

Securing Decentralized Finance: A Comprehensive Survey of Maximal Extractable Value and Its Countermeasures

Md Monjurul Karim , Dong Hoang Van, Qiang Qu

PII: S2096-7209(26)00017-5
DOI: <https://doi.org/10.1016/j.bcra.2026.100455>
Reference: BCRA 100455



To appear in: *Blockchain: Research and Applications*

Received date: 29 September 2025
Revised date: 22 December 2025
Accepted date: 22 January 2026

Please cite this article as: Md Monjurul Karim , Dong Hoang Van, Qiang Qu, Securing Decentralized Finance: A Comprehensive Survey of Maximal Extractable Value and Its Countermeasures, *Blockchain: Research and Applications* (2025), doi: <https://doi.org/10.1016/j.bcra.2026.100455>

This is a PDF of an article that has undergone enhancements after acceptance, such as the addition of a cover page and metadata, and formatting for readability. This version will undergo additional copyediting, typesetting and review before it is published in its final form. As such, this version is no longer the Accepted Manuscript, but it is not yet the definitive Version of Record; we are providing this early version to give early visibility of the article. Please note that Elsevier's sharing policy for the Published Journal Article applies to this version, see: <https://www.elsevier.com/about/policies-and-standards/sharing#4-published-journal-article>. Please also note that, during the production process, errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

© 2026 Published by Elsevier Ltd on behalf of Zhejiang University Press.
This is an open access article under the CC BY-NC-ND license
(<http://creativecommons.org/licenses/by-nc-nd/4.0/>)

Securing Decentralized Finance: A Comprehensive Survey of Maximal Extractable Value and Its Countermeasures

Md Monjurul Karim^a, Dong Hoang Van^{a,b}, Qiang Qu^{a,*}

^aShenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, Shenzhen 518055, China

^bUniversity of Chinese Academy of Sciences, No.1 Yanqihu East Rd, Huairou District, Beijing 101408, China

Abstract

The rapid advancement of blockchain network protocols has positioned decentralized finance (DeFi) as a key distributed application ecosystem in modern digital infrastructure. These distributed network systems are reshaping traditional financial paradigms by leveraging peer-to-peer protocols for accessible, transparent, and efficient services. However, the underlying network infrastructure faces significant security challenges, particularly concerning transaction manipulation within the framework of Maximal Extractable Value (MEV). MEV has emerged as a critical network security vulnerability due to its exploitation of transaction-ordering mechanisms in blockchain consensus protocols. Despite extensive research on MEV, critical gaps remain in understanding and securing distributed ledger networks against these vulnerabilities across various blockchain platforms. In this paper, we present a comprehensive survey of MEV within DeFi ecosystems through a multi-faceted approach. We provide a detailed taxonomy of MEV attack strategies targeting network protocol vulnerabilities. Furthermore, we offer a categorization of security countermeasures spanning consensus protocols, base-layer network design, and application-level defenses. Additionally, we present an empirical analysis of MEV dynamics across different blockchain networks, quantifying their impact on network performance, security, and fairness. This study contributes to enhancing the security of distributed network applications and advancing more robust and equitable network protocols for decentralized systems.

Keywords: MEV; DeFi; Blockchain; Arbitrage; Front-running.

1. Introduction

The financial sector is experiencing a significant shift due to blockchain technology and the increasing prominence of digital currencies. Key innovations such as Decentralized Finance (DeFi) and Central Bank Digital Currencies (CBDC) are leading this transformative wave, offering the potential to fundamentally reshape the financial industry [1, 2]. According to market analysis, DeFi is predicted to expand at a compound annual growth rate (CAGR) of 42.5% between 2022 and 2030, potentially reaching a valuation of 230 billion US dollars by 2030¹. DeFi relies on smart contracts to provide financial functionalities similar to conventional finance, such as trading and lending services. The functionality of these smart contracts depends on transaction sequencing, where specific ordering influences transaction outcomes [3], presenting significant security challenges regarding data integrity, transparency, and accuracy [4]. DeFi operates on distributed ledgers where transaction data is cryptographically stored as

immutable structures, ensuring transparency and integrity across network nodes [5–8]. Smart contract execution is driven by algorithms managing consensus mechanisms and transaction validation without central authority reliance [9, 10]. The real-time dissemination of transaction details and price updates reduces information asymmetries, contributing to ecosystem transparency. Cross-chain solutions and decentralized oracles exemplify seamless data exchange between blockchain networks [11, 12]. As DeFi grows, scaling these capabilities while maintaining security presents both challenges and opportunities.

1.1. Motivation of this Survey

The rapid expansion of DeFi has introduced increasingly complex transaction dynamics on blockchain networks, particularly Ethereum. As these transaction sequences become more sophisticated, new opportunities and challenges arise, especially concerning transparency and fairness. One critical challenge is the concept of *maximal extractable value (MEV)*, which quantifies the potential profits achievable by strategically altering the order, inclusion, or exclusion of transactions. The substantial growth in DeFi applications, including cryptocurrencies, stablecoins, decentralized lending, price oracles, and flash loans, has significantly elevated MEV's economic importance. As shown in Figure 1a, the

*Corresponding Author: Qiang Qu

Email addresses: karim@siat.ac.cn (Md Monjurul Karim), hoang@siat.ac.cn (Dong Hoang Van), qiang@siat.ac.cn (Qiang Qu)

¹<https://www.grandviewresearch.com/industry-analysis/decentralized-finance-market-report>

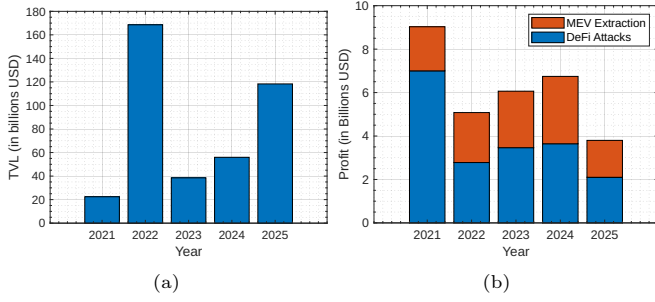


Figure 1: a) Growth of DeFi [13]; b) Impact of MEV attacks [14].

total value locked (TVL) in DeFi reached a peak of approximately 168.57 billion USD in 2022, stabilizing around 118.32 billion USD by 2025, reflecting sustained interest and confidence in the ecosystem. However, this growth coincided with an increase in DeFi attacks, prominently featuring MEV extraction, as depicted in Figure 1b. These developments underscore the necessity of addressing MEV-related security concerns to enhance DeFi sustainability.

Recent analytics indicate that validators and searchers have collectively earned nearly 700 million USD from MEV within Ethereum’s TVL of about 32.30 billion USD, facilitating a total trading volume of 664.83 billion USD [14]. Additionally, on blockchains such as Algorand², cumulative MEV market values have surpassed 1 billion USD, playing a significant role in over half of trading activities and contributing to 309.9 billion USD in trading volume. Furthermore, Dune Analytics reports an average daily MEV volume of 43.40% on Uniswap v3 as of January 2023, driven primarily by arbitrage and sandwich transactions [15]. MEV is similarly prevalent on major Ethereum-based decentralized exchanges (DEXs), including Uniswap³ and Curve⁴. In 2022, users lost 129.9 million USD to DeFi attacks, averaging 750 USD per user [16, 17]. These figures underscore the need for comprehensive MEV investigation, as participants employ various strategies to maximize profits [18–21]. Furthermore, Ethereum’s transition from version 1.0 to 2.0 marked a pivotal shift from Proof of Work (PoW) to Proof of Stake (PoS). While Ethereum 1.0 involved computational competition among miners, Ethereum 2.0 randomly selects block proposers who prepare blocks for validator verification. This transition from competitive mining to structured validator systems introduces different MEV extraction dynamics, necessitating reevaluation of existing strategies and mitigation techniques [20–22].

1.2. Related Work

In recent years, extensive research has examined the economic and security aspects of DeFi and MEV. Zhao

et al. [23] explored the critical role of oracles in providing off-chain data for decentralized applications, categorizing them into aggregation, staking, game theory, and reputation-based types. Werner et al. [24] systematically outlined key DeFi primitives and protocols, including smart contracts, oracles, DEXs, lending markets, stablecoins, and derivatives. Similarly, Xu et al. [26] presented a comparative analysis of major DEX protocols through a state-space modeling framework, assessing their mechanisms, transaction costs, pricing strategies, and potential market-induced losses. Xu and Feng [27] further examined yield farming protocols, highlighting associated security and economic risks such as flash loan attacks, reentrancy exploits, yield dilution, and liquidations. Zhou et al. [17] introduced a comprehensive five-layer framework classifying DeFi vulnerabilities spanning network, consensus, smart contract, protocol, and auxiliary service layers. Xiang et al. [29] provided empirical insights into developers’ responses to security incidents during DeFi project development.

Regarding MEV-specific research, several studies have investigated transaction-ordering manipulation and corresponding mitigation approaches. Baum et al. [28] discussed adversarial profit through front-running and evaluated mitigation methods such as fair ordering protocols, blinded input batching, and private user balances. Yang et al. [30] developed a detailed taxonomy classifying 28 MEV countermeasures according to factors including MEV auctions, order fairness, and MEV-aware application designs. Heimbach and Wattenhofer [31] critically assessed current MEV mitigation schemes, highlighting their trade-offs and effectiveness in achieving fair transaction ordering. Alipanahloo et al. [32] proposed a practical roadmap categorizing MEV mitigation strategies within Ethereum’s Layer 1 (L1) and Layer 2 (L2) solutions. Materwala et al. [33] classified MEV transactions with illustrative examples, analyzed detection approaches, explored simulation methods, and identified key challenges for mitigation. Gramlich et al. [34] systematically reviewed MEV literature, categorizing attack vectors and examining their impacts on DeFi, while addressing socio-economic, technical, and regulatory countermeasures. Despite these comprehensive investigations, opportunities remain for a more integrated treatment of MEV strategies, mitigation mechanisms, and empirical methods. Existing MEV-focused surveys provide in-depth coverage of transaction-ordering attacks, countermeasures, and protocol-level design choices [28, 30–34]. At the same time, these works often emphasize specific aspects, such as front-running and fair ordering protocols, Ethereum-centric L1 and L2 roadmaps, or detection pipelines and simulation frameworks.

1.3. Contributions and Organization

To address the above needs, our survey synthesizes and extends recent MEV-focused surveys into a single multi-perspective view of MEV. We build on these foundations and on broader DeFi and vulnerability surveys [17, 23, 24, 26, 27, 29] and connect three strands that usually

²<https://algorand.co/>

³<https://app.uniswap.org>

⁴<https://curve.fi>

Table 1: Comparison between existing surveys and ours

Ref.	Fundamental Topics Covered				MEV-based Discussion			Overall Attributes		
	Blockchain	DeFi	AMM	DEX	Strategies	Solutions	Empirical Analysis	Privacy	Security	Economic
[17]	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓
[23]	✓	✓	✗	✓	✗	✗	✗	✓	✓	✓
[24]	✓	✓	✓	✓	✓	✗	✗	✓	✗	✓
[25]	✓	✓	✓	✓	✗	✗	✗	✗	✓	✓
[26]	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓
[27]	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓
[28]	✗	✓	✓	✗	✓	✓	✗	✓	✓	✓
[29]	✓	✓	✗	✓	✗	✗	✗	✓	✓	✓
[30]	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗
[31]	✗	✓	✓	✓	✓	✗	✗	✓	✗	✓
Ours	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

appear separately: (i) a value-source-oriented taxonomy that spans classical and emerging MEV strategies, (ii) a cross-layer view of mitigation across consensus, base infrastructure, and application design, and (iii) an integrated perspective that combines theoretical models and empirical measurements across different blockchain platforms. Table 1 summarizes how our scope and emphasis complement existing surveys on MEV and DeFi security. Compared with prior MEV taxonomies that focus primarily on transaction-level patterns or ordering-based categorizations [28, 30, 33, 34], our classification extends these frameworks in three directions. First, it shifts the emphasis from isolated attack patterns to strategy families defined by their underlying value source and position in the MEV supply chain. Second, it links each family to both technical execution mechanisms and economic impact and summarizes available evidence on profitability and reproducibility. Third, it makes the distinction between extractive and productive MEV explicit and uses this axis to connect protocol-level analysis with ethical, market-structure, and regulatory questions. Our goal is to provide an integrative synthesis that supports protocol designers, system builders, and regulators.

Our main contributions are summarized as follows:

- We extend existing MEV surveys through a structured classification of MEV strategies by underlying value source. The classification covers established techniques such as front-running and sandwich attacks and incorporates emerging phenomena such as time-bandit attacks, cross-domain and cross-chain MEV, consensus-level bribery, and oracle-based manipulation.
- We organize MEV mitigation approaches across three blockchain layers (consensus, base, and application) and explain how design choices at each layer, such as MEV auctions, batch auctions, encrypted or private mempools, and MEV-aware application designs, interact in practical deployments.
- We relate MEV to theoretical perspectives from optimization theory, game theory, auction theory, and

information theory and use these lenses to clarify the incentive structures and fairness trade-offs that drive MEV across the full supply chain.

- We survey empirical methods and datasets for quantifying MEV. These include heuristic analyses, relay-based measurements, and machine-learning approaches. We highlight how architectural differences across Ethereum, L2 rollups, and non-EVM platforms such as Algorand and Solana shape observable MEV patterns.
- We synthesize open problems that cut across strategies, mitigation mechanisms, theory, and measurement and outline future research directions with a focus on adaptive detection pipelines, incentive-compatible mitigation, and socio-technical and regulatory questions around extractive versus productive MEV.

The remainder of this survey is structured as follows: Section 2 covers foundational concepts essential for understanding MEV. Section 3 provides a primer on MEV’s components and mechanisms. Section 4 details our research methodology, including literature search and selection criteria. Section 5 examines specific MEV strategies comprehensively. Section 6 categorizes and discusses existing mitigation solutions. Section 7 analyzes MEV using optimization and game theory perspectives. Section 8 highlights empirical analyses and practical implications, including MEV bots and relays. Section 9 discusses ongoing challenges and future research opportunities. Finally, Section 10 concludes the survey, summarizing key insights.

2. Background

In this section, we lay the groundwork for an in-depth exploration of MEV by introducing key foundational topics to provide readers with the essential background needed to fully understand the complexities of MEV in subsequent discussions.

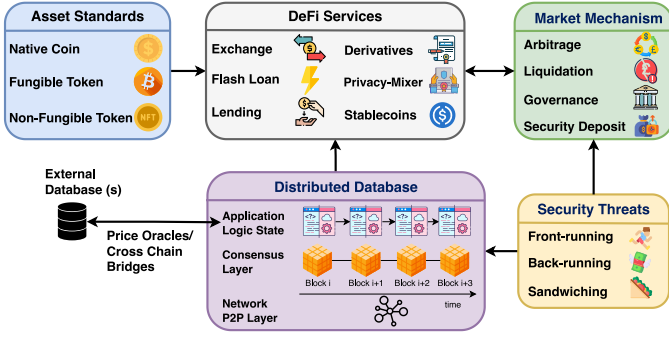


Figure 2: Components of DeFi.

2.1. Blockchain

Blockchain is a decentralized ledger technology enabling permanent and verifiable recording of transactions [35, 36]. Transactions are grouped into blocks that are cryptographically linked using hashes. Prominent blockchain platforms such as Bitcoin [37] and Ethereum [38] employ consensus protocols (e.g., PoW, PoS) to securely validate new blocks through crypto-economic incentives that discourage malicious behavior [39]. Each block contains multiple transactions that become immutable upon inclusion in the blockchain, safeguarding against unauthorized alterations [40]. Nodes in the blockchain network maintain synchronized copies of the ledger and collectively participate in consensus processes, ensuring ledger consistency. Additionally, cryptographic techniques involving public and private keys enable secure peer-to-peer transactions without intermediaries, establishing blockchain as the foundational infrastructure for diverse decentralized applications [41]. While Ethereum has historically been the primary platform for MEV activities, other blockchains such as Solana, Binance Smart Chain, and Base have also encountered MEV-related challenges, leading to the adoption of protective measures against such exploits.

2.2. Decentralized Finance

Decentralized finance (DeFi) comprises smart contracts providing financial services similar to traditional finance, including exchanges, lending, and derivatives [24, 42]. As illustrated in Figure 2, DeFi ecosystems integrate asset standards, market mechanisms, and distributed databases through price oracles and cross-chain bridges. Smart contracts exhibit transaction order dependencies, where outcomes depend on execution sequence, creating opportunities for MEV extraction [17]. Popular DeFi services include DEXs (e.g., Uniswap, SushiSwap), stablecoins (e.g., USDC, USDT), lending protocols (e.g., Aave, Compound), derivatives (e.g., dYdX), and asset management platforms (e.g., Enzyme), with Ethereum hosting the majority of DeFi applications. While MEV creates incentives for validators, it raises concerns about fairness and transparency in DeFi as optimizing transaction sequencing enables blockchain participants to extract extra profits from DeFi protocols [43–45]. One critique of MEV in DeFi is the uncertainty and

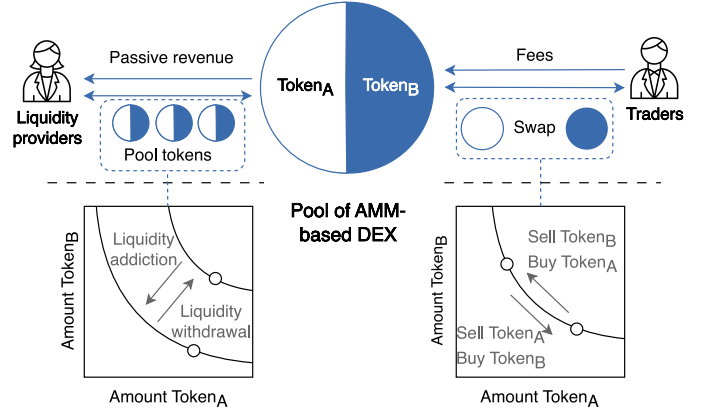


Figure 3: Overview of AMM.

potential manipulation it introduces, as traders may not know if their transactions are being processed fairly when validators reorder them for maximum profit [17]. To address these issues, DEXs implement auction models to process trades more fairly and transparently, allowing users to estimate and visualize MEV prevalence across various blockchains. DeFi protocols inherently create MEV opportunities through price discrepancies across different platforms, enabling arbitrage extraction when identical assets trade at different prices simultaneously [21]. As DeFi expands, managing MEV continues to pose a significant challenge for blockchain protocols [24].

