Electronic Markets (2024) 34:49
https://doi.org/10.1007/s12525-024-00727-x

RESEARCH PAPER

Maximal extractable value: Current understanding, categorization, and open research questions

Vincent Gramlich[1] · Dennis Jelito[2] · Johannes Sedlmeir[3]

Received: 28 February 2024 / Accepted: 5 August 2024

Abstract

In traditional financial markets, front-running is a well-structured phenomenon. It represents a form of privileged actors utilizing knowledge or power advantages to extract undue profit at the cost of other stakeholders. Various mitigation strategies have emerged, ranging from market design to regulatory measures. More recently, a similar and substantially richer variety of means to gain unethical profit from power asymmetries has appeared in the context of blockchain-based decentralized applications. This phenomenon is called "maximal extractable value" (MEV). Despite the decentralized nature and inherent transparency of blockchain ledgers, MEV is particularly prevalent and challenging to mitigate. While related work in computer science and algorithmic game theory has already identified several different ways in which MEV manifests in decentralized finance (DeFi) and outlined partial solution approaches, a discussion of its impacts in the information systems (IS) domain is still absent. A holistic definition of MEV and how it can be exploited is necessary for the discussion of its potential implications for blockchain-based IS for businesses and public institutions. This paper conducts a systematic literature review to close this gap. It consolidates the diverging definitions of MEV and provides a categorization of the different ways in which it can manifest. As such, we synthesize and review the existing state of knowledge on MEV and point to undiscovered areas relevant to decentralized electronic markets in the form of a research agenda.

Keywords Blockchain · Decentralization · DeFi · Front-running · MEV · Sandwich attack

JEL Classifications G15 · G18 · G23 · K20 · O33

Introduction

Access to information has long been known to be a key determinant for the proper functioning of markets (Arrow, 1963). While information asymmetries are a natural consequence of the specialization happening in competition (Stiglitz, 2002), they can also have a plethora of harmful effects. For instance, information asymmetries can lead to market failures through adverse selection in the "market for lemons" (Akerlof, 1970), introduce moral hazard (Stiglitz, 1983), and inhibit Pareto efficiency in general (Winseck, 2002; Hartwich et al., 2023). In financial markets, such as stock markets, knowledge advantages over rivals can be exploited by privileged players (e.g., brokers) in the form of insider trading and front-running. Insider trading refers to buying or selling financial instruments based on material, non-public information (Leland, 1992). Front-running, on the other hand, describes knowledge advantages about upcoming transactions and the power to create own transactions and decide on or influence their relative positioning (e.g., shorting an asset before a trade that drives its price down substantially or longing it when the next trade will drive the price up) (Röell, 1990). To mitigate these negative implications of information and power asymmetries,

Responsible Editor: Gabriele D'Angelo

✉ Vincent Gramlich
vincent.gramlich@fit.fraunhofer.de

Dennis Jelito
dennis.jelito@possehl-secure.de

Johannes Sedlmeir
johannes.sedlmeir@uni.lu

[1] Branch Business Information Systems Engineering, Fraunhofer FIT, Bayreuth, Germany

[2] University of Bayreuth, Bayreuth, Germany

[3] SnT - Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg, Luxembourg

Published online: 03 October 2024

different countermeasures, including market design, reputation mechanisms, and legal measures, have been proposed and deployed (Eskandari et al., 2020; Heimbach and Wattenhofer, 2022; Zhou et al., 2021).

The digital transformation has substantially accelerated many economic interactions. Consequently, it has also reduced the time scales at which information and power asymmetries can be exploited and increased the potential for harmful behavior. For instance, while digital trading platforms technically grant each user non-discriminatory access to system information and transaction processing, small discrepancies can arise in the speed at which transaction requests can be submitted (Hartwich et al., 2023). Because of the corresponding opportunities to profit when new information is available, there are now arms races for nanosecond latency advantages in information acquisition, processing, or delivery. This phenomenon manifests in inefficient resource allocation through sometimes enormous investments in parallel processing and minimizing network latencies, e.g., by reducing the physical distance or building straight fiber-optic cables between stakeholders' servers and those of the exchanges (MacKenzie, 2021; Ye et al., 2013; Levens, 2015). In response, novel designs for electronic markets that are less time-sensitive, such as frequent batch auctions (Budish et al., 2015), have been proposed.

Following the advent of bitcoin and the corresponding blockchain technology in 2009 (Nakamoto, 2009), a new form of electronic markets has emerged. The system of blockchain-based financial applications—also known as decentralized finance (DeFi) (Gramlich et al., 2023)—has at times exceeded $ 180 B in total value locked (DeFiLlama, 2024). While blockchain ledgers are by design decentralized and transparent, a closer look reveals that there are nevertheless many natural appearances of power and information asymmetries (Sedlmeir et al., 2022). More specifically, power asymmetries appear during the ledger synchronization process, which relies on pseudonymous short-time monopolists in the form of block proposers that decide on which transactions from a transparent pool of queued transactions to include (Schwarz-Schilling et al., 2023; Chitra, 2023; Bonneau et al., 2015). As a consequence, the block proposer not only has a short-term information advantage regarding the future blockchain state: When block proposers are known ahead of time, clients can also submit transactions only to them and bribe them to not forward them to the mempool.

Owing to the lack of central authorities to pursue effective legal actions in permissionless blockchains, there are also hardly any effective means to enforce countermeasures against abuses of these knowledge and power advantages. This exposure of blockchain-based applications to front-running was already anticipated by the algorithmic trader pmcgoohan in 2014, one year before Ethereum as the earliest and largest blockchain for broad financial applications was launched (pmcgoohan, 2021). Thus far, research has demonstrated that abuses of power and information asymmetries on blockchains are much broader than in centralized systems, comprising more than just front-running and also affecting multiple stakeholder groups. The phenomenon of corresponding opportunities for value extraction has been summarized under the umbrella term *maximal extractable value (MEV)* (Daian et al., 2020). The original definition describes the additional profits block proposers ("miners") can make through their short-term monopoly for block production, allowing them to decide on the selection of transactions to be included and their order (Chitra, 2023; Schwarz-Schilling et al., 2023). The impact of MEV was found to frequently be detrimental to DeFi users, with a value extracted from hundred thousands or even millions of transactions exceeding $ 500 M just on Ethereum until the Merge, i.e., its switch from proof-of-work (PoW) to proof-of-stake (PoS), in September 2022 (Qin et al., 2022; Chi et al., 2024) and over 500,000 ETH (equivalent to over $ 1 B) since that date (Chi et al., 2024; Flashbots, 2024). Besides the financial disadvantage for users, MEV can also worsen the functionality of the underlying blockchain infrastructure, as MEV can incentivize nodes to engage in active attempts to ignore and overwrite previously published blocks ("re-orgs") to maximize their revenues, thus reducing security guarantees (Daian et al., 2020; Pillai, 2023; Obadia et al., 2021), or to withhold blocks as long as possible, thus increasing latency (Öz et al., 2023).

Owing to its relevance in DeFi and its connection to both economic market design and technical design questions, MEV has attracted many researchers in computer science and algorithmic game theory. Within the IS literature, the only short mentions of MEV we found in our search process spanning a variety of databases and a broad search string (see Section "Research approach") are in the context of cryptocurrency market manipulation (Eigelshoven et al., 2021), attacks on decentralized finance (Meyer et al., 2022), and problematic phenomena ("violations") in digital assets markets (Clapham et al., 2023). Front-running is also only briefly mentioned in the systematic review of centralized and decentralized exchanges by Hägele (2024). Potential impacts of MEV on blockchain-based applications beyond DeFi in the IS discourse, such as institutional financial contract execution (Egelund-Müller et al., 2017), intellectual property rights management (Gürkaynak et al., 2018), decentralized markets for (green) electricity and renewable energy sources (Alt and Wende, 2020; Tsao and Thanh, 2021), supply chain and trade finance (Jensen T. et al., 2019), or secondary markets for event ticketing (Regner et al., 2019), have not been discussed in previous research that proposed or analyzed such solutions. Thus, we posit that previous IS research on decentralized applications and, in particular, blockchain-based electronic markets has not yet grasped the breadth, relevance, and potential implications of MEV. Specifically in design-oriented research that proposes blockchain-based IS for organizations acting in regulated environments, it is imperative to not only consider potential technical attack vectors (e.g., on the consensus or smart contract layers) but also corresponding economic incentives and potentials for misaligned incentives and fraud, as in the case of MEV. As such, the goal of this work is to summarize and review the existing state of knowledge on MEV and to point to empty spots on the research map to meet the increasing demand for knowledge. More specifically, we pose the following research questions:

1. *What is the current, common understanding and definition of MEV, and which aspects are ambiguous?*
2. *What are the underlying categories of MEV-related attack vectors, and what are exemplary applications vulnerable to the different categories?*

This paper aims to close this research gap by conducting a systematic literature review (SLR) following the guidelines of Webster and Watson (2002). As such, it structures current knowledge by consolidating definitions and key characteristics observed in the DeFi literature and generalizes them in the context of blockchain-based decentralized applications. In this light, we call for greater awareness and understanding of MEV in designing and evaluating blockchain-based IS, considering MEV implications early in the design process of related applications and developing effective mitigation strategies. In Section "Background", we cover the prerequisites to understand why MEV emerges in blockchains and impacts decentralized applications. In Section "Research approach", we describe how we conducted our SLR. Thereafter, we answer the research questions by extracting a holistic definition of MEV (Section "Defining maximal extractable value") from the references we identified in our SLR and structuring the different ways in which it can manifest (Section "Defining maximal extractable value"). We discuss our results in the light of MEV mitigation measures and their limitations in Section "Discussion: different perspectives on MEV countermeasures", give an overview of open research questions in Section "Open research questions", and conclude in Section "Conclusion".

Background

Blockchains and smart contracts

Blockchains are distributed and synchronized systems of computers ("nodes") keeping a synchronized append-only record of transactions ("ledger") (Butijn et al., 2020). For efficiency reasons (e.g., to track current balances when transactions only include transaction amounts), nodes usually also maintain an additional database ("state") that is updated deterministically whenever a new batch of transactions ("block") is added (Butijn et al., 2020). A decentralized agreement ("consensus") mechanism ensures that honest nodes have consistent (non-contradictory) ledgers (and, therefore, states) by incentivizing them to behave in a desirable manner. In permissionless blockchains that do not restrict participation in consensus, incentives manifest in certain payments in the blockchain's native cryptocurrency to the proposer of a block (Aune et al., 2017; Qin et al., 2022; Varun et al., 2022; Capretto et al., 2022). A node's probability of being allowed to contribute the next block in permissionless blockchains is usually proportional to their provable investment into a scarce resource, such as processing power in PoW or the native crypto asset in PoS (Piet et al., 2022; Rieger et al., 2022).

Transactions are typically created and digitally signed by users before they are submitted to a certain node, which—potentially after validation—initiates the distribution of this transaction to all blockchain nodes via a peer-to-peer gossip protocol (Butijn et al., 2020). A subset of these pending (i.e., not yet confirmed in the ledger) transactions in what is called the "mempool" are then included into blocks by a consensus participant ("'miner," "validator," or "block proposer"), who, in turn, is determined by the consensus mechanism. Because the data- and computation-related space in a block is limited (Torres et al., 2021), users not only pay for a transaction's execution costs that depend on the size and computational complexity of their transaction but also include a priority fee ("tip") for the block proposer as an incentive to prioritize its inclusion in a block (Aune et al., 2017; Spain et al., 2020; Varun et al., 2022; Qin et al., 2022; Heimbach and Wattenhofer, 2022; Spain et al., 2020; Zhou et al., 2021).

"Smart contracts" allow users to not only perform simple payments in transactions but also to upload any deterministic program to a blockchain that exposes certain functionalities, and to interact with such programs. In particular, smart contracts allow the generalization of tradable assets from units of the native cryptocurrency underlying public permissionless blockchains' consensus mechanisms to "tokens," i.e., any objects obeying customizable rules as long as they allow for the digital representation of ownership relations on a blockchain (Sunyaev et al., 2021; Hartwich et al., 2022). Corresponding decentralized applications (DApps) (Bünz et al., 2020; Sariboz et al., 2022; Spain et al., 2020; Varun et al., 2022; Kursawe, 2021) have already created an alternative financial ecosystem called decentralized finance (DeFi) that makes traditional financial services possible without established trusted intermediaries (Qin et al., 2022; Gramlich et al., 2023; Govindarajan et al., 2022). One widely used application of smart contracts are decentralized exchanges (DEXes), which allow trading tokens without a trusted intermediary.

Instead, trading happens directly against inquiries created by other participants to a smart contract-managed decentralized order book or via direct interaction with a shared reserve of liquid tradable assets in what is called automated market makers (AMMs) (Torres et al., 2021; Daian et al., 2020; Hägele, 2024). In the latter case, the trading price is determined based on the ratio of the supply of assets in a pool (Struchkov et al., 2021; Heimbach and Wattenhofer, 2022; Zhou et al., 2021). On many exchanges based on the AMM model, the product of the number of both assets thus remains invariant under every trade (Xue et al., 2022; Heimbach and Wattenhofer, 2022; Zhou et al., 2021; Torres et al., 2021; Qin et al., 2022).

