SoK: MEV Countermeasures

Sen Yang
sen.yang@yale.edu
Yale University
New Haven, CT, United States

Fan Zhang
f.zhang@yale.edu
Yale University
New Haven, CT, United States

Ken Huang
kenhuangus@gmail.com
DistributedApps.ai
Fairfax, VA, United States

Xi Chen
xichen1987@gmail.com
New York University
New York, NY, United States

Youwei Yang*
chinayyw@gmail.com
Bit Mining Limited
Secaucus, NJ, United States

Feng Zhu
fzhu@hbs.edu
Harvard University
Cambridge, MA, United States

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 reordering 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 to mitigate the negative effects of MEV, 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 existing MEV countermeasures. The contribution is twofold. First, we present a comprehensive taxonomy of 32 proposed MEV countermeasures, covering four different technical directions. Second, we summarize four security problems caused by MEV and examine whether different MEV countermeasures can effectively address these problems. Our work also helps identify directions for future research on MEV and MEV mitigation.

CCS Concepts

• **Security and privacy → Distributed systems security**.

Keywords

Decentralized Finance, Miner/Maximal Extractable Value, Ethereum

ACM Reference Format:
Sen Yang, Fan Zhang, Ken Huang, Xi Chen, Youwei Yang, and Feng Zhu. 2024. SoK: MEV Countermeasures. In *Proceedings of the Workshop on Decentralized Finance and Security (DeFi '24), October 14–18, 2024, Salt Lake City, UT, USA.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3689931.3694911

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* [19]. 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 [49] Bob and reap a profit. Daian et al. [19] 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 reordering user transactions.

MEV bears profound implications for the security and decentralization of blockchain systems. Some MEV occurs 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 across exchanges), but uncoordinated extraction can cause network congestion and high transaction fees [19]. Moreover, when MEV dominates block rewards (which it already does quite often in Ethereum), blockchain consensus could be destabilized [16]. Last but not least, MEV can lead to centralization, as finding sophisticated MEV opportunities requires significant resources (money and talent), which only large players can afford [13].

Academia and industry have attempted countermeasures from several different directions to reduce the negative effects of MEV (for simplicity, "MEV countermeasures" will specifically refer to those aimed at mitigating the negative effects of MEV in the following sections). At the highest level of abstraction, two schools of thought were explored: 1) to facilitate MEV extraction so that the process is efficient, decentralized, and transparent [13, 26, 29], and 2) to stop MEV extraction by ordering transactions in a way that renders order manipulation infeasible (e.g., [14, 37, 38]). As readers can notice, these two directions aim to lead to different and possibly incompatible futures. Currently, there is no consensus on the best countermeasures. Moreover, while academics have better explored the second approach, it is the first approach that has been widely adopted in practice thus far.

Our contribution. This paper systematizes the knowledge of MEV countermeasures, covering both academically proposed solutions and the popular choices of practitioners. Our contribution is twofold: First, we present a comprehensive taxonomy of recently proposed MEV countermeasures, covering four different technical

*Also with Schumpeter Data Asset Research Institute.

DeFi '24, October 14–18, 2024, Salt Lake City, UT, USA

ACM ISBN 979-8-4007-1227-2/24/10
https://doi.org/10.1145/3689931.3694911

directions. Second, we summarize the security implications caused by MEV and evaluate how different classes of countermeasures mitigate these risks.

A taxonomy of MEV countermeasures. We selected 32 recent projects and papers that proposed representative MEV countermeasures, from the following four categories. The first category aligns with the first school of thought, and the others align with the second.

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 which 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. These 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. [37, 38] proposed receive-order fairness, which requires that if a majority of nodes receive T_1 before T_2, then the final blockchain should respect that order. Order linearizability [85], κ-differential order-fairness [14], and timed-relative fairness [41] 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 their transaction before others). While weaker, content-agnostic ordering is popular for its simplicity, and multiple implementations have been proposed [1, 7, 39, 47, 66–68, 84].

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 [12, 51] (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 [73]. 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 [70]. Bribery is explicit MEV created by attackers to induce desired behaviors of miners. In [17, 73], authors further showed MEV-extracting miners themselves can mount bribery attacks or collude with other participants to break the countermeasure in [70], and proposed countermeasures.

In Sec. 3, we deep dive into the technical details of each proposed scheme, comparing their goals, solutions, and trust assumptions. Then, we discuss how each category of ideas approaches the MEV problem, noting that not all address every aspect.

Roadmap. In Sec. 2, we review the common types of MEV and the security implications. In Sec. 3, we present the taxonomy of 32 proposed MEV countermeasures and the comparison of them. In Sec. 4, we discuss related works. Finally, we conclude with a discussion on 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. [19] 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. We do not provide a mathematical definition of MEV, as it is not essential for the scope of this paper. Readers interested in it can refer to [2, 3, 57].

In practice, MEV extraction 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 their 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 Sec. 3).

While being a relatively new topic, there is already substantial literature on understanding, quantifying, and mitigating MEVs [6, 17, 22, 24, 27, 35, 40, 64, 73, 78, 87]. We will defer a systematic review of MEV countermeasures to Sec. 3. Below we briefly review common MEV sources and their security implications.