2.3. Mempool

The mempool (memory pool) is a temporary storage area where unconfirmed transactions await validation and inclusion in blockchain blocks [46]. Each network node maintains in-memory data structures containing pending transactions, with miners and validators typically prioritizing transactions offering higher fees for faster block inclusion [47]. This fee-based selection mechanism prevents double-spending while ensuring only valid transactions reach the blockchain. Transaction ordering within the mempool varies across blockchain networks, as different systems adopt distinct prioritization rules. For instance, Ethereum uses gas-price-based ordering, allowing participants to pay higher transaction fees to prioritize their transactions [22]. In contrast, the Algorand blockchain implements a First-Come-First-Served (FCFS) ordering approach, processing transactions based on their arrival time rather than fees [48]. While this prevents traditional front-running, it opens the door for back-running strategies that target transactions after execution. L2 solutions such as Arbitrum and Optimism employ private mempool systems with centralized sequencers that reorder transactions according to custom algorithms, which lead to different vulnerability patterns [49].

2.4. Automated Market Maker

Automated Market Makers (AMMs) are decentralized protocols that use algorithms to automatically facilitate

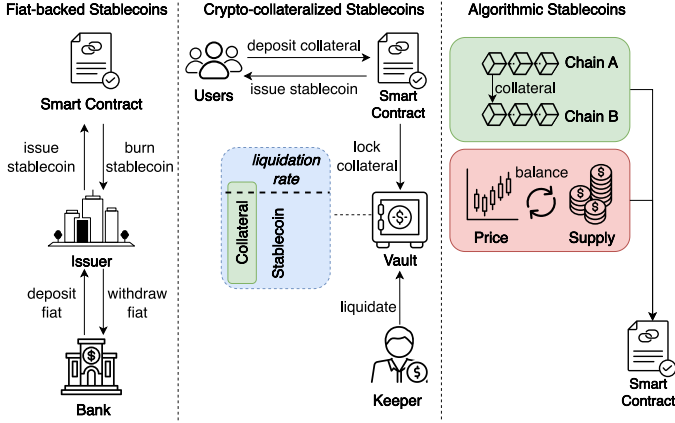


Figure 4: Different types of Stablecoin.

digital asset exchange without central authorities [26]. As illustrated in Figure 3, liquidity providers deposit tokens into pools and earn trading fees, which incentivizes market liquidity contribution. Unlike traditional order books, users trade directly against algorithmic pricing mechanisms, which positions AMMs as primary DeFi trading infrastructure with deep liquidity and continuous availability. AMMs employ various mathematical models including Constant Product Market Makers (CPMMs) such as Uniswap [50], Constant Mean Market Makers (CMMMs) such as Balancer, and Constant Sum Market Makers (CSMMs) exemplified by mStable for stablecoin trading [51]. Advanced variants include Hybrid Function Market Makers (HFMMs) such as Curve Protocol, Dynamic AMMs such as Bancor [52], and Constant Function Market Makers (CFMMs) such as Uniswap v3 with concentrated liquidity features. In the MEV setting, these algorithmic pricing rules and the resulting slippage behavior determine how trades impact pool prices and create conditions for various MEV strategies, which we discuss systematically in Section 5.

2.5. Stablecoin

Stablecoins are cryptocurrencies designed to maintain stable value by pegging to fiat currencies, primarily USD, and they serve as crucial DeFi infrastructure for transactions and value storage [53, 54]. As illustrated in Figure 4, three main types exist: fiat-backed stablecoins (for example, USDT and USDC) backed by traditional currency reserves, crypto-collateralized stablecoins (for example, DAI) backed by cryptocurrency held in smart contracts, and algorithmic stablecoins that maintain pegs through automated supply adjustments without collateral backing. These mechanisms provide volatility reduction compared to traditional cryptocurrencies such as Bitcoin [37], which facilitates DeFi ecosystem stability and cross-protocol interoperability [55]. Because these designs rely on collateralization, liquidation, and peg-restoration mechanisms, stablecoins are tightly linked to MEV-driven

liquidations and arbitrage opportunities, which we analyze later in Section 8.6.

3. A Quick Primer on MEV

In this section, we set the stage for the readers to deep dive into the conceptual overview of MEV by discussing the associated concepts to fully understand the working principle of MEV.

3.1. Overview of MEV

MEV refers to the total amount an individual makes by strategically reordering or censoring transactions on a blockchain. More specifically, MEV refers to the profit that miners or validators can extract from trades, contracts, or other operations on the blockchain. The concept was first introduced by Daian et al. [22], who described the ability of miners to manipulate user transactions to capture value strategically. While initially focused on miners, the term has evolved to encompass value extraction by any block proposer, including validators in PoS systems. MEV is primarily observed on Ethereum due to its smart contract capabilities and the rise of DeFi platforms. With significant capital committed to smart contracts, the scope for MEV is substantial. MEV has the potential for extracting value in ways that not only bring opportunities for the validators and extractors but also introduce security, integrity, and stability concerns in the blockchain. Thus, a comprehensive understanding of its mechanics becomes imperative for all stakeholders beyond Ethereum.

From both ethical and economic perspectives, MEV-driven activity is not a homogeneous phenomenon. Recent policy and legal analyses commonly differentiate between *extractive* MEV and *productive* MEV according to their effects on users and protocols [34, 56–58]. *Extractive* MEV comprises strategies through which searchers or validators increase their payoffs by degrading the execution quality of particular user transactions or by impairing network conditions, as in classical mempool front-running and sandwich attacks. By contrast, *productive* MEV denotes profit-seeking strategies that concurrently improve market quality or protocol safety, such as cross-venue arbitrage that reduces price discrepancies or protocol-designed liquidation mechanisms that help preserve solvency in lending platforms [34, 59]. This distinction serves as a useful conceptual framework for organizing MEV strategies and for designing and evaluating corresponding mitigation mechanisms.

The operational mechanics of the MEV supply chain are illustrated in Figure 5. The workflow traces the lifecycle of a user transaction (e.g., swapping 10 ETH for DAI) as it is transformed into a searcher bundle, aggregated by a builder, verified by a relay, and ultimately finalized by a validator. The process begins with the user and transaction-generation phase, during which the user’s intent is broadcast to the network. After entering the public

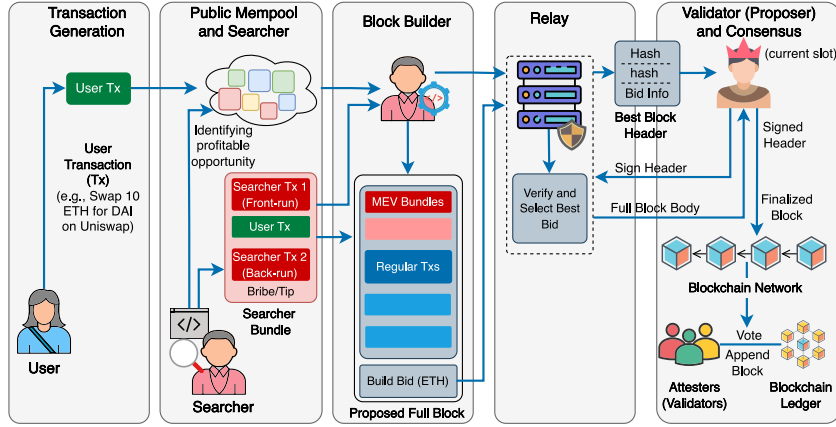


Figure 5: End-to-end workflow of the MEV supply chain.

mempool, the transaction is detected by searchers, who identify potential arbitrage or sandwiching opportunities. Rather than simply reposting the transaction, the searcher encapsulates it within a *searcher bundle*, typically inserting a front-running and back-running transaction around the user's trade and attaching a bribe or tip. These bundles are forwarded to the block-builder phase, where they are aggregated into a *proposed full block* that prioritizes high-value MEV bundles over regular transactions, resulting in a corresponding *builder bid*. To ensure trust-minimized execution, a relay serves as an intermediary that verifies the proposed block and forwards only the *block header* and associated bid information to the validator. In the validator and consensus phase, the proposer selects the highest bid and signs the header. The relay then releases the full *block body* to the validator, enabling the block's proposal and finalization on the blockchain ledger.

3.2. Building Blocks of MEV

MEV is enabled by a complex ecosystem of actors and entities that interact to monitor the pending transaction pool, identify profitable opportunities, assemble blocks of transactions, and influence transaction ordering and confirmation. To understand how MEV is extracted in practice, it is important to outline the key participants in this ecosystem and their respective roles. Each component focuses on a different part of the pipeline that ultimately allows miners, sequencers, relays, and bots to profit from manipulations that are detrimental to regular users. By coordinating and optimizing their strategies, these entities are able to extract significant value, necessitating countermeasures to realign incentives.

3.2.1. Participants of MEV

The primary participants of MEV play distinct yet interconnected roles within the ecosystem to orchestrate the identification, extraction, and optimization of value from blockchain transactions. Users and wallets initiate transactions and ensure security, while searchers, builders, MEV relays, and validators engage in more intricate

activities. These latter groups strategically manipulate and assemble transaction blocks to extract profits through mechanisms known as MEV. The primary participants of MEV are listed as follows:

- **Users:** Users generate transactions to execute state changes on the blockchain, whether for simple value transfers, interactions with decentralized applications, or executing complex smart contracts. Their primary goal is to ensure that their transactions are confirmed efficiently and as intended.
- **Wallets:** Wallets not only allow users to easily create and broadcast transactions, but also manage private keys, enforce security practices, and sometimes facilitate interaction with decentralized apps. Leading wallets continue to add features to improve the blockchain experience.
- **Searchers:** Searchers analyze the mempool and inspect pending transactions to identify opportunities for profitable value extraction. There are advanced searchers that employ ML techniques, such as adaptive learning and graph neural networks (GNN) to model user behavior and predict high-value transactions [60].
- **Builders:** Builders assemble blocks of transactions to submit to the chain. They optimize the transaction mix to maximize fees collected based on pending transactions and MEV opportunities. Some builders may operate mining pools or work closely with mining entities.
- **Relays:** Relays act as intermediaries to integrate builders with validators by maintaining private transaction pools. They capitalize on network topology knowledge and low-latency connections to efficiently propagate builder blocks. Their profitability depends on offering value-added services that enable MEV extraction. According to Coincashew⁵, MEV relays

⁵<https://www.coincashew.com/>

are categorized by network types, including Ethereum mainnet, Goerli⁶, and Sepolia Testnets⁷. Each relay is described with attributes, including whether they are non-censoring. This means they do not filter or censor transactions and operate without regulation, ensuring a censorship-free and ethical environment. This indicates that non-censoring relays refrain from engaging in activities like front-running, sandwich attacks, or harming other users' transactions. For example, MEV Watch⁸ helps users to monitor the reliability, uptime, and performance of relays and block builders through detailed tracking and analytics.

- **Validators:** Validators (or block proposers) play a crucial role in controlling the order of transactions and deciding which transactions are included. The likelihood of a validator being selected as a proposer is determined by the size of their stake in the network. To maximize their position's benefits, validators extract MEV by collaborating with relays and builders. This collaboration leverages their temporary status as proposers, allowing them to capitalize on the opportunity to influence transaction ordering for financial gain.

3.2.2. Formalization of MEV

We formalize an MEV activity in the form of a sandwich attack, which is divided into front-running and back-running phases. In the front-running phase, an adversary places a transaction before a legitimate user's order. The aim is to manipulate the asset's price and liquidity to the adversary's advantage. As for the back-running phase, the adversary places another transaction after the user's trade in order to profit from the adjusted market conditions. Figure 6 illustrates the state of the AMM pool immediately before the attacker intervenes, after the attacker's first trade, after the victim's trade, and after the attacker's second trade. The three phases shown at the bottom correspond to the three transactions encoded in the equations below. The highlighted slippage loss in the victim panel and the attacker's profit in the final panel visually correspond to the loss and gain terms in our formal definition of MEV.

To insert sandwich transactions, attackers strategically place a front-running transaction before and a back-running transaction after a victim's trade, forming a "sandwich" around the target transaction. This strategic insertion is achieved by monitoring the mempool for profitable opportunities and using gas fee prioritization to ensure proper execution order (see Section 5.1.3 and Figure 10 for detailed illustration). For our readers' convenience, we divide the formalization process into multiple parts:

User's Transaction: Consider a user $u \in U$ who submits a transaction T_u to exchange a certain amount of an input token for an output token within a liquidity pool with reserves (R_1, R_2) . Let the user's transaction details include the exchanged amount x (in the input token) and the transaction fee f . Before the user's transaction is executed, the expected amount of output tokens that the user aims to receive is given by:

$$y_u^{\text{exp}} = \frac{R_2(1-f) \cdot x}{R_1 + (1-f) \cdot x},$$

where the standard constant-product formula for AMM is applied.

Searcher's Pre-transaction (Front-Run): A searcher $s \in S$, acting as an adversary, inserts a transaction T_s^{pre} before the user's T_u . In this transaction, the searcher swaps x_s units of the same input token for the output token. The immediate output to the searcher's pre-transaction is:

$$y_s^{\text{pre}} = \frac{R_2(1-f) \cdot x_s}{R_1 + (1-f) \cdot x_s}.$$

Consequently, the pool reserves become $R'_1 = R_1 + x_s$ and $R'_2 = R_2 - y_s^{\text{pre}}$.

User's Transaction under Modified Reserves: After the searcher's pre-transaction modifies the pool, the user's transaction T_u is processed with the new reserves (R'_1, R'_2) . Assuming the user's slippage tolerance is not exceeded, the user's received output token amount is now reduced to:

$$y_u = \frac{(R_2 - y_s^{\text{pre}})(1-f) \cdot x}{(R_1 + x_s) + (1-f) \cdot x}.$$

Due to the pool imbalance introduced by the searcher, y_u is strictly less than the original user expectation y_u^{exp} .

Searcher's Post-Transaction (Back-Run): Once the user's transaction is executed, the searcher executes a second transaction T_s^{post} to reverse (or partially reverse) its initial trade and secure a profit. Before post-transaction, the reserves are $R''_1 = R'_1 + x = R_1 + x_s + x$ and $R''_2 = R'_2 - y_u = R_2 - y_s^{\text{pre}} - y_u$. The searcher's post-transaction sells y_s^{pre} units of the output token back into the pool. The resulting amount of the input token that the searcher receives is:

$$x_s^{\text{post}} = \frac{(R_1 + x_s + x)(1-f) \cdot y_s^{\text{pre}}}{(R_2 - y_s^{\text{pre}} - y_u) + (1-f) \cdot y_s^{\text{pre}}}.$$

Searcher's Profit and MEV Extraction: Let b represent the base fee for each transaction submission. The searcher pays fees for both T_s^{pre} and T_s^{post} , totaling $2b$. The searcher's profit Π_s from the sandwich attack is shown as:

$$\Pi_s = x_s^{\text{post}} - x_s - 2b.$$

We use σ_{t-1} to denote the blockchain state immediately before T_s^{pre} . Likewise, σ_t , σ_{t+1} , σ_{t+2} is used to denote

⁶<https://goerli.net/>

⁷<https://github.com/eth-clients/sepolia>

⁸<https://www.mevwatch.info/>

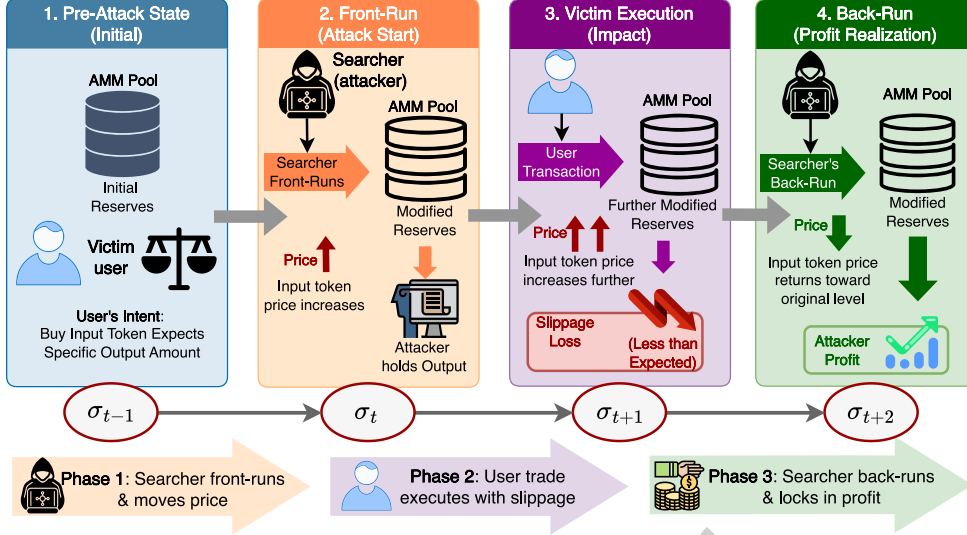


Figure 6: Schematic view of a sandwich attack in an AMM pool.

the subsequent states after each of the three transactions $\{T_s^{\text{pre}}, T_u, T_s^{\text{post}}\}$. Besides, $B_s(\sigma)$ denotes the searcher's token balance at state σ . By considering these elements, extracted MEV is formulated as:

$$\text{MEV} = (B_s(\sigma_{t+2}) - B_s(\sigma_{t-1})) - 2b.$$

Role of Validators: Validators on the blockchain are responsible for ordering and executing transactions within a block. In a sandwich attack, these validators include the searcher's pre-transaction T_s^{pre} and post-transaction T_s^{post} on either side of the user's transaction T_u . The final state σ' of the block as compared to the initial state σ is presented as:

$$\sigma' = T_s^{\text{post}}(T_u(T_s^{\text{pre}}(\sigma))). \quad (1)$$

Eq.(1) indicates the sequential application of the three transactions. By manipulating this transaction ordering, the searcher leverages the altered pool dynamics to extract MEV. This formalization illustrates how sandwich attacks adversely impact user trades and highlights the crucial role of validators in orchestrating the transaction sequence.

