction. However, another searcher captured this private transac-

tion, packed it between a frontrunning transaction [5] and the backrunning transaction [6], and earned 52 USDC from this sandwich attack.

One explanation for this leakage is uncle bandit attacks [27] since transactions in uncle blocks (including private transactions) will be re-broadcast to the public mempool as the block is forked out. While MEV auction platforms generally warn users of the risks of uncle blocks, this finding highlights a tension between full privacy and quick confirmation. Although [72] observed private leakage as well, they did not identify specific attacks. Also, since they

---

4. 0xdd6e4a7ab7b2c6ad5cc7aad171ee3d601a9e6cce45a355d2baa3bca65b29e156

5. 0xbbac6ef9ff32b3a2bc4ac5faa4fceaf28187f60c73155c559c106784e6dc08b5

6. 0x5f869f0a9d92d4a8c7cd7e5d8966d3a4429a22fd6a35e200a860a2433cb0033a

use Etherscan "private transaction" labels to identify private transactions, the leakage may be due to mislabelling. See appendix for an example Fig. 6a where Etherscan mislabels the public victim of sandwich attacks as private; at one point Etherscan labels all Flashbots bundles as private. The error has been later corrected.

The other possibility for private transaction leakage is simply the malice or incompetency of MEV auction platforms. After all, there are no technical means to verify. This is particularly conceivable for small MEV auction platforms which do not have a strong reputation. In the list, two private transactions were not sent through any public MEV auction platform known to us, which suggests there exist some non-public MEV auction platforms.

4.2. MEV auction platforms post Merge

As discussed in Section 3.1.2, MEV-Boost is an implementation of PBS by Flashbots, acting as a sidecar for the PoS node which outsources block-building to a network of builders.

At the time of writing, more than 90% of Ethereum blocks are produced by MEV-Boost [65]. As of November 2022, there are eight public relays in the MEV-Boost ecosystem as summarized in Table 7. Relays adhere to the MEV-Boost Relay API specification and provide the same endpoint where block builders can submit their blocks and proposers can query potential blocks.

In this section, we first provide a summary of the current MEV-Boost ecosystem, focusing on its silent feature, the diversity of relays and builders. Then, we use data to understand the relay and builder markets. Finally, we investigate the role of MEV auction platforms in prevalent censorship as a result of the recent OFAC sanction against Tornado Cash [26], in particular the effectiveness and the impact of the sanction against a decentralized system.

Data collection. Part of the standard relay API is for publishing various usage data, from which we can estimate the market share of builders and relays accurately. Specifically, we query the endpoint `ProposerPayloadsDelivered` of eight public relays to collect information about blocks built through MEV-Boost (hereafter referred to as *MEV-Boost blocks*), including their slot numbers, builder public keys, proposer public keys, etc. The range is from block 15537394 (the Merge, Sept 15th, 2022) to 16086233 (Nov 30th, 2022).

4.2.1. Relay differentiation. An interesting development of the MEV Boost ecosystem is the emergence of relays with differentiating product offerings. Based on their official documents, announcements, and previous summary [73], we highlight the following differentiating attributes to understand the intended usage of each relay.

- **Censorship free:** Whether the relay will refuse the propagate certain transactions and bundles (e.g., those interacting with the sanctioned addresses).
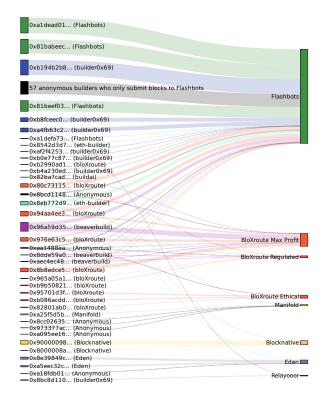- **Builder permissionless:** Whether any builder can submit to the relay.

Figure 3: Relationship between builders and relays (as of Nov 30th, 2022. The figure is inspired by [74] but we were able to identify 14 more builders.

- **All MEV Allowed**: Whether the relay will filter out certain predatory MEV transactions such as generalized frontrunning and sandwiches.
- **Open Source:** Whether the implementation of the relay is open source.
- **Profit Sharing Model**: How are the profit distribution among the relay, builders, and proposers?

As shown in Table 7, the Flashbots relay is permissionless and welcomes all MEV activities, but it will refuse to propagate blocks including transactions violating OFAC sanctions. bloXroute provides three versions of relays to meet the different needs for censorship and MEV activities. Builders who want to maximize their profit or ensure OFAC compliance can choose the Max profit or Regulated relay respectively. The Ethical relay and Blocknative relay will try to filter out MEV bundles which include generalized frontrunning and sandwiching. Eden relay also guarantees that their private RPC transactions will not be frontrun [73].

4.2.2. Understanding the relays and builders markets. Similar to the pre-Merge analysis, we trace the flow of MEV-Boost blocks to reveal the interaction between builders and relays. While the identity of relays is public, there is no central registrar for builders. We need to first identify builder public keys and cluster different addresses to reduce clutter.

Identifying builders. We combine three data sources to identify builders' public keys. First, we collect the allowlist

of builder public keys included in the source code of each relay. E.g., four public keys are listed in Eden's GitHub repository [75]. The second source is the marks left by builders in the "extra field" of their blocks. For example, the mark of Flashbots builders is "`Illuminate Dmocratize Dstribute`" and the mark of bloXroute builders is "`Powered by bloXroute`". Since such marks are not authenticated, we only consider a mark trustworthy if the builder keeps producing blocks with it (more than 100 blocks). The third source is the official documents and posts published by builders and relays. E.g., we confirm that builder0x69 is related to the relay Relayooor according to their tweet[7]. As shown in the table 6 in Appendix, We successfully identify 34 builders from 97 public keys.

With builder labels identified as above, we plot the block flows in Fig. 3. The figure is inspired by [74] but we independently reproduced builder identities and we were able to identify 14 more builders (one buildai builder (0x82ba7cad), one Blocknative builder (0x8000008a), two beaverbuild builders (0x8dde59a0 and 0xaec4ec48), etc.).