2.1.1 *Common types of MEV in decentralized finance applications.*

MEV may arise in various decentralized 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

[1] 0xb40fd0c9a2ba2d1d5e7ee5e322f9afc5e2ec1b7e2d520b638ea83dcc9c850d02
[2] 0xbc2cb18d0e58418d8d9c948cab319460bd409d7bd5f2978f3e52e445b351c522

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 [63] for an empirical study on liquidation.

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 [87].

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.

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 [70, 81]. 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 [73], bribery attacks are detrimental.

2.2 Security Implications

User loss. Some MEV extraction directly causes users to lose money. For example, from September 2022 to June 2024, predatory sandwich attackers made a profit of more than $41 million [45], at the expense of victims.

Inefficiency due to the lack of coordination. In this paper, we focus on inefficiency as the waste of resources and increased costs caused by uncoordinated competition among MEV searchers. Originally observed in [19], 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, the competition may shift to off-chain latency wars [48].

Destabilizing consensus. Carlsten et al. [16] 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 [27]. Daian et al. [19] also described another attack vector exploiting MEV called Time-bandit attacks, which essentially augments reorg/51% attacks with subsidy from MEV.

A centralizing force. Among many, Vitalik argued that MEV could cause centralization because there is a significant economy of scale in finding sophisticated MEV extraction opportunities [13]. We want to avoid a centralized and monopolized future because it harms transparency and decentralization. Another worry is that MEV can encourage "vertical integration" [32] of block producers and traders to form closed-door systems that harm the transparency and permissionlessness of the blockchain.

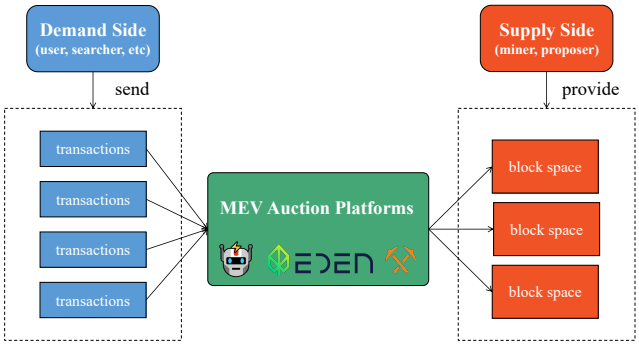

Figure 1: Schematic Diagram of MEV auction platforms

3 MEV Countermeasures

Recall that we defined four classes of MEV countermeasures in Sec. 1. In this section, we first present a taxonomy of 32 proposed schemes from the four categories in Tab. 1. Then, we compare how different classes of solutions address each aspect of the MEV problem as defined in Sec. 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. Fig. 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). Note that the privacy provided by MEV auction platforms relies on trust assumptions, unlike the cryptographic guarantees for privacy offered by content-agnostic ordering, which we will discuss in Sec. 3.3.

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 Ethereum Merge [30] 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 [25] 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 Flashbots 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.

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 [25], Eden Network [59], Ethermine [23] (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 [29]	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 [28], Ethermine RPC [23], Eden Network RPC [54], bloXroute ETH Protect [10]	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 [53], MEV Blocker [18], BackRunMe [9]	Enable users to selectively disclose the information of their transactions and capture the generated MEV via a centralized service that matches user transactions with searcher transactions.	The service is fully trusted for sharing privacy and matching transactions.
II: Time-based ordering properties (Notation: suppose the committee has n nodes and up to f are malicious)		
Aequitas [38]	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 [37]	Same as above	$n \geq \frac{4f+1}{2\gamma-1}$
Pompē [85]	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 [14]	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 [4]	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 [41]	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 [39]	Users encrypt transactions using timelock puzzles. Timelock puzzles ensure that all transactions are revealed. A similar idea is mentioned in Veedo [66].	The attacker cannot solve timelock puzzles much faster than honest users.
Tesseract [7]	Users encrypt transactions using keys generated in TEEs.	Integrity and confidentiality of TEEs
F3B [84]	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 [68], Osmosis [1], Shutter Network [67]	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 [47]	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 [62]	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 [51]	Frequent batch auctions realized with zero-knowledge proofs and value commitment.	-
Verifiable Sequencing Rules [82]	Constrain the valid execution orderings miners should respect, which is verifiable so that everyone can efficiently verify if a miner follows the rule.	-
A^2MM [86]	Atomically route user trades across AMMs to avoid sandwich and arbitrage opportunities.	-
P2DEX [5]	Order matching using secure multiparty computation (MPC).	-
Optimal slippage for eliminating sandwich [34]	Algorithmically set the slippage to balance the cost of transaction failure and that of MEV attacks.	-
He-HTLC [73] and Rapidash [17]	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.	-

Eden Network [59] 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 [23] it allows users to submit bundles faster than going through the Flashbots relay, by providing a direct channel to their mining nodes.

Trust assumptions. The relay is trusted for ensuring privacy and transaction ordering.