3.2.3. MEV Bots

An MEV bot is a software tool designed to identify and take advantage of profitable opportunities on the Ethereum blockchain by adjusting the order of transactions within a block. MEV bots play a crucial role in the MEV ecosystem, exploiting opportunities to extract MEV from blockchains. Their ability to monitor transactions, analyze market conditions, and execute trades swiftly grants them a significant advantage in capturing MEV. Typically, MEV bots are initialized to carry out actions like arbitrage, front-running, sandwich attacks, and flash loans [61]. Such actions exploit price differences, transaction sequencing, and temporary liquidity on DEX

platforms like Uniswap [62] and PancakeSwap [63]. By doing so, MEV bots potentially alter market fairness and clarity, favoring those with more resources, inside knowledge, or control over the blockchain. This negatively impacts other participants who might not be aware of or able to compete with these bots. For example, in arbitrage, bots identify price discrepancies across different DEXs and capitalize on these differences by buying the asset at a lower price on one DEX and selling it at a higher price on another. Front-running involves bots anticipating large transactions and placing their own trades ahead of them, allowing them to benefit from the price movements caused by the larger transaction. Sandwiching involves bots placing buy and sell orders around a large transaction, profiting from the narrow price spread created by the large trade. Liquidation bots monitor loan positions and initiate liquidations when borrowers' collateral falls below the required threshold, capturing liquidation fees and potentially acquiring undervalued assets.

3.3. On-Chain and Off-Chain MEV

There are two distinct approaches within the domain of MEV in blockchain [64]. On-chain MEV refers to the exploitation of blockchain mechanisms by traders to prioritize their transactions using higher gas fees in the public mempool. In contrast, off-chain MEV involves private or permissioned mempools, where validators and traders engage in fee auctions through private channels. This highlights a more controlled and direct interaction that bypasses the public bidding process.

On-chain MEV allows traders to exploit blockchain mechanisms to facilitate transaction execution. When an MEV opportunity arises, traders submit their transactions to the public mempool, where they await retrieval by validators. To improve their chances of success, traders often allocate high gas fees to these transactions,

incentivizing validators to prioritize them in upcoming blocks. While smart contract packaging ensures precise transaction sequencing, traders still face limitations in controlling transaction ordering for certain types of MEV. A major drawback occurs when MEV transactions enter the mempool and become visible to other traders. These competitors attempt to front-run the original trader by submitting higher-fee transactions to exploit the same MEV opportunity, diverting the attention of validators. This reduces the effectiveness of the initial strategy. Examples of on-chain MEV include front-running, sandwiching, and liquidation.

The emergence of off-chain MEV, often referred to as private or permissioned mempools, has simplified the interaction between validators and searchers. These platforms enable fee auctions where searchers compete for validator assistance by proposing higher fees. In off-chain MEV, searchers establish private channels with validators, who are responsible for proposing subsequent blocks. Searchers then use these channels to propose MEV-enhanced blocks, ensuring that the fees within their blocks surpass those validators could obtain from public mempool transactions. Off-chain MEV is particularly well-suited for PoS-based blockchains, where block proposers have enough time for validator-searcher negotiations. The most common types of off-chain MEV include free auctions, private block proposals, and bundle deals.

4. Research Methodology

In this section, we outline the systematic methodology adopted to identify, review, and synthesize the existing body of work on MEV in the context of DeFi. We follow the established systematic review principles inspired by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines [65]. Our approach ensures that studies included in this survey are rigorously selected through transparent and reproducible criteria to address well-defined research questions while maintaining high relevance and methodological quality.

4.1. Selection of Keywords in Literature Search

A comprehensive list of keywords was formulated to capture a wide range of publications related to MEV, DeFi security, blockchain-based transaction ordering, and smart contracts. These keywords were iteratively refined to ensure broad coverage, while remaining focused on the core concepts relevant to the survey. Specifically, we used logical combinations (e.g., AND/OR) of terms involving “DeFi”, “Maximal Extractable Value”, “Miner Extractable Value”, and “blockchain extractable value”. The following sample keyword string illustrates our selection process:

(“extractable value” OR “blockchain extractable value” OR “Maximal Extractable Value” OR “Miner Extractable Value”)
AND

(blockchain OR DeFi OR “decentralized finance” OR arbitrage OR “front-run” OR “frontrunning” OR MEV)

Additionally, synonyms and closely related phrases were incorporated to maximize recall and ensure relevant studies were not overlooked. For instance, we included terms such as “sandwich attacks”, “transaction reordering”, “consensus instability”, “smart contract security”, and “validator incentives”. Whenever possible, we also substituted or supplemented DeFi references with terms related to lending, yield farming, stablecoins, and automated market makers to capture the breadth of research on MEV-relevant issues.

4.2. Database Exploration and Selection Methodology

We conducted our literature search across multiple scientific databases and repositories to ensure comprehensive and unbiased coverage of pertinent publications. The primary sources included IEEE Xplore Digital Library, ACM Digital Library, SpringerLink, ScienceDirect, Web of Science, arXiv, SSRN, and Google Scholar. These platforms were selected for their wide-ranging access to peer-reviewed journal articles, conference papers, and preprints, which provided a robust foundation for our analysis. By searching across these established databases, we ensured that our review would capture a broad spectrum of relevant research on MEV in the context of DeFi and blockchain technologies.

We restricted our search timeframe to the years 2020–2025 to capture the critical period during which DeFi and MEV research grew most rapidly. The search query was adapted slightly to match the indexing peculiarities of each database (e.g., handling of special characters, differences in Boolean operators). We also manually examined the bibliographies of key surveys, review papers, and highly cited technical reports to identify additional relevant sources potentially missed by the initial queries. Fig. 7 provides an overview of the MEV literature corpus used in this survey. Fig. 7a summarizes the selected publications by publication year and venue type, and Fig. 7b reports their distribution across execution platforms. The resulting distributions show rapid growth of MEV research after 2020 and a strong concentration on Ethereum L1, with comparatively fewer studies on L2 rollups, non-EVM L1s, and cross-chain or cross-domain settings.

Search and Screening Phases: The initial search yielded a set of approximately 350 candidate publications. We then followed a multi-phase screening procedure:

1. **Title and Abstract Screening:** Each publication’s title and abstract were checked against our keywords and preliminary inclusion criteria to remove out-of-scope papers (e.g., unrelated cryptographic primitives, purely theoretical finance work without blockchain context). This step reduced the pool to 300.
2. **Full-Text Assessment:** We downloaded the remaining full papers to evaluate their focus on MEV or

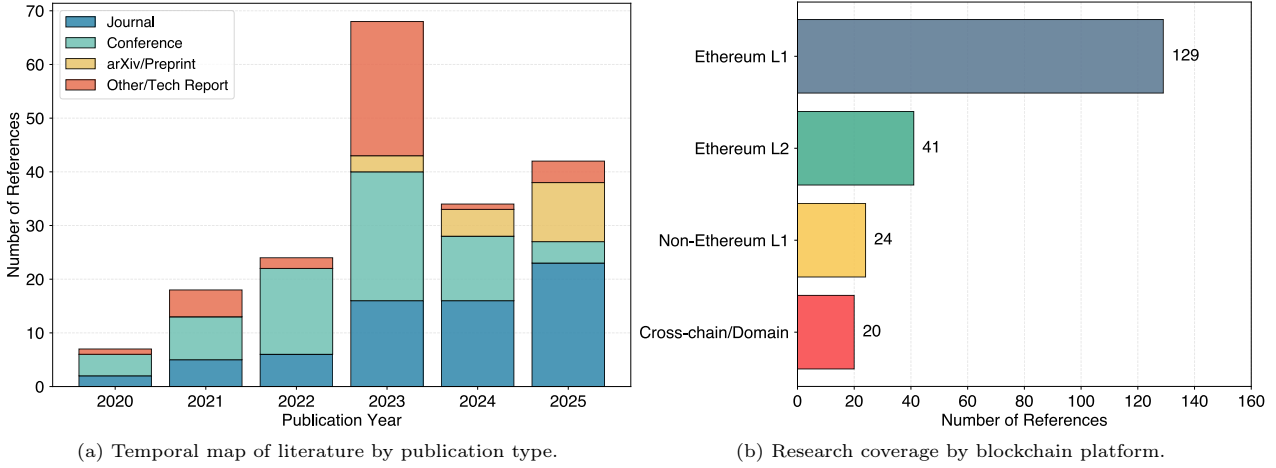


Figure 7: Overview of MEV literature corpus.

DeFi-based transaction manipulation. At this stage, we excluded works that discussed decentralized applications but lacked any treatment of MEV, transaction ordering, or protocol-level manipulations. We also removed duplicate entries. This step reduced the pool to 250 papers.

3. **Relevance to Research Questions:** Finally, each candidate was mapped to one or more of our research questions (see below) to ensure that only papers providing explicit insights on MEV strategies, mitigation measures, on-chain empirical analyses, or cross-chain considerations were retained. This step resulted in a final corpus of 200 references used in our survey.

4.3. Inclusion and Exclusion Criteria

We established transparent and reproducible inclusion and exclusion criteria to ensure systematic study selection while maintaining methodological rigor. For inclusion, we applied specific operational definitions to identify relevant literature:

Topical Relevance: Studies were included if they explicitly addressed MEV-related challenges, operationally defined as research that (1) analyzes specific MEV attack vectors (arbitrage, front-running, sandwich attacks, liquidation exploits, time-bandit attacks, or transaction ordering manipulation), (2) proposes or evaluates MEV mitigation strategies (consensus protocol modifications, fair ordering mechanisms, private mempools, or application-level defenses), (3) provides empirical analysis of MEV extraction patterns using blockchain data, or (4) presents theoretical frameworks for understanding MEV dynamics through game theory, optimization, or economic analysis. Additionally, our review targeted research focused on blockchain-based DeFi applications vulnerable to MEV, specifically including DEXs, automated market makers, lending protocols, stablecoins, yield farming, and cross-chain bridges.

Publication Type and Quality Standards: We retained studies meeting the following criteria: (i) peer-reviewed journal articles from established venues (e.g., ACM Computing Surveys, IEEE Transactions, Springer journals, or domain-specific blockchain journals), (ii) conference papers from reputable venues (e.g., IEEE Symposium on Security and Privacy, ACM CCS, Financial Cryptography, or blockchain-focused conferences with international scope), (iii) workshop papers from high-quality venues (e.g., ACM CCS Workshop on Decentralized Finance and Security), and (iv) technical reports and white papers from established research institutions or recognized protocol teams with demonstrated technical rigor.

Methodological Rigor for Preprints: For preprints, we required demonstration of methodological rigor through either: (1) comprehensive technical implementation with publicly available source code, datasets, or experimental frameworks enabling reproducibility verification, (2) detailed empirical analysis using verifiable blockchain data with transparent data collection and analysis procedures, (3) formal theoretical contributions with mathematical proofs or rigorous modeling frameworks, or (4) systematic evaluation methodologies with clearly defined metrics and validation procedures. This approach ensures inclusion of high-quality preprint research while maintaining academic standards through reproducibility and technical depth assessment rather than arbitrary citation thresholds.

Research Question Alignment: Each candidate study had to address at least one of our four research questions (**RQ-1 to RQ-4**) to guarantee relevance for subsequent taxonomy development, mitigation survey, or empirical analysis. This alignment was assessed through systematic evaluation of abstracts and methodology sections, ensuring each included study contributed meaningful insights to our comprehensive MEV analysis framework:

- **RQ-1:** Which MEV strategies (e.g., front-running, sandwich attacks, liquidation) have been identified, and how do they impact DeFi protocols?

- **RQ-2:** What existing solutions or countermeasures (e.g., consensus protocols, fair ordering approaches, private mempools) are proposed to mitigate MEV exploitation?
- **RQ-3:** How is MEV empirically measured and analyzed in live blockchain systems (e.g., use of relays, replay analysis, heuristic or ML-based transaction detection)?
- **RQ-4:** Which open research challenges remain for future exploration, including emerging trends in cross-chain MEV and theoretical frameworks?

Exclusion Criteria: For exclusion, we removed studies that fell outside our defined research scope while maintaining comprehensive coverage of MEV-related phenomena. Specifically, we excluded research on blockchain infrastructure, consensus mechanisms, or cryptographic protocols that did not connect to transaction ordering dynamics or value extraction vulnerabilities. Studies addressing DeFi protocol design, smart contract security, or financial mechanisms were excluded only when they lacked analysis of MEV implications, attack vectors, or ordering-dependent vulnerabilities. We also excluded general cryptocurrency market analysis, regulatory surveys, and adoption studies unless they provided technical insights into MEV extraction patterns or mitigation effectiveness. Additionally, we removed duplicate publications and studies with insufficient methodological detail for quality assessment. These exclusion criteria ensure systematic focus on MEV research while maintaining inclusive coverage of related DeFi vulnerabilities and value extraction mechanisms that contribute to our comprehensive analysis framework.

4.4. Quality Assessment

To ensure the inclusion of studies with high empirical and theoretical quality, we evaluated each publication based on carefully considered criteria. For empirical robustness, we assessed several key aspects of each study’s methodology. These included the sample size and the experimental design, focusing on whether the study employed standard, reproducible methods for data collection and analysis. We also evaluated the statistical significance of the findings and whether the study provided evidence that could be generalized across different contexts. Furthermore, we considered the reproducibility of results, giving preference to studies that made their data, code, and methods publicly accessible to allow for replication.

For theoretical contributions, we examined the novelty and originality of the models or frameworks proposed by each study, considering how these contributions advanced the understanding of MEV and its impact on DeFi systems. We also evaluated the clarity and coherence of the theoretical explanations, as well as the practical applicability of the models in real-world blockchain systems.

Lastly, we considered the impact of each contribution on the broader field, prioritizing studies that addressed significant gaps in the literature and offered meaningful insights for future research or implementation. As part of the evaluation process, we also ensured that each study was relevant to one or more of the research questions outlined in the survey. This step further strengthened the methodological rigor and transparency of the review. The importance of methodological rigor in blockchain-related research contextualizes the need for rigorous methodological assessment [66]. The qualitative assessment allowed us to maintain a high standard of quality while ensuring that the studies included in our survey made meaningful contributions to the field. We ensured that each screened article had a clear and consistent scope. By systematically applying this multi-step selection methodology, we obtained a robust and relevant dataset of publications to draw upon in our subsequent analyses of MEV strategies, mitigation techniques, and empirical insights. Consequently, this rigorous process lays a solid foundation for developing a comprehensive, evidence-based understanding of MEV in the DeFi ecosystem.

5. MEV Strategies: Taxonomy, Mechanisms, and Impacts

In this section, we move from the structural and protocol-level view of MEV to a strategy-centered analysis of how MEV is realized in practice. Existing work often treats MEV strategies as an open-ended list of ad hoc attacks. To provide deeper synthesis, we organize concrete MEV strategies into four families based on their primary *value source*: (i) *trade-centric ordering strategies*, (ii) *price alignment strategies*, (iii) *state-transition and position strategies*, and (iv) *consensus and blockspace strategies*. This value-source taxonomy focuses on what is monetized by searchers rather than only how individual contracts behave.

5.1. Trade-centric Ordering Strategies

Trade-centric ordering strategies extract value from the placement and sequencing of user trades within a block or bundle. They rely on fine-grained control over transaction ordering and access to orderflow, often through public mempools, private relay channels, or orderflow auctions. In this family, searchers treat user orders as informational signals and use privileged ordering to step in front of, behind, or around them. We focus on three key variants: front-running, back-running, and sandwich strategies.

5.1.1. Front-running Strategy

In front-running scenario, an adversary observes a pending user transaction and injects a competing transaction that executes earlier in the block. In DeFi, this often appears as a searcher who anticipates a large swap on an AMM or a large limit order on an on-chain order book and then

trades first to capture favorable price movement. Figure 8 illustrates the basic pipeline: a user submits a transaction, the adversary detects it in the mempool or through private orderflow, submits a higher-fee or priority transaction, and the block producer includes the adversary's transaction ahead of the user. In our taxonomy, front-running belongs to the family of *trade-centric ordering strategies*. The primary value source is the informational advantage about an imminent trade combined with control over ordering. The adversary monetizes the predictable price impact of the user order. This strategy typically has a strongly extractive and user-harmful impact because it deteriorates the victim's execution quality through additional slippage or worse prices, even when it does not alter protocol-level solvency. Front-running interacts with other strategies in several ways. It often appears inside more complex bundles, for example when a searcher front-runs a large trade and then closes the position via an arbitrage leg across multiple DEXs. It also interacts with congestion and bribery strategies when searchers use priority fees, bundle auctions, or explicit payment channels to secure the lead position in a block [67]. These compositions blur the line between pure front-running and multi-leg MEV and are visible in empirical traces of MEV bundles.