In the context of AMMs, arbitrage trading is relevant not only for creating profits but also indispensable for price discovery (Zhou et al., 2021; Struchkov et al., 2021; Daian et al., 2020): Given a fixed ratio between two assets, the market price changes with every token swap (Helmy, 2021), resulting in an imbalance compared to other exchanges that is resolved through arbitrage traders (Qin et al., 2022; Struchkov et al., 2021). The smart contract-based construction of DEXes makes future price changes on these exchanges predictable when observing upcoming transactions in the mempool and, therefore, also opens up the opportunity to make profits.

Another prominent and important DeFi application is lending protocols that facilitate collateralized loans, enabling mutually distrustful parties to lend each other digital assets (tokens) by depositing a collateral with a higher valuation than the borrowed assets (Perez et al., 2021; Heimbach and Wattenhofer, 2023a; Qin et al., 2022). The valuation, in turn, is received from "Oracles," i.e., by querying the state of other smart contracts that provide this information. For instance, an AMM-based Oracle derives the valuation from the current exchange rate on the AMM determined by the supply ratio of the two assets in the liquidity pool. Other Oracles rely on a smart contract that regularly receives updates through transactions submitted by a consortium of partially trustworthy actors (Breidenbach et al., 2021). In cases where the collateral is not sufficient anymore due to price fluctuations and lenders fail to top their deposits up in time, the collateral is offered to arbitrageurs at a (often substantial) discount in what is called liquidations. Consequently, Oracles have frequently been targeted for exploiting lending platforms, either by triggering liquidations or enabling effective undercollateralization (Gramlich et al., 2023). To do so, attackers often leverage "FlashLoans"—uncollateralized, potentially massive (often worth millions of USD) loans that must be paid back within the very transaction where they are taken to drastically increase the amount of capital they can leverage for their attack (Qin et al., 2021).

Front-running and maximal extractable value

The synchronization of the blockchain ledger and, therefore, state that underlies a consensus mechanisms' consistency guarantees implies perfect information symmetry for finalized transactions, i.e., eventually, every honest node will receive the transactions included in other honest nodes' ledgers. Nevertheless, a transaction's full lifecycle before being finalized in the ledger entails substantial power and information asymmetries (Sedlmeir et al., 2022). During the distribution in the mempool via a peer-to-peer (P2P) network, and in the block creation and propagation process, transactions may only be visible to a subset of nodes, and at different times. As such, establishing a direct and low-latency connection to many blockchain nodes may give a block proposer significant knowledge advantages about the transactions pending in the mempool and the current blockchain state, similar to the scenario in centralized systems discussed in Section "Introduction". One straightforward way to utilize such information advantages is front-running. Front-running was generally defined by the US Securities and Exchange Commission (SEC) as an action performed based upon non-public information in order to profit when these predictions come true (Helmy, 2021). Since the mempool is public by default, gaining an advantage in a blockchain system may require only observing and reacting faster than competitors instead of assuming a privileged position (Helmy, 2021; Zhang H et al., 2022; Li et al., 2022; Baum et al., 2021; Kokoris-Kogias et al., 2021; Blackshear et al., 2021).

Independent of the consensus mechanism at hand (e.g., PoW or PoS in permissionless blockchains, or voting-based in permissioned blockchains), block proposers have additional power advantages because they have a (temporary) monopoly of transaction selection and ordering for the block they submit. In other words, while decision-making power regarding transaction confirmation is decentralized in blockchains over long periods with different block proposers, it is centralized in the short term (for each individual block) (Aune et al., 2017; Qin et al., 2022; pmcgoohan, 2021; Torres et al., 2021). Block proposers are in an advantageous position because transaction inclusion and ordering of individual blocks lie in a single block proposer's hand and cannot be controlled by the consensus protocol (Arulprakash and Jebakumar, 2022; Zhou et al., 2021). As such, the block proposer can abuse this power in various ways (Chitra, 2023), e.g., by observing other users' transaction intents and using the gained knowledge to create its own transactions and to include them in favorable spots. Alternatively, proposers can offer favorable placements as a service for a fee—often called "bribing" (Barczentewicz, 2023; Judmayer et al., 2021). This has led to the term of maximal extractable value (MEV), initially coined "miner extractable value," which Daian et al. (2020) introduced to describe the profit block proposers (such as miners in PoW blockchains) can obtain from the strategic inclusion, exclusion, and re-ordering of transactions via the blocks they create and disseminate (pmcgoohan, 2021; Bartoletti et al., 2022). As such, MEV also provides clients with an incentive to bribe block proposers to include their transactions in a certain order and not to forward them in the mempool, which further exacerbates information asymmetries during the ledger synchronization process.

Research approach

This paper aims to create a comprehensive definition of MEV that is thus far absent in the field of MEV research and to convey an understanding of the topic not only for computer scientists and mechanism designers working at the forefront of the field but also to IS researchers that need to understand MEV and its implications on the applications of blockchains beyond DeFi, e.g., in regulated and organizational environments. Although we discuss some regulatory aspects along the way, we do not aim to provide an extensive legal assessment of MEV exploitation. To systematically structure the existing research in this relatively novel field, we conduct a systematic literature following Kitchenham and Charters (2007). This method is well established and has proven effective in systematizing novel research areas for IS researchers in general (Webster and Watson, 2002; Vom Brocke et al., 2015). SLRs have also been applied to related topics in the field of emerging blockchain-based electronic markets, such as tokens (Schwiderowski et al., 2024), DeFi (Gramlich et al., 2023), and cryptocurrency exchanges (Hägele, 2024). Our goal is to capture any articles that contribute to some aspect of our research questions, e.g., literature that implicitly or explicitly formulates a definition or conceptualization of MEV or publications surveying practical manifestations of MEV in blockchain networks. To identify a suitable search string, we extracted keywords and their synonyms associated with MEV from an initial basket of seminal publications on MEV that dominate the discourse (e.g., Daian et al., 2020) and refined them through corresponding forward and backward searches, as well as an unstructured search on Google Scholar. We evaluated every newly obtained term regarding the number of added search results and their inclusion rate. After multiple iterations, we arrived at the following final search string:

> "maximal extractable value" OR
> "miner extractable value" OR
> ("front*running" AND ("decentrali*ed finance" OR "distributed ledger" OR "blockchain" OR "Ethereum"))

The search string consists of two parts, with the first two terms covering historically relevant synonyms for MEV and the remaining terms combining the arguably most prominent manifestation, front-running, with several options for keywords occurring in the context of DeFi. Publications using other synonyms for MEV, such as "blockchain extractable value" (e.g., Qin et al., 2022) and "expected extractable value" (e.g., Judmayer et al., 2021), turned out to be already covered by our search string.

We considered established academic databases for computer science, IS, and economics to reflect the interdisciplinarity of the research area of MEV (Webster and Watson, 2002). We included the databases *Springer Link*, *IEEE Xplore*, *EBSCO Host*, *Web of Science (WoS)*, *ACM Digital Library*, *Science Direct*, *AIS eLibrary*, *Wiley Online Library*, and *Emerald Insight*. Because MEV only started receiving broader attention with the emergence of DeFi and the seminal work by Daian et al. (2020), and articles published in peer-reviewed conference proceedings and journals often face long publication cycles, the number of publications in these venues was relatively limited. One way to tackle this issue and take into account fast-moving, novel research areas is involving preprint databases and practitioner-focused articles in the SLR (Garousi et al. 2019). Therefore, we extended our selection of academic databases by *Google Scholar* and

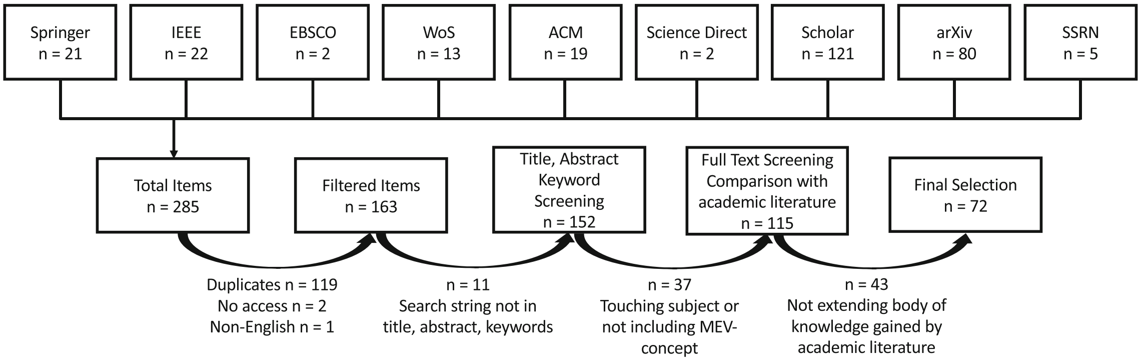
Springer n = 21
IEEE n = 22
EBSCO n = 2
WoS n = 13
ACM n = 19
Science Direct n = 2
Scholar n = 121
arXiv n = 80
SSRN n = 5
Total Items n = 285
Filtered Items n = 163
Title, Abstract Keyword Screening n = 152
Full Text Screening Comparison with academic literature n = 115
Final Selection n = 72
Duplicates n = 119
No access n = 2
Non-English n = 1
n = 11
Search string not in title, abstract, keywords
n = 37
Touching subject or not including MEV-concept
n = 43
Not extending body of knowledge gained by academic literature

Fig. 1 SLR search process and selection steps

the popular preprint servers *arXiv* (computer science focus) and *SSRN* (economics focus).

Our search in abstract, title, and keywords, which we conducted in August 2023, identified 285 publications of potential interest. As Google Scholar yielded an extensive number of results, we adopted the stopping criterion proposed by Butijn et al. (2020) and searched on the first eight pages with 10 entries each and continued the search only if at least half of the results on the previous page remained after applying our exclusion criteria. Searching the databases *AIS eLibrary*, *Wiley Online Library*, and *Emerald Insight* yielded no results. In the next step, we excluded 119 duplicates, two articles with no available full text, and one article not written in English language. We followed the guidelines by Kitchenham and Charters (2007), with two authors iteratively screening the remaining titles, abstracts, and full texts, applying in- and exclusion criteria, and resolving disagreements on papers discussions in the circle of all authors. We included publications that provide a definition or conceptualization of MEV or showcase specific ways in which MEV manifests. On the other hand, we excluded literature items that did not explore MEV or—in the case of non-peer-reviewed publications—did not extend the body of knowledge already gained by academic literature. This left us with a final selection of 72 publications. In the full-text analysis, we utilized MAXQDA (2024) to systematize content extraction and, especially, to code the 35 MEV definitions and the 24 identified different definition fragments within them (see Table 1 and Appendix Table 6) and highlight attack vectors presented in these papers since they are key in answering our research questions. Figure 1 features an overview of the steps in our SLR.

Defining maximal extractable value

Our understanding of MEV, the scope of phenomena associated with it and terminology-related aspects have dynamically evolved, and no consistent definition has emerged thus far (Momeni et al. 2023; Judmayer et al. 2021). To fill this gap and to answer RQ1 by creating a "current, common understanding and definition of MEV," we establish a definition of MEV that is as precise and explicit as possible, comprehensive, and consistent with the majority of definitions that have been proposed in the literature. To pursue this goal, we first screened all papers we selected in our SLR. We found explicit definitions of MEV in 37 out of the 72 literature items. Next, we applied a coding system to disassemble the definitions into individual terms and aspects. Finally, we aggregated the individual terms and aspects by establishing ties and synonyms for our set of final definition fragments based on their roles and our knowledge of the technical foundation of blockchain networks. For instance, we subsumed the roles of "network operators" and "block proposers" under the term "validators." We then performed a quantitative analysis of the extracted definitions and counted the number of times these definition fragments (or their synonyms) appeared in the 37 definitions. Our final definition includes terms exceeding a threshold of 20% among the extracted definitions. Table 1 provides an overview of our quantitative analysis for the definition fragments that exceeded the 20% threshold. A more detailed overview of the full analysis, including the databases corresponding to the publications (Table 4), extracted definitions (Table 5), and the quantitative analysis of all coded definition fragments and the assigned synonyms (Table 6), is included in the Appendix. Based on these results, we propose the following definition of MEV:

Miner or maximal extractable value (MEV) corresponds to the value that can be extracted on a blockchain by miners and other stakeholders at the cost of users by leveraging control of transaction inclusion, exclusion, or ordering in a block.