3.1.2 Post-Merge MEV auction platforms. In future versions of Ethereum, MEV auctions will see native support in the form of enshrined Proposer-Builder Separation (PBS) [20]. Enshrined 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 enshrined PBS is implemented, MEV-Boost [29] 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 instead of the block content.

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 [8, 11].

Trust assumptions. Users pick a builder to use (or become a builder) and fully trust it, including the relay it chooses.

3.1.3 Private channels. Given the complexity of sending bundles, most MEV auction platforms offer a simplified service called *private channels* for users who typically have no need to send bundles and only want to ensure the privacy of their transactions. This service is accessible via RPC endpoints, making it easy to use, as users can simply add these endpoints to their wallets. Every transaction sent from the wallet is sent directly to the block builder through private channels, bypassing mempools and thereby ensuring privacy. Examples include Flashbots Protect [28], Ethermine RPC [23] (which stopped operation after the Merge), Eden Network RPC [54], and bloXroute ETH Protect [10].

Trust assumptions. The services are fully trusted for privacy.

3.1.4 MEV redistribution. Different from the above solutions that ensure full privacy, the idea of MEV redistribution is that users can selectively share transaction information with searchers, allow searchers to backrun immediately after users' transactions, and capture a portion of the MEV generated as a return (kickback).

To receive a kickback, a user needs to submit a transaction to an intermediate service provided by MEV auction platforms and disclose transaction information. The user's transaction creates an MEV opportunity, such as price differences necessary for arbitrage. Based on the disclosed information, a searcher can propose an arbitrage transaction to extract MEV from this opportunity. The service matches the user's transaction with the searcher's transaction as a bundle and sends it to a block builder. Finally, the service ensures that the builder sends a portion of the MEV from the received bundle as a kickback to the user. Examples include MEV-Share [53], MEV Blocker [18], and BloXroute BackRunMe [9].

Trust assumptions. The services are fully trusted for sharing privacy and matching transactions.

3.2 Time-based Ordering Properties

Drastically different from MEV auction platforms, the second category of solutions in Tab. 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 [38]. 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 [37] achieves the same fairness as Aequitas [38], but with stronger liveness and less communication complexity. κ-differential-order-fairness achieved by Quick-Fairness [14] can also be treated as a reparameterization of batch-order-fairness as claimed in [37]. Tab. 1 presents the technical definitions more precisely.

Chainlink Fair Sequencing Service (FSS) [36] plans to use a receive-order fairness protocol such as Aequitas [38].

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[41] (also known as Vega [72]) 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 [85] proposes a similar notion called ordering-linearizability. Indeed, [37] shows 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 [4] assigns every transaction a fair timestamp, which is the median of the time each node claims to have first received it. However, [38] 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 [35] and casual ordering [65]) 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 supermajority). 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 [68], Osmosis [1], and Shutter Network [67] are systems that integrate threshold encryption to Ethereum (and potentially other blockchains). Meanwhile, Fino[47] proposes a way to efficiently integrate threshold encryption and secret sharing with DAG-based BFT protocol. F3B [84] uses a secret-management committee to store encryption keys so that when the underlying consensus layer has committed the transaction, its content will be later revealed by a decentralized secret-management committee.

We use (a simplified description of) Shutter Network [67] 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 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 [39], 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 [66].

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 [50], and upcoming (and potentially better) implementations include Keystone [43], and Nvidia H100 GPU [56]. 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. However, a caveat is that TEEs do not guarantee availability. Care must be taken to ensure the liveness of TEE-based protocols.

Tesseract [7] 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.

3.4.1 Batch auction. Frequent Batch Auctions (FBAs) [12] 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 [62] and FairTraDEX [51] 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.

3.4.2 Verifiable sequencing rules. [82] initiates the study of verifiable sequencing rules that constrain the valid execution orderings miners should respect, which are efficiently and publicly verifiable for users. A concrete example is the greedy sequencing rule [44, 82], which greedily balances the DEX liquidity pool by ordering transactions back and forth around the initial state. This rule structurally inhibits the feasibility of sandwich attacks.

3.4.3 Publicly verifiable multi-party computation. P2DEX [5] proposes a decentralized exchange construction using publicly verifiable multi-party computation where orders are matched privately

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.	Yes and No. Facilitating MEV extraction so non-miners can also extract MEV but the current system relies on centralized services.
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 may introduce 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.

via MPC servers, and misbehavior can be identified by publicly verifiable proofs and punished.

3.4.4 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) [87], by combining multiple AMMs, A^2MM [86] 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.

3.4.5 Optimal slippage setting. To use AMMs, users set a slippage to tolerate unexpected price movements. Using a low slippage runs 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). [34] 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 Sec. 2, we defined four problems that MEV may cause. Next, we will discuss in detail whether different MEV countermeasures can effectively address these problems. The results are summarized in Tab. 2.

Preventing user loss. All approaches can (partly) reduce user loss. On the one hand, users can use MEV auction platforms to protect their transactions and reduce their losses. On the other hand, attackers also use MEV auction platforms to perform MEV activities, which results in losses for users. Both time-based ordering properties and content-agnostic ordering can prevent user loss by preventing ex-post order manipulation. However, for content-agnostic ordering, metadata leakage blind frontrunning is still possible to result in user loss. MEV-aware application design can prevent user loss when users use specific given applications.