The operational mechanism of front-running has evolved from manual intervention to generalized, automated exploitation. This evolution is exemplified by "imitation attacks", where adversaries replicate profitable transactions observed in the mempool without needing to understand the underlying contract logic [68]. Qin et al. [68] demonstrate that such strategies are highly scalable; their generalized imitation tool, APE, utilizes dynamic program analysis to synthesize adversarial contracts in real-time. The empirical impact of this automation is substantial, with their evaluation attributing over 190 million USD in aggregate profit to imitation-style front-running across Ethereum and BSC. This confirms that the *informational signal* provided by pending transactions is sufficient for value extraction, even absent semantic understanding of the target protocol. Despite the high economic impact, accurately detecting front-running attempts remains a significant challenge due to the complexity of inter-contract interactions. Zhang et al. [69] highlight the limitations of current detection methodologies, introducing a benchmark of 513 real-world attacks to evaluate state-of-the-art tools. Their analysis reveals a low recall rate (approximately 6%), which they attribute to four primary technical hurdles: poor inter-contract analysis, difficulties with cryptographic operations, ineffective detection patterns, and the oversight of token-based profit analysis. These findings underscore the difficulty of monitoring *trade-centric strategies* when execution logic spans multiple smart contracts. Given the difficulty of detection, alternative approaches focus on neutralizing the *ordering control* that makes front-running possible. Doe et al. [70] propose a mitigation framework that fundamentally alters transaction sequencing rules on DEXs. By implementing a

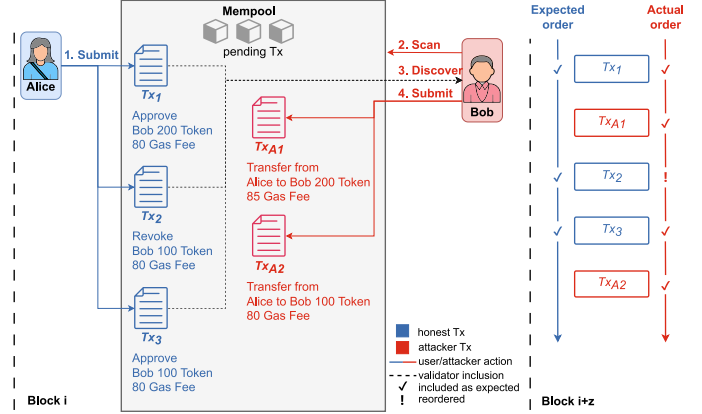


Figure 8: Illustration of front-running strategy involving user and attacker. ① Alice (user) submits transactions (Tx_1, Tx_2, Tx_3) to the mempool; ② Bob (attacker) scans the mempool to identify profitable opportunities; ③ Bob discovers exploitable transactions and generates new ones (TxA_1, TxA_2); ④ Bob rebroadcasts modified transactions with higher gas fees to manipulate the execution order for profit.

weighted counting sort algorithm and a decentralized oracle network, their mechanism orders transactions based on user preferences for delay tolerance rather than gas fees alone. This approach attempts to remove the adversary's ability to "step in front" of the victim. Their evaluation suggests that re-engineering the ordering logic can boost miner utility while simultaneously reducing user costs by approximately 64%, thereby addressing the extractive nature of this MEV strategy at the protocol level.

5.1.2. Back-running Strategy

Back-running strategy aims the price and state changes that follow a user transaction rather than the state before it. A typical back-running scenario (in Figure 9) involves a large swap on an AMM, a large liquidation, or a protocol state transition that creates an arbitrage opportunity. The searcher monitors the mempool or bundled orderflow, waits for the triggering transaction, and then submits a transaction that executes immediately afterward to capture the transient arbitrage or reward. Back-running also falls under *trade-centric ordering strategies* because the value source is a predictable sequence of trades around a prominent user transaction. The searcher profits from structured patterns in price trajectories or state updates that follow large orders, including liquidity mining events or reward distributions. Unlike front-running, back-running can in some circumstances contribute to faster price alignment or liquidity rebalancing; however, it frequently internalizes most of the surplus for the searcher and can expose users to subtle forms of value loss when they face worse effective prices or less favorable post-trade conditions.

The scale and operational mechanics of back-running have been substantiated through several studies. For instance, Oz et al. [71] provide a critical distinction in execution modalities by categorizing strategies into *Network State Back-running* (reliant on latency in First-Come-First-

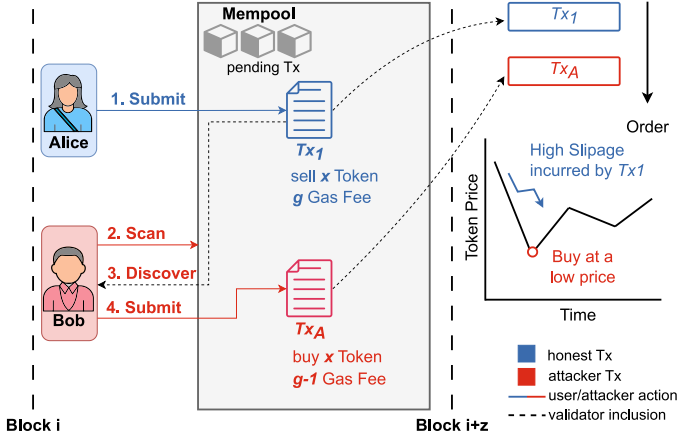


Figure 9: Illustration of back-running strategy involving user and attacker. ① Alice (user) submits a large sell transaction Tx_1 to the public mempool; ② Bob (attacker) monitors the mempool for profitable opportunities; ③ upon detecting Tx_1 , Bob creates a buy transaction Tx_A aimed at exploiting the slippage caused by Tx_1 ; ④ Bob resubmits Tx_A with a deliberately chosen gas price and submission delay so that validators include it immediately after Tx_1 in block $i+z$, enabling the attacker to purchase at the temporarily depressed price and profit when the price rebounds.

Served ordering) and *Block State Back-running* (reliant on specific block positioning). In their study of over 1.1 million arbitrage instances, they observed that searchers predominantly utilized Network State strategies, a behavior driven by the default ordering rules of the underlying network. To understand the relationship between profit and block position, the authors employed an “octile” analysis, which maps the distribution of arbitrage transactions across different segments of a block. Their results reveal a heavy concentration of arbitrage events at the very beginning of blocks. This distribution underscores the intense competition for top-of-block priority, distinguishing the chaotic nature of public mempool back-running from the precise, deterministic positioning enabled by private relay services. In essence, back-running interacts tightly with arbitrage and liquidation strategies. For example, a large Aave liquidation or a large Uniswap trade often creates a short-lived price discrepancy across DEXs. Sophisticated searchers insert a back-running transaction that bridges this discrepancy through multi-hop arbitrage routes. Back-running also couples with consensus and blockspace strategies, where searchers use high gas bids, private relays, or builder channels to ensure that their back-running transaction occupies the optimal position directly after the triggering event.

5.1.3. Sandwich Strategy

Sandwich strategy is a canonical composition of front-running and back-running around a victim’s trade on an AMM. An attacker first places a buy order ahead of the victim to push the price in an unfavorable direction, then allows the victim’s trade to execute at the worse price, and finally places a sell order afterward to realize a profit. Figure 6 and the formalization in Section 3.2.2 show the

three transaction legs and their effect on pool reserves, prices, and the victim’s slippage. Within our taxonomy, sandwich MEVs represent the most prominent *trade-centric ordering strategy*. The value source is the combination of the victim’s price impact and the attacker’s control over ordering. The victim experiences both increased slippage and a worse execution point on the AMM curve. This makes sandwich MEVs strongly extractive and user-harmful. They degrade user trust in AMMs and prompt users to adopt higher slippage tolerances, private routing, or intent-based execution. Sandwich MEVs also act as a building block for more complex strategies. A searcher can embed a sandwich leg inside a broader arbitrage path that spans multiple pools and even multiple chains. For example, a searcher observes a large stablecoin swap on Uniswap, pre-buys the asset to front-run the victim, lets the victim complete the swap, then sells the asset not only on Uniswap but also on SushiSwap or Curve to close an additional arbitrage loop. In cross-chain settings, a sandwich executed on one chain can synchronize with a bridge transfer and a back-running trade on another chain, which illustrates how trade-centric strategies compose with price alignment and cross-chain MEV.

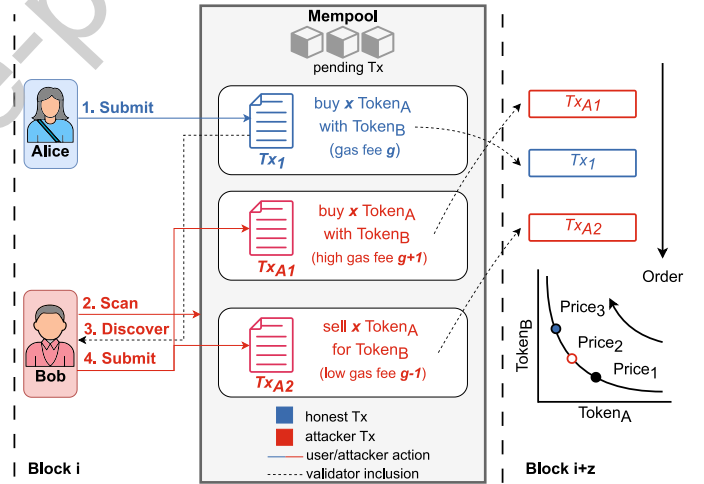


Figure 10: Illustration of sandwich strategy involving user and attacker. ① Alice (user) submits a buy transaction Tx_1 that will move the AMM price curve; ② Bob (attacker) scans the mempool for such price-moving orders; ③ Bob submits a front-running buy Tx_{A1} with a higher gas fee so it is executed immediately before Tx_1 ; ④ Bob then submits a back-running sell Tx_{A2} with a lower gas fee so it lands immediately after Tx_1 in block $i+z$. The sequence $Tx_{A1} \rightarrow Tx_1 \rightarrow Tx_{A2}$ forms the “sandwich,” letting the attacker buy Token A at price₂ and sell at the higher price₃ created by Alice’s trade, thereby capturing the spread as profit.

An augmented variant of on-chain AMM-based sandwich is formalized in [18] to manipulate asset prices and profit from victim transactions. The authors present an analytical framework to model the interactions between an adversarial trader and a victim trader on the AMM-type DEXs. Attacks from both liquidity takers and liquidity providers are considered, in addition to single and multiple adversaries. Their empirical analysis on

Uniswap demonstrates a daily revenue of over \$3,414 by exploiting victim transactions with suitable slippage tolerance. While the study provided a comprehensive analysis of sandwich attacks, it has some limitations. On the other hand, Heimbach et al. [72] address the problem of sandwich attacks on Uniswap and SushiSwap. The authors introduce a game-theoretic model named the “sandwich game” to analyze the interactions between traders, bots, and miners. It is found that using a constant auto-slippage is suboptimal because it fails to adapt to trade size and pool characteristics. A simple algorithm is proposed for traders to dynamically adjust slippage tolerance based on anticipated price movements. The proposed algorithm reduces the cost by more than a factor of 100 compared to Uniswap’s auto-slippage. However, for larger trades (e.g., 1 million US dollars or more), the algorithm does not entirely prevent the attacks but rather reduces their occurrence. For instance, the impact of flash loans is not considered which amplifies the severity of sandwich attacks. Moreover, the paper does not account for the behavioral aspects of traders, which may influence their slippage tolerance settings and responses to sandwich attacks.

5.2. Price Alignment Strategies

Price alignment strategies extract value from price discrepancies across venues or domains. They rely on differences in liquidity, latency, and execution rules across DEXs, centralized exchanges, and distinct chains or rollups. In contrast to pure trade-centric strategies, where value comes primarily from the victim’s own price impact, price alignment strategies exploit inconsistencies between markets and often contribute to price discovery. We highlight arbitrage and cross-chain MEV as key representatives.

5.2.1. Arbitrage Strategy

Arbitrage is one of the most pervasive MEV strategies across DeFi. In a simple cross-DEX arbitrage, a searcher observes that a token pair trades at a lower price on one AMM than on another. The searcher buys the asset on the cheaper venue and sells it on the more expensive venue, profiting from the price difference. More sophisticated methods include multi-hop arbitrage across several pools, CeFi-DeFi arbitrage between centralized and decentralized venues, and triangular arbitrage among correlated assets. In the proposed taxonomy, arbitrage is a *price alignment strategy*. The primary value source is the violation of the law of one price across venues or assets. Arbitrage can improve overall market efficiency by narrowing spreads and aligning prices, which gives it a productive role at the system level. At the same time, access to privileged orderflow, low-latency infrastructure, and preferential positions inside blocks concentrates arbitrage profit among a small set of well-equipped searchers. This concentration creates fairness concerns even when end-user execution quality improves on average. Arbitrage interacts with trade-centric strategies

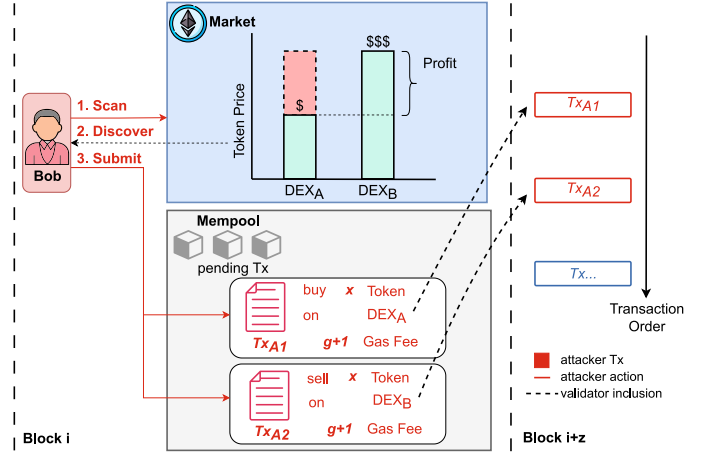


Figure 11: Illustration of arbitrage strategy involving two DEXs. ① Bob (attacker) scans the mempool and market prices across DEXs for price discrepancies; ② An arbitrage opportunity is discovered by identifying a price difference between DEX_A and DEX_B ; ③ Bob submits transactions (Tx_{A1} to buy tokens on DEX_A and Tx_{A2} to sell tokens on DEX_B) with higher gas fees to ensure priority in execution; ④ Profits are achieved from the price difference by completing the buy-sell cycle.

when searchers layer front-running or back-running around user orders that open arbitrage opportunities. For example, a searcher can front-run a large user swap that pushes a pool far from its external reference price, then use an arbitrage leg across another DEX to restore alignment. Arbitrage also interacts with consensus-level strategies when searchers use bribery, private relays, or builder markets to secure inclusion of complex arbitrage bundles that would otherwise fail or suffer from race conditions. Figure 11 illustrates the process of MEV extraction through arbitrage MEV. Arbitrageurs capitalize on price differences and market irregularities across diverse DEXs and DeFi platforms.

The implementation of arbitrage strategies in Ethereum has been shown to generate substantial profits, with some studies reporting returns exceeding hundreds of millions of dollars [20, 73–77]. For instance, if ETH is priced at 2000 USD on Uniswap and 2100 USD on SushiSwap, an arbitrageur purchases on Uniswap and immediately sells on SushiSwap, earning a 100 USD ETH profit. With the rapid evolution in arbitrage methods, defining a universal arbitrage strategy in MEV becomes challenging as identifying these arbitrage transactions has become more complex and time-consuming [39]. For example, [20] introduces two tools named DEFIPOSER-ARB and DEFIPOSER-SMT to automatically create profitable DeFi transactions by using arbitrage detection and state transition models, respectively. The Ethereum-based analysis revealed that the tools uncovered revenue opportunities amounting to 5.65 million US dollars over 150 days. This includes identifying the attack on Ooki platform (formerly bZx [78]) that generated 0.48 million US dollars, with some transactions detected surpassing the Ethereum block reward by 874 times, potentially encouraging miners to fork the chain. While these tools may

help protocol designers, liquidity providers, and traders in capitalizing on DeFi opportunities and navigating its risks, they overlook the effects of unconfirmed transactions and potential collaboration between traders and miners. On the other hand, McLaughlin et al. [79] conduct a detailed study of arbitrage within the Ethereum blockchain, uncovering 3.8 million transactions with a total of 321 million US dollars in profits. They identify four billion opportunities with a potential weekly gain of 395 Ether. Extensive analysis of DEX applications introduces support for complex price models to accommodate a spectrum of exchanges with diverse pricing structures and fee-on-transfer token mechanisms. An increase in arbitrage revenue is reported, potentially impacting consensus stability. Furthermore, arbitrage appears to reduce the cost of price-oracle manipulation [80], as evidenced by empirical data. Meanwhile, the study acknowledges some limitations, including potential inaccuracies in identifying and detecting arbitrage opportunities, the omission of arbitrage effects on various DeFi applications, and the neglect of the strategic behavior of arbitrageurs.