The Sankey graph allows us to understand the market shares of relays and builders and the relationship among different parties.

Market shares of relays and builders. Same as before the Merge, Flashbots still currently dominate the MEV-Boost ecosystem, both in relays and builders. The Flashbots relay propagated nearly 80% of Ethereum blocks. Again, the ecosystem evolves fast, and we refer readers to sources such as [65] for up-to-date numbers.

Focusing on the builder side, four Flashbots builders are responsible for 33.87% of MEV-boosted blocks as of Nov 30th, 2022. After Flashbots builders, the next biggest builder (organization) is builder0x69, which contributes 19.45% of the MEV-Boost blocks.
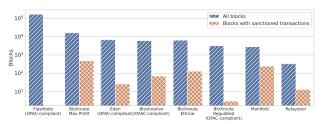
Relationship between builders and relays. Builders are free to submit their blocks to all available relays (except that permissioned relays will refuse connections from builders not on the allowlist). We observed that builder-relay relationships could be exclusive, collaborative, or even abusive.

As shown in Fig. 3, most relays also run builders who exclusively serve the respective relays. This applies to Flashbots, Blocknative, Eden, and Manifold. However, we do observe cooperation among different organizations. Some BloXroute builders also use the Flashbots relay. Eth-Builder uses three relays (Eden, Blocknative, and Manifold) at the same time, and beaverbuilder uses other three relays (Flashbots, bloXroute (Max profit), and bloXroute (Regulated)).
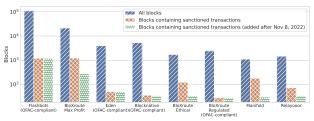
As for builder0x69, the second largest group of builders, one of their builders only submits blocks to their own relay Relayooor, and the other builders exclusively submit to the Flashbots relay. We notice that there is a long tail of anonymous builders that submit their blocks to the Flashbots relay since it is the only permissionless relay before Relayooor and Manifold appear.

We found that malicious builders may even attack the relay for profit. Manifold, one of the permissionless relays,

accepted 183 blocks from three anonymous builders and lost 7.47 ETH as a result. An official blog post [76] explains that these anonymous builders exploited a bug to bypass Manifold's check and changed the proposed reward address. This finding shows that besides exclusive and cooperative relationships, builders may also abuse relays.

(a) Sept 15th, 2022 to Nov 7th, 2022

(b) Nov 8th, 2022 to Nov 30th, 2022. The third column is the number of blocks containing transactions that interact with sanctioned addresses added on Nov 8th, 2022.

Figure 4: The number of MEV-Boost blocks that include sanctioned transactions. Relays marked with OFAC-compliant are not supposed to relay blocks with sanctioned transactions.

4.2.3. Censorship in MEV-Boost ecosystem. An ongoing controversy looming over the MEV-Boost ecosystem is the ability of relays to censor transactions. For background, the U.S. Treasury's Office of Foreign Assets Control (OFAC) recently placed a sanction on virtual currency mixer Tornado Cash [26]. To comply with OFAC requirements, some relays refuse to propagate transactions that interact with Tornado Cash and associated sanctioned addresses (we refer to such transactions as *sanctioned transactions*).

To identify sanctioned transactions, we collect the sanctions list from [77] and extract sanction addresses. A transaction is said to be sanctioned if 1) the sender or receiver is a sanctioned address, or 2) the execution calls a contract at a sanctioned address, or transfers ETH to a sanctioned address. We obtain transaction execution data from Etherscan [78] to identify sanctioned transactions.

As the story is actively unfolding, we leave a comprehensive analysis for future work. However, we do note two interesting points.

Are relays actually compliant? As shown in Table 7, multiple relays claim to be OFAC-compliant. However, the compliance status we found does not seem to match their claims.

Figure 4 plots the total number of blocks relayed by each relay and the number of blocks that include sanctioned

---

7. https://twitter.com/builder0x69/status/1585287608858451970

transactions, before and after November 8th, 2022. (The significance of this date will become clear momentarily.)

Interestingly, Fig. 4 shows that *only* Flashbots is fully OFAC compliant before Nov 8th, 2022. While the other three relays, bloXroute (Regulated), Blocknative, and Eden, who claim to be OFAC compliant, still proposed blocks containing sanctioned transactions.
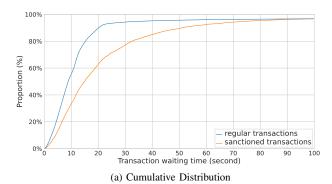
On Nov 8th, 2022, OFAC updated the sanctions list, but all of the OFAC-compliant relays failed to promptly adapt to the new list. The third column in Fig. 4b shows the number of blocks containing transactions that interact with newly sanctioned addresses. Notably, Flashbots has been compliant until then, but it started to accept newly sanctioned transactions after the update by OFAC. As one example, address `0x77777FeDdddFfC19Ff86DB637967013e6C6A116C` (Tornado.Cash: TORN Token) was added to the sanctions list on Nov 8th, 2022 [79]. As of the timing of this paper (Nov 30th, 2022), transactions to this addressed are still accepted by relays. `0x0e399228c201352c27d7becee194a46ef2505b 3f254470cc6afc479d467b8700` is sent and included on Nov 29th, 2022 in a block relayed by Flashbots.

It is conceivable that keeping constant track of OFAC updates is a burden for MEV auction platform maintainers and human errors are possible. However, once any oversight occurs, it would become impossible to rectify retroactively since blockchain is immutable. While we gave an example with Flashbots, all relays have accepted sanctioned transactions as shown in Fig. 4b. The full list of non-compliant transactions has been published at https://tinyurl.com/ofac-non-compliant-txs.

What is the impact of the sanction? Due to the decentralized nature of blockchains, it is even unclear what a sanction is supposed to achieve on a blockchain. However, we are still able to measure what it *did* achieve. In short, since not all relays are censoring sanctioned transactions, the implication of the sanction is not transactions being excluded, but them being delayed.