Reducing inefficiency due to lack of coordination. Off-chain auctions of MEV auction platforms make competition for MEV opportunities more efficient and reduce network congestion caused by priority gas auction (PGA). Time-based ordering properties can prevent an on-chain bidding war; however, using a first-come-first-served sequencing policy may introduce an off-chain latency war [48]. This issue may need to be further addressed through geographical decentralization [58] or an improved sequencing policy [48]. Whether content-agnostic ordering can improve efficiency depends on the ordering mechanism, it does in most cases, but an on-chain bidding war is possible if transactions are ordered by fees. MEV-aware application design reduces inefficiency by eliminating MEV for given applications.

Reducing consensus destabilizing risk. Since the idea of MEV auction platforms is making the best of MEV rather than reducing MEV, MEV is still present in blocks and consensus destabilizing risk still exists. Other approaches prevent MEV, thereby reducing consensus destabilizing risk.

Reducing centralization. MEV auction platforms democratize MEV extraction by allowing a broader range of participants beyond centralized miners to partake in the process, thereby reducing centralization to some extent. Furthermore, PBS enhances validator decentralization by outsourcing MEV extraction to specialized builders [13]. However, current MEV auction platforms still rely on centralized services, and block-building remains a centralized process [74]. MEV-aware applications also only partially address this problem by removing the ordering privilege from miners for specific applications. Both time-based ordering properties and content-agnostic ordering remove the ordering privilege from miners, whereas protocol-specific trust assumptions (e.g., a permissioned committee) may reduce decentralization.

4 Related Works

SoKs on related topics. Eskandari et al. [22] 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. [6] 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 Tab. 1. Heimbach et al. [35] focus on categorizing transaction reordering manipulation mitigation schemes and analyzing the strengths and weaknesses of each mitigation scheme with a qualitative approach. Our work further examines whether different MEV mitigations can protect users from losses and contribute to consensus stability.

MEV and MEV auction platforms are also important topics in SoK papers on DeFi, though not their main focus. Werner et al. [80] discuss MEV in the context of DeFi. Zhou et al. [88] modeled MEV auction platforms as a key component in the network layer to evaluate and compare real-world DeFi attacks. MEV is also considered a security concern in AMM-based DEX evaluations [83].

Study on MEV auction platforms. Among the four categories of MEV countermeasures, MEV auction platforms are the most popular in practice. Therefore, multiple works studied MEV auction platforms and the related private transactions in MEV auction platforms. Qin et al. [64] collected privately mined transactions before the emergence of MEV auction platforms. Their analysis focused on mining pools' engagement in privately mining transactions. Piet et al. [60] 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 and 65.9% of MEV profits are made by miners. Capponi et al. [15] drew a similar conclusion through a game theoretic analysis with empirical data support. However, it is unclear if these conclusions remain robust after the Merge, given the changes in MEV auction platforms. Weintraub et al. [79] compared MEV extraction before and after the introduction of Flashbots. They show that Flashbots disproportionately benefit miners at the expense of non-miners (i.e., searchers). Lyu et al. [46] analyzed private transactions on their characteristics, transaction costs, miner profits, and security impacts.

These works focus on the implications of pre-Merge MEV auction platforms, and their findings are consistent with Tab. 2: both users and MEV searchers can leverage MEV auction platforms, complicating efforts to mitigate user losses.

Post-Merge MEV auction platforms. Heimbach et al. examined the MEV-Boost ecosystem, and their findings showed significant centralization among the builders and relays in the current landscape [33]. A similar study conducted by [76] also confirmed the centralization among the builders and relays. Moreover, multiple dashboards [31, 42, 74] provide dynamic insights into the ecosystem's centralization trends through real-time PBS analytics. The findings of these works align with Tab. 2, indicating that the centralization problem still exists in the current MEV auction platforms and needs to be addressed by the community.

Quantifying MEV. A reasonable approach to evaluating user losses caused by MEV is quantifying the total revenue generated from MEV activities. Analyzing blockchain to identify and quantify MEV began with the original MEV paper [19], followed by improved techniques for identifying and quantifying MEV [15, 46, 60, 64, 69, 77, 79]. Besides, online dashboards [21, 27, 45, 61] provide real-time MEV analytics. In this paper, we focus on solutions to mitigate the negative effects of MEV rather than accurate quantification.

5 Discussion and Future Works

Legal implications of MEV. MEV auction platforms' involvement in enforcing the Office of Foreign Assets Control (OFAC) sanctions against Tornado Cash [71] raises interesting legal questions. Wahrstätter et al. examined the effectiveness of MEV auction platforms' enforcement of OFAC sanctions [75], and further research could explore the legal implications of OFAC violations in decentralized systems.

Cross-domain MEV. MEV extraction is possible across multiple blockchains, Layer 2 systems, and exchanges (on-chain or off-chain). [57] initiated the research on formalizing *cross-domain* MEV. However, understanding and mitigating cross-domain MEV largely remains an open problem.