5.2.2. Cross-chain Strategy

Cross-chain strategy represents a fundamental paradigm shift from single-chain MEV due to the loss of atomicity and the introduction of asynchronous state transitions across heterogeneous security domains. Unlike atomic single-chain transactions that either execute completely or revert, cross-chain MEV strategies face settlement risk because a profitable strategy decomposes into transactions on separate ledgers, where one leg succeeds while another fails due to latency, congestion, or slippage [81, 82]. In our taxonomy, cross-chain MEV extends *price alignment strategies* across domains. The value source lies in price discrepancies, liquidity fragmentation, and settlement asynchrony between chains, rollups, and bridges. Searchers construct paths that trade the same or correlated assets across multiple domains, use bridges to move assets or proofs, and rely on their ability to predict confirmation patterns and delays. The strategy covers both sequence-dependent arbitrage, which requires asset transfer across chains, and sequence-independent arbitrage, where the searcher maintains inventory on multiple chains. Cross-chain MEV interacts with several other strategy families. For example, time-bandit strategy become more complex in multi-domain settings, as reorgs or delayed finality on one chain can affect cross-chain positions. Cross-chain arbitrage bundles often incorporate sandwich or back-running legs on the source or destination chain and liquidation or oracle-related legs on lending protocols that span chains. These compositions amplify both the profit potential and the systemic risk, which complicates the design of safe bridges and interoperability protocols.

Cross-chain scenario represents a fundamental paradigm shift from single-chain MEV due to the loss of atomicity and the introduction of asynchronous state transitions across heterogeneous security domains [81]. Unlike single-chain

environments where transactions are atomic, meaning they either execute completely or revert with no state change, cross-chain MEV strategies decompose into transactions on separate ledgers (e.g., Arbitrum [83], Optimism⁹, and Polygon [84]) with distinct block intervals and finality mechanisms. This introduces significant *execution risk*, where a searcher may successfully execute the first leg of an arbitrage on one chain but fail on the second due to latency or congestion, leaving them with unintended inventory exposure [82]. To mitigate this, strategies are categorized based on their dependency on asset transfer. *Sequence-Dependent Arbitrage (SDA)* relies on bridges to move assets and introduces latency that exposes traders to price slippage; whereas *Sequence-Independent Arbitrage (SIA)* involves maintaining liquidity inventory on multiple chains to execute parallel trades [85, 86]. Furthermore, liquidity fragmentation across domains turns cross-chain MEV into a complex coordination problem. Frameworks like FluxLayer [87] argue that arbitrage is constrained by pool depth and settlement speed, proposing intent-centric liquidity layers and restaking-based settlement to make execution practical at scale.

Beyond execution complexity, the infrastructure connecting these domains introduces novel attack vectors that do not exist in single-chain settings. Li et al. [88] identify *cross-chain sandwich attacks* as a critical vulnerability where adversaries exploit the public emission of bridge events on the source chain to front-run transactions on the destination chain before they even appear in the local mempool, effectively bypassing traditional mempool privacy defenses. This parallels the rise of “optimistic MEV” on Layer 2 networks, where searchers engage in speculative probing of sequencer ordering to capture value amidst uncertain cross-domain states [89]. Measuring these phenomena requires correlating activity across multiple ledgers and infrastructure layers, a task with significant engineering overhead compared to single-chain analysis. For instance, early detection methods [90] often focused solely on Uniswap across limited domains, disregarding activity on other major DEXs like SushiSwap¹⁰ or PancakeSwap¹¹. Consequently, recent large-scale empirical studies confirm that these technical barriers have restricted profitable extraction to a small set of sophisticated actors, driving centralization across the ecosystem [82].

5.3. State-transition and Position Strategies

State-transition and position strategies extract value from discrete protocol events and the management of positions such as loans, collateral, or oracle-referenced obligations. They rely less on immediate price impact of user trades and more on the sequencing and triggering of protocol-defined transitions. We focus on liquidation MEV

⁹<https://www.optimism.io/>

¹⁰<https://www.sushi.com>

¹¹<https://pancakeswap.finance/>

and oracle manipulation as two central representatives of this family.

5.3.1. Liquidation Strategy

Liquidation strategy arises in lending and margin protocols that rely on over-collateralization [19]. When a borrower's collateral value falls below a safety threshold, the protocol permits or incentivizes liquidators to repay debt in exchange for a portion of the collateral. Figure 12 illustrates a typical scenario: a price drop pushes a position into the liquidation region, an oracle updates the price, and then a liquidator transaction repays debt and receives discounted collateral. Searchers compete to be the first liquidator and capture the associated reward. In the value-source taxonomy, liquidation is a *state-transition and position strategy*. The key value source is the discrete protocol transition that moves a position from healthy to liquidatable. Liquidation has an inherently dual role. It stabilizes the protocol by preventing under-collateralization, which is productive at the system level. At the same time, design choices such as high liquidation discounts, limited auction competition, or restricted participation can turn liquidations into strongly extractive events for borrowers and smaller liquidators [91]. Liquidation interacts with oracle manipulation and arbitrage in practice. An attacker who artificially depresses a price on an oracle-dependent DEX creates a window in which previously safe positions become liquidatable. The same attacker then liquidates these positions at a discount and closes residual exposure through arbitrage across other venues. This composition combines state-transition MEV with oracle-based information manipulation and price alignment, which complicates forensic analysis and mitigation.

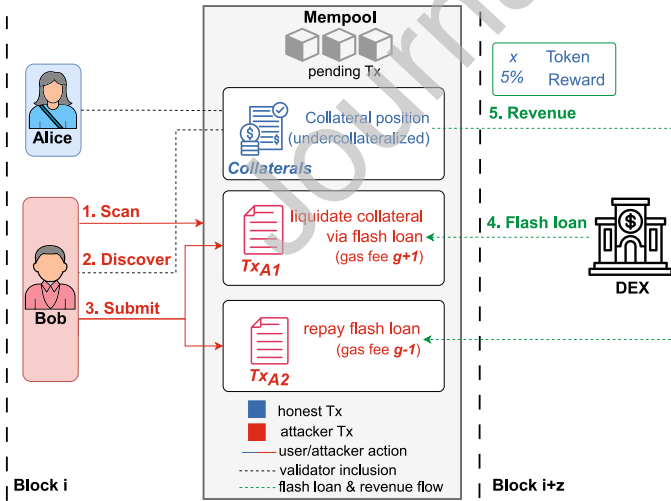


Figure 12: Illustration of liquidation strategy involving user and attacker. ① Bob (attacker) scans the mempool; ② after detecting an under-collateralized position, Bob prepares to liquidate it; ③ Bob submits two transactions: Tx_{A1} liquidates the collateral via a flash loan (gas fee $g+1$) and Tx_{A2} repays that flash loan within the same block (gas fee $g-1$); ④ the flash-loan principal is obtained from an external DEX; ⑤ the protocol pays Bob a liquidation bonus, realizing revenue.

The practice of liquidation MEV exploits has several negative impacts on the DeFi ecosystem. It increases the cost of borrowing as MEV extractors include the cost of preemptive transaction fees in their charges, making loans more expensive for borrowers. Additionally, it compromises the efficiency of lending pools because extractors withdraw value from these pools, reducing the potential gains for both borrowers and lenders. These effects cumulatively lead to a more expensive and less stable DeFi system. For example, [92] discusses the potential of MEV redistribution in PoS, where the authors demonstrate the efficacy of MEV redistribution and protocol-owned liquidity in maintaining minimum staking levels and smoothing reward distributions. The authors explore the dynamics of rational validators' MEV revenue from an on-chain liquidation perspective to discourage validator disengagement. Additionally, the adaptability of MEV redistribution is accommodated with sub-exponential inflation schedules to reduce wealth concentration and inflationary costs within PoS systems. While the study effectively explores the impact of MEV redistribution from on-chain lending liquidations, it does not consider other MEV sources such as front-running, arbitrage, and sandwich attacks. Moreover, the assumption of fixed borrowing demand and deterministic lending overlooks the impact of staking derivatives on the effective staked supply.

5.3.2. Oracle Manipulation Strategy

Oracle manipulation targets the data sources that protocols use to determine prices, collateralization ratios, or other critical parameters [93, 94]. In DeFi, many protocols rely on on-chain oracles that aggregate price feeds from AMMs, order books, or external data providers. Within our taxonomy, oracle manipulation constitutes a *state-transition and position strategy*. The primary value source is not the immediate execution of the trade itself, but the induced shift in protocol state boundaries. By artificially distorting the reference price, an attacker alters the criteria for solvency, thereby unlocking underpriced borrow positions, triggering unwarranted liquidations, or enabling favorable stablecoin issuance. This strategy is inherently systemic and extractive, as it undermines the foundational trust in pricing data and often precipitates cascading insolvency events. Consequently, oracle manipulation rarely occurs in isolation; instead, it frequently serves as the catalyst in a multi-stage attack graph. A canonical example involves manipulating a low-liquidity pool to force a target position into liquidation, allowing the attacker to purchase the collateral at a discount before rebalancing exposure through arbitrage on deeper venues [82]. This composability highlights the necessity for defenses that model the entire attack lifecycle rather than individual exploits.

The operational complexity of these attacks depends heavily on the specific aggregation mechanism used by the target protocol. Mackinga et al. [95] scrutinize the vulnerabilities inherent in Time-Weighted Average

Price (TWAP) oracles through a comparative analysis of *single-block manipulation* and *Multi-block MEV (MMEV)* strategies. The latter represents a sophisticated evolution of *state-transition strategies*, wherein the adversary collaborates with block proposers to secure control over consecutive blocks. This collusion significantly lowers the capital requirements for price distortion. Their findings indicate that while single-block attacks suffice for certain extensive manipulations, MMEV strategies exploit privileged access to consensus to fundamentally alter the protocol's internal valuation logic. To mitigate these risks, the authors advocate for statistical hardening at the protocol level, specifically the replacement of arithmetic means with geometric means or medians to increase resistance against outlier data.

5.4. Consensus and Blockspace Strategies

Consensus and blockspace strategies extract value from control over block construction, chain history, and the allocation of scarce blockspace. They move beyond individual contracts or trades and operate at the level of the consensus mechanism, the mempool, and the block producer. We consider bribery, time-bandit and clogging strategies as the main representatives of this family.

5.4.1. Bribery Strategy

Bribery strategies refer to mechanisms where searchers or external parties pay block producers, committee members, or other validators to favor specific transactions, bundles, or blocks. Bribes can take explicit forms, such as out-of-band payments and auction-style block markets, or implicit forms, such as fee rebates and preferential orderflow routing. Figure 13 depicts a typical bribery pipeline where searchers submit MEV bundles to a builder, the builder constructs a block that maximizes shared profit, and the block producer receives a direct payment for including that block. In the value-source taxonomy, bribery constitutes a *consensus and blockspace strategy*. The primary value source here is the commoditization of block construction rights and the precise allocation of blockspace. This dynamic transforms block production into a tradable asset, channeling a portion of MEV from searchers to validators. While this can improve protocol sustainability by replacing opaque off-chain deals with transparent auctions, it simultaneously introduces risks of centralization and cartel formation if a small set of actors dominates the bidding pipeline. Bribery strategies interact heavily with trade-centric and price alignment strategies; most complex arbitrage or sandwich bundles now reach block producers through bribery-like channels (e.g., Proposer-Builder Separation) [49]. Furthermore, they interact with clogging and time-bandit strategies, as actors with privileged access to block producers can crowd out competitors or influence chain reorganization decisions.

The feasibility and economic incentives of these strategies have been rigorously modeled in recent literature. Ruan

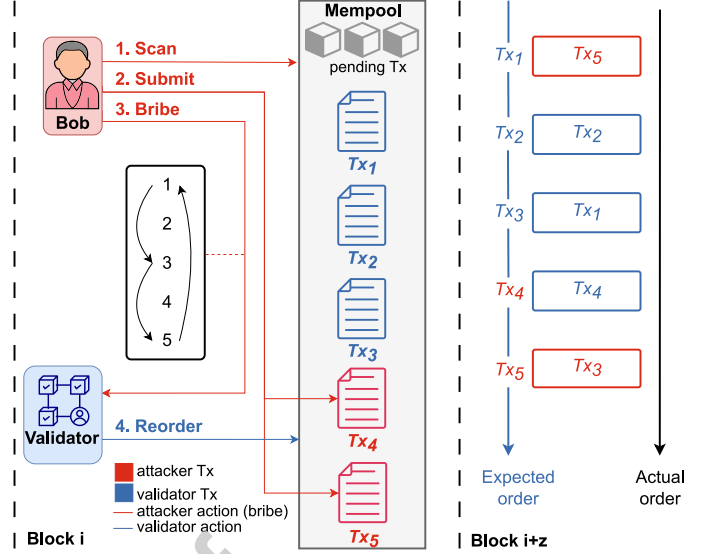


Figure 13: Illustration of bribery strategy involving attacker and validator. ① Bob (attacker) scans the mempool for profitable reordering opportunities; ② Bob submits replacement transactions Tx_4 and Tx_5 that yield higher profit if they execute ahead of Tx_{1-3} ; ③ Bob sends an off-chain bribe to the validator to incentivize the reorder; ④ the validator accepts the bribe, reorders the pending list (executing Tx_5 first and pushing Tx_3 to the end), and produces block $i+z$.

et al. [96] propose a quantitative framework specifically designed to evaluate the impact of bribery on consensus security. By employing a Markov decision process, they model the behavior of rational miners and demonstrate how bribery alters the equilibrium of consensus protocols to incentivize double-spending and transaction reordering. This theoretical risk is compounded by practical execution mechanisms; McCorry et al. [97] introduce smart contract architectures that trustlessly facilitate bribe payments between attackers and miners, thereby automating the corruption process. Further expanding the threat landscape, Judmayer et al. [98] provide evidence that bribery decouples attack feasibility from computational resources. Their analysis proves that adversaries can disrupt consensus or censor transactions without possessing significant hash power, provided they have sufficient capital to bribe the existing validator set. Collectively, these studies underscore that market-based bribery channels can be as destabilizing as cryptographic attacks like selfish mining, highlighting the need for robust, MEV-aware consensus designs.

5.4.2. Time-bandit Strategy

Time-bandit strategies involve the retrospective alteration of blockchain history to capture previously exposed MEV opportunities [22]. In this scenario, a miner or coalition of miners observes a past block containing high-value transactions, such as significant arbitrages or liquidations. Instead of extending the canonical chain, the attacker forks the network at a previous height and re-mines the block to redirect the value to themselves. Crucially, this strategy

requires the attacker to command majority hash power (the 51% threshold) to override the legitimate chain and enforce their alternative history as canonical. We classify this approach under *consensus and blockspace strategies*. The primary value source is the manipulation of consensus finality and the economic incentives inherent in block production, rather than simple intra-block ordering. Consequently, time-bandit strategies are highly extractive and pose a fundamental systemic risk by eroding transaction immutability. They demonstrate a critical interaction between application-layer rewards and protocol-layer security: as the profitability of other MEV strategies (like cross-chain arbitrage) increases, the economic incentive to destabilize the consensus layer through chain reorganization grows proportionally. This dependency implies that infrastructure improvements which concentrate MEV can inadvertently lower the security threshold of the entire network.

5.4.3. Clogging Strategy

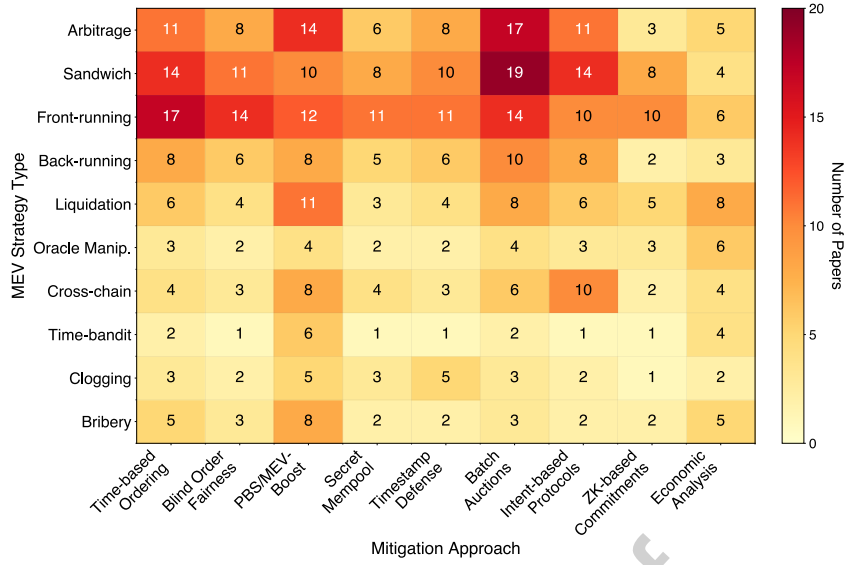
Clogging strategies involve the systematic flooding of the mempool or blockspace to crowd out competing transactions. By broadcasting a high volume of transactions with competitive fees, an adversary dominates block inclusion, thereby artificially inflating gas prices and network congestion [21]. We classify this approach under *consensus and blockspace strategies* because the primary value source derives from the monopolization of network capacity rather than the ordering of specific trades. Consequently, clogging is strongly extractive; it degrades application liveness and imposes direct costs on neutral users. Beyond direct denial-of-service, these strategies frequently serve as a force multiplier for other MEV forms. For instance, searchers may leverage clogging to delay oracle updates, thereby amplifying liquidation opportunities, or to stifle competition during high-value arbitrage windows. In extreme scenarios, the induced congestion masks more sophisticated vectors, such as time-bandit reorgs, by rendering the distinction between organic demand and malicious spam indistinguishable to external observers.