The definitions present in the current literature showcase several disparities. Some of them can be attributed to historical developments of the blockchain ecosystem, while others suggest profound differences in the understanding of MEV, the actions and actors involved in extracting it, as well as the assessment of its impact and consequences. The first and arguably most obvious difference in the landscape of definition attempts is the choice and the meaning of the MEV acronym itself, which was first introduced by Daian et al. (2020). Initially, i.e., in all publications in our SLR from 2020 and 2021, the phenomenon was unambiguously termed *miner extractable value*. The acronym was first adapted to *maximal extractable value* in 2022 by Piet et al. (2022). This can be attributed to the shift of Ethereum, arguably the first and thus far most relevant DeFi ecosystem, from the PoW consensus mechanism (where blocks are proposed by miners) to the PoS consensus mechanism (in which block proposers are commonly referred to as stakers or validators). To preserve the MEV acronym and at the same time indicate that MEV should comprise all potential sources of value extraction, "miner" was substituted by "maximal." Some more recent publications have further changed the acronym to *blockchain extractable value (BEV)*, continuing the trend toward a more generalized definition that considers additional entities that may play a role in the emergence or exploitation of MEV and covers attacks with growing levels of intricacy (Qin et al., 2022; Heimbach and Wattenhofer, 2023a; Malkhi and Szalachowski, 2022). The following discussion of the other aspects of the definition of MEV illustrates why this generalization may be reasonable but we still stick to the terms "miner" and "maximal" in our definition due to the low number of occurrences of the term BEV in the current body of literature.

Table 1 Detailed analysis of MEV definitions in our literature basket, sorted by publication year

Source	BEV	MEV	Maximal	Miner	Other stakeholders	Blockchain	At the cost of users	Control of transaction in- and exclusion	Control of transaction ordering	In a block
Daian et al. (2020)		x		x					x	
Judmayer et al. (2021)		x		x					x	
Nadahalli et al. (2021)		x		x		x		x		x
Obadia et al. (2021)					x			x	x	x
Perez et al. (2021)		x		x				x	x	x
Züst (2021)		x		x				x	x	x
Zhou et al. (2021)		x		x				x		
Bartoletti et al. (2022)		x		x		x	x		x	
Carranti (2022)		x	x			x		x	x	
Chitra and Kulkarni (2022)		x	x		x			x	x	
Churiwala and Krishnamachari (2022)		x		x	x		x		x	x
Heimbach and Wattenhofer (2022)		x		x				x	x	x
Lyu et al. (2022)		x		x				x	x	
Malkhi and Szalachowski (2022)	x	x	x	x		x				
Mazorra et al. (2022)		x		x				x	x	x
Montiel et al. (2022)		x		x	x		x			
Piet et al. (2022)		x	x	x	x			x	x	x
Poux et al. (2022)		x			x		x			
Qin et al. (2022)	x				x	x				
Sariboz et al. (2022)		x		x					x	
Sekar (2022)		x		x				x	x	x
Weintraub et al. (2022)		x			x					
Barczentewicz (2023)				x	x		x		x	
Barczentewicz et al. (2023)		x	x		x				x	
Constantinescu et al. (2023)					x			x	x	x
Ferreira et al. (2023)				x				x	x	x
Heimbach and Wattenhofer (2023a)	x	x		x		x		x	x	x
J.R. Jensen et al. (2023)		x			x	x			x	
Kamphuis et al. (2023)		x		x				x	x	
Kulkarni et al. (2023)		x	x	x			x		x	x
Mazorra and Penna (2023)		x			x		x	x	x	
Momeni et al. (2023)		x	x					x	x	x
Pillai (2023)		x	x		x					
Qin et al. (2023)		x		x		x			x	
Ramos and Ellul (2023)				x	x			x	x	
Wahrstätter et al. (2023)		x						x	x	x
Yang et al. (2023)				x	x		x	x	x	
Count	3	30	8	24	16	8	8	21	29	15

A key difference between the different acronyms MEV and BEV and their meaning that is also reflected in further discrepancies between the definitions is the group of actors that are extracting this value. While "miner extractable value" clearly attributes value extraction to miners on a PoW-based blockchain, "maximal extractable value" and "blockchain extractable value" are blockchain- and actor-agnostic. Some publications that use the term "miner extractable value" acknowledge that the value can also be extracted by participants beyond miners, e.g., users (Barczentewicz et al., 2023; Ramos and Ellul, 2023; Churiwala and Krishnamachari, 2022; Montiel et al., 2022; Yang et al., 2023). Since no specific group beyond miners was mentioned sufficiently often to exceed our 20% threshold in the publications we surveyed, we summarized them as "other stakeholders," including "validators" (Barczentewicz, 2023; Ramos and Ellul, 2023; Mazorra and Penna, 2023), "block proposers" (Constantinescu et al., 2023; Mazorra and Penna, 2023), and "network operators" (Poux et al., 2022). Further, more abstract actors like bots (Barczentewicz et al., 2023; Qin et al., 2022; Churiwala and Krishnamachari, 2022; Yang et al., 2023; J.R. Jensen et al., 2023; Kursawe, 2020), (strategic) users (Chitra and Kulkarni, 2022; Montiel et al., 2022; Obadia et al., 2021; Pillai, 2023), and opportunistic traders (Qin et al., 2022) were also mentioned. For these actors, it was often highlighted that they cannot decide on transaction in- and exclusion or ordering directly but do so indirectly via bribing corresponding stakeholders with high tips or through side-channel payments (i.e., payments outside the consensus protocol) (Qin et al., 2022; Chitra and Kulkarni, 2022; Churiwala and Krishnamachari, 2022).

Another discrepancy among the definitions entails the context wherein MEV can be extracted. While the majority of publications in our SLR posits that the value is extracted on a blockchain by leveraging control of transactions inclusion, exclusion, or ordering in a block, some authors highlight more specific aspects. For instance, the environment of extraction has been confined to "(DeFi) smart contracts" (Daian et al., 2020; Nadahalli et al., 2021; Qin et al., 2022; Piet et al., 2022; Weintraub et al., 2022) in general, "AMMs" in specific (Bartoletti et al., 2022), or narrowed down to the "Ethereum" ecosystem (Wahrstätter et al., 2023). Furthermore, Momeni et al. (2023) highlight that MEV can encompass not only transactions within one block but also across multiple blocks. Our definition comprises all these special cases and is also applicable in contexts such as permissioned blockchains and agnostic of application patterns (see, e.g., Sedlmeir et al., 2022).

Arguably the most controversial among the definitions of MEV is the assessment of MEV and its impact from a technical, economic, and ethical perspective. While most definitions do not include corresponding specifications, a considerable share of publications still considers that value extraction occurs at the cost of users (see Table 1). Most of them, however, do not ethically judge MEV and just refer to the observation that MEV can worsen trade outcomes for users, similar to arbitrageurs which on the one side can lead to worse prices for users but on the other side are fundamental for the functioning and efficiency of DeFi protocols such as DEXes (Bartoletti et al., 2022). Only some fundamentally condemn this extraction as dishonest behavior from an ethical perspective (Qin et al., 2022), while Daian et al. (2020); Yang et al. (2023) highlight the consequences of MEV from a technical perspective as potentially harmful for consensus stability and, therefore, the whole blockchain network (Ciampi et al., 2022).

The different forms of MEV

This chapter aims to answer our second research question: "What are the underlying categories of MEV attack vectors and what are exemplary applications vulnerable to the different categories?" Therefore, we systematically screened the literature from our SLR for abstract concepts and explicit examples of MEV extraction. We found two existing categorizations related to MEV. The first one was presented as a taxonomy by Eskandari et al. (2020) and structures front-running attacks into displacement attacks, insertion attacks, and suppression attacks. While we consider this categorization of front-running attacks helpful, MEV extraction techniques go beyond front-running attacks that target specific transactions or applications. For instance, making use of arbitrage opportunities from AMM-based DEXes via back-running extracts value from the AMM's shared liquidity pool instead of a single transaction and is indispensable for the AMM's price discovery mechanism. Consequently, back-running is discussed explicitly by related work. On the other hand, Qin et al. (2022) present a transaction ordering taxonomy that distinguishes between destructive front-running, tolerating front-running, back-running, and clogging. While this classification dissects technical ordering aspects, the binary distinction between destructive and tolerating front-running is not exhaustive from an economic perspective. For instance, extracting only a part of the value of a transaction through front-running without causing the corresponding transaction to fail causes ambiguities as it is neither totally destructive nor tolerating from an economic point of view. Moreover, Qin et al. (2022) do not include sandwich attacks as a separate category in their categorization but instead argue that from a transaction ordering perspective, sandwich attacks correspond to a combination of front- and back-running. Nevertheless, we added sandwich attacks as a separate category because they showcase unique dynamics and application areas and need to be considered an atomic category because their separation would not be economically attractive. Many literature items collected in our review also specifically focus on this type of attack.

In general, we observe a strong focus on the Ethereum blockchain in our literature basket, while other blockchains with DeFi activities (e.g., Solana, Polygon, Cosmos) are only investigated by individual publications. We structure the following aggregation and discussion of the present body of knowledge according to our refinement of these categorizations. The categories we obtained are front-running (Section "Front-running"), back-running (Section "Back-running"), sandwiching (Section "Sandwich"), and suppression (Section "Suppression"). We also provide a detailed listing of MEV attack vector categories and the respective applications discussed in the literature in Table 2.

Front-running

The aim of front-running a transaction is to gain a (typically riskless) profit from observing a transaction in the mempool, creating a transaction in response that makes use of the new knowledge gained from this transaction, and making sure this own transaction is included earlier. Front-running often makes the initial observed transaction fail or useless. Generally, the effect on the original transaction does not matter to the front-runner (Struchkov et al., 2021; Eskandari et al., 2020). The most prominent example of profitable transactions to be observed in the mempool is arbitrage opportunities between two AMMs, i.e., exploiting price differences of two different exchanges, amounting to over $250 M value

Table 2 Applications affected by the four categories of MEV exploitation as mentioned in the existing literature

MEV category	Literature discussing the category	Affected applications
Front-running	Arulprakash and Jebakumar (2022); Aune et al. (2017); Baum et al. (2021); Eskandari et al. (2020); Struchkov et al. (2021); Carranti (2022); Montiel et al. (2022); Poux et al. (2022); Qin et al. (2023); Chitra and Kulkarni (2022); Churiwala and Krishnamachari (2022); Qin et al. (2022); Torres et al. (2021); Piet et al. (2022); Varun et al. (2022); Mazorra and Penna (2023); Obadia et al. (2021); Heimbach and Wattenhofer (2023a); Park et al. (2023); Wahrstätter et al. (2023); Breidenbach et al. (2018); Seike et al. (2021, 2018); Doweck and Eyal (2020); Li et al. (2022); Song and Hong (2019); Zhou et al. (2021); Häfner and Stewart (2021); Strehle and Ante (2020); Bentov et al. (2019); Carrillo and Hu (2023); Seike et al. (2018, 2021); Qin et al. (2022)	Arbitrage on AMMs Smart contract vulnerabilities Order-book-based DEXes Liquidations in lending protocols Solutions for puzzles Crowdsensing Bug bounties Domain name protocols
Back-running	Qin et al. (2022); Yang et al. (2023); Montiel et al. (2022); Tatabitovska et al. (2021); Heimbach and Wattenhofer (2023a); Torres et al. (2021); Pillai (2023); Constantinescu et al. (2023); Perez et al. (2021); Eskandari et al. (2020); Spain et al. (2020); Carranti (2022); Sariboz et al. (2022); Perez et al. (2021)	Arbitrage on AMMs Liquidations in lending protocols ICOs NFT releases
Sandwich	Torres et al. (2021); Ferreira et al. (2023); Carranti (2022); Kulkarni et al. (2023); Heimbach and Wattenhofer (2022); Sariboz et al. (2022); Tatabitovska et al. (2021); Montiel et al. (2022); Mazorra and Penna (2023); Park et al. (2023); Eskandari et al. (2020); Varun et al. (2022); Stathakopoulou et al. (2021); Yang et al. (2023); Pillai (2023); Galal and Youssef (2021); Torres et al. (2021); Zhou et al. (2021); Qin et al. (2022); Torres et al. (2021); Struchkov et al. (2021); Varun et al. (2022); Xue et al. (2022); Montiel et al. (2022); Ramos and Ellul (2023); Mazorra et al. (2022); Kulkarni et al. (2023); Heimbach and Wattenhofer (2022); Qin et al. (2022); Heimbach and Wattenhofer (2022); Helmy (2021); Torres et al. (2021); Zhou et al. (2021); Pillai (2023); Struchkov et al. (2021); Züst (2021); Heimbach and Wattenhofer (2022); Zhou et al. (2021); Tatabitovska et al. (2021); Helmy (2021); Züst (2021); Zhou et al. (2021); Xue et al. (2022); Tatabitovska et al. (2021)	AMMs
Suppression	Torres et al. (2021); Eskandari et al. (2020); Zhang H et al. (2022); Kamphuis et al. (2023); Qin et al. (2022); Torres et al. (2021); Varun et al. (2022); Qin et al. (2022); Eskandari et al. (2020); Torres et al. (2021); Struchkov et al. (2021); Varun et al. (2022); Stathakopoulou et al. (2021); Torres et al. (2021); Eskandari et al. (2020); Sariboz et al. (2022); Constantinescu et al. (2023)	Gambling and lotteries Deadline-based smart contracts

extracted on popular Ethereum DEXes such as Uniswap, Curve, Swerve, 1Inch, and Bancor (Baum et al., 2021; Li et al., 2022; Song and Hong, 2019; Zhou et al., 2021; Doweck and Eyal, 2020; Qin et al., 2022). In this simple case, the front-runner can create a new transaction by copying the original transaction that includes all the instructions for a profitable activity and only needs to replace the sender's address and digital signature to receive the corresponding profits instead of the sender of the observed transaction in case it is included in a block (Montiel et al., 2022; Carranti, 2022; Qin et al., 2023; Poux et al., 2022; Häfner and Stewart, 2021). Correspondingly, attacks that target other users' transactions via front-running are also coined transaction imitation (Qin et al., 2023). The front-runner then bribes block proposers for earlier inclusion than the observed transaction, either through simply increasing gas fees or through private channel payments (Arulprakash and Jebakumar, 2022; Chitra and Kulkarni, 2022; Strehle and Ante, 2020). Because the time aspect is critical, this process should happen automatically. Arguably, identifying and copying (with minor modifications, e.g., of the recipient address) transactions that would successfully exploit an arbitrage opportunity represents a much simpler task for automation with bots than searching for arbitrage opportunities directly in many cases (Torres et al., 2021; Qin et al., 2022; Churiwala and Krishnamachari, 2022). The context-independent simplicity of this type of attack is also particularly clear in the context of another front-running example: transactions exploiting smart contract vulnerabilities (both by non-ethical and ethical hackers). Identifying an exploitable vulnerability is usually a complex task that is hard to automate, whereas testing whether the transaction that exploits the smart contract vulnerability leads to a profitable outcome and copying it is easily automatable (Varun et al., 2022; Torres et al., 2021; Piet et al., 2022).