Alternative PBS designs. As discussed in Sec. 3.1, current PBS implementation still depends on trusted third-party relays, and any vulnerabilities in these relays can severely impact security. For instance, on April 3rd, 2023, a malicious proposer exploited a vulnerability in a relay, resulting in the theft of about $25 million from multiple MEV searchers [52].

The enshrined PBS aims to eliminate trust requirements by implementing PBS at the consensus level [20]. Although this proposal can mitigate the centralization issue of MEV-Boost relays, it does not address the consensus destabilizing risk. An alternative design is execution tickets [55], which involves selling the right to build blocks through a lottery rather than an auction. This design can remove MEV from the consensus layer, thereby shielding decentralized validators from the implications of MEV. However, the community has yet to determine the optimal alternative PBS design, leaving opportunities for researchers to propose innovative designs to reduce the negative effects of MEV.

6 Conclusion

In this paper, we identified four primary security implications caused by MEV, including user loss, inefficiency, consensus destabilizing risk, and centralizing force. Our review of 32 projects and papers proposing MEV countermeasures led to the creation of a comprehensive taxonomy, which categorizes these countermeasures into four schemes: MEV auction platforms, time-based ordering properties, content-agnostic ordering, and MEV-aware application design. We compared these schemes in terms of their goals, technical details, and trust assumptions, and discussed how each addresses the identified security implications. Notably, no single MEV countermeasure effectively mitigates all security implications, highlighting the ongoing need for innovation in MEV mitigation.

Acknowledgements

This work is in part supported by an Ethereum Academic Grant FY22-0649.

References

[1] atom_crypto. 2022. The MEV Game of the Crypto Economy: Osmosis' Threshold Encryption vs. SGX of Flashbot? https://mirror.xyz/infinet.eth/SFjR1H1-RMnKoIoPjqkxpauVPrLYGqLHQP1dY9FHvx4. Accessed: 2024-07-13.

[2] Kushal Babel, Philip Daian, Mahimna Kelkar, and Ari Juels. 2023. Clockwork Finance: Automated Analysis of Economic Security in Smart Contracts. In *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE.

[3] Kushal Babel, Mojan Javaheripi, Yan Ji, Mahimna Kelkar, Farinaz Koushanfar, and Ari Juels. 2023. Lanturn: Measuring economic security of smart contracts through adaptive learning. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*. 1212–1226.

[4] Leemon Baird, Atul Luykx, and Paul Madsen. 2022. Hedera Technical Insights: Fair Timestamping and Fair Ordering of Transactions. https://hedera.com/blog/fair-timestamping-and-fair-ordering-of-transactions. Accessed: 2022-11-28.

[5] Carsten Baum, Bernardo David, and Tore Kasper Frederiksen. 2021. P2DEX: privacy-preserving decentralized cryptocurrency exchange. In *International Conference on Applied Cryptography and Network Security*. Springer, 163–194.

[6] Carsten Baum, James Hsin-yu Chiang, Bernardo David, Tore Kasper Frederiksen, and Lorenzo Gentile. 2022. SoK: Mitigation of Front-Running in Decentralized Finance. In *International Conference on Financial Cryptography and Data Security*. 250–271.

[7] Iddo Bentov, Yan Ji, Fan Zhang, Lorenz Breidenbach, Philip Daian, and Ari Juels. 2019. Tesseract: Real-Time Cryptocurrency Exchange Using Trusted Hardware. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 1521–1538.

[8] bloXroute. 2024. List of bloXroute Builders. https://docs.bloxroute.com/apis/mev-solution/list-of-bloxroute-builders. Accessed: 2024-09-06.

[9] bloXroute Labs. 2023. Introduction to BackRunMe. https://docs.bloxroute.com/introduction/backrunme. Accessed: 2024-07-13.

[10] bloXroute Labs. 2024. ETH Protect RPC. https://docs.bloxroute.com/introduction/protect-rpcs/eth-protect-rpc. Accessed: 2024-07-13.

[11] bloXroute Labs. 2024. MEV Relay for Validators. https://docs.bloxroute.com/apis/mev-solution/mev-relay-for-validators. Accessed: 2024-07-14.

[12] Eric Budish, Peter Cramton, and John Shim. 2015. The High-Frequency Trading Arms Race: Frequent Batch Auctions as a Market Design Response. *The Quarterly Journal of Economics* 130, 4 (2015), 1547–1621.

[13] Vitalik Buterin. 2021. Proposer/block builder separation friendly fee market designs. https://ethresear.ch/t/proposer-block-builder-separation-friendly-fee-market-designs/9725. Accessed: 2024-07-13.

[14] Christian Cachin, Jovana Mićić, Nathalie Steinhauer, and Luca Zanolini. 2022. Quick Order Fairness. In *International Conference on Financial Cryptography and Data Security*. Springer, 316–333.

[15] Agostino Capponi, Ruizhe Jia, and Ye Wang. 2022. The Evolution of Blockchain: from Lit to Dark. *arXiv preprint arXiv:2202.05779* (2022).