5.5. Ethical and Economic Impact of MEV Strategies

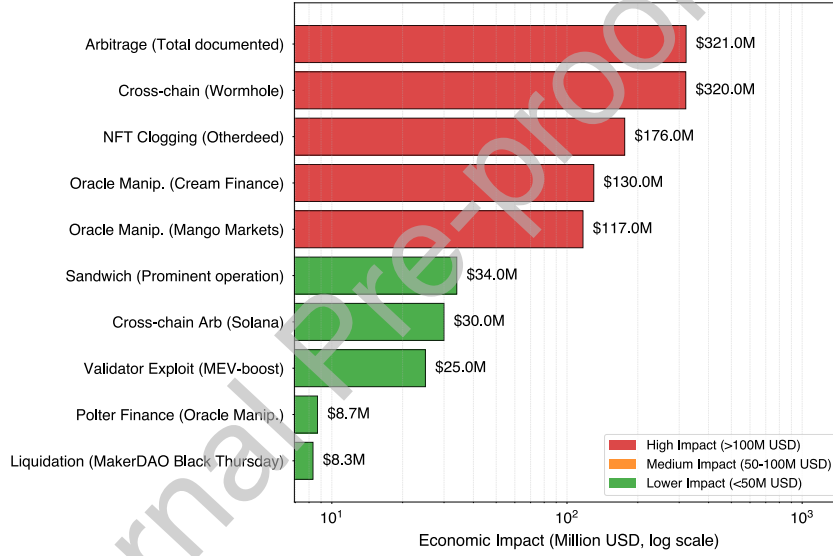
Building on the taxonomy, we now assess how the four strategy families position themselves along the continuum between *extractive* and *productive* MEV. Using the framework established in Section 3.1, we evaluate these strategies based on their net impact on user welfare and protocol robustness [34, 56, 57]. Strategies such as time-bandit, bribery, clogging, and oracle manipulation strategies fall squarely into the extractive category. They capture value by undermining consensus stability, distorting validator incentives, or corrupting price signals. These actions impose direct operational costs on other participants and degrade the integrity of the protocol [33, 72, 99]. Conversely, cross-venue arbitrage and protocol-designed liquidations generally align with productive MEV, as they provide intermediation services

that reduce price dispersion and maintain solvency in lending markets [34, 100]. However, many MEV strategies exist on a spectrum where execution details determine the realized economic impact. While pure arbitrage improves price alignment, the associated competition mechanisms (e.g., priority gas auctions) often introduce extractive spillovers through network congestion and elevated transaction costs for unrelated users [57, 58]. Liquidations exhibit similar nuances; although necessary for preventing bad debt, aggressive liquidation races concentrate profits and amplify penalties for distressed borrowers. This competitive intensity often shifts the activity toward the extractive end of the spectrum [33, 34]. Classical front-running and sandwich MEV remain prototypical extractive strategies, as they generate profit by intentionally degrading the execution quality of victim transactions. From a system-wide perspective, these extractive forms act as negative externalities on the blockchain commons, threatening both decentralization and user trust [59]. Consequently, effective mitigation should not aim to eliminate all profit opportunities, but rather to suppress extractive behavior while channeling productive activity into transparent, protocol-aligned mechanisms [33, 72]. Figure 14 complements this qualitative assessment by mapping how frequently the surveyed literature analyzes each combination of MEV strategy type and mitigation approach. The resulting distribution reveals dense coverage for several well-studied MEV strategies and mitigation mechanisms, alongside noticeable gaps for others. Figure 14b summarizes the realized economic scale of representative MEV incidents and shows that some of the largest documented losses stem from diverse exploit categories, which reinforces the need to prioritize mitigation efforts toward the most systemically harmful forms of extractive MEV. In addition, we synthesize representative studies across different protocol layers, analytical methods, and reported profit models in Table 2. The comparison details the operational layer, attack vectors, profit estimation methodologies, and the replicability of empirical findings. We classify replicability as high (source code and testbeds are available), medium (experimental scenarios are reconstructible), or low (insufficient details are provided for reproduction).

Insights: The comprehensive analysis of MEV strategies reveals the sophisticated and evolving nature of value extraction techniques in DeFi ecosystems. The examined strategies demonstrate a clear progression from simple arbitrage opportunities to complex multi-chain manipulations, highlighting how attackers continuously adapt to exploit new vulnerabilities as blockchain technology advances. The analysis underscores three critical insights: first, the transparency inherent in blockchain systems creates systematic vulnerabilities that enable predictable value extraction; second, the economic incentives driving MEV extraction often exceed traditional block rewards, potentially threatening consensus stability; and third, the interconnected nature of DeFi protocols amplifies the impact and profitability of



(a) Strategy vs mitigation coverage heatmap.



(b) Economic impact of MEV strategies.

Figure 14: Mitigation coverage and economic footprint of key MEV strategies.

individual attacks across entire ecosystems.

6. MEV Mitigation Solutions

In this section, we discuss different mitigation (or countermeasure) strategies for MEV. Given the diverse nature of the MEV exploiting strategies, it is essential to address them across all layers of the blockchain ecosystem. For instance, arbitrage and front-running exploit mempool transparency and transaction ordering vulnerabilities, while sandwich attacks leverage predictable execution sequences to extract value from user transactions. Similarly, liquidation strategies target protocol-specific design weaknesses, while cross-chain MEV exploits interoperability gaps between blockchain ecosystems. These diverse attack vectors demonstrate that MEV vulnerabilities span multiple system components, making single-point mitigation solutions

insufficient as attackers can adapt by shifting between different exploitation mechanisms when individual attack paths are blocked. Comprehensive MEV defense therefore requires coordinated mitigation strategies that address vulnerabilities simultaneously across different blockchain layers to prevent adversarial adaptation and ensure robust protection [102].

We divide the existing countermeasures into four levels – i) consensus, ii) base, iii) application, and iv) other solutions. Figure 15 presents our comprehensive four-layer taxonomy that systematically categorizes existing MEV mitigation approaches, mapping each countermeasure to its corresponding implementation layer within the blockchain stack to provide a structured framework for understanding defense strategies across different system levels. In addition, we compare existing MEV mitigation

Table 2: Comparative analysis of different MEV strategies.

Ref.	MEV Type	Layer	Method	Framework	Profits	Basis	Replicable	Remarks
[18]	Sandwich	Application	CP	AT	3K USD	Avg. daily USD	H	Single/multi-adversary; excludes on-chain AMM
[20]	Arbitrage	Application	BFM	CTD	5.7K ETH	Avg. weekly ETH	H	Significant weekly revenue; path explosion issues
[21]	Arbitrage, liquidation, sandwich	Application	Tx replay	relay	540M USD	On-chain events	H	Large MEV assessment; replay-attack algorithm
[79]	Arbitrage, back-running, sandwich	Application	DMG	AD	321M USD	Bundle aggregation	H	Multi-million arbitrages; non-CP pricing
[69]	Front-running	Application	SVL	DTA	1.18K ETH	Token balance	M	Smart contract security benchmark
[68]	Front-running	Application	AAS	CFG	192M USD	Asset gain minus costs	H	No consensus changes; EVM compatible
[70]	Front-running	Application	WCS	WSS	2.5K USD	Utility function	H	Improves utility; oracle implementation
[72]	Sandwich	Application	AST	GT	<1M USD	Liquidity & Tx ratio	M	Models traders/bots; fails at larger trades
[92]	Liquidation	Consensus	AG	SL	N/A	Reward & burn ratio	L	MEV redistribution; staking-lending dynamics
[90]	Cross-domain	Application	SEA	relay	0.2 WETH	Token swap differences	H	Uniswap-focused; real-time tracking
[101]	Arbitrage, sandwich	Consensus	OM	GT	N/A	PoA	L	Nash equilibrium; knapsack optimization
[95]	Oracle manipulation	Application	CM	AVA	1.46 ETH	Hashpower cost	L	Cost-effective TWAP
[96]	Bribery	Base	QA	MDP	N/A	MB & FB	L	Systematic attacks; profit quantification

Abbreviations: AAS: Automated Adversarial Synthesis; AG: Agent-based; AD: Arbitrage Detection; AST: Auto Slippage Tolerance; AT: Adversarial Trading; AVA: Attack Vector Analysis; BFM: Bellman Ford Moore; CFG: Control Flow Graph; CM: Collusive Mining; CP: Constant Product; CTD: Complex Transaction Detection; DMG: Directed Multi Graph; DTA: Dynamic Taint Analysis; FB: Fixed-Fee Bribery; GT: Game Theory; MB: Markov Bribery; MDP: Markov Decision Process; OM: Ordering Mechanism; PoA: Price of Anarchy; QA: Quantitative Analysis; SEA: Swap Events Analysis; SL: Staking and Lending; SVL: Scalable Vulnerability Localization; Tx: Transaction; WCS: Weighted Counting Short; WETH: Wrapped Ether; WSS: Weighted Sequencing Service; **Replicability:** H = High (full code/data available); M = Medium (limited reproducibility); L = Low (methodology only); **Others:** N/A = Not Available (Specific amount of profit is not mentioned).

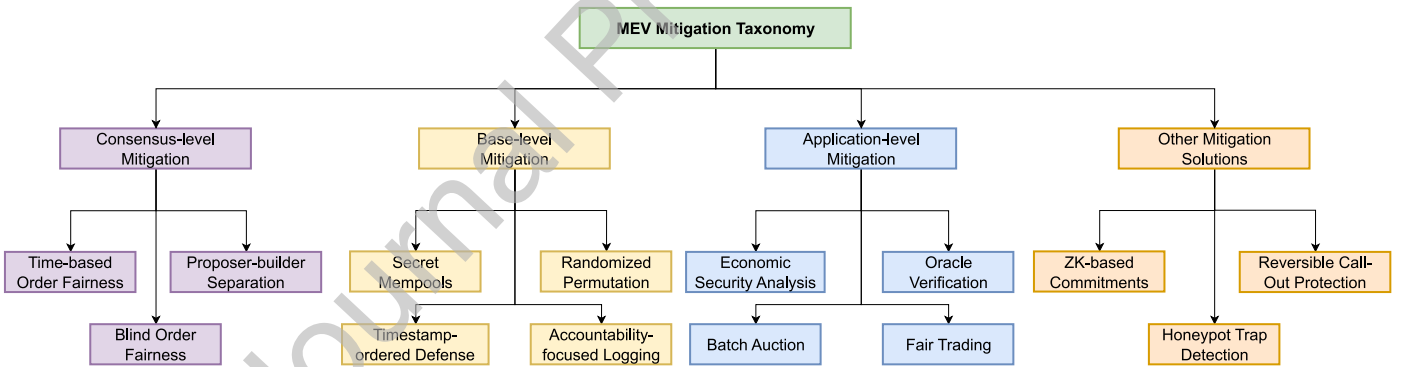


Figure 15: Multi-layer taxonomy of MEV mitigation solutions.

studies in Table 3 based on various criteria: types of MEV, the mitigation layer, mechanisms employed for MEV mitigation, frameworks utilized in the mitigation process, scalability of the proposed solutions, interoperable with different blockchain systems, the presence of any formal analysis, the replicability of the methods, and additional remarks. To make the qualitative ratings in Table 3 explicit, we adopt a unified set of criteria for *Scalability*, *Replicability*, and *Interoperability*. Scalability reflects the expected deployment overhead and evaluation scale of each proposal. A solution is labeled high (H) when the design introduces low per-transaction overhead and the paper either reports experiments at blockchain scale (for example, tens of thousands of transactions

or large validator sets) or provides asymptotic analysis that supports such deployment. We use medium (M) when the scheme introduces moderate cryptographic or coordination overhead and the evaluation is limited to small or medium size testbeds. We assign low (L) when the proposal is mainly conceptual, lacks performance evaluation, or requires heavyweight coordination that would restrict throughput in practice. Replicability reflects the availability of implementation artifacts and experimental details. We assign high (H) when open-source code, configuration scripts, and datasets are available so that the reported results are reproducible end-to-end, medium (M) when the paper provides detailed algorithmic descriptions and partial artifacts that enable partial reproduction,

and low (L) when only a high-level design or limited pseudocode is provided without public artifacts. Finally, Interoperability assesses the solution's adaptability. We assign a supported mark (✓) if the mechanism is designed to function across multiple blockchain architectures or consensus protocols, and a not-supported mark (✗) if the solution is strictly tailored to a specific chain or fixed environment.

6.1. Consensus-level Mitigation

Based on the existing studies focusing on MEV mitigation, we classify the consensus-level mitigation solution into – i) Time-based Order Fairness, ii) Blind Order Fairness, and iii) Proposer-builder Separation.

Time-based Order Fairness (TOF): TOF is a robust and efficient approach to mitigate MEV attacks in blockchain systems. By leveraging the relative arrival times of transactions at a majority of validators, TOF ensures that transactions are processed in a fair and tamper-proof manner. This mechanism effectively prevents malicious actors from exploiting network delays and transaction contents to their advantage. It also offers several benefits, including ensuring fairness for all participants by determining transaction order, strengthening trust through transparent ordering processes, and potentially reducing latency by separating ordering from execution. Several works [103, 113–120] aim to separate the process of determining transaction order from transaction execution, in order to achieve more fair sequencing.

Helix [113] ensures transactions are selected and sequenced in blocks through a randomized mechanism, dependent on a beacon within the consensus protocol. Similarly, Aequitas [114] offers guarantees on the sequence of transactions within a block. However, it works in the most optimal manner in a controlled environment, leading to increased communication demands. Moreover, Pompe [115] is a Byzantine ordered consensus (BOC) method that determines a transaction's sequence by allocating it a unique identifier. Furthermore, Wendy [116, 117] outlines ordering protocols specifically for controlled systems. To maintain relative order, it is essential to create a dependency network ensuring transactions are not processed before their prerequisites [118, 119].

Masquerade [103] is a lightweight solution, which employs a token-number system to address the problem of transaction reordering attacks caused by MEV. The authors demonstrate that the proportion of front-running transactions is inherently limited by the ratio of the adversary's wealth to the user's wealth. Additionally, they illustrate that the wealth ratio decreases over time, causing the proportion of front-run transactions to asymptotically approach zero. This effectively eliminates the front-running threat as the user's wealth accumulates. Nevertheless, there are several limitations to this solution. Firstly, it assumes that both the user and the adversary adhere to fixed policies for purchasing and utilizing tokens, which does not accurately reflect the real-world behavior of rational

agents. Secondly, it fails to account for the influence of network delays, transaction fees, and gas prices on the token system. Thirdly, it lacks a formal security analysis of the token issuance algorithm and the token verification process.

Blind Order Fairness (BOF): BOF ensures a fair and tamper-proof transaction ordering process without compromising transaction privacy. This makes it a scalable and adaptable solution for various blockchain ecosystems. BOF solutions [31, 104–107, 121] typically utilize commit-reveal schemes and threshold encryption to hide transaction details without revealing their contents until the order is determined. BOF focuses on pre-ordering and decoupling the transaction ordering process from its execution to achieve fair and equitable sequencing.

Heimbach and Wattenhoffer [31] propose a method that encrypts transaction details, sequences them, and reveals them after they have been sequenced using a commit-reveal scheme. Consequently, Fino [104] adopts an innovative commit-reveal strategy, incorporating MEV mitigation within a Byzantine fault-tolerant (BFT) [122] protocol combined with a directed acyclic graph (DAG)-based communication protocol under a partially synchronous model. Specifically, it introduces a framework where users first send encrypted transactions to validators, who commit to an ordering of transactions blindly without seeing the contents. The decryption keys are secret-shared among validators, and revealed only after the ordering is finalized. This ensures blind order fairness, preventing attackers from manipulating transaction order based on contents. By integrating the commit-reveal framework into the DAG-based BFT protocol with minimal overhead, Fino balances scalability, high performance, and MEV resilience. It prevents reordering of encrypted transactions and achieves blind order fairness.

Lyra [105] addresses the widespread challenge of transaction reordering attacks in blockchains by employing a commit-reveal mechanism that relies on Verifiable Secret Sharing (VSS). It integrates a commit-reveal scheme to obfuscate transactions and a leaderless ordered consensus protocol for sequencing transaction inclusion, thereby ensuring optimal latency, protection from reordering attacks, and scalable throughput. On the other hand, Piet et al. [106] propose two extensions for Ethereum's PoW and PoS protocols to mitigate MEV by leveraging the transaction execution order and protecting transactions until their inclusion in the blockchain. The PoW extension incorporates a randomized ordering mechanism to generate random data for each block, using randomness beacons, commit-reveal schemes, and threshold public-key encryption. Meanwhile, the PoS solution adapts the Ferveo algorithm [107] to be compatible with Ethereum's GASPER [123] consensus protocol. While both solutions effectively reduce MEV by limiting the use of transaction order information, they also pose challenges. For example, PoS experiences a decrease in throughput, while PoW faces increased latency.

Table 3: Comparative analysis of MEV mitigation studies.