Front-running can also appear in less complex situations, e.g., as a reaction of users trying to cancel orders on orderbook-based DEXes when they are not profitable anymore, where the front-runner is made aware of potential profits by seeing the cancellation transaction in the mempool and takes their order before the order cancellation is executed (Eskandari et al., 2020; Aune et al., 2017). This type of front-running has also been termed "cancellation grief" (Eskandari et al., 2020). Obadia et al. (2021) as well as Mazorra and Penna (2023) highlight that front-running transactions leveraging arbitrage opportunities can also span across multiple blockchains, i.e., price differences for an atomic swap of digital assets on two different blockchains (Bentov et al., 2019), opening up the potential for cross-domain MEV that is more difficult to discover. Atomic swaps refer to a pair of transactions where a mechanism ensures that not only one of the transactions can be executed, i.e., either both or none of the two transactions can take place. Furthermore, arbitrage opportunities can also span across multiple AMMs, often involving far more than two AMMs in practice (Zhou et al., 2021; Carrillo and Hu, 2023). Another typical example of front-running occurs in the context of liquidations. On most DeFi lending protocols, assets to be liquidated are offered at a discount, leading to a profit for the user liquidating the position in order to incentivize timely liquidations (Park et al., 2023; Qin et al., 2022; Heimbach and Wattenhofer, 2023a; Carranti, 2022). When observing a transaction of a borrower that tries to add collateral to an otherwise liquidatable position, a front-runner can extract the information from this transaction to locate and liquidate the loan before the borrower can add additional collateral (Park et al., 2023). Alternatively, liquidation transactions can also be front-run directly as they pose riskless profits when being combined with an arbitrage trade (Qin et al., 2022; Heimbach and Wattenhofer, 2023a; Carranti, 2022).

Overall, most front-running opportunities, e.g., price arbitrage or liquidations, are generated by price changes. In this context, Wahrstätter et al. (2023) showcase through an empirical longitudinal study that front-running profits can increase by up to 1 000% during times of market stress. This can result in extractable value exceeding the regular block rewards by almost three orders of magnitude (Zhou et al., 2021). Beyond financial applications, front-running has been observed when rewards can be claimed from creative work, such as the submission of a solution for puzzles (Varun et al., 2022; Torres et al., 2021), crowdsensing tasks (Arulprakash and Jebakumar, 2022), bug bounty programs (Eskandari et al. 2020; Breidenbach et al. 2018), or registering domain names (Eskandari et al., 2020; Seike et al., 2018, 2021). As such, front-running must also be considered in designing blockchain-based information systems beyond financial applications, e.g., for intellectual property rights management.

Back-running

The aim of back-running a transaction is to gain a (typically riskless) profit from observing one or multiple transactions in the mempool, anticipating the state change they cause when being executed, creating a transaction that leverages this new state, and making sure this own transaction is included directly behind it/them. In other words, back-running attempts to be the first (or among the first) transactions being processed after a certain event. Back-running hence involves foreseeing an upcoming profitable state before it has been written to the blockchain and instantly creating a transaction that can subsequently exploit this anticipated state (Qin et al., 2022; Yang et al., 2023; Montiel et al., 2022). From a transaction ordering perspective, back-running can be seen as the counter-part of front-running (Qin et al., 2022; Tatabitovska et al., 2021) as it relies on bribing block producers to include the back-running transaction directly (or soon) after the target transaction (Yang et al., 2023). As opposed to front-running, back-running does not impact the observed transaction but instead makes use not only of the knowledge gained from it but also its processing.

Two examples of situations where back-running appears are (again) arbitrage trades and liquidations. In case of massive swaps on AMMs that substantially modify the exchange rate of a digital asset on these AMMs, an actor can directly place their arbitrage transaction after the trade to balance out the exchange rate difference with other AMMs or exchanges for guaranteed profit (Qin et al., 2022; Heimbach and Wattenhofer, 2023a; Torres et al., 2021; Pillai, 2023; Constantinescu et al., 2023). Regarding lending protocols, back-running can occur if a transaction makes a loan liquidatable, e.g., by a price change according to an Oracle update transaction. In this situation, the exploiting party can instantly liquidate a loan directly after the transaction (Perez et al., 2021; Qin et al., 2022; Heimbach and Wattenhofer, 2023a; Yang et al., 2023). Further opportunities of back-running are early initial coin offering (ICO) (Eskandari et al., 2020; Spain et al., 2020; Carranti, 2022) or non-fungible token (NFT) (Qin et al., 2022; Sariboz et al., 2022; Carranti, 2022) buy-ins, where the tokens are bought immediately after their launch by back-running the transaction that deploys the corresponding smart contract and opens up the sale.

It is important to note that front- and back-running often cannot be strictly separated. For instance, if there is competition between multiple MEV bots to insert their transaction first behind another transaction (back-running), it may not be clear if awareness for this opportunity was created by the original transaction that opens up a back-running opportunity or by spotting another bot's profitable back-running transaction and trying to front-run it.

Similar to front-running, back-running also needs to be considered in blockchain-based applications outside of DeFi. For instance, while the opportunity of back-running Oracle update transactions for triggering liquidations in DeFi has already been discussed (Heimbach and Wattenhofer, 2023a; Perez et al., 2021; Qin et al., 2022; Yang et al., 2023), it appears that Oracle-based applications such as insurances on blockchains (Zhang W et al., 2021) might also be exposed to back-running.

Sandwich

The aim of sandwiching another user's transaction is to create a profitable state by manipulating the entire environment of the target transaction (Torres et al., 2021; Ferreira et al., 2023; Carranti, 2022; Kulkarni et al., 2023) through a combination of a transaction in front of and after the victim's transaction, creating a trio called sandwich (Heimbach and Wattenhofer, 2022; Sariboz et al., 2022; Tatabitovska et al., 2021; Montiel et al., 2022; Mazorra and Penna, 2023; Park et al., 2023). The idea was already described by pmcgoohan (2021) back in 2014. Alternative notions for sandwiching are insertion attacks (Eskandari et al., 2020), adopted also by Torres et al. (2021) and Varun et al. (2022). The arguably most prominent case for sandwich attacks is large AMM trades, where the exploiter places a transaction buying resp. selling the same asset to inflate resp. deflate its price right before the victim's transaction (Stathakopoulou et al., 2021; Yang et al., 2023; Pillai, 2023; Galal and Youssef, 2021) and afterward back-runs it to obtain profits due to the price change caused by the victim's transaction (Zhou et al., 2021; Qin et al., 2022; Torres et al., 2021; Struchkov et al., 2021; Varun et al., 2022; Xue et al., 2022; Montiel et al., 2022; Ramos and Ellul, 2023). This attack is one of the most common, both in transaction number and value extracted—over 700,000 transactions with more than $ 170 M extracted on the Ethereum DEXes Uniswap, Sushiswap, and Bancor until 2022 alone (Mazorra et al., 2022; Kulkarni et al., 2023; Qin et al., 2022)—and in the frequency it is discussed and analyzed in our literature review (e.g., definition, optimization methods, and empirical analyses of attacks). To protect AMM users against unpredictable price changes not only from sandwich attacks but also from other users' trades, the concept of "slippage tolerance" has been introduced (Heimbach and Wattenhofer, 2022; Qin et al., 2022). Users can specify a slippage tolerance to define the maximum acceptable price movement they accept for their trade (Heimbach and Wattenhofer, 2022; Helmy, 2021; Torres et al., 2021). With slippage tolerance, users try to strike a balance between ensuring that a minor price change caused by another transaction between the submission and inclusion of the user's transaction does not cause their transaction to fail while on the other hand protecting them from receiving an unacceptably bad price due to unexpected, major price changes (e.g., caused by a front-running transaction that represents a part of a sandwich attack) (Zhou et al., 2021; Pillai, 2023). Yet, an attacker can still calculate the maximal possible profits from a sandwich from the tolerable slippage as specified by the user, which is a part of the transaction data and, therefore, publicly available in the mempool (Struchkov et al., 2021). An analysis carried out by Züst (2021) revealed that in almost all cases of these simple sandwich attacks, the maximal possible profit was gained, with an average difference between the maximum acceptable slippage set by the victim and the actual outcome of less than 1%.

Oftentimes, large trades or low liquidity for one asset in the trading pair is necessary to make sandwich attacks profitable, particularly when taking into account the fixed transaction execution costs and variable AMM usage fees (Heimbach and Wattenhofer, 2022; Zhou et al., 2021; Tatabitovska et al., 2021; Helmy, 2021; Züst, 2021). In this context, Zhou et al. (2021) and Xue et al. (2022) present another type of sandwich attack in which a liquidity provider for an AMM targets a trader's transaction. In this case, the transaction that marks the front-running part of the sandwich removes liquidity, causing a higher sensitivity of the token price to trading activities and, therefore, increasing the value that can be extracted from slippage. This situation can create a profitable condition for the attacker when depositing the asset back into the pool through back-running. A recent development for alleviating sandwich attacks on AMM traders is the concept of "concentrated liquidity," where liquidity providers bound their supply to a specific price range. This approach decreases the price slippage and, therefore, the vulnerability to sandwich attacks by increasing the effective liquidity (Tatabitovska et al., 2021). However, it also opens novel MEV extraction opportunities for liquidity providers: Using sandwiching, they can only provide their liquidity during a large trade to avoid the risk of "impermanent loss"—the exposure of other liquidity providers to changes in the relative prices of tokens that negatively affect the value of their liquidity.

Suppression

The aim of suppressing another user's transaction is to delay or prevent its execution (Torres et al., 2021; Eskandari et al., 2020; Zhang H et al., 2022; Kamphuis et al., 2023) by clogging one or multiple upcoming blocks with own transactions or bribing block proposers to leave blocks empty (Qin et al., 2022). Thereby, it does not matter whether these clogging transactions will be successfully executed or if they just take up block space to exclude the attacked transaction (Eskandari et al., 2020). Consequently, the transactions themselves are just a means-to-an-end of pursuing another goal, namely preventing another transaction from being executed in due time (Eskandari et al., 2020). Compared to a front-running attack where the adversary tries to execute the same transaction with a higher priority, in this case, multiple transactions are chosen as long as they are executed with a higher priority and consume enough block space to prevent the timely inclusion of the victim's transaction (Torres et al., 2021; Varun et al., 2022; Qin et al., 2022). Other terms for this phenomenon that have been used are displacement attacks (Eskandari et al., 2020; Torres et al., 2021; Struchkov et al., 2021; Varun et al., 2022; Stathakopoulou et al., 2021), block stuffing (Torres et al., 2021; Eskandari et al., 2020), clogging, (Qin et al., 2022), blocking front-running (Sariboz et al., 2022), and destructive front-running (Qin et al., 2022; Sariboz et al., 2022; Constantinescu et al., 2023).

Suppression attacks have emerged mainly in the context of gambling (Sariboz et al., 2022) and lotteries (Torres et al., 2021; Varun et al., 2022) or other deadline-based smart contracts that award the winnings to the last account entering (Eskandari et al., 2020; Qin et al., 2022; Torres et al., 2021). An incident in August 2018, when transactions unrelated to a gambling, lottery, or other deadline-based smart contract clogged the Ethereum blockchain for 66 consecutive blocks, illustrates the practicality of these attacks (Qin et al., 2022; Eskandari et al., 2020). Furthermore, Qin et al. (2022) identify 14 more clogging events on Ethereum with a duration from 11 to 37 blocks and costs of over 2000 Ether, worth over $4 M as-of-today, implying an even higher value extracted on the assumption that these attacks were profitable.