To illustrate the point, we compare the waiting time [28] of sanctioned transactions and regular ones. The waiting time of a given transaction is the time between when it first appears in the mempool and when it is minded in a block. In Fig. 5, we plot the distribution of waiting time for regular transactions and sanctioned transactions. The median waiting times of regular transactions and sanctioned transactions are 8.87s and 14.93s respectively, thus sanctioned transactions have to wait for about 68% longer on average than regular transactions before they can be included in a block.

More sophisticated models can be developed to, e.g., take other factors that might affect waiting time into consideration, but the above finding shows there is a significant difference between sanctioned transactions and non-sanctioned ones, potentially caused by the sanction.
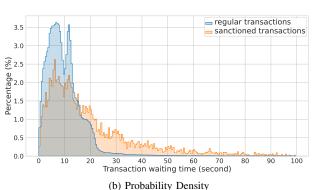

(a) Cumulative Distribution

(b) Probability Density

Figure 5: Distribution of waiting time for regular transactions and sanctioned transactions. (Sept 15th, 2022 to Nov 30th, 2022)

5. Related works

Study on private transactions. Multiple works studied private transactions in Ethereum. Qin et al. [37, Appendix C] collected privately mined transactions prior to the emergence of MEV auction platforms. Their analysis focused on mining pools' engagement in privately mining transactions. Piet et al. [71] studied MEV extraction activities in private transactions, and tested if Flashbots indeed mitigates negative externality. They found that 91.5% of MEV activities are performed in private transactions (a conclusion we support) and 65.9% of MEV profits are made by miners. Capponi et al. [80] drew a similar conclusion through a game theoretic analysis with empirical data support. Though it is unclear if the conclusions are robust after recent development in MEV auction platforms. Weintraub et al. [64] compared MEV extraction before and after the introduction of Flashbots. They show Flashbots disproportionately benefit miners at the expense of non-miners (i.e., searchers). They also identified unknown private pools besides Flashbots ([64, Section 6]), but they did not study the MEV auction platform ecosystem as a whole. They found Flexpool and F2Pool participate in other private pools besides Flashbots, consistent with our findings. Lyu et al. [72] analyzed private transactions on their characteristics, transaction costs, miner profits, and security impacts. [72] reported private transactions leakage, though they use Etherscan labels to identify private transactions, the soundness of which is unclear.

These works focus on the implications of private transactions, but we use private transactions to understand the MEV auction platform ecosystem, including the market shares of various platforms, the relationship amongst different parties, and whether they uphold the security guarantees.

SoKs on related topics. Eskandari et al. [30] are the first to propose a taxonomy of frontrunning attacks and map the possible mitigation to front-running attacks into three categories (transaction sequencing, confidentiality, and design practices). Similarly, Baum et al. [31] assess three front-running mitigation categories (fair ordering, batching of blinded inputs, and private user balances & secret input store) according to adversarial power of manipulating transaction order and inferring user intense. They only focus on frontrunning mitigation, which is a subset of MEV countermeasures as shown in Table 1. Heimbach et al. [34] focus on categorizing transaction reordering manipulation mitigation schemes and analyzing the strengths and weaknesses of each mitigation scheme with a qualitative approach. While our work leverages both qualitative and quantitative approaches to understand MEV countermeasures as well as their real-world deployment.

MEV and MEV auction platforms are important topics in SoK papers on DeFi too, though not as the main subject. Werner et al. [81] discuss MEV in the context of DeFi. Zhou et al. [82] modeled MEV auction platforms as a key component in the network layer to evaluate and compare real-world DeFi attacks. MEV is also considered as one of the security concerns to evaluate the AMM-based DEX in [83].

Quantifying MEV. Analyzing blockchain and mempool data to identify and quantify MEV starts with the original MEV paper [1]. Subsequently, a line of works improves the techniques for MEV identification and quantification [37], [64], [71], [72], [80], [84], [85]. Besides, several online dashboards present real-time MEV analytic including Flashbots Dashboard [38], EigenPhi [69], and ZeroMEV [66], etc. Our works rely on external tools to get labels of MEV activities, but our focus is to understand different solutions and their effects on MEV rather than quantifying MEV.

6. Discussion and future works

Legal Implications of MEV. In traditional financial markets, regulated intermediaries must process trades in the best interest of the traders, in line with best execution rules. Activities such as front-running are illegal in most jurisdictions (see, e.g., [2]). However, there is currently no direct applicable security law governing blockchain transaction ordering in any jurisdiction.

The recent Bank for International Settlements (BIS) research paper [86] has linked MEV to illegal market manipulation in traditional markets. The paper suggests that regulators must establish whether MEV is illegal and whether current insider trading provisions apply to MEV activities and also suggested that permissioned blockchains based on trusted intermediaries with publicly known identities may tackle MEV. From the point of view of who engages in MEV extraction, while the decentralization nature of MEV may provide some level of regulatory protection, it has been argued that regulators may not agree with this thesis [87]. However, since miners' identities are unknown, it may be difficult to enforce any regulatory measures.

MEV auction platforms' engagement in enforcing OFAC's sanction against Tornado Cash poses interesting legal questions. This paper examines the effectiveness of MEV auction platforms' enforcement of OFAC sanctions, but further research should analyze the legal implication of violating OFAC regulation in a decentralized system and if MEV auction platforms present a regulatory opportunity.

Cross-domain MEV. MEV extraction is possible across multiple blockchains, Layer 2 systems, and exchanges (on-chain or off-chain). [88] initiated the research on formalizing *cross-domain* MEV. However, understanding and mitigating cross-domain MEV largely remains an open problem.

MEV and Quant Trading. In the traditional financial market, quantitative trading algorithms can be leveraged for value extraction from trading activities. There are a few attempts to apply similar techniques for MEV purposes. E.g., [89] uses Bellman-Ford-Moore and SMT solver to find optimal arbitrage paths. Exploring how one can leverage quantitative trading algorithms for MEV is an interesting direction.