Ref.	MEV Type	Layer	Mechanism	Framework	Scalability	Interoperability	Replicable	Remarks
[103]	Sandwich, arbitrage, liquidation	Application	TO	UA	M	✗	H	Predictable ordering; low protocol disruption
[104]	Arbitrage	Consensus	DAG	CR	H	✗	L	BFT DAG consensus; pre-commits tx order
[105]	Front-running, sandwich	Consensus	DAG-OF	LSMR	H	✗	M	Order fairness; VSS obfuscation
[106]	Front-running, arbitrage	Consensus	DKG+TPKE	RTE	M	✓	H	Random tx execution; tested on PoW and PoS
[107]	Front-running	Base	DKG+TPKE	AM	H	✓	L	Threshold encryption; Tendermint compatible
[108]	Front-running	Base	TE	SMC	H	✓	M	Encrypted execution; uses secret committee
[109]	Arbitrage	Application	AE	FV	H	✓	H	Verified smart contract; real use cases
[110]	Front-running	Application	FBA	CR	M	✗	L	ZKPs; protects retail users
[111]	Front-running, back-running	Base	MR	TSO	H	✓	M	Fair tx selection; mempool integrity
[112]	Sandwich	Base	RP	PVSS	M	✗	M	Encrypted mempool; PoW/BFT adaptable

Abbreviations: TO: Token Ordering, DAG: Directed Acyclic Graph, DAG-OF: DAG with Order Fairness, DKG: Distributed Key Generation, TPKE: Threshold Public Key Encryption, TE: Threshold Encryption, AE: Automated Extraction, FBA: Frequent Batch Auction, MR: Mempool Reconciliation, RP: Randomized Permutation; UA: User-Adversary, CR: Commit-Reveal, LSMR: Leaderless State Machine Replication, RTE: Randomized Transaction Execution, AM: Asynchronous Model, SMC: Secret Management Committee, FV: Formal Verification, TSO: Transaction Selection and Ordering, PVSS: Publicly Verifiable Secret Sharing

Scalability: **H** (High) = Low overhead/complexity, suitable for high-throughput chains; **M** (Medium) = Moderate overhead, feasible with trade-offs; **L** (Low) = High overhead/latency, potential bottlenecks.

Replicability: **H** (High) = Source code/data publicly available; **M** (Medium) = Detailed pseudocode/simulation parameters; **L** (Low) = Methodology only, limited implementation details.

Interoperability: ✓ = supports multiple chains/consensus; ✗ = chain-specific/fixed environment.

Proposer-builder Separation (PBS): PBS aims to reduce MEV impact. Notably, PBS is implemented by Flashbots on the Ethereum blockchain to simplify the block building process and mitigate public mempool front-running by differentiating the roles of proposer and builder [124]. Focusing on the novel design of PBS, Ramos et al. [58] provide a descriptive and analytic approach to explain the concept and evolution of MEV, including potential vulnerability factors and attack vectors under PBS, such as builder centralization, collusion, and front-running. They further propose innovative solutions to enhance decentralization, transparency, and accountability in block building, including reputation systems [125], fee escalators [58], and trusted execution environments [126]. Meanwhile, Alnajjar et al. [127] propose an enhanced verifiable decryption process to address the limitations of existing PBS protocols. The proposed decryption scheme mitigates the ability of block proposers to decline auctioned blocks and the ability of block builders or executors to deny or reorder transactions. Additionally, they define a comprehensive adversary model to encompass various MEV attack vectors and demonstrate the protocol’s resilience against all identified threats. However, the performance analysis reveals efficiency and scalability comparable to existing solutions, but there are some limitations.

MEV-Boost is an open-source middleware that implements PBS for Ethereum [128]. It serves as an intermediary layer that enables private coordination among users, searchers, builders, relays, and validators. As illustrated in Figure 16, MEV-Boost orchestrates a workflow that

links the asynchronous block-building market with the synchronous block-proposal process. Before participating in block procurement, a validator must complete an infrequent setup stage (Step 0), during which it registers with one or more relays. This registration step provides the validator’s public information and establishes the trust context necessary for relays to recognize and serve the validator during later interactions. Although Step 0 appears in the figure, it is not part of the per-block workflow; rather, it is a prerequisite that enables the subsequent steps to function correctly. The operational workflow begins when users submit signed transactions (Step 1), which are propagated to the public mempool (Step 2). Searchers monitor the mempool and construct MEV bundles that are sent to multiple block builders (Step 3). Builders produce candidate execution payloads and forward them to relays (Step 4). Relays perform background tasks such as payload validation, bid computation, and block storage (Step 5).

When a validator becomes eligible to propose a block, the synchronous procurement phase begins. The validator requests candidate block headers from MEV-Boost (Step 6). MEV-Boost obtains these headers from relays (Step 7) and receives corresponding header-bid pairs (Step 8). It verifies the candidates and selects the highest-value payload (Step 9), which is then returned to the validator (Step 10). The validator blindly signs the chosen header without accessing the underlying block contents (Step 11). The signed header is sent back to MEV-Boost (Step 12) and forwarded to the winning relay (Step 13). After confirming the signature, the relay releases the full execution payload

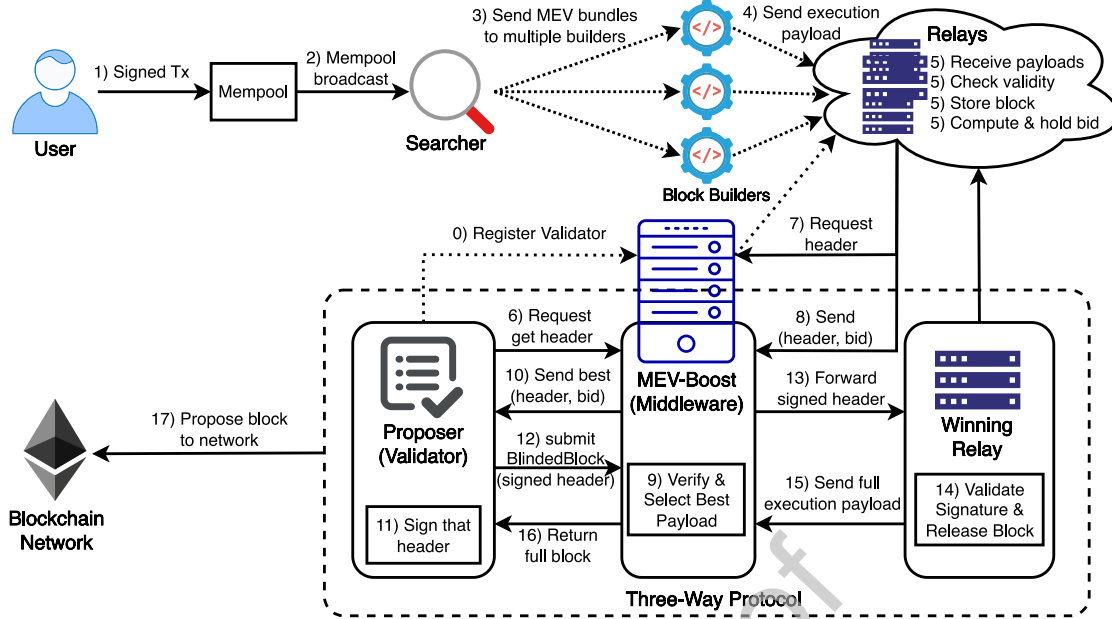


Figure 16: Overview of MEV-Boost block-building and block-proposal process.

(Steps 14-15), which MEV-Boost delivers to the validator (Step 16). The validator then assembles and proposes the complete block to the blockchain network (Step 17). This structured workflow preserves consensus integrity while enabling validators to benefit from optimized blocks produced by competitive builders. The modular design allows validators to capture enhanced MEV rewards without requiring substantial changes to existing validator infrastructure.

6.2. Base-level Mitigation

Base-level mitigation operates at the network layer situated between consensus mechanisms and application logic. Its primary objective is to reduce MEV opportunities before block finalization by modifying how transactions are revealed, ordered, or logged.

Secret Mempools: Secret mempools conceal transaction details until after their ordering has been finalized, preventing potential frontrunners from accessing information that could otherwise be censored, reordered, or manipulated. For example, F3B [108] employs a commit-and-reveal framework that encrypts transactions in real-time to mitigate front-running. It utilizes a decentralized secret-management committee [129] to securely manage the release of transaction information. Similarly, Ferveo [107] proposes a protocol specifically tailored to ensure mempool privacy within Byzantine Fault-Tolerant (BFT) consensus environments.

Timestamp-ordered Defense: A timestamp-ordered defense enforces insertion of transactions into a first-in-first-out (FIFO) queue based on arrival times, thereby eliminating proposer discretion over ordering. ZeroMEV¹²

operates as a validator execution client derived from a fork of Geth on public Ethereum. It organizes transactions strictly according to their arrival timestamps, enforcing a local FIFO ordering mechanism to mitigate MEV. However, a key limitation of this approach is its lack of built-in accountability measures, which necessitates substantial trust in validator integrity.

Accountability-focused Logging: These schemes force every node to commit to its mempool view and processing log, so any deviation (e.g., withholding or repositioning a transaction) can be proven afterward. For example, LØ [111] addresses transaction manipulation in permissionless blockchains. The protocol prioritizes accurate detection of such manipulations and assigns accountability to specific mining nodes. It mandates that all miners (including the misbehaving ones) log every transaction into a secure mempool structure and maintain a verifiable record of processing. Commitments regarding mempool contents are exchanged and recorded, enabling inconsistencies (e.g., transaction withholding) to be clearly identified when compared against the mempool of a compliant miner.

Randomized Permutation: This approach shuffles or obfuscates transaction order by using encryption or similar techniques to prevent attackers from gaining predictive control while preserving liveness. For instance, BlindPerm [112] introduces a multi-layered mechanism that targets both the base and consensus layers. It combines an encrypted mempool with permutation to achieve an efficient design with no overhead compared to plain blind ordering. However, it has limitations in addressing certain types of MEV, especially those that depend on blockchain state or involve collusion and bribery attacks.

¹²<https://zeromev.org/>

6.3. Application-level Mitigation

Application-level mitigation operates at the smart contract and protocol design layer, implementing direct countermeasures within DeFi applications themselves. These approaches focus on modifying transaction processing mechanisms, enhancing security verification, and redesigning protocol incentives to reduce MEV opportunities at the application interface.

Batch Auctions and Fair Trading: Batch auction mechanisms mitigate the influence of temporal priority by aggregating individual transactions into groups that are processed collectively. By clearing orders at uniform prices rather than executing them sequentially upon arrival, this design dismantles the latency races characteristic of continuous limit order markets. For example, FairTraDEX [110] instantiates a width-sensitive frequent batch auction. It enables users to submit market orders within a specified spread and employs cryptographic techniques to provide game-theoretic guarantees against specific forms of value extraction for retail traders. Designs such as the Automated Arbitrage Market Maker (A2MM) [130] internalize arbitrage across selected pools and therefore reduce residual MEV that would otherwise be captured by external arbitrageurs. Batch auctions significantly curb front-running and sandwich attacks because orders in the same batch clear at a uniform execution price. However, they introduce distinct trade-offs. FairTraDEX, for instance, assumes that external prices serve as fully informative public signals and relies on a trusted setup for zero-knowledge parameters, and the analysis does not fully capture collusion or strategic behavior among sophisticated market participants. The transition from continuous to discrete clearing times also requires users to tolerate increased latency. This transition in turn requires careful consideration of liquidity and usability constraints during deployment.

Solver Networks and Intent-based Protocols: Intent-based protocols generalize application-level mitigation by separating user intent expression from the concrete transaction path. Early MEV-aware DEX designs (e.g., CoW Protocol¹³) combine batch auctions with a decentralized solver network that proposes settlement solutions for each batch. Recent solutions such as UniswapX [131] and 1inch Fusion [132] employ competitive Dutch auction mechanisms. Users sign off-chain orders that decay in price over a brief period, and a decentralized network of “fillers” or “resolvers” competes to fill these orders once the execution becomes profitable. In this model, a large fraction of the arbitrage value that would otherwise accrue to independent MEV bots is instead captured as price improvement for the user in the form of better execution prices. These architectures reduce the attack surface for classical front-running because user intents do not appear as susceptible individual transactions in the public mempool, and they shift competition away from pure latency and toward the

quality of settlement routes. Beyond simple swaps, protocol such as Anoma [133] aim to standardize generalized intents so that users can express complex, multi-chain state preferences that solvers fulfill atomically. At the same time, intent-based systems introduce new risks, in particular with respect to solver centralization and the opacity of off-chain order flow. If the solver set evolves into a permissioned oligopoly, the censorship-resistance and neutrality guarantees of the underlying blockchain can be undermined. From the perspective of our extractive versus productive MEV framework in Section 5.5, solver networks and intent-based protocols seek to transform order-flow races that generate extractive MEV into more productive forms of intermediation, while still leaving residual externalities and concentration risks.

Economic Security Analysis: Economic security analysis provides formal verification methods to identify and quantify potential attack vectors in DeFi protocols before they can be exploited. A notable example is the Clockwork Finance Framework (CFF) [109], which redefines “extractable value (EV)” to encompass a wider array of economic attack vulnerabilities beyond traditional MEV. The CFF includes a verification tool designed to identify potential attack vectors and assess the integrity of smart contract transactions. Its efficiency has been evaluated in DeFi protocols such as Uniswap and MakerDAO, revealing significant monthly EV instances averaging 56 million US dollars. However, the computational intensity of the CFF tool and challenges in scaling for larger or more complex transactions are acknowledged limitations, as is its reliance on the accuracy of user-provided contract models.

Oracle Verification: Oracle verification provides real-time monitoring and validation of external data feeds that smart contracts rely upon for price information and other critical parameters. These systems aim to detect manipulated or anomalous oracle data that could enable MEV extraction through price oracle attacks. To address the challenges of real-time monitoring of price oracles, Mo et al. [134] introduce VeriOracle, a formal verification framework designed to automatically detect unexpected price feed activities within smart contracts. The authors categorize price oracles into decentralized oracle networks [135] and DEX oracles (e.g., PancakeSwap, Liquity), while providing an in-depth analysis of each type’s security vulnerabilities, data source reliability, duration of price information, and associated query costs.

6.4. Other Mitigation Solutions

Other mitigation solutions encompass a variety of techniques designed to address specific MEV challenges. These strategies leverage advanced cryptography and economic incentives to enhance transaction security and ensure fairness across decentralized networks.

ZK-based Commitments: Zero-Knowledge (ZK)-based solutions utilize cryptographic proofs to enhance privacy and security in transaction processing, thereby preventing malicious actors from exploiting transaction

¹³<https://docs.cow.fi>

details for MEV. McMenamin et al. [136] integrate smart contract wallets with non-interactive ZK proofs to transform MEV into a censorship issue that makes exploitative actions prohibitively expensive. The solution maintains transactional efficiency by offloading costly ZK operations off-chain, requiring only minimal additional mapping checks. This approach proves particularly effective in DEXs and liquidations, as it allows frequent batch auctions and interactions with AMMs aligned with external market prices. However, the reliance on relays for posting collateral introduces unpredictability and dependence on external entities, which impacts the protocol’s reliability and trustworthiness.

Reversible Call-Option Protection: A reversible call option is a financial instrument used to protect against MEV in lending platforms by allowing contract termination under predefined conditions. Qin et al. [137] propose Miqado, a protocol that integrates reversible call options into DeFi lending platforms. Miqado enables sellers to terminate contracts at a premium before maturity based on the Black-Scholes model [138]. Despite performance gains on Aave and Compound platforms, Miqado overlooks long-term market dynamics such as collateral supply (or demand), interest rates, and risk premiums. It also fails to account for Ethereum’s gas fees and transaction latency, which affect its practical feasibility over time.

Honeypot Trap Detection: Honeypot traps are deceptive strategies in DEXs that aim to exploit users. Detection mechanisms seek to identify and neutralize these threats to prevent financial losses. Gan et al. [139] propose a taxonomy to categorize honeypot traps into invalid buying, unauthorized transfers, and inability to sell. The authors also develop a detection scheme that combines historical data analysis with transaction simulation to identify potential traps. Unlike traditional methods, the solution targets high-tax, hidden-tax, unauthorized transfer, and whitelist (or blacklist) traps to uncover numerous abnormal pools in Uniswap and other DEXs.

Insights: MEV mitigation strategies demonstrate the necessity of implementing defense mechanisms across multiple blockchain layers, as each level addresses distinct vulnerabilities in the transaction processing pipeline. The analysis reveals that effective MEV protection requires coordinated defense frameworks that integrate mechanisms spanning consensus protocols, network infrastructure, and application design, rather than relying on piecemeal solutions. Furthermore, the economic incentive structures underlying these mitigation approaches must fundamentally realign validator and user motivations to make honest participation more profitable than value extraction. Future MEV defense will depend on developing adaptive security frameworks that can evolve alongside emerging attack vectors while maintaining the core principles of decentralization, transparency, and accessibility that define blockchain ecosystems. One promising direction for MEV mitigation is the integration of advanced cryptographic techniques, such as quantum key distribution (QKD)

and post-quantum cryptographic algorithms [140]. These quantum-resistant protocols have the potential to enhance transaction privacy and security, preventing adversarial manipulation of transaction ordering. However, their practical applicability in DeFi, particularly regarding gas costs and latency constraints, requires further investigation.

7. Theoretical Implications of MEV

In this section, we discuss the theoretical implications of MEV, focusing on formalizing MEV games, analyzing different ordering mechanisms, and computing the price of MEV. Our goal is to establish rigorous conceptual foundations for understanding MEV and designing mechanisms that mitigate its negative externalities. The comparative analysis of theoretical MEV-based studies is presented in Table 4.