Discussion: different perspectives on MEV countermeasures

MEV has its roots in fundamental technical design choices of blockchains and the competing incentives of different stakeholders, i.e., block producers and users. A recent result by Bahrani et al. (2023) proves that under quite general assumptions, the presence of MEV prevents the simultaneous incentive compatibility of welfare-maximizing transaction fee mechanisms from the perspective of users and block producers. Consequently, mitigating the negative impacts of MEV is desirable but at the same time does not seem to be resolvable with economic (market design) methods only. Therefore, the previously introduced definition and categorization of MEV need to be put into context and discussed against its different approaches to countermeasures. We analyzed partial solutions that reduce the amount of MEV that can be extracted or some of its negative impacts in our basket of literature and found that while most approaches are based on technical measures, such as cryptographic techniques that restrict block producers' opportunities to control transaction selection and ordering, also economic and legal measures have been suggested. As none of these suggestions seems to be able to avoid the negative aspects of MEV entirely, we consider these mechanisms largely complementary and discuss them in the described structure in the following.

Economic measures

While the previous section laid out the different types of how MEV appears from a transaction ordering viewpoint, there is an underlying, shared dynamic to all MEV exploitation: achieving the desired transaction ordering. Similar to the evolution of actors involved in value extraction (as discussed in Section "Defining maximal extractable value"), the means of achieving the desired ordering have changed substantially over time. Because of the direct agency of the block proposer on the transaction ordering and a lack of awareness of the impact of ordering, blockchain users' opportunities to influence the transaction ordering were initially limited to adjusting their priority fee (tip). Block proposers would usually sort all transactions according to their priority fee in descending order and fill their block starting from the top. Following this simple (and obviously suboptimal when considering that transaction sizes are different while block sizes are fixed) heuristic, miners were hoping to get close to maximizing their revenues. Thus, front-runners had to slightly overbid the fee of the target transaction while back-runners would pay a priority fee that is just below the target transaction's priority fee (Qin et al., 2022).

When multiple actors spot a front-running opportunity in the mempool (including other actors' front-running transactions), this caused what is called priority gas auctions (PGAs): the actors would repeatedly try to overbid each other, creating an auction-like competitive game in which they drive their profits (i.e., value extracted from front-running minus transaction fees) toward zero (Daian et al., 2020; Ciampi et al., 2022; Carranti, 2022). When competition among MEV extractors is not perfect (e.g., because of the short time frames), they may also reach an equilibrium > 0 (Mazorra et al., 2022). Daian et al. (2020) conduct a game-theoretic analysis of PGAs with two main strategies—blind raising and counter-bidding—to place the bids.

As all MEV participants got more sophisticated, block proposers moved away from the somewhat arbitrary descending-sorting heuristic and congestion, causing PGAs to target service offerings for atomically including users' "transaction bundles" without forwarding them to the mempool. Instead, relayers submit these transaction bundles directly to block proposers to offload PGAs from the mempool and alleviate the risk of becoming a target of MEV themselves (Chitra and Kulkarni, 2022; Piet et al., 2022). In contrast to PGAs, MEV extraction through transaction bundling could also be transferred to other blockchain fee models, like fixed gas price blockchains (Carrillo and Hu, 2023). Note that relayers do not need to trust block proposers with the confidentiality of blocks and the included bundles, as they do not learn about the block's content during the bidding process. However, there are also risks that need to be resolved, e.g., through reputation systems: users must trust relayers not to split up their bundles and extract MEV from them—an exploit that has empirically been observed (bert, 2023).

The trend of differentiating between the actors in control of proposing blocks in consensus and the actors trying to find favorable orderings and submitting them in fixed bundles is also seen as an effective measure to mitigate some of the negative implications of MEV. This concept is coined as proposer-builder separation (PBS), where proposers denote the already existing consensus participant that was selected to propose the next block and builders are the actors trying to find optimal blocks not just by arranging transactions from the mempool within a block but also by constructing the entire block with potential transaction bundles they receive bilaterally from users (Bahrani et al., 2024; Heimbach and Wattenhofer, 2023a). PBS aims at separating these two tasks on a protocol level and enforcing proposers to accept the blocks of the builder willing to pay the highest total fee. In this way, not only is transparency reinforced and some centralization risks originating from network effects for relayers can be mitigated, but it is also possible for the protocol itself to measure the value extracted, as it can be approximated with the fee paid, assuming a competitive market. This would further allow for MEV redistribution, where the value extracted is redistributed to all consensus participants to reduce consensus stability threats arising from strong fluctuations in block rewards (Chitra and Kulkarni, 2022).

Technical measures

Related work has discussed a variety of technical countermeasures that aim to mitigate or eliminate the exploitation of MEV. At first glance, it may appear helpful to impose consensus-based rules on how transactions should be ordered to reduce the attack surface (consider, e.g., sorting in ascending order according to the transaction hash). Unfortunately, because transaction senders also have degrees of freedom (e.g., the choice of the counter for signing—a measure to avoid unwanted duplicate inclusions of the same transaction), this measure is not effective. It also appears that because any ordering rule must be deterministic and fast to apply, any user can adapt the transaction they submit to the mempool accordingly. Moreover, algorithmic "fair ordering" approaches have natural issues with the lack of verifiable transaction submission times and Condorcet cycles. Nevertheless, certain forms of fair ordering can be instantiated using complex cryptographic constructions (Kelkar et al., 2023). A promising recent approach involves multiple entities in block creation which split the responsibility for transaction selection and ordering. If one of the block proposers attempts collusion, the other block proposer can forward the corresponding message and claim a reward (taken from a collateral of the misbehaving block proposer) that is guaranteed to be higher than the share of MEV they would get (Droll et al., 2024). However, by using confidential computing, e.g., with trusted execution environments (TEEs), block producers can collude without the risk of creating punishable evidence. Therefore, it is questionable that this approach provides a strong guarantee on MEV mitigation in the long run.

Arguably one of the most promising ways to address MEV extraction in many applications is by separating the steps of transaction ordering and execution in what is called a "commit-reveal" scheme (Arulprakash and Jebakumar, 2022; Doweck and Eyal, 2020). Because only transaction execution requires public visibility, the transactions' content can remain hidden during the ordering step and mitigate front-running as well as potentially other forms of MEV extraction without relying on non-collusion assumptions. If a smart contract-based application supports such a commit-reveal scheme, in the first step, a user registers a transaction that does not include the transaction details required for processing ("calldata," e.g., the address of the smart contract to be targeted, transaction amount, etc.) but only their hash. After this transaction has been included in a block, the user can follow up with the detailed transaction data and be assured that the smart contract allows for no other transaction to be included before theirs for a certain time (Arulprakash and Jebakumar, 2022). While this approach only introduces moderate overhead on processing capacity, it still challenges smart contracts with high use frequency and raises several additional problems. For instance, a user could refuse to execute the "reveal" step when their transaction has become less favorable in the meantime (e.g., a previous user has already won the lottery). To mitigate these issues, additional cryptographic approaches, such as time-based encryption or threshold encryption that allow block proposers to determine the calldata after a certain time period, even without the help of the user, have been proposed (Sekar, 2022; Nadahalli et al., 2021). Another mechanism that is applicable, for instance, in applications with predictable outcomes is based on a cryptographic (zero-knowledge) proof of over-collateralization, such that the commit step already provides more funds than a user could possibly lose in the reveal step as a collateral that will be burned or redistributed if the user fails to follow up with the calldata in due time. When this time horizon is sufficiently large, clogging attacks on the calldata-revealing transaction can be made very expensive and, thus, impractical.

Despite the variety of suggestions for technical mitigation approaches, thus far, no satisfactory generic solution has been found (Heimbach and Wattenhofer, 2023a; Häfner and Stewart, 2021). Thus, the different use cases and blockchain applications still require specifically tailored mitigation strategies to prevent by – or in most current cases, at least reduce – the negative aspects of MEV. Eskandari et al. (2020) and Tatabitovska et al. (2021) add that developers of smart contracts often do not have the necessary incentives and resources to develop specific protections for their applications, thus increasing the demand for solutions on the blockchain protocol layer. On the other hand, Noyes (2021) encourages developers to improve user experience by incorporating MEV mitigation measures in their decentralized applications, which can also help to stand out from the competition.

Regulatory and governance measures

One viewpoint on MEV that is thus far largely unexplored is its legal categorization. In this realm, only a few publications (Barczentewicz, 2023; Ramos and Ellul, 2023), some stemming from the IS literature (Eigelshoven et al., 2021; Clapham et al., 2023), have started to examine the legal assessment on MEV. Eigelshoven et al. (2021) and Clapham et al. (2023) both consider MEV in the context of DeFi as a form of market manipulation and violations of digital asset markets. Whether MEV constitutes market abuse in the sense of regulations is a novel and ongoing discussion. However, the European "Markets in Crypto Assets" (MiCA) Regulation in Article 92 on "Prevention and detection of market abuse" states the obligation to report "any reasonable suspicion regarding an order or transaction, including any cancellation or modification thereof, and other aspects of the functioning of the distributed ledger technology such as the consensus mechanism" (European Parliament, 2023). In their third consultation paper under MiCA, the European Securities and Market Authority (2024) interprets this as a clear indication that "other aspects of the distributed ledger technology may suggest the existence of market abuse e.g., the well-known Maximum Extractable Value (MEV)," not only characterizing MEV as market abuse but also to be regulated under the MiCA regulation. A very recent and first-of-its-kind court case related to MEV took place in the USA in May of 2024. In this case, the Department of Justice (2024) does not accuse the operators of the private mempool (flashbots) used for MEV or the actors active on them but rather incriminates two brothers that exploited a vulnerability in this private mempool to get access to transactions that were submitted as bundles for MEV extraction and to break these bundles and extract MEV from their parts. They could extract $ 25 M from transactions that were themselves meant to extract value from other transactions, i.e., a sandwich attack on a sandwich attack (Coindesk, 2024). This case has sparked the debate on the legality of MEV also in the USA, as some see the recent court case as an incident of "stealing from thieves" (Dailycoin, 2024).

While regulators are starting their discourse on establishing a legal classification of MEV, a major hurdle that remains in the legal assessment and especially potential prosecution is the definition and identification of MEV from a legal standpoint. Helmy (2021) point out that just paying a higher priority fee than other users for a transaction should not be considered front-running, as front-running additionally involves reacting to information outside the blockchain ledger and state, for example, in the public mempool. Furthermore, proving that a transaction is based on observations of the mempool and not just coincidence is not only a problem for researchers trying to quantify the amount of MEV (Qin et al., 2022; Judmayer et al., 2021; Lyu et al., 2022) but also that courts ruling on MEV cases may face. While similar problems occur in prosecuting insider trading in traditional financial markets, the globality and pseudonymity of public, permissionless blockchains can impede the enforcement of accountability and the identification of jurisdictional affiliation. However, during investigations, blockchain's pseudonymity does not necessarily pose a hurdle as modern on-chain analysis tools can often facilitate de-anonymization (Gramlich et al., 2024).

Besides the problems in clearly identifying and providing evidence for MEV attacks, the current assessment focuses very specifically on the context of fungible tokens and can, therefore, not be directly transferred to other blockchain-based applications involving other types of digital assets. In particular, permissioned blockchains proposed by many IS papers for applications in organizations have not been considered at all in current MEV literature. They could play a special role in MEV and its possible regulation. For instance, in permissioned blockchains, block proposers are no longer unknown but registered participants with a much higher degree of accountability.

Open research questions

Our systematic review has identified and structured the current body of literature on MEV and the knowledge base and discussions it entails. As a highly practitioner-driven research stream, our review has revealed many unresolved challenges and open questions in the context of MEV in the current literature. Naturally, the research questions that were raised directly by the publications in our SLR are predominantly focused on foundational, computer science-focused questions, just like the current research stream itself. However, as one of the objectives of this paper is to convey a fundamental understanding of MEV and awareness of its relevancy and potential impact to the more application-focused experts of the information systems domain, especially in electronic markets, we add upon these foundational questions with other research questions focused on the legal or application-focused viewpoint. We list the open research questions emerging from our literature review in Table 3 and elaborate on them in the following.

Table 3 Overview of open research questions

Question type	Research question
Foundational	• How can MEV be formalized and quantified in DeFi but also beyond? • In which cases can MEV exploitation be identified with certainty? • How does the presence of MEV influence current developments in the blockchain infrastructure layer such as fee mechanism design or rollups? • How do PBS and other mitigation or MEV redistribution measures influence the MEV landscape? • Which MEV categories or vulnerable applications allow for effective mitigation techniques?
Legal	• How should MEV be classified from a legal standpoint? • How can instances of MEV be legally identified and proven? • Should contractual or legal measures against MEV be general or use-case specific?
Application	• Which blockchain applications outside of DeFi are influenced by MEV? • Is it possible to derive patterns for applications exposed to MEV and its different categories? • How can information systems designers be made aware of MEV and its implications when building blockchain-based applications? • How can MEV be mitigated or governed in permissioned blockchains and enterprise blockchain projects?