AI/ML and MEV. Can AI and ML be used to analyze on-chain data to predict MEV events and build algorithms to profit from it? To the best of our knowledge, there are currently no published papers on applying AI/ML for MEV opportunities. Nevertheless, in the traditional stock market, AI/ML is used for trading. E.g., Light Gradient Boosting Machine (LightGBM) algorithm can be used in stock price prediction by constructing the minimum variance portfolio of the mean-variance model with Conditional Value at Risk (CVaR) [90].

Acknowledgements

References

[1] P. Daian, S. Goldfeder, T. Kell, Y. Li, X. Zhao, I. Bentov, L. Breidenbach, and A. Juels, "Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability," in *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2020, pp. 910–927.

[2] J. W. Markham, "Front-Running–Insider Trading Under the Commodity Exchange Act," *Cath. UL Rev.*, vol. 38, p. 69, 1988.

[3] M. Carlsten, H. Kalodner, S. M. Weinberg, and A. Narayanan, "On the Instability of Bitcoin Without the Block Reward," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 154–167.

[4] Proposer/block builder separation-friendly fee market designs - economics - ethereum research. [Online]. Available: https://ethresear.ch/t/proposer-block-builder-separation-friendly-fee-market-designs/9725

[5] Flashbots, "Flashbots Docs," 2022. [Online]. Available: https://docs.flashbots.net/

[6] "Mev-Boost GitHub," 2022. [Online]. Available: https://github.com/flashbots/mev-boost

[7] V. Buterin, "Proposer/block builder separation-friendly fee market designs," 2021. [Online]. Available: https://ethresear.ch/t/proposer-block-builder-separation-friendly-fee-market-designs/9725

[8] M. Kelkar, F. Zhang, S. Goldfeder, and A. Juels, "Order-Fairness for Byzantine Consensus," in *Annual International Cryptology Conference*. Springer, 2020, pp. 451–480.

[9] M. Kelkar, S. Deb, S. Long, A. Juels, and S. Kannan, "Themis: Fast, Strong Order-Fairness in Byzantine Consensus," *Cryptology ePrint Archive*, 2021.

[10] C. Cachin, J. Mićić, N. Steinhauer, and L. Zanolini, "Quick Order Fairness," in *International Conference on Financial Cryptography and Data Security*. Springer, 2022, pp. 316–333.

[11] Y. Zhang, S. Setty, Q. Chen, L. Zhou, and L. Alvisi, "Byzantine Ordered Consensus without Byzantine Oligarchy," in *14th USENIX Symposium on Operating Systems Design and Implementation (OSDI 20)*, 2020, pp. 633–649.

[12] K. Kursawe, "Wendy, the Good Little Fairness Widget: Achieving Order Fairness for Blockchains," in *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, 2020, pp. 25–36.

[13] R. Khalil, A. Gervais, and G. Felley, "TEX - A Securely Scalable Trustless Exchange," *Cryptology ePrint Archive*, 2019.

[14] K. Segal and T. Brand, "Presenting: VeeDo, a STARK-based VDF Service," 2020. [Online]. Available: https://medium.com/starkware/presenting-veedo-e4bbff77c7ae

[15] I. Bentov, Y. Ji, F. Zhang, L. Breidenbach, P. Daian, and A. Juels, "Tesseract: Real-Time Cryptocurrency Exchange Using Trusted Hardware," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp. 1521–1538.

[16] H. Zhang, L.-H. Merino, V. Estrada-Galinanes, and B. Ford, "Flash Freezing Flash Boys: Countering Blockchain Front-Running," in *The Workshop on Decentralized Internet, Networks, Protocols, and Systems (DINPS)*, 2022.

[17] Sikka inc., "Sikka Projects," 2022. [Online]. Available: https://sikka.tech/projects/

[18] atom_crypto, "The MEV Game of the Crypto Economy: Osmosis' Threshold Encryption vs. SGX of Flashbot?" 2022. [Online]. Available: https://mirror.xyz/infinet.eth/SFjR1H1-RMnKoIoPjqkxpauVPrLYGqLHQP1dY9FHvx4

[19] Shutter Network, "Shutter Network Blog," 2022. [Online]. Available: https://blog.shutter.network/

[20] D. Malkhi and P. Szalachowski, "Maximal Extractable Value (MEV) Protection on a DAG," *arXiv preprint arXiv:2208.00940*, 2022.

[21] E. Budish, P. Cramton, and J. Shim, "The High-Frequency Trading Arms Race: Frequent Batch Auctions as a Market Design Response," *The Quarterly Journal of Economics*, vol. 130, no. 4, pp. 1547–1621, 2015.

[22] C. McMenamin, V. Daza, M. Fitzi, and P. O'Donoghue, "FairTraDEX: A Decentralised Exchange Preventing Value Extraction," in *Proceedings of the 2022 ACM CCS Workshop on Decentralized Finance and Security*, 2022, pp. 39–46.

[23] S. Wadhwa, J. Stoeter, F. Zhang, and K. Nayak, "He-HTLC: Revisiting Incentives in HTLC," Cryptology ePrint Archive, Paper 2022/546, 2022, https://eprint.iacr.org/2022/546. [Online]. Available: https://eprint.iacr.org/2022/546

[24] I. Tsabary, M. Yechieli, A. Manuskin, and I. Eyal, "MAD-HTLC: because HTLC is crazy-cheap to attack," in *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2021, pp. 1230–1248.