[16] Miles Carlsten, Harry Kalodner, S Matthew Weinberg, and Arvind Narayanan. 2016. On the Instability of Bitcoin Without the Block Reward. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. 154–167.

[17] Hao Chung, Elisaweta Masserova, Elaine Shi, and Sri AravindaKrishnan Thyagarajan. 2022. Rapidash: Foundations of side-contract-resilient fair exchange. *Cryptology ePrint Archive* (2022).

[18] CoW Protocol. 2024. MEV Blocker: The Best MEV Protection Under the Sun. https://cow.fi/mev-blocker. Accessed: 2024-07-12.

[19] Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels. 2020. Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 910–927.

[20] Francesco D'Amato, Barnabé Monnot, Michael Neuder, Potuz, and Terence Tsao. 2024. EIP-7732: Enshrined Proposer-Builder Separation [DRAFT]. *Ethereum Improvement Proposals* 7732 (June 2024). https://eips.ethereum.org/EIPS/eip-7732.

[21] EigenPhi. 2024. EigenPhi. https://eigenphi.io/. Accessed: 2024-07-13.

[22] Shayan Eskandari, Seyedehmahsa Moosavi, and Jeremy Clark. 2019. SoK: Transparent Dishonesty: front-running attacks on Blockchain. In *International Conference on Financial Cryptography and Data Security*. Springer, 170–189.

[23] Ethermine. 2022. Ethermine MEV-Relay. https://ethermine.org/mev-relay. Accessed: 2022-10-09.

[24] Ester Félez-Viñas, Luke Johnson, and Tālis J Putniņš. 2022. Insider Trading in Cryptocurrency Markets. *Available at SSRN 4184367* (2022).

[25] Flashbots. 2022. Flashbots Auction Overview. https://docs.flashbots.net/flashbots-auction/overview. Accessed: 2022-11-14.

[26] Flashbots. 2024. Flashbots Documentation. https://docs.flashbots.net/. Accessed: 2024-07-13.

[27] Flashbots. 2024. Flashbots Explore. https://explore.flashbots.net/. Accessed: 2024-07-13.

[28] Flashbots. 2024. Flashbots Protect Overview. https://docs.flashbots.net/flashbots-protect/overview. Accessed: 2024-07-13.

[29] Flashbots. 2024. MEV-Boost. https://github.com/flashbots/mev-boost. Accessed: 2024-07-13.

[30] Ethereum Foundation. 2024. Ethereum Roadmap: The Merge. https://ethereum.org/en/roadmap/merge/. Accessed: 2024-07-13.

[31] Chris Hager. 2024. RelayScan. https://www.relayscan.io/. Accessed: 2024-07-14.

[32] Hasu and Stephane Gosselin. 2022. Why Run MEV-Boost? https://writings.flashbots.net/why-run-mevboost. Accessed: 2024-07-13.

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

[34] Lioba Heimbach and Roger Wattenhofer. 2022. Eliminating Sandwich Attacks with the Help of Game Theory. In *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*. 153–167.

[35] Lioba Heimbach and Roger Wattenhofer. 2022. SoK: Preventing Transaction Reordering Manipulations in Decentralized Finance. In *Proceedings of the 4th ACM Conference on Advances in Financial Technologies*. 47–60.

[36] Ari Juels, Lorenz Breidenbach, and Florian Tramer. 2020. Fair Sequencing Services: Enabling a Provably Fair DeFi Ecosystem. https://blog.chain.link/chainlink-fair-sequencing-services-enabling-a-provably-fair-defi-ecosystem/. Accessed: 2022-10-05.

[37] Mahimna Kelkar, Soubhik Deb, Sishan Long, Ari Juels, and Sreeram Kannan. 2023. Themis: Fast, strong order-fairness in byzantine consensus. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*. 475–489.

[38] Mahimna Kelkar, Fan Zhang, Steven Goldfeder, and Ari Juels. 2020. Order-Fairness for Byzantine Consensus. In *Annual International Cryptology Conference*. Springer, 451–480.

[39] Rami Khalil, Arthur Gervais, and Guillaume Felley. 2019. TEX - A Securely Scalable Trustless Exchange. *Cryptology ePrint Archive* (2019).

[40] Kshitij Kulkarni, Theo Diamandis, and Tarun Chitra. 2022. Towards a Theory of Maximal Extractable Value I: Constant Function Market Makers. *arXiv preprint arXiv:2207.11835* (2022).

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

[42] Rated Labs. 2024. Rated | Ethereum Mainnet Explorer. https://explorer.rated.network/network?network=mainnet Accessed: 2024-07-14.

[43] Dayeol Lee, David Kohlbrenner, Shweta Shinde, Krste Asanovic, and Dawn Song. 2020. Keystone: An Open Framework for Architecting Trusted Execution Environments. In *Proceedings of the Fifteenth European Conference on Computer Systems (EuroSys'20)*.

[44] Yuhao Li, Mengqian Zhang, Jichen Li, Elynn Chen, Xi Chen, and Xiaotie Deng. 2023. MEV Makes Everyone Happy under Greedy Sequencing Rule. In *Proceedings of the 2023 Workshop on Decentralized Finance and Security*. 9–15.