While our paper has consolidated the different definitions and understandings of MEV into one common definition, this quest has also revealed the lack of an agreed-on mathematical, formal definition that can be used to quantify MEV within DeFi and beyond. For instance, the definition by Angeris et al. (2023) that compares the MEV extractable for a given transaction ordering with the average across all potential orderings only considers permutations within a block and ignores the choice of transaction in- and exclusion. Furthermore, without a sophisticated decomposition strategy, it is impractical to compute the average across all potential orderings, as the number of orderings is $N!$ and, therefore, grows super-exponentially in N where N is the number of transactions in a block. On the other hand, Bahrani et al. (2023) only give a non-constructive definition via the surplus of active block producers in a PBS setting. Related to this ambiguity, current literature also highlights the difficulties of forensic, quantitative analysis of MEV in identifying MEV exploitation with certainty and differentiating it from transactions resembling MEV exploitation (Judmayer et al., 2021; Lyu et al., 2022; Qin et al., 2022). Further foundational questions are especially related to future developments. In the context of developments aiming to improve the scalability of blockchain infrastructures with second-layer approaches, called rollups have emerged (Principato et al., 2023). Rollup operators are responsible for aggregating transactions and publishing a verifiable compressed state on the ledger (Noyes, 2021). While they are untrusted with regard to the integrity of transaction processing, these actors can still, for instance, inspect transactions they receive outside the mempool, predict their impact, and offer profitable bundles facilitated by control of transaction ordering, even across multiple blocks. As a consequence, they could potentially play a crucial role in future MEV hierarchies and attack vectors that require further investigation (Capretto et al., 2022; Tatabitovska et al., 2021; Heimbach and Wattenhofer, 2022; Eskandari et al., 2020; Strehle and Ante, 2020). Shared sequencers that allow to leverage MEV also across different rollups by sometimes creating a block for two different rollups at the same time may provide a substantial competitive edge (Gogol et al., 2024).

Furthermore, it remains an open question how PBS, other (cryptography-based) MEV mitigation approaches, or MEV redistribution measures impact the different roles, categories, and vulnerable applications within the MEV landscape. Lastly, while many approaches to mitigating MEV have been proposed and discussed, they mainly focus on specific categories and vulnerable applications within DeFi and no generalizable solution has been found (Häfner and Stewart, 2021; Heimbach and Wattenhofer, 2023a) (see Section "Technical measures"). Thus, it remains an open question which MEV categories can be completely resolved and which categories or applications necessarily involve MEV as a foundation for corresponding electronic markets upon blockchain infrastructure, e.g., arbitrage-based AMMs (Carranti, 2022), such that fair redistribution measures should be implemented at least as a complementary measure.

As highlighted in Section "Regulatory and governance measures", MEV has not only been barely considered from a blockchain-based information systems design perspective but also from a legal point of view. The first and foremost open question in this regard is a legal definition of MEV. While Clapham et al. (2023) and Eigelshoven et al. (2021) both consider MEV as a form of market manipulation, an assessment and definition of MEV from a regulatory body is still absent and it remains an open question whether MEV should be regulated in a general or use-case specific way. Given an established legal classification of MEV, pathways to identifying and proving the presence of MEV exploitation with a high degree of confidence will be required. Lastly, a completely unexplored topic is that of MEV emergence in permissioned blockchains. Permissioned blockchains have frequently been proposed in IS literature as a response to permissionless blockchains' scalability and data protection issues (Guggenberger et al., 2022; Sedlmeir et al., 2022) and might offer an additional measure against MEV in the form of contractual rules among the consensus participants, which are typically identifiable and accountable in permissioned blockchains. Whether contractual measures could or should be used to mitigate MEV in permissioned is to be investigated by future research.

Lastly, and maybe most important for IS research, extending our understanding of MEV and its impact on blockchain-based applications is imperative. While DeFi protocols have received a lot of research attention, as also illustrated in Table 2, MEV's impact on applications outside of DeFi, especially in IS research focused on organizational applications of blockchain technology, remains unexplored, as highlighted by only three papers in the AIS eLibrary that mention "MEV," "Miner extractable value," or "Maximal extractable value" (Clapham et al., 2023; Meyer et al., 2022; Eigelshoven et al., 2021). Thus, it remains an open question which of the countless blockchain applications outside of DeFi, many of which have been proposed in IS literature, e.g., for the energy sector (Alt and Wende, 2020; Tsao and Thanh, 2021), supply chain and trade finance (Jensen T. et al., 2019), and intellectual property rights (Gürkaynak et al., 2018) or ticket management (Regner et al., 2019), might be exposed to MEV. In this context, a valuable future research avenue may involve deriving patterns for applications exposed to the MEV extraction categories we identified in Section "The different forms of MEV". With such patterns at hand, IS researchers and practitioners developing blockchain-based applications could get a better understanding of when MEV needs to be considered. However, other ways to convey an understanding and awareness of MEV to information systems designers could be valuable as well. Lastly, once a better understanding of MEV's impact is established, designers of blockchain-based applications need to investigate the opportunities and challenges of existing mitigation approaches, conceptualize new mitigation techniques, derive impossibility results, or examine to which extent governance measures, especially in permissioned blockchains, can be leveraged to contain the negative implications of MEV.

Conclusion

MEV is an emergent topic in the young and rapidly evolving space of blockchain-based applications. However, just as the rapid rise of DeFi has demonstrated the potential relevance of blockchain technology in the financial sector, it has led to the emergence of MEV. As we argue in this paper, the impact of short-time monopolies on transaction selection and ordering in blockchain consensus and a corresponding generalization of MEV must be considered also for the wider space of blockchain-based applications. Researchers and practitioners working on blockchain-based IS, particularly in regulated domains, are often not aware of the existence and potential impact of MEV. Our research has revealed that the current discourse is still in search of a uniform understanding of what constitutes MEV, its prerequisites, and its impact. While there is an ongoing controversial discourse on the ethicality of MEV, the majority of current literature agrees that some form of MEV such as front-running arbitrage trades, should be considered vital to the functioning of the affected protocols. Furthermore, the complexity and multi-faceted impacts of MEV on blockchain-based markets make it hard to detect and quantify. Technical works have already explored mitigation strategies and boundaries where these are not applicable. Yet, the assessments and countermeasures from an economic and legal perspective required to address MEV in a holistic manner are still in a nascent state.

To lay the foundation for future research, we conducted a systematic literature review and established a definition of MEV that is as specific as possible while being consistent with the majority of the literature. Furthermore, we distilled four major categories of MEV exploitation—front-running, back-running, sandwiching, and suppression—from the surveyed literature. We then used these categories to aggregate key insights, discussions, and open questions presented in the literature and allocated them to the respective category. We found that the literature's most mature understanding is on AMMs and lending platforms in DeFi and pointed out how they can be affected by the different categories. Other DeFi applications have only rarely been considered, and blockchain-based applications outside of DeFi have not been considered at all. For the underlying principles of MEV, e.g., the importance of placing transactions directly before or after another one, or immediately exploiting a state change caused by updated information through an Oracle, it seems plausible that they could also apply to other blockchain-based applications, in one way or another. Thus, we call upon IS researchers to be aware of the concept and the impact of MEV on their blockchain-based applications, to assess whether they harm existing or proposed IS concepts, and to design or evaluate application-specific mitigation approaches.

Supplementary Information The online version contains supplementary material available at https://doi.org/10.1007/s12525-024-00727-x.

Acknowledgements We thank the editor and the anonymous reviewers for their highly valuable and constructive feedback. We are also grateful for the helpful suggestions for improvement by Orestis Papageorgiou, Nadia Pocher, and Yunxiu Zhou. For the purpose of open access, and in fulfilment of the obligations arising from the grant agreements, the authors have applied a Creative Commons Attribution 4.0 International (CC BY 4.0) license to any Author Accepted Manuscript version arising from this submission.

Funding Open Access funding enabled and organized by Projekt DEAL. This research was funded in part by the Bavarian Ministry of Economic Affairs, Regional Development and Energy through the project "Fraunhofer Blockchain Center (20-3066-2-6-14)" and the Luxembourg National Research Fund (FNR) in the FiReSPArX (grant reference *14783405*) and PABLO (grant reference *16326754*) projects, as well as Banque et Caisse d'Épargne de l'État, Luxembourg (Spuerkeess) and the Directorate-General for Financial Stability, Financial Services and Capital Markets Union (DG FISMA).

Declarations

Conflict of interest The authors declare no competing interests.

References

Akerlof, G. A. (1970). The market for "lemons": Quality uncertainty and the market mechanism. *The Quarterly Journal of Economics, 84*(3), 235–251. https://doi.org/10.2307/1879431

Alt, R., & Wende, E. (2020). Blockchain technology in energy markets - An interview with the European Energy Exchange. *Electronic Markets, 30*(2), 325–330. https://doi.org/10.1007/s12525-020-00423-6

Angeris, G., Chitra, T., Diamonds, T., & Kulkarni, K. (2023). The specter (and spectra) of miner extractable value. https://arXiv.org/abs/2310.07865

Arrow, K.J. (1963). Uncertainty and the welfare economics of medical care. *American Economic Review*, *53*(5), 941–973. https://www.jstor.org/stable/1812044

Arulprakash, M., & Jebakumar, R. (2022). Commit-reveal strategy to increase the transaction confidentiality in order to counter the issue of front running in blockchain. *AIP Conference Proceedings*, *2460*(1). https://doi.org/10.1063/5.0095700

Aune, R.T., Krellenstein, A., O'Hara, M., & Slama, O. (2017). Footprints on a blockchain: Trading and information leakage in distributed ledgers. *The Journal of Trading 12*, 5–13. https://doi.org/10.3905/jot.2017.12.3.005

Bahrani, M., Garimidi, P., & Roughgarden, T. (2023). Transaction fee mechanism design with active block producers. https://doi.org/10.48550/arXiv.2307.01686

Bahrani, M., Garimidi, P., & Roughgarden, T. (2024). Centralization in block building and proposer-builder separation. https://arxiv.org/abs/2401.12120

Barczentewicz, M. (2023). MEV on Ethereum: A policy analysis. https://doi.org/10.2139/ssrn.4332703

Barczentewicz, M., Sarch, A.F., & Vasan, N. (2023). Battle of the crypto bots: Automated transaction copying in decentralized finance. https://ssrn.com/abstract=4411448

Bartoletti, M., Chiang, J.H., & Lluch Lafuente, A. (2022). Maximizing extractable value from automated market makers. *Financial cryptography and data security: 26th international conference* 3–19. https://doi.org/10.1007/978-3-031-18283-9_1

Baum, C., yu Chiang, J.H., David, B.,Frederiksen, T.K., & Gentile, L. (2023). SoK: Mitigation of front-running in decentralized finance. *Financial cryptography and data security: 27th international conference.* https://doi.org/10.1007/978-3-031-32415-4_17

Baum, C., David, B., & Frederiksen, T.K. (2021). P2DEX: Privacy-preserving decentralized cryptocurrency exchange. *Applied cryptography and network security: 19th international conference* 163–194. https://doi.org/10.1007/978-3-030-78372-3_7

Bentov, I., Ji, Y., Zhang, F., Breidenbach, L., Daian, P., & Juels, A. (2019). Tesseract: Real-time cryptocurrency exchange using trusted hardware. *Proceedings of the acm sigsac conference on computer and communications security* 1521–1538 . https://doi.org/10.1145/3319535.3363221.

bert (2023). Post mortem: April 3rd, 2023 MEV-boost relay incident and related timing issue. Retrieved February 16, 2024 https://collective.flashbots.net/t/post-mortem-april-3rd-2023-mev-boost-relay-incident-and-related-timing-issue/1540

Blackshear, S., Chalkias, K., Chatzigiannis, P., Faizullabhoy, R., Khaburzaniya, I., Kogias, E.K., & Zakian, T. (2021). Reactive key-loss protection in blockchains. *Financial cryptography and data security: 25th international conference* 431–450 . https://doi.org/10.1007/978-3-662-63958-0_34

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J.A., & Felten, E.W. (2015). SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies. *Symposium on security and privacy* 104–121. https://doi.org/10.1109/SP.2015.14

Breidenbach, L., Cachin, C., Chan, B., Coventry, A., Ellis, S., Juels, A., et al. (2021). Chainlink 2.0: Next steps in the evolution of decentralized oracle networks. *Chainlink Labs, 1*, 1–136.