[25] H. Chung, E. Masserova, E. Shi, and S. A. Thyagarajan, "Rapidash: Foundations of Side-Contract-Resilient Fair Exchange," Cryptology ePrint Archive, Paper 2022/1063, 2022, https://eprint.iacr.org/2022/1063. [Online]. Available: https://eprint.iacr.org/2022/1063

[26] U.S. Department of the Treasury, "U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash," 2022. [Online]. Available: https://home.treasury.gov/news/press-releases/jy0916

[27] E. Halpern, "Unmasking the ethereum uncle bandit," 2021. [Online]. Available: https://medium.com/alchemy-api/unmasking-the-ethereum-uncle-bandit-a2b3eb694019

[28] Y. Liu, Y. Lu, K. Nayak, F. Zhang, L. Zhang, and Y. Zhao, "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*, ser. CCS '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 2099–2113. [Online]. Available: https://doi.org/10.1145/3548606.3559341

[29] L. Zhou, K. Qin, C. F. Torres, D. V. Le, and A. Gervais, "High-Frequency Trading on Decentralized On-Chain Exchanges," in *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2021, pp. 428–445.

[30] S. Eskandari, S. Moosavi, and J. Clark, "SoK: Transparent Dishonesty: front-running attacks on Blockchain," in *International Conference on Financial Cryptography and Data Security*. Springer, 2019, pp. 170–189.

[31] C. Baum, J. H.-y. Chiang, B. David, T. K. Frederiksen, and L. Gentile, "SoK: Mitigation of Front-running in Decentralized Finance," *Cryptology ePrint Archive*, 2021.

[32] Y. Wang, P. Zuest, Y. Yao, Z. Lu, and R. Wattenhofer, "Impact and User Perception of Sandwich Attacks in the DeFi Ecosystem," in *CHI Conference on Human Factors in Computing Systems*, 2022, pp. 1–15.

[33] K. Kulkarni, T. Diamandis, and T. Chitra, "Towards a Theory of Maximal Extractable Value I: Constant Function Market Makers," *arXiv preprint arXiv:2207.11835*, 2022.

[34] L. Heimbach and R. Wattenhofer, "SoK: Preventing Transaction Reordering Manipulations in Decentralized Finance," *arXiv preprint arXiv:2203.11520*, 2022.

[35] E. Félez-Viñas, L. Johnson, and T. J. Putniņš, "Insider Trading in Cryptocurrency Markets," *Available at SSRN 4184367*, 2022.

[36] H. Chung, E. Masserova, E. Shi, and S. A. Thyagarajan, "Ponyta: Foundations of Side-Contract-Resilient Fair Exchange," *Cryptology ePrint Archive*, 2022.

[37] K. Qin, L. Zhou, and A. Gervais, "Quantifying blockchain extractable value: How dark is the forest?" in *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2022, pp. 198–214.

[38] Flashbots, "Transparency dashboard | Flashbots," 2022. [Online]. Available: https://dashboard.flashbots.net/

[39] K. Qin, L. Zhou, P. Gamito, P. Jovanovic, and A. Gervais, "An Empirical Study of DeFi Liquidations: Incentives, Risks, and Instabilities," in *Proceedings of the 21st ACM Internet Measurement Conference*, 2021, pp. 336–350.

[40] F. Winzer, B. Herd, and S. Faust, "Temporary Censorship Attacks in the Presence of Rational Miners," in *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2019, pp. 357–366.

[41] EigenPhi, "Sandwich overview | EigenPhi," 2022. [Online]. Available: https://eigenphi.io/mev/ethereum/sandwich

[42] Hasu and S. Gosselin. Why run mev-boost? | Flashbots. [Online]. Available: https://writings.flashbots.net/why-run-mevboost/

[43] Flashbots, "Flashbots Auction," 2022. [Online]. Available: https://docs.flashbots.net/flashbots-auction/overview

[44] C. Piatt, J. Quesnelle, and C. Sheridan, "EDEN Network Whitepaper," 2021. [Online]. Available: https://edennetwork.io/EDEN_Network_ __Whitepaper___2021_07.pdf

[45] Ethermine, "Ethermine MEV-Relay," 2022. [Online]. Available: https://ethermine.org/mev-relay

[46] Flashbots, "Flashbots docs | private transaction status API," 2022. [Online]. Available: https://docs.flashbots.net/flashbots-protect/rpc/status-api

[47] Eden Network, "Eden Network RPC - Trade Better," 2022. [Online]. Available: https://rpc.edennetwork.io/

[48] bloXroute Labs, "Fast Protect - bloXroute Documentation," 2022. [Online]. Available: https://docs.bloxroute.com/introduction/fast-protect

[49] Flashbots, "Mev-share: programmably private orderflow to share mev with users," 2023. [Online]. Available: https://collective.flashbots.net/t/mev-share-programmably-private-orderflow-to-share-mev-with-users/1264

[50] bloXroute Labs, "Backrunme - bloxroute documentation," 2022. [Online]. Available: https://docs.bloxroute.com/introduction/backrunme

[51] L. Baird, A. Luykx, and P. Madsen, "Hedera Technical Insights: Fair Timestamping and Fair Ordering of Transactions," 2022. [Online]. Available: https://hedera.com/blog/fair-timestamping-and-fair-ordering-of-transactions

[52] C. Protocol, "CoW Swap | The smartest way to trade cryptocurrencies," 2022. [Online]. Available: https://swap.cow.fi/#/swap?chain=mainnet

[53] L. Zhou, K. Qin, and A. Gervais, "A2MM: Mitigating Frontrunning, Transaction Reordering and Consensus Instability in Decentralized Exchanges," *arXiv preprint arXiv:2106.07371*, 2021.

[54] C. Baum, B. David, and T. K. Frederiksen, "P2DEX: privacy-preserving decentralized cryptocurrency exchange," in *International Conference on Applied Cryptography and Network Security*. Springer, 2021, pp. 163–194.

[55] L. Heimbach and R. Wattenhofer, "Eliminating Sandwich Attacks with the Help of Game Theory," in *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*, 2022, pp. 153–167.