[45] LibMEV. 2024. LibMEV Leaderboard. https://libmev.com/leaderboard. Accessed: 2024-07-12.

[46] Xingyu Lyu, Mengya Zhang, Xiaokuan Zhang, Jianyu Niu, Yinqian Zhang, and Zhiqiang Lin. 2022. An Empirical Study on Ethereum Private Transactions and the Security Implications. *arXiv preprint arXiv:2208.02858* (2022).

[47] Dahlia Malkhi and Pawel Szalachowski. 2023. Maximal Extractable Value (MEV) Protection on a DAG. In *4th International Conference on Blockchain Economics, Security and Protocols*. 1.

[48] Akaki Mamageishvili, Mahimna Kelkar, Jan Christoph Schlegel, and Edward W Felten. 2023. Buying Time: Latency Racing vs. Bidding for Transaction Ordering. In *5th Conference on Advances in Financial Technologies (AFT 2023)*. Schloss-Dagstuhl-Leibniz Zentrum für Informatik.

[49] Jerry W Markham. 1988. Front-Running–Insider Trading Under the Commodity Exchange Act. *Cath. UL Rev.* 38 (1988), 69.

[50] Frank McKeen, Ilya Alexandrovich, Alex Berenzon, Carlos V Rozas, Hisham Shafi, Vedvyas Shanbhogue, and Uday R Savagaonkar. 2013. Innovative instructions and software model for isolated execution. *Hasp@ isca* 10, 1 (2013).

[51] Conor McMenamin, Vanesa Daza, Matthias Fitzi, and Padraic O'Donoghue. 2022. FairTraDEX: A Decentralised Exchange Preventing Value Extraction. In *Proceedings of the 2022 ACM CCS Workshop on Decentralized Finance and Security*. 39–46.

[52] Robert Miller. 2023. Post Mortem: April 3rd, 2023 MEV-Boost Relay Incident and Related Timing Issue. https://collective.flashbots.net/t/post-mortem-april-3rd-2023-mev-boost-relay-incident-and-related-timing-issue/1540. Accessed: 2024-07-14.

[53] Robert Miller. 2024. MEV-Share: Programmably Private Orderflow to Share MEV with Users. https://collective.flashbots.net/t/mev-share-programmably-private-orderflow-to-share-mev-with-users/1264. Accessed: 2024-07-13.

[54] Eden Network. 2024. Eden Network RPC. https://rpc.edennetwork.io/. Accessed: 2024-07-13.

[55] Mike Neuder. 2023. Execution Tickets. https://ethresear.ch/t/execution-tickets/17944 Accessed: 2024-07-06.

[56] NVIDIA. 2024. Confidential Computing. https://www.nvidia.com/en-us/data-center/solutions/confidential-computing/. Accessed: 2024-07-13.

[57] Alexandre Obadia, Alejo Salles, Lakshman Sankar, Tarun Chitra, Vaibhav Chellani, and Philip Daian. 2021. Unity is Strength: A Formalization of Cross-Domain