Breidenbach, L., Daian, P., Tramer, F., & Juels, A. (2018). Enter the Hydra: Towards principled bug bounties and exploit-resistant smart contracts. *Proceedings of the 27th usenix security symposium* 1335–1352. https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-breidenbach.pdf

Budish, E., Cramton, P., & Shim, J. (2015). The high-frequency trading arms race: Frequent batch auctions as a market design response. *The Quarterly Journal of Economics, 130*(4), 1547–1621. https://doi.org/10.1093/qje/qjv027

Bünz, B., Aal, S., Zamani, M., & Boneh, D. (2020). Zether: Towards privacy in a smart contract world. *Financial cryptography and data security: 24th international conference* 423–443. https://doi.org/10.1007/978-3-030-51280-4_23

Butijn, BJ., Tamburri, D.A., & van den Heuvel, WJ. (2020). Blockchains: A systematic multivocal literature review. *ACM Computing Surveys*, *53*(3). https://doi.org/10.1145/3369052

Capretto, M., Ceresa, M., Anta, A. F., Russo, A., & Sánchez, C. (2022). Setchain: Improving blockchain scalability with Byzantine distributed sets and barriers. *International Conference on Blockchain,* 87–96. https://doi.org/10.1109/Blockchain55522.2022.00022

Carranti, D. (2022). Flash Boys 3.0: Is MEV a choice?. https://ssrn.com/abstract=4351266

Carrillo, F., & Hu, E. (2023). MEV in fixed gas price blockchains: Terra Classic as a case of study. https://arxiv.org/abs/2303.04242

Chi, T., He, N., Hu, X., & Wang, H. (2024). Remeasuring the arbitrage and sandwich attacks of maximal extractable value in Ethereum. https://doi.org/10.48550/arXiv.2405.17944

Chitra, T. (2023). Towards a theory of maximal extractable value II: Uncertainty. https://arXiv.org/abs/2309.14201

Chitra, T., & Kulkarni, K. (2022). Improving proof of stake economic security via MEV redistribution. *Proceedings of the ccs workshop on decentralized finance and security*. https://doi.org/10.1145/3560832.3564259

Churiwala, D., & Krishnamachari, B. (2022). Comma protocol: Towards complete mitigation of maximal extractable value (MEV) attacks. https://doi.org/10.48550/arXiv.2211.14985

Ciampi, M., Ishaq, M., Magdon-Ismail, M., Ostrovsky, R., & Zikas, V. (2022). FairMM: A fast and frontrunning-resistant crypto market-maker. *Cyber security, cryptology, and machine learning: 6th international symposium* 428–446. https://doi.org/10.1007/978-3-031-07689-3_31.

Clapham, B., Jakobs, J., Schmidt, J., Gomber, P., & Muntermann, J. (2023). A taxonomy of violations in digital asset markets. *44th international conference on information systems*. https://aisel.aisnet.org/icis2023/blockchain/blockchain/12/

Coindesk (2024). *Brothers accused of $ 25m Ethereum exploit as U.S. reveals fraud charges*. Retrieved June 11, 2024, https://www.coindesk.com/policy/2024/05/15/brothers-accused-of-25m-ethereum-exploit-as-us-reveals-fraud-charges/

Constantinescu, A., Ghinea, D., Heimbach, L., Wang, Z., & Wattenhofer, R. (2023). A fair and resilient decentralized clock network for transaction ordering. https://doi.org/10.48550/arXiv.2305.05206

Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., & Juels, A. (2020). Flash Boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability. *Symposium on security and privacy* 910–927. https://doi.org/10.1109/SP40000.2020.00040

Dailycoin (2024). *Why first Ethereum MEV case is seen as a double standard*. Retrieved June 11, 2024, https://dailycoin.com/why-first-ethereum-mev-case-is-seen-as-a-double-standard/

DeFiLlama (2024). Retrieved June 10, 2024, https://defillama.com/

Department of Justice (2024). *Two brothers arrested for attacking Ethereum blockchain and stealing $ 25m in cryptocurrency*. Retrieved June 11, 2024 https://www.justice.gov/opa/pr/two-brothers-arrested-attacking-ethereum-blockchain-and-stealing-25m-cryptocurrency

Doweck, Y., & Eyal, I. (2020). Multi-party timed commitments. https://arxiv.org/abs/2005.04883

Droll, J., Stengele, O., & Hartenstein, H. (2024). Unpredictable transaction arrangement for MEV mitigation in Ethereum. *Proceedings of the 6th international conference on blockchain and cryptocurrency*. https://doi.org/10.1109/ICBC59979.2024.10634470

Egelund-Müller, B., Elsman, M., Henglein, F., & Ross, O. (2017). Automated execution of financial contracts on blockchains. *Business & Information Systems Engineering, 59*(6), 457–467. https://doi.org/10.1007/s12599-017-0507-z

Eigelshoven, F., Ullrich, A., & Parry, D.A. (2021). Cryptocurrency market manipulation: A systematic literature review. *42nd international conference on information systems*. https://aisel.aisnet.org/icis2021/fintech/fintech/1/

Eskandari, S., Moosavi, S., & Clark, J. (2020). SoK: Transparent dishonesty: Front-running attacks on blockchain. *Financial cryptography and data security: 24th international conference* 170–189. https://doi.org/10.1007/978-3-030-43725-1_13

European Parliament (2023). *Regulation on markets in crypto-assets (mica)*. Retrieved June 21, 2024 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1114

European Securities and Market Authority (2024). *Consultation paper on the technical standards specifying certain requirements of MiCA*. Retrieved June 11, 2024 . https://www.esma.europa.eu/press-news/esma-news/esma-launches-third-consultation-under-mica

Ferreira, X., Venturyne, M., & Parkes, D.C. (2023). Credible decentralized exchange design via verifiable sequencing rules. *Proceedings of the 55th annual acm symposium on theory of computing* 723–736. https://doi.org/10.1145/3564246.3585233

Flashbots. (2024). *Flashbots transparency dashboard*. Retrieved June 10, 2024, from https://explore.flashbots.net/

Galal, H.S., & Youssef, A.M. (2021). Publicly verifiable and secrecy preserving periodic auctions. *Financial cryptography and data security: International workshops* 348–363. https://doi.org/10.1007/978-3-662-63958-0_29

Garousi, V., Felderer, M., & Mäntylä, M.V. (2019). Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. *Information and Software Technology*, *106* 101–121. https://doi.org/10.1016/j.infsof.2018.09.006

Gogol, K., Messias, J., Miori, D., Tessone, C., & Livshits, B. (2024). Layer-2 arbitrage: An empirical analysis of swap dynamics and price disparities on rollups. https://arxiv.org/abs/2406.02172

Govindarajan, K., Vinayagamurthy, D., Jayachandran, P., & Rebeiro, C. (2022). Privacy-preserving decentralized exchange marketplaces. *Proceedings of the 4th international conference on blockchain and cryptocurrency*. https://doi.org/10.1109/ICBC54727.2022.9805505

Gramlich, V., Guggenberger, T., Principato, M., Schellinger, B., Duda, S., & Stoetzer, J. (2024). In decentralized finance nobody knows you are a dog. *Proceedings of the 57th hawaii international confer-*

ence on system sciences. https://scholarspace.manoa.hawaii.edu/items/82c23b77-3cd7-43a6-abc4-836628706d13

Gramlich, V., Guggenberger, T., Principato, M., Schellinger, B., & Urbach, N. (2023). A multivocal literature review of decentralized finance: Current knowledge and future research avenues. *Electronic Markets, 33*, 11. https://doi.org/10.1007/s12525-023-00637-4

Guggenberger, T., Sedlmeir, J., Fridgen, G., & Luckow, A. (2022). An in-depth investigation of the performance characteristics of Hyperledger Fabric. *Computers and Industrial Engineering, 173*. https://doi.org/10.1016/j.cie.2022.108716

Gürkaynak, G., Yılmaz, I., Yeşilaltay, B., & Bengi, B. (2018). Intellectual property law and practice in the blockchain realm. *Computer Law & Security Review, 34*(4), 847–862. https://doi.org/10.1016/j.clsr.2018.05.027

Häfner, S., & Stewart, A. (2021). Front-running, smart contracts, and candle auctions. https://doi.org/10.2139/ssrn.3846363

Hägele, S. (2024). Centralized exchanges vs. decentralized exchanges in cryptocurrency markets: A systematic literature review. *Electronic Markets*, *34*, 33. https://doi.org/10.1007/s12525-024-00714-2.

Hartwich, E., Ollig, P., Fridgen, G., & Rieger, A. (2022). Probably something: A multi-layer taxonomy of non-fungible tokens. *Internet Research*. https://doi.org/10.1108/INTR-08-2022-0666

Hartwich, E., Rieger, A., Sedlmeir, J., Jurek, D., & Fridgen, G. (2023). Machine economies. *Electronic Markets, 33*, 36. https://doi.org/10.1007/s12525-023-00649-0

Heimbach, L., & Wattenhofer, R. (2022). Eliminating sandwich attacks with the help of game theory. *Proceedings of the Asia Conference on computer and communications security* 153–167. https://doi.org/10.1145/3488932.3517390.

Heimbach, L., & Wattenhofer, R. (2023). SoK: Preventing transaction reordering manipulations in decentralized finance. *Proceedings of the 4th ACM conference on advances in financial technologies*. https://doi.org/10.1145/3558535.3559784

Helmy, B. (2021). *Exploring blockchain-based decentralized exchanges*. https://crypto.unibe.ch/archive/theses/2021.bsc.benjamin.helmy.pdf

Jensen, J.R., von Wachter, V., & Ross, O. (2023). Multi-block MEV. https://doi.org/10.48550/arXiv.2303.04430

Jensen, T., Hedman, J., Henningsson, S. (2019). How TradeLens delivers business value with blockchain technology. *MIS Quarterly Executive*, *18*, 221–243. https://doi.org/10.17705/2msqe.00018.

Judmayer, A., Stifter, N., Schindler, P., & Weippl, E. (2021). Estimating (miner) extractable value is hard, let's go shopping! https://eprint.iacr.org/2021/1231

Kamphuis, F., Magri, B., Lamberty, R., & Faust, S. (2023). Revisiting transaction ledger robustness in the miner extractable value era. *Extend to: 21st international conference on applied cryptography and network security* 675–698. https://link.springer.com/chapter/10.1007/978-3-031-33491-7_25

Kelkar, M., Deb, S., Long, S., Juels, A., & Kannan, S. (2023). Themis: Fast, strong order-fairness in Byzantine consensus. *Proceedings of the 2023 acm sigsac conference on computer and communications security* 475–489. https://doi.org/10.1145/3576915.3616658

Kitchenham, B.A., & Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering*. Keele University and Durham University Joint Report. https://www.elsevier.com/data/promis/misc/525444systematicreviewsguide.pdf

Kokoris-Kogias, E., Alp, E.C., Gasser, L., Jovanovic, P., Syta, E., & Ford, B. (2021). CALYPSO: Private data management for decentralized ledgers. *Proceedings of the VLDB Endowment*, *14* 586–599. https://doi.org/10.14778/3436905.3436917

Kulkarni, K., Diamandis, T., & Chitra, T. (2023). Towards a theory of maximal extractable value I: Constant function market makers. https://arxiv.org/abs/2207.11835

Kursawe, K. (2020). Wendy, the good little fairness widget: Achieving order fairness for blockchains. *Proceedings of the 2nd acm conference on advances in financial technologies* 25–36. https://doi.org/10.1145/3419614.3423263.

Kursawe, K. (2021). Wendy grows up: More order fairness. *Financial cryptography and data security: 25th international conference* 191–196. https://doi.org/10.1007/978-3-662-63958-0_17.

Leland, H.E. (1992). Insider trading: Should it be prohibited? *Journal of Political Economy*, *100*(4), 859–887. https://www.jstor.org/stable/2138691

Levens, T. E. (2015). Too fast, too frequent? High-frequency trading and securities class actions. *The University of Chicago Law Review, 82* (3), 1511–1557. https://www.jstor.org/stable/43575203

Li, R., Xie, Y., Ning, Z., Zhang, C., & Wei, L. (2022). Privacy-preserving decentralized cryptocurrency exchange without price manipulation. *IEEE/CIC International Conference on Communications in China* 274–279. https://doi.org/10.1109/ICCC55456.2022.9880750

Lyu, X., Zhang, M., Zhang, X., Niu, J., Zhang, Y., & Lin, Z. (2022). An empirical study on Ethereum private transactions and the security implications. https://doi.org/10.48550/arXiv.2208.02858

MacKenzie, D. (2021). Trading at the speed of light: How ultrafast algorithms are transforming financial markets. *Princeton University Press*. https://doi.org/10.1515/9780691217796

Malkhi, D., & Szalachowski, P. (2022). Maximal extractable value (MEV) protection on a DAG. https://doi.org/10.48550/arXiv.2208.00940

MAXQDA (2024). Retrieved May 29, 2024, https://www.maxqda.com/

Mazorra, B., & Penna, N.D. (2023). Towards optimal prior-free permissionless rebate mechanisms, with applications to automated market makers & combinatorial orderflow auctions. https://doi.org/10.48550/arXiv.2306.17024

Mazorra, B., Reynolds, M., & Daza, V. (2022). Price of MEV: Towards a game theoretical approach to MEV. *Proceedings of the ACM ccs workshop on decentralized finance and security* 15–22. https://doi.org/10.1145/3560832.3563433.