[56] V. Buterin, "State of research: increasing censorship resistance of transactions under proposer/builder separation (PBS)," 2021. [Online]. Available: https://notes.ethereum.org/@vbuterin/pbs_censorship_resistance

[57] Ethereum, "The Merge | ethereum.org," 2022. [Online]. Available: https://ethereum.org/en/upgrades/merge/

[58] A. Juels, L. Breidenbach, and F. Tramer, "Fair Sequencing Services: Enabling a Provably Fair DeFi Ecosystem," 2020. [Online]. Available: https://blog.chain.link/chainlink-fair-sequencing-services-enabling-a-provably-fair-defi-ecosystem/

[59] Vega, "Vega Protocol: Blockchain derivatives," 2022. [Online]. Available: https://vega.xyz/

[60] M. K. Reiter and K. P. Birman, "How to securely replicate services," *ACM Transactions on Programming Languages and Systems (TOPLAS)*, vol. 16, no. 3, pp. 986–1009, 1994.

[61] F. McKeen, I. Alexandrovich, A. Berenzon, C. V. Rozas, H. Shafi, V. Shanbhogue, and U. R. Savagaonkar, "Innovative instructions and software model for isolated execution." *Hasp@ isca*, vol. 10, no. 1, 2013.

[62] D. Lee, D. Kohlbrenner, S. Shinde, K. Asanovic, and D. Song, "Keystone: An Open Framework for Architecting Trusted Execution Environments," in *Proceedings of the Fifteenth European Conference on Computer Systems*, ser. EuroSys '20, 2020.

[63] Confidential computing | NVIDIA. [Online]. Available: https://www.nvidia.com/en-us/data-center/solutions/confidential-computing/

[64] B. Weintraub, C. Ferreira Torres, C. Nita-Rotaru, and R. State, "A Flash(bot) in the Pan: Measuring Maximal Extractable Value in Private Pools," in *Proceedings of the 22nd ACM Internet Measurement Conference (IMC '22)*. Nice, France: Association for Computing Machinery, 2022.

[65] A. Agnihotri, "mevboost.org," 2022. [Online]. Available: https://github.com/Anish-Agnihotri/mevboost.org

[66] Pmcgoohan, "data and technical | zeromev," 2022. [Online]. Available: https://info.zeromev.org/technical.html

[67] Flashbots, "Flashbots Blocks API," 2022. [Online]. Available: https://blocks.flashbots.net/

[68] Eden Network, "Eden Network Explorer," 2022. [Online]. Available: https://explorer.edennetwork.io/

[69] EigenPhi, "Eigenphi: Wisdom of DeFi," 2022. [Online]. Available: https://eigenphi.io/

[70] Etherscan, "Label Word Cloud | Etherscan," 2022. [Online]. Available: https://etherscan.io/labelcloud

[71] J. Piet, J. Fairoze, and N. Weaver, "Extracting godl [sic] from the salt mines: Ethereum miners extracting value," in *Workshop on the Economics of Information Security*, 2022.

[72] X. Lyu, M. Zhang, X. Zhang, J. Niu, Y. Zhang, and Z. Lin, "An Empirical Study on Ethereum Private Transactions and the Security Implications," *arXiv preprint arXiv:2208.02858*, 2022.

[73] E. S. Educators, "MEV relay list for Mainnet," 2022. [Online]. Available: https://github.com/eth-educators/ethstaker-guides/blob/main/MEV-relay-list.md

[74] T. Wahrstätter, "MEV-Boost Dashboard," 2022. [Online]. Available: https://mevboost.pics/

[75] Eden Network, "mev-boost Relay," 2022. [Online]. Available: https://github.com/eden-network/mev-boost-relay

[76] Manifold Finance, "Postmortem of incident on 2022-10-15," 2022. [Online]. Available: https://hackmd.io/@manifold/2022-10-15

[77] U.S. Department of the Treasury, "OFAC Specially Designated Nationals Data," 2022. [Online]. Available: https://www.treasury.gov/ofac/downloads

[78] Etherscan, "Introduction - Etherscan," 2022. [Online]. Available: https://docs.etherscan.io/

[79] U.S. Department of the Treasury. (2022) Burma-related Designations; North Korea Designations; Cyber-related Designation; Cyber-related Designation Removal; Publication of Cyber-related Frequently Asked Questions. [Online]. Available: https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20221108

[80] A. Capponi, R. Jia, and Y. Wang, "The Evolution of Blockchain: from Lit to Dark," *arXiv preprint arXiv:2202.05779*, 2022.

[81] S. M. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, and W. J. Knottenbelt, "SoK: Decentralized Finance (DeFi)," *arXiv preprint arXiv:2101.08778*, 2021.

[82] L. Zhou, X. Xiong, J. Ernstberger, S. Chaliasos, Z. Wang, Y. Wang, K. Qin, R. Wattenhofer, D. Song, and A. Gervais, "SoK: Decentralized Finance (DeFi) Incidents," *arXiv preprint arXiv:2208.13035*, 2022.

[83] J. Xu, K. Paruch, S. Cousaert, and Y. Feng, "SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols," *arXiv preprint arXiv:2103.12732*, 2021.

[84] C. F. Torres, R. Camino *et al.*, "Frontrunner Jones and the Raiders of the Dark Forest: An Empirical Study of Frontrunning on the Ethereum Blockchain," in *30th USENIX Security Symposium (USENIX Security 21)*, 2021, pp. 1343–1359.

[85] Y. Wang, Y. Chen, H. Wu, L. Zhou, S. Deng, and R. Wattenhofer, "Cyclic arbitrage in decentralized exchanges," *Available at SSRN 3834535*, 2022.

[86] R. Auer, J. Frost, J. M. V. Pastor *et al.*, "Miners as intermediaries: extractable value and market manipulation in crypto and DeFi," Bank for International Settlements, Tech. Rep., 2022.

[87] A. Walch, "Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems," *Institute for International Economic Law at Georgetown Law School on Nov*, vol. 5, p. 8, 2018.

[88] A. Obadia, A. Salles, L. Sankar, T. Chitra, V. Chellani, and P. Daian, "Unity is strength: A formalization of cross-domain maximal extractable value," *arXiv preprint arXiv:2112.01472*, 2021.