Maximal Extractable Value. *arXiv preprint arXiv:2112.01472* (2021).
[58] Philip Daian. 2023. Decentralized Crypto Needs You to Be a Geographical Decentralization Maxi. https://collective.flashbots.net/t/decentralized-crypto-needs-you-to-be-a-geographical-decentralization-maxi/1385 Accessed: 2024-09-10.
[59] Chris Piatt, Jeffrey Quesnelle, and Caleb Sheridan. 2021. EDEN Network Whitepaper. https://edennetwork.io/EDEN_Network___Whitepaper___2021_07.pdf. Accessed: 2022-10-06.
[60] Julien Piet, Jaiden Fairoze, and Nicholas Weaver. 2022. Extracting Godl [sic] from the Salt Mines: Ethereum Miners Extracting Value. In *Workshop on the Economics of Information Security*.
[61] Pmcgoohan. 2022. data and technical | zeromev. https://info.zeromev.org/technical.html. Accessed: 2024-07-12.
[62] CoW Protocol. 2024. CoW Swap. https://swap.cow.fi/. Accessed: 2024-07-13.
[63] Kaihua Qin, Liyi Zhou, Pablo Gamito, Philipp Jovanovic, and Arthur Gervais. 2021. An Empirical Study of DeFi Liquidations: Incentives, Risks, and Instabilities. In *Proceedings of the 21st ACM Internet Measurement Conference*. 336–350.
[64] Kaihua Qin, Liyi Zhou, and Arthur Gervais. 2022. Quantifying blockchain extractable value: How dark is the forest?. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 198–214.
[65] Michael K Reiter and Kenneth P Birman. 1994. How to securely replicate services. *ACM Transactions on Programming Languages and Systems (TOPLAS)* 16, 3 (1994), 986–1009.
[66] Kineret Segal and Tom Brand. 2020. Presenting: VeeDo, a STARK-based VDF Service. https://medium.com/starkware/presenting-veedo-e4bbff77c7ae. Accessed: 2022-10-09.
[67] Shutter Network. 2024. Shutter Network Blog. https://blog.shutter.network/. Accessed: 2024-07-13.
[68] Sikka inc. 2022. Sikka Projects. https://sikka.tech/projects/. Accessed: 2022-10-06.
[69] Christof Ferreira Torres, Ramiro Camino, et al. 2021. 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)*. 1343–1359.
[70] Itay Tsabary, Matan Yechieli, Alex Manuskin, and Ittay Eyal. 2021. MAD-HTLC: because HTLC is crazy-cheap to attack. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1230–1248.
[71] U.S. Department of the Treasury. 2022. U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash. https://home.treasury.gov/news/press-releases/jy0916. Accessed: 2022-11-15.
[72] Vega. 2022. Vega Protocol: Blockchain derivatives. https://vega.xyz/. Accessed: 2022-10-06.
[73] Sarisht Wadhwa, Jannis Stoeter, Fan Zhang, and Kartik Nayak. 2023. He-HTLC: Revisiting Incentives in HTLC. In *Network and Distributed System Security Symposium (NDSS)*.
[74] Anton Wahrstätter. 2024. MEV Boost Pics. https://mevboost.pics/. Accessed: 2024-07-14.
[75] Anton Wahrstätter, Jens Ernstberger, Aviv Yaish, Liyi Zhou, Kaihua Qin, Taro Tsuchiya, Sebastian Steinhorst, Davor Svetinovic, Nicolas Christin, Mikolaj Barczentewicz, et al. 2024. Blockchain censorship. In *Proceedings of the ACM on Web Conference 2024*. 1632–1643.
[76] Anton Wahrstätter, Liyi Zhou, Kaihua Qin, Davor Svetinovic, and Arthur Gervais. 2023. Time to bribe: Measuring block construction market. *arXiv preprint arXiv:2305.16468* (2023).
[77] Ye Wang, Yan Chen, Haotian Wu, Liyi Zhou, Shuiguang Deng, and Roger Wattenhofer. 2022. Cyclic arbitrage in decentralized exchanges. In *Companion Proceedings of the Web Conference 2022*. 12–19.
[78] Ye Wang, Patrick Zuest, Yaxing Yao, Zhicong Lu, and Roger Wattenhofer. 2022. Impact and User Perception of Sandwich Attacks in the DeFi Ecosystem. In *CHI Conference on Human Factors in Computing Systems*. 1–15.
[79] Ben Weintraub, Christof Ferreira Torres, Cristina Nita-Rotaru, and Radu State. 2022. A Flash(bot) in the Pan: Measuring Maximal Extractable Value in Private Pools. In *Proceedings of the 22nd ACM Internet Measurement Conference (IMC '22)*. Association for Computing Machinery, Nice, France. https://doi.org/10.1145/3517745.3561448
[80] Sam Werner, Daniel Perez, Lewis Gudgeon, Ariah Klages-Mundt, Dominik Harz, and William Knottenbelt. 2022. SoK: Decentralized Finance (DeFi). In *Proceedings of the 4th ACM Conference on Advances in Financial Technologies*. 30–46.
[81] Fredrik Winzer, Benjamin Herd, and Sebastian Faust. 2019. Temporary Censorship Attacks in the Presence of Rational Miners. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 357–366.
[82] Matheus Venturyne Xavier Ferreira and David C Parkes. 2023. Credible decentralized exchange design via verifiable sequencing rules. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*. 723–736.
[83] Jiahua Xu, Krzysztof Paruch, Simon Cousaert, and Yebo Feng. 2023. SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols. *Comput. Surveys* 55, 11 (2023), 1–50.
[84] Haoqian Zhang, Louis-Henri Merino, Vero Estrada-Galinanes, and Bryan Ford. 2022. Flash Freezing Flash Boys: Countering Blockchain Front-Running. In *The Workshop on Decentralized Internet, Networks, Protocols, and Systems (DINPS)*.
[85] Yunhao Zhang, Srinath Setty, Qi Chen, Lidong Zhou, and Lorenzo Alvisi. 2020. Byzantine Ordered Consensus without Byzantine Oligarchy. In *14th USENIX Symposium on Operating Systems Design and Implementation (OSDI 20)*. 633–649.
[86] Liyi Zhou, Kaihua Qin, and Arthur Gervais. 2021. A2MM: Mitigating Frontrunning, Transaction Reordering and Consensus Instability in Decentralized Exchanges. *arXiv preprint arXiv:2106.07371* (2021).
[87] Liyi Zhou, Kaihua Qin, Christof Ferreira Torres, Duc V Le, and Arthur Gervais. 2021. High-Frequency Trading on Decentralized On-Chain Exchanges. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 428–445.
[88] Liyi Zhou, Xihan Xiong, Jens Ernstberger, Stefanos Chaliasos, Zhipeng Wang, Ye Wang, Kaihua Qin, Roger Wattenhofer, Dawn Song, and Arthur Gervais. 2023. SoK: Decentralized Finance (DeFi) Attacks. In *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2444–2461.