Meyer, E., Welpe, I.M., & Sandner, P.G. (2022). Decentralized finance - a systematic literature review and research directions. *Proceedings of the 30th European Conference on information systems*. https://aisel.aisnet.org/ecis2022/_rp/25/

Momeni, P., Gorbunov, S., & Zhang, B. (2023). FairBlock: Preventing blockchain front-running with minimal overheads. *Security and privacy in communication networks* 250–271. https://doi.org/10.1007/978-3-031-25538-0_14

Montiel, M. D., Guerraoui, R., & Roman, PL. (2022). A decentralized anonymous blockchain intercommunication system via zero knowledge proofs: SurferMonkey. https://doi.org/10.48550/arXiv.2210.13242

Nadahalli, T., Khabbazian, M., & Wattenhofer, R. (2021). Timelocked bribing. *Financial cryptography and data security: 25th international conference* 53–72. https://doi.org/10.1007/978-3-662-64322-8_3

Nakamoto, S. (2009). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf

Noyes, C. (2021). *MEV and me*. Retrieved February 16, 2023 https://research.paradigm.xyz/MEV

Obadia, A., Salles, A., Sankar, L., Chitra, T., Chellani, V., & Daian, P. (2021). Unity is strength: A formalization of cross-domain maximal extractable value. https://arxiv.org/abs/2112.01472

Öz, B., Kraner, B., Vallarano, N., Kruger, B.S., Matthes, F., & Tessone, C.J. (2023). Time moves faster when there is nothing you anticipate: The role of time in MEV rewards. *Proceedings of the workshop on decentralized finance and security*. https://doi.org/10.1145/3605768.3623563

Park, S., Jeong, W., Lee, Y., Son, B., Jang, H., & Lee, J. (2023). Unraveling the MEV enigma: ABI-free detection model using graph neural networks. https://doi.org/10.48550/arXiv.2305.05952

Perez, D., Werner, S.M., Xu, J., & Livshits, B. (2021). Liquidations: DeFi on a knife-edge. *Financial cryptography and data security: 25th international conference* 457–476. https://doi.org/10.1007/978-3-662-64331-0_24

Piet, J., Fairoze, J., & Weaver, N. (2022). Extracting Godl [sic] from the salt mines: Ethereum miners extracting value. https://doi.org/10.48550/arXiv.2203.15930

Pillai, B. (2023). *Blockchain MEV minimisation solution with price guarantee reward*. https://doi.org/10.36227/techrxiv.21345306.v1.

pmcgoohan (2021). *Exploring miner extractable value (MEV) with Pmcgoohan*. Retrieved February 16, 2023, https://anchor.fm/chainlinkgod/episodes/Exploring-Miner-Extractable-Value-MEV-with-Pmcgoohan-e13ufaj

Poux, P., De Filippi, P., & Deffains, B. (2022). Maximal extractable value and the blockchain commons. https://doi.org/10.2139/ssrn.4198139

Principato, M., Babel, M., Guggenberger, T., Kropp, J., & Mertel, S. (2023). Towards solving the blockchain trilemma: An exploration of zero-knowledge proofs. *Proceedings of the 44th international conference on information systems.* https://aisel.aisnet.org/icis2023/blockchain/blockchain/5/

Qin, K., Chaliasos, S., Zhou, L., Livshits, B., Song, D., & Gervais, A. (2023). The blockchain imitation game. *Proceedings of the 32nd usenix conference on security symposium* 3961–3978. https://dl.acm.org/doi/10.5555/3620237.3620459

Qin, K., Zhou, L., & Gervais, A. (2022). Quantifying blockchain extractable value: How dark is the forest? *IEEE Symposium on Security and Privacy* 198–214. https://doi.org/10.1109/SP46214.2022.9833734

Qin, K., Zhou, L., Livshits, B., & Gervais, A. (2021). Attacking the DeFi ecosystem with flash loans for fun and profit. *International conference on financial cryptography and data security: 25th international conference* 3–32. https://doi.org/10.1007/978-3-662-64322-8_1

Ramos, S., & Ellul, J. (2023). The MEV saga: Can regulation illuminate the dark forest? https://doi.org/10.48550/arXiv.2305.03718

Regner, F., Urbach, N., & Schweizer, A. (2019). NFTs in practice - non-fungible tokens as core component of a blockchain-based event ticketing application. *Proceedings of the 39th international conference on information systems.* https://aisel.aisnet.org/icis2019/blockchain_fintech/blockchain_fintech/1/

Rieger, A., Roth, T., Sedlmeir, J., & Fridgen, G. (2022). We need a broader debate on the sustainability of blockchain. *Joule, 6*, 1137–1141. https://doi.org/10.1016/j.joule.2022.04.013

Röell, A. (1990). Dual-capacity trading and the quality of the market. *Journal of Financial Intermediation, 1*(2), 105–124. https://doi.org/10.1016/1042-9573(90)90001-V

Sariboz, E., Panwar, G., Vishwanathan, R., & Misra, S. (2022). FIRST: Frontrunning resilient smart contracts. https://10.48550/arXiv.2204.00955

Schwarz-Schilling, C., Saleh, F., Thiery, T., Pan, J., Shah, N., & Monnot, B. (2023). Time is money: Strategic timing games in proof-of-stake protocols. https://arXiv.org/abs/2305.09032

Schwiderowski, J., Pedersen, A. B., & Beck, R. (2024). Crypto tokens and token systems. *Information Systems Frontiers, 26*(1), 319–332. https://doi.org/10.1007/s10796-023-10382-w

Sedlmeir, J., Lautenschlager, J., Fridgen, G., & Urbach, N. (2022). The transparency challenge of blockchain in organizations. *Electronic Markets, 32*(3), 1779–1794. https://doi.org/10.1007/s12525-022-00536-0

Seike, H., Aoki, Y., & Koshizuka, N. (2021). Blockchain-based scalable ubiquitous code allocation method resilient to congestion. *Proceedings of the international conference on blockchain* 272–279 . https://doi.org/10.1109/Blockchain53845.2021.00044

Seike, H., Hamada, T., Sumitomo, T., & Koshizuka, N. (2018). Blockchain-based ubiquitous code ownership management system without hierarchical structure. ..structure. "2018 IEEE SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI" 271–276. https://doi.org/10.1109/SmartWorld.2018.00081

Sekar, V. (2022). *Preventing front-running attacks using timelock encryption* . https://vsekar.me/assets/diss.pdf

Song, CY., & Hong, S. (2019). One way to solve the problem of presales of Ethereum: How to use public key cryptography. *International journal of advanced science and convergence 1*(2), 27–31. https://doi.org/10.22662/IJASC.2019.1.2.027

Spain, M., Foley, S., & Gramoli, V. (2020). The impact of Ethereum throughput and fees on transaction latency during ICOs. V. Danos, M. Herlihy, M. Potop-Butucaru, J. Prat, and S. Tucci-Piergiovanni (Eds.), *International Conference on Blockchain Economics, Security and Protocols 71*(9), 1–15). https://doi.org/10.4230/OASIcs.Tokenomics.2019.9

Stathakopoulou, C., Rüsch, S., Brandenburger, M., & Vukolić, M. (2021). Adding fairness to order: Preventing front-running attacks in BFT protocols using TEEs. *40th international symposium on reliable distributed systems* 34–45. https://doi.org/10.1109/SRDS53918.2021.00013

Stiglitz, J.E. (1983). Risk, incentives and insurance: The pure theory of moral hazard. *The geneva papers on risk and insurance-issues and practice 8*, 4–33. https://www.jstor.org/stable/41950058

Stiglitz, J.E. (2002). Information and the change in the paradigm in economics. *American Economic Review*, *92*(3), 460–501. https://www.jstor.org/stable/3083351

Strehle, E., & Ante, L. (2020). Exclusive mining of blockchain transactions. https://doi.org/10.2139/ssrn.3686529

Struchkov, I., Lukashin, A., Kuznetsov, B., Mikhalev, I., & Mandrusova, Z. (2021). Agent-based modeling of blockchain decentralized financial protocols. *29th conference of open innovations association* 337–343. https://doi.org/10.23919/FRUCT52173.2021.9435601

Sunyaev, A., Kannengießer, N., Beck, R., Treiblmaier, H., Lacity, M., Kranz, J., & Luckow, A. (2021). Token economy. *Business & Information Systems Engineering, 63*, 457–478. https://doi.org/10.1007/s12599-021-00684-1

Tatabitovska, A., Ersoy, O., & Erkin, Z. (2021). *Mitigation of transaction manipulation attacks in UniSwap*. https://repository.tudelft.nl/islandora/object/uuid:d4ad2e4e-1f42-41f4-8808-554f3ba7d1cf

Torres, C.F., Camino, R., & State, R. (2021). Frontrunner Jones and the raiders of the dark forest: An empirical study of frontrunning on the Ethereum blockchain. *Proceedings of the 30th usenix security symposium* 1343–1359. https://www.usenix.org/conference/usenixsecurity21/presentation/torres

Tsao, Y.-C., & Thanh, V- V. (2021). Toward sustainable microgrids with blockchain technology-based peer-to-peer energy trading mechanism: A fuzzy meta-heuristic approach. *Renewable and Sustainable Energy Reviews, 136*. https://doi.org/10.1016/j.rser.2020.110452

Varun, M., Palanisamy, B., & Sural, S. (2022). Mitigating frontrunning attacks in Ethereum. *Proceedings of the 4th international symposium on blockchain and secure critical infrastructure* 115–124. https://doi.org/10.1145/3494106.3528682.

Vom Brocke, J., Simons, A., Riemer, K., Niehaves, B., Plattfaut, R., & Cleven, A. (2015). Standing on the shoulders of giants: Challenges and recommendations of literature search in information systems research. *Communications of the association for information systems, 37*(1). https://doi.org/10.17705/1CAIS.03709.

Wahrstätter, A., Zhou, L., Qin, K., Svetinovic, D., & Gervais, A. (2023). Time to bribe: Measuring block construction market. https://arXiv.20org/abs/2305.16468

Webster, J., & Watson, R.T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly, 26*(2), 13–23. http://www.jstor.org/stable/4132319

Weintraub, B., Torres, C.F., Nita-Rotaru, C., & State, R. (2022). A flash(bot) in the pan: measuring maximal extractable value in private pools. *Proceedings of the 22nd acm internet measurement conference.* https://doi.org/10.1145/3517745.3561448

Winseck, D. (2002). Illusions of perfect information and fantasies of control in the information society. *Citizenship and Participation in the Information Age* 33–55. https://doi.org/10.1177/14614440222226280

Xue, Y., Fu, J., Su, S., Bhuiyan, Z.A., Qiu, J., Lu, H., & Tian, Z. (2022). *Preventing price manipulation attack by front-running*. *Advances in artificial intelligence and security* 309–322. https://doi.org/10.1007/978-3-031-06764-8_25

Yang, S., Zhang, F., Huang, K., Chen, X., Yang, Y., & Zhu, F. (2023). SoK: MEV countermeasures: Theory and practice. arXiv:2212.05111

Ye, M., Yao, C., & Gai, J. (2013). The externalities of high frequency trading. https://doi.org/10.2139/ssrn.2066839

Zhang, H., Merino, L- H., Estrada-Galiñanes, V., & Ford, B. (2022). Flash freezing flash boys: Countering blockchain front-running. *42nd international conference on distributed computing systems workshops* 90–95. https://doi.org/10.1109/ICDCSW56584.2022.00026

Zhang, W., Wei, C- P., Jiang, Q., Peng, C- H., & Zhao, J.L. (2021). Beyond the block: A novel blockchain-based technical model for long-term care insurance. *Journal of Management Information Systems, 38*(2), 374–400. https://doi.org/10.1080/07421222.2021.1912926

Zhou, L., Qin, K., Cully, A., Livshits, B., & Gervais, A. (2021). On the just-in-time discovery of profit-generating transactions in DeFi protocols. *IEEE Symposium on Security and Privacy* 919–936. https://doi.org/10.1109/SP40001.2021.00113

Zhou, L., Qin, K., & Gervais, A. (2021). A2MM: Mitigating frontrunning, transaction reordering and consensus instability in decentralized exchanges. https://doi.org/10.48550/arXiv.2106.07371

Zhou, L., Qin, K., Torres, C.F., Le, D.V., & Gervais, A. (2021). High-frequency trading on decentralized on-chain exchanges. *IEEE Symposium on Security and Privacy* 428–445. https://doi.org/10.1109/SP40001.2021.00027

Züst, P. (2021). *Analyzing and preventing sandwich attacks in Ethereum* . Retrieved February 16,2024, https://www.smartcontractresearch.org/t/research-summary-analyzing-and-preventing-sandwich-attacks-in-ethereum/1033/1

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.