[89] L. Zhou, K. Qin, A. Cully, B. Livshits, and A. Gervais, "On the Just-In-Time Discovery of Profit-Generating Transactions in DeFi Protocols," in *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2021, pp. 919–936.

[90] Y. Chen, K. Liu, Y. Xie, and M. Hu, "Financial Trading Strategy System Based on Machine Learning," *Mathematical problems in engineering*, vol. 2020, 2020.

[91] Flashbots, "Flashbots Boost Relay - Mainnet," 2022. [Online]. Available: https://boost-relay.flashbots.net/

[92] bloXroute Labs, "bloXroute MEV Relay - Max-profit," 2022. [Online]. Available: https://bloxroute.max-profit.blxrbdn.com/

[93] bloXroute Labs, "bloXroute MEV Relay - Ethical," 2022. [Online]. Available: https://bloxroute.ethical.blxrbdn.com/

[94] bloXroute Labs, "bloXroute MEV Relay - Regulated," 2022. [Online]. Available: https://bloxroute.regulated.blxrbdn.com/

[95] Blocknative, "Blocknative documentation," 2022. [Online]. Available: https://docs.blocknative.com/

[96] Eden Network, "Eden Relay - Mainnet," 2022. [Online]. Available: https://relay.edennetwork.io/info

[97] Manifold Finance, "SecureRpc Relay," 2022. [Online]. Available: https://mainnet-relay.securerpc.com/

[98] relayooor, "mev-boost relay," 2022. [Online]. Available: https://github.com/relayooor/mev-boost-relay

Appendix

Full list of sandwich attacks with private transactions as victims

Table 5 shows the details of eight sandwich attacks whose victim transaction is a private transaction, including their block number, MEV transaction types, which MEV auction platforms they use, transaction hashes, along with from and to addresses.

Example of Etherscan mislabelling

Fig. 6 gives an example that a transaction is public but mislabeled by Etherscan. From Fig. 6a, we can find this transaction (whose hash is `0x8d0c16210335a9ee8815d7b0dba22134f9dc722047e8f2d6` is labeled as a private transaction on Sept 12th, 2022. Although Etherscan had realized this problem and updated its label, as shown in Fig. 6b.

(a) Screenshot from Sept 12th, 2022

(b) Screenshot from Dec 2nd, 2022

Figure 6: An example of a mislabelled private transaction in Etherscan

Identification of MEV-Boost builders

Table 6 gives a complete list of the MEV-Boost builders we identify, including eight builders and 33 public keys they owned.

Summary of MEV-Boost relay

Table 7 is a summary of eight public relays. Manifold turned to permissioned after the attack [76] and became permissionless again on Nov 21st, 2022.

TABLE 5: Private transactions under sandwich attacks

block number	MEV type	MEV auction platform	transaction hash	from address	to address
15468530	frontrun	Ethermine	0x98ec45c7dc3808a773ab220d7aae416c967281dd7f5e0e0eaf20e2b9cadaf297	0x7944e84d18803f926743fa56fb7a9bb9ba5f5f24	0xe8c060f8052e07423f71d445277c61ac5138a2e5
15468530	victim	Ethermine	0xcb95d8a6b675dbde7237c795322bb60e4fbb32ec01dfafd983eb8f68a3952628	0x25173f370af28592354098a18e583f8eaa7ab264	0x0ef8b4525c69bfa7bdece3ab09f95bbf0944b783
15468530	backrun	Ethermine	0x75eb85a97f273b017f86215072fe5408d817d803eab63687255343f67c60bdbd	0x7944e84d18803f926743fa56fb7a9bb9ba5f5f24	0xe8c060f8052e07423f71d445277c61ac5138a2e5
15442739	frontrun	unknown	0xa4ef3607a0cc57e8275a4100147cdcf43d001e35117a148c55f19f8627cd7018	0xb58555fcba6479fced7de1485eb054943a09af7b	0x00000000003b3cc22af3ae1eac0440bcee416b40
15442739	victim	unknown	0xd7555c744a92834d6210a73b4846d9f7e2f6d1de718260ce41e69d218365c821	0xa30622a0061513b1b6971307b66e8ba4c4f52f3c	0x0000000000007f150bd6f54c40a34d7c3d5e9f56
15442739	backrun	unknown	0x31210110d3c21e136f7e770e2e2537574781006f2f624f5506718c3199ab7e093	0xb58555fcba6479fced7de1485eb054943a09af7b	0x00000000003b3cc22af3ae1eac0440bcee416b40
15436306	frontrun	Flashbots	0xd3dbbff16a1bbee3f81eb7ca595dd5c2f78ebbc97f443c99629ac6dd65fb32ec	0xb58555fcba6479fced7de1485eb054943a09af7b	0x00000000003b3cc22af3ae1eac0440bcee416b40
15436306	victim	Flashbots	0x7b679ef1e3d9c1ecb2930f885d039d08c9e0f8ed9b5502a3ffeb19de425a95d0	0xeee3109f51f0eac5212574634df62e997e550e19	0x0ef8b4525c69bfa7bdece3ab09f95bbf0944b783
15436306	backrun	Flashbots	0x2374434602350661339338ae559614507ebf5de1ea5ec26a005276fc75fbe428b	0xb58555fcba6479fced7de1485eb054943a09af7b	0x00000000003b3cc22af3ae1eac0440bcee416b40
15383442	frontrun	Flashbots	0xce2a15c9eead75e8d90d8c16a3781686f4bfdf04d15f809dc7fed19f14638434	0x4970197593ef5aed9d2c33409b953f5f9bb22563	0x00000000008c4fb1c916e0c88fd4cc402d935e7d
15383442	victim	Flashbots	0x9d287971021c5b93756e446a7962dedf5203728ca9552de704c9169e48e2cf71	0x16745d124412d0d3c2a83ee82ced2d93c7b4c660	0x2f1d79860cf6ea3f4b3b734153b52815773c0638
15383442	backrun	Flashbots	0x6b59e2b188b7392375ce6e93573486630946ca2b9fa1d6ffbd98c4cb36c54d68	0x4970197593ef5aed9d2c33409b953f5f9bb22563	0x00000000008c4fb1c916e0c88fd4cc402d935e7d
15368962	frontrun	unknown	0xc8e441cdcec3f71a46484520eebc504c26137bede6d88313b5c89f780c0ebcf3	0xe2ca3167b89b8cf680d63b06e8aeefc5e4ebe907	0xe8c060f8052e07423f71d445277c61ac5138a2e5
15368962	victim	unknown	0x2d3358b38672b23b575c751e2f5629c703ebc06863f769c69df20dc2670b838c	0x0cac3d1a887206e0f6169222c4504301a8b4b993	0xa57bd00134b2850b2a1c55860c9e9ea100fdd6cf
15368962	backrun	unknown	0x6a74371bb1fb15bb1b2ce73492cc3d83ce48cb175e3d344fb045f964f81e5d98	0xe2ca3167b89b8cf680d63b06e8aeefc5e4ebe907	0xe8c060f8052e07423f71d445277c61ac5138a2e5
15350565	frontrun	Flashbots	0x97c0628e13773f9565102f2ff447b5d89064020bdfbd2ddfd8ab15ea5b292881	0x38563699560e4512c7574c8cc5cf89fd43923bca	0x00000000035b5e5ad9019092c665357240f594e
15350565	victim	Flashbots	0x3f161a35c38ee1b5e20ef8f2fc3843e747456f3f12877a4c6b9f9319a79c374b	0x000000cea33e55d04fb10a1af69efeb8f7e6c7f2	0x9cdc00c3cf228100674e4d0000e732f78d004320
15350565	backrun	Flashbots	0xb71089ecdd3276e7bf7e3b06857c4dfaf051490facee91c55d6f645a2b37305b	0x38563699560e4512c7574c8cc5cf89fd43923bca	0x00000000035b5e5ad9019092c665357240f594e
15314350	frontrun	Flashbots	0xbbac6ef9ff32b3a2bc4ac5faa4fceaf28187f60c73155c559c106784e6dc08b5	0x36baf0d6c97efd5fd6ae995d760a84f936078759	0x00000000008c4fb1c916e0c88fd4cc402d935e7d
15314350	victim	Flashbots	0xdd6e4a7ab7b2c6ad5cc7aad171ee3d601a9e6cce45a355d2baa3bca65b29e156	0x52a2753f420d7ad2a6588008d722b1679fad331	0x2f1d79860cf6ea3f4b3b734153b52815773c0638
15314350	backrun	Flashbots	0x5f869f0a9d92d4a8c7cd7e5d8966d3a4429a22fd6a35e200a860a2433cb0033a	0x36baf0d6c97efd5fd6ae995d760a84f936078759	0x00000000008c4fb1c916e0c88fd4cc402d935e7d
15260256	frontrun	Flashbots	0x5117c46039e5bbf3cecb4b941ec09415260db3bc50c7b655b4f64ca386ef21fc	0x7944e84d18803f926743fa56fb7a9bb9ba5f5f24	0xe8c060f8052e07423f71d445277c61ac5138a2e5
15260256	victim	Flashbots	0xd2c01976298422bd56a3430ddbc9ebc2f9aca06a387b76af3dc75d7f0acb4493	0xd03154dbc4ae6beafa79f7ae6d99c12ce58f5b64	0x0000000000007f150bd6f54c40a34d7c3d5e9f56
15260256	backrun	Flashbots	0x3d4e04e3d385fe22668781c631871c9ad07712201eeb910148f6a5bcedd22aaa	0x7944e84d18803f926743fa56fb7a9bb9ba5f5f24	0xe8c060f8052e07423f71d445277c61ac5138a2e5

TABLE 6: Identified Builder

Builder	Mark	Public Key (Prefix)
Flashbots	Illuminate Dmocratize Dstribute	0xa1dead01... 0x81babeec... 0x81beef03... 0xa1defa73...
bloXroute	Powered by bloXroute	0x94aa4ee3... 0x80c73115... 0x8b8edce5... 0x95701d3f... 0xb086acdd... 0x976e63c5... 0xb9b50821... 0x82801ab0... 0xb2990ad1... 0x965a05a1...
builder0x69	@builder0x69 builder0x69 by builder0x69 Viva relayooor.wtf by @builder0x69 builder0x69 by @builder0x69	0xb194b2b8... 0xa4fb63c2... 0xb8fceec0... 0x8bc8d110... 0xb4a230ed... 0xaf2f4253... 0xb0e77c87...
Eden		0x8e39849c... 0xa5eec32c... 0x8931ae67... 0xb1d229d9...
Blocknative	Made on the moon by Blocknative	0x90000098... 0x8000008a...
Manifold	Manifold	0xa25f5d5b...
eth-builder	https://eth-builder.com	0x8eb772d9... 0x8542d3d7...
beaverbuild	beaverbuild.org	0x96a59d35... 0xaec4ec48... 0x8dde59a0...
buildai	BuildAI (https://buildai.net)	0x82ba7cad...

TABLE 7: Public Relays

Relay	Censorship Free	Builder Permissionless	All MEV Allowed	Open Source	Profit Sharing Model
Flashbots [91]	✗	✓	✓	✓	Specific to builder
bloXroute (Max profit) [92]	✓	✗	✓	✗	Unknown
bloXroute (Ethical) [93]	✓	✗	✗	✗	Unknown
bloXroute (Regulated) [94]	✗	✗	✓	✗	Unknown
Blocknative [95]	✗	✗	✗	✓	100% to validator
Eden [96]	✗	✗	✗	✓	100% to validator
Manifold [97]	✓	✓	✓	✗	Specific to builder
Relayooor [98]	✓	✓	✓	✓	Specific to builder