7.1. Optimization Perspectives

Optimization theory provides mathematical models and techniques to analyze how miners and validators maximize their MEV. This involves formulating the transaction ordering problem as an optimization problem and applying methods like linear programming and dynamic programming to derive optimal strategies that maximize MEV. Overall, optimization theory delivers a rigorous analytical approach to determine profit-maximizing transaction ordering and extraction strategies. For example, Babel and Baker [141] present an optimization solution for peer selection in blockchain networks to maximize profits from transaction fees by extracting MEV. The authors formally model the objective of maximizing the expected MEV-weighted adversarial advantage under different consensus protocols. They propose an efficient localized algorithm called MEV-Peri, that adapts existing latency optimization techniques to account for transaction utility. Simulations using real-world data show that MEV-Peri substantially outperforms baseline latency-based peer selection. This demonstrates the importance of strategic peering based on transaction metadata to maximize extractable value. However, the paper ignores the stability and reliability of peer connections, which affect the algorithm’s performance in dynamic and adversarial environments. Additionally, it does not account for the impact of private relay services and mempools, that reduce the visibility and opportunity of public mempool activity. Similarly, Angeris et al. [142] introduce the “cost of MEV” framework to quantify MEV’s economic impact by measuring the difference in profit between worst-case and average transaction orderings for a validator. The authors leverage connections between the cost of MEV, payoff function smoothness, and spectral properties to bind and analyze MEV behavior. The potential MEV vulnerabilities are identified by distinguishing worst-case and average-case payoffs to pave the way for designing fair mechanisms. The proposed framework offers valuable

Table 4: Comparative analysis of theoretical MEV-based studies.

Ref.	MEV Type	Model	Solution	Complexity	Scalability	Fairness	Application	Remarks
[141]	Front-running, sandwich	Optimization	Heuristic	High	Medium	Low	DEXs, Ethereum bots	Time and leader-based consensus
[142]	Arbitrage, front-running	Game theory, optimization	Spectral graph theory	High	High	Medium	DeFi protocols, NFT auction, liquidation events	Focus on MEV cost; expand theoretical bounds on MEV
[143]	Front-running, back-running	Game theory, optimization	Incentivize adversarial behavior	Medium	Low	Low	Smart contract interaction, DeFi	Estimate MEV for consensus instability; MEV mitigation
[144]	Front-running, back-running, sandwich	Auction theory	Dominant strategy equilibrium	Low	Medium	Medium	Congestion reduction for Ethereum	Eliminate PGA; reduce gas price inflation
[145]	Front-running, back-running	Game theory, non-interference	Token redistribution	High	Medium	High	Crowdfund, bounty contracts	Real-world contract validation; monotonic adversarial gains
[146]	Arbitrage, front-running, sandwich	Game theory, auction theory	Bayesian and max-min optimization	High	Medium	Medium	DEXs auction, cross-domain exchanges	Sybil-proof rebate mechanism; address MEV in AMM
[147]	Sandwich	Game theory	Reordering and routing MEV	High	Low	Medium	CFMM-based trading	Bounds on sandwich; Competitive ratios for MEV profit
[148]	Arbitrage	Information theory	Entropy reduction	Medium	Low	Medium	AMM, transaction ordering	Entropy-based classification; Cross-domain mitigation
[149]	Arbitrage	Non-interference	Algorithmic state-stripping	Low	Medium	High	DeFi lending, smart contract development	Contract and token independence; front-running resistance

insights for developing mechanisms and applications with minimized MEV impact. For example, the front-running scenario showcases the framework’s theoretical utility in optimizing protocols for minimal MEV impact.

7.2. Game and Auction Theory Perspectives

Game theory provides a rigorous framework for understanding the behavior of rational players competing for MEV opportunities. In MEV games, players – typically miners, validators, or bot operators seek to maximize their gains from the reordering, insertion, or omission of transactions in a blockchain [143, 144]. These actors analyze the potential value of different transaction sequences to determine the most profitable course of action. The strategic interplay among these participants is modeled using game theory, which allows us to predict outcomes under various scenarios. This approach is crucial in understanding the dynamics of MEV, specifically how players might react to various network conditions and protocol changes. Furthermore, game theory helps identify equilibrium strategies, where no player is incentivized to deviate unilaterally. This is particularly relevant in blockchain ecosystems, where trustless interactions and decentralized decision-making are paramount. On the other hand, an auction provides a structured framework for analyzing MEV. By applying auction theory to MEV, valuable insights are extracted in terms of transaction ordering, bidder behavior, and revenue generation [146]. Modeling transaction ordering as auctions enables analytical reasoning about efficiency, incentives, and revenues, ultimately informing the design of mechanisms that address MEV incentives.

For instance, Mazon et al. [146] propose a theoretical framework to formalize MEV games and compares different ordering mechanisms and their externalities. The authors

model the behavior and incentives of rational players competing for MEV opportunities using concepts from game theory, optimization, and economics. The study offers several contributions to the theoretical aspect of MEV and DeFi. First, it presents a general and abstract definition of the MEV game, capturing various types of MEV opportunities such as arbitrage, sandwich attacks, and cross-chain MEV. Second, the equilibrium and efficiency properties of different ordering mechanisms (e.g., priority gas auctions, first input first output, sealed bid auctions) are analyzed. Third, the price of MEV for different cost functions and domains is computed to minimize the negative externalities of MEV games. However, the study does not consider the impact of MEV on individual users suffering from front-running or manipulation by privileged players. Additionally, they assume that players have a common valuation of tokens and a linear utility function over their balances, which does not reflect the reality of heterogeneous preferences and risk attitudes. Moreover, no empirical evidence or simulations are provided to support the theoretical results to compare the proposed mechanisms with existing ones. Bartoletti and Zunino [145] propose a formal framework for analyzing MEV from a game-theoretic perspective. The proposed model allows adversaries to combine internal knowledge with mempool information, leading to a comprehensive understanding of potential attack vectors. The problem is formulated as a strategic game between honest players minimizing losses and adversaries maximizing gains to define MEV as the maximal gain achievable by any adversary, regardless of identity or wealth. While the model captures the strategic interaction, it overlooks the MEV-driven economic forces. In addition, the model currently assumes rational players, but real-world actors exhibit bounded rationality

and strategic uncertainty.

In regards to MEV auction, the study [146] focuses on developing optimal mechanisms for rebating in permissionless blockchain systems, particularly in the context of Liquidity Provision (LP) [27] of CFMM and MEV in blockchain auctions. The term “rebating” stands for the strategic redistribution of a MEV portion back to various network participants (e.g., users or liquidity providers) to ensure fairness and provide resistance against Sybil attacks within the blockchain system. The study involves formulating and analyzing cooperative games, particularly focusing on the Shapley value [150] and Banzhaf value [151]. It constructs and examines various operators under different conditions (e.g., Sybil-proofness, efficiency, and no-deficit) and explores their implications in blockchain auction models. Similarly, Kulkarni et al. [147] explore the game-theoretic dynamics of MEV in CFMMs, providing a detailed analysis of MEV’s impact on DEXs in blockchain networks. The authors focus specifically on a common form of MEV where attackers exploit user transactions for personal gain. Using both analytical and numerical methods, they explore how these attacks influence trade routing in CFMM networks and the resultant excess price impact. Besides, they introduce innovative metrics such as the price of anarchy and the cost of feudalism to measure MEV’s effects on different stakeholders.

7.3. Information Theory Perspectives

Information theory provides a unique framework for understanding MEV by emphasizing the value and flow of information in blockchain transactions. In this context, MEV is conceptualized as an intrinsic characteristic of all non-trivial blockchains and decentralized applications, inherently tied to the entropy or disorder within a blockchain system. Using information theory, MEV stems from the variability and unpredictability of user transactions by introducing an entropy. This defines MEV as beneficial or detrimental based on its impact on the state’s entropy. For example, Hughes et al. [148] propose a novel information-theoretic perspective on MEV, identifying it as critical for the stability of all non-trivial blockchains. The authors introduce the concept of “good MEV”, defining it as atomic transactions (e.g., individual, indivisible actions) that decrease the blockchain’s entropy (e.g., uncertainty), a shift from traditional player-centric definitions. In contrast, they define “bad MEV” as any atomic transaction that increases the balance of a player (their holdings within the blockchain) but also increases the entropy (or disorder) of the blockchain state. The proposed framework offers insights into how user transactions generate MEV to impact into the system’s disorder. This distinction between good and bad MEV is crucial in understanding the impact of different types of transactions on the overall order and efficiency of blockchain systems from an information-theoretic perspective.

7.4. Non-interference Perspectives

The non-interference concept is derived from the traditional ε -composability by focusing on preventing adversaries from exploiting dependencies in compound smart contracts. The study [149] introduces a novel security notion by introducing MEV non-interference, a novel concept designed to enhance the security of DeFi services. The theory of local MEV is formulated to categorize economic attacks based on the adversary’s wealth and providing a nuanced understanding of vulnerabilities in DeFi ecosystems. They establish sufficient conditions for ensuring MEV non-interference, which underscores the resilience of the proposed approach against front-running MEV and emphasizes contract and token independence. While applying these principles to real-world DeFi protocols, the study also acknowledges some limitations, such as the abstraction from certain blockchain features (e.g., gas, consensus, reentrancy), and the absence of a generalized algorithm for broader application.

Insights: Theoretical analysis of MEV reveals that value extraction is not merely an exploitative phenomenon but a fundamental characteristic embedded within the economic structures of blockchain systems. Rational actors will inevitably compete for MEV opportunities, creating predictable equilibrium states where extraction strategies become systematized rather than opportunistic behaviors. These theoretical foundations collectively indicate that sustainable MEV management requires fundamental changes to protocol incentive structures rather than merely implementing defensive countermeasures, as rational actors will inevitably optimize their strategies to exploit any remaining extraction opportunities within existing system architectures.

8. Empirical Analysis of MEV

While theoretical frameworks provide essential foundations for understanding MEV, empirical validation is necessary to compare these predictions with real-world blockchain behavior and to quantify the impact of MEV strategies. The empirical approach enables researchers to evaluate theoretical models, assess mitigation effectiveness, and identify emergent behaviors not captured by theory alone. In addition, empirical analysis provides critical feedback to refine theoretical assumptions, leading to more accurate predictive models. The convergence of theoretical insights with empirical evidence is essential for designing robust MEV detection algorithms and effective mitigation strategies that can be deployed in production blockchain systems. Existing empirical studies focus on the impact of MEV by examining real-world data, block production, user experience, and the overall status of the blockchain network. The empirical studies employ diverse data collection methodologies, primarily drawing from four distinct sources with specific technical approaches:

Table 5: Comparison of empirical analysis-based studies.

Ref.	Method	Tx	Time	Scale	Dataset	Plat.	Remarks
[21]	Heuristic	Public	~3 yrs	6.8M–13M blk	AN+DEX	Eth.	BEV lower-bound quantification; DEX+lending coverage; multi-strategy accounting
[45]	Heuristic	Public	17 mo.	60M+ tx	EXP+BQ	Multi-chain	Cross-chain attack measurement; AMM log driven; attacker-victim behavior analysis
[60]	ML-based	Public	13 mo.	8,128 blk	AN+FA+DEX	Eth.	GNN-style adaptive learning; protocol security scoring; simulation-based assessment
[71]	Other-chain	Public	22 mo.	13.7M blk	RPC	Algorand	FCFS ordering effects; 1.1M arbitrage events; batch-tx strategy evidence
[152]	Heuristic	Public	64 mo.	11.3M blk	AN+MP	Eth.	Mempool manipulation study; three frontrun strategies; conservative lower bounds
[153]	Relay-based	Priv. & Pub.	23 mo.	4.5M MEV tx	AN+FA+MP	Eth.	Flashbots impact measurement; miner advantage quantified; centralization indicators
[154]	Relay-based	Private	12 days	74.5K blk	FA	Eth.	Private-tx dominance evidence; miner profit share quantified; graph-based detection
[155]	ML-based	Private	22 mo.	6.6M bdl	FA+AN	Eth.	Representation learning; iterative clustering; new MEV pattern discovery
[156]	Cross-chain	Public	22 mo.	7.7M tx	MP+RPC+DEX	Multi-L2	L2 MEV comparison; Polygon dominance reported; tool-assisted identification
[67]	Relay-based	Public	8 mo.	1.6M blk	MB+AN	Eth.	PBS/MVB dynamics analysis; MEV-Time Law; relay market-share evidence
[157]	ML-based	Private	7 mo.	1.3M blk	FA+AN	Eth.	Bid prediction models; auction behavior analysis; profitability optimization focus
[158]	Time-based	Priv. & Pub.	2 days	12.5K slot	MB	Eth.	Slot-time vs rewards; time-bandit risk analysis; multi-relay evaluation
[159]	Stablecoin-based	Public	7 mo.	2.8M blk	AN+DEX	Eth.	UST-centered arbitrage; path length shortening; success vs profit correlation

Dataset: FA = Flashbots API; MB = MEV-Boost relay/API; AN = Archive node; RPC = RPC endpoint; MP = mempool/mev-inspect-py; DEX = DEX logs/oracles; EXP = Explorer crawl (Etherscan/BSCscan); BQ = BigQuery.

Platform: Multi-L2 = Polygon, Arbitrum, Optimism; Multi-chain = Ethereum + BSC.

Transaction: Priv./Pub. = Private/Public channels (bundles/relay vs public mempool).

Scale: blk = blocks; tx = transactions; bdl = bundles; slot = Ethereum slots.

- **Blockchain Node:** Direct blockchain node queries through JSON-RPC interfaces and archive data extraction using specialized node implementations such as Erigon¹⁴ and Geth¹⁵,
- **Specialized APIs:** MEV infrastructure APIs including Flashbots relay endpoints for bundle submission data and MEV-boost relay providers (Ultra Sound, Agnostic) that capture bid timestamps, block values, and builder identities, with researchers implementing robust retry logic and caching strategies to handle API rate limits of 100-1000 requests per minute,
- **Protocols and Event Logs:** DEX protocols and smart contract event logs accessed through web3 libraries (web3.py, ethers.js) by filtering events using topic hashes, decoding parameters, and employing multi-call contracts to batch hundreds of queries into single RPC calls for efficiency,
- **Third-party Platforms:** third-party analytics platforms including Dune Analytics¹⁶ which provides SQL-queryable datasets with pre-decoded transaction logs and standardized cross-protocol schemas (e.g., dex.trades, lending.liquidations), Etherscan¹⁷ offering RESTful API endpoints with rate limits of 5

calls/second for transaction receipts and token transfers, and MEV-Boost Dashboard¹⁸ aggregating relay performance metrics.

Table 5 presents a consolidated comparison of empirical MEV studies across multiple dimensions. These include the detection methodology, transaction visibility (public versus private channels), observation period, and measurement scale (blocks, transactions, bundles, or slots). The table also reports the underlying datasets, execution platforms, and key empirical findings. By aligning heterogeneous datasets from Ethereum, Algorand, and multi-chain or multi-L2 environments, the table facilitates cross-study comparison. In particular, it highlights how different works select their data sources (e.g., archive nodes, relay APIs, mempools, or DEX logs), the time spans and data volumes they analyze, and the specific MEV aspects they emphasize. These aspects include lower-bound estimation, cross-chain behavior, relay centralization, and ML-based pattern discovery.

This systematic comparison aims to provide a clear overview of the empirical research conducted in the field, highlighting the scope and depth of each study and the practical implications of their findings. Across these studies, results are typically validated by several factors: (i) cross-checking transaction hashes and state roots against multiple public explorers, (ii) replaying candidate transactions on

¹⁴<https://github.com/ledgerwatch/erigon>

¹⁵<https://github.com/ethereum/go-ethereum>

¹⁶<https://dune.com/home>

¹⁷<https://etherscan.io/>

¹⁸<https://mevboost.pics/>

local archive nodes, and (iii) hand-auditing random samples to bound false positives and negatives. Monetary figures are normalized with daily closing exchange rates at the block timestamp for comparability.

8.1. Heuristics Analysis

Heuristic analysis plays an essential role in identifying MEV activities by offering simple, rule-driven techniques that detect transaction patterns with low computational overhead. For instance, Torres et al. [152] study 11.3 million Ethereum blocks¹⁹ to highlight displacement, insertion, and suppression strategies in the mempool. Likewise, Zhou et al. [20] analyze approximately 950,000 blocks collected from December 2019 to May 2020²⁰ to uncover just-in-time arbitrage paths. Qin et al. [21] quantify sandwich, liquidation, and DEX-arbitrage profits across a three-year slice of Ethereum trades (from blocks 6.8 million to 13.0 million), drawing order flow from seven leading DEXs and three lending protocols. Chen et al. [45] examine more than 60 million transactions on Ethereum and BSC, while Zhang et al. [160] perform 62 real-world exploits cataloged by DeFiLlama²¹ and Web3Sec²².

In terms of transparency and fairness of MEV, Ankile et al. [161] employ heuristic techniques to track manipulative behaviors in DeFi. Park et al. [39] focuses on simplified sandwich transaction patterns to analyze token transfer dynamics without relying on contract data. Li et al. [155] examine Flashbots bundles to uncover new forms of MEV activities. The authors emphasize the role of transaction sequences and token cycles in identifying profitable MEV opportunities. Furthermore, Yaish et al. [162] utilize heuristics to pinpoint suboptimal transaction sequences for improved profitability in DeFi, while Oz et al. [48] adapt heuristics to the Algorand blockchain to find the unique optimization strategies from fee-priority mechanisms. Heimbach et al. [124] investigate non-atomic arbitrage across decentralized and centralized exchanges, applying heuristics to detect MEVs in high-value transactions with an emphasis on privacy and timing.

While heuristic-based methods have significantly contributed to MEV detection through clearly defined transaction patterns, they face challenges, such as reliance on assumptions that may not hold in the dynamic blockchain environment. This limitation can lead to false negatives and positives. Additionally, heuristics tend to focus on known patterns, restricting their ability to adapt to emerging attack vectors and increasing the computational burden due to necessary runtime checks.

8.2. Relay-based Analysis

Relay-based empirical research using MEV-boost and its other Flashbots-based counterparts has illuminated new

perspectives on MEV dynamics. For example, Weintraub et al. [153] analyze the impact of Flashbots to collect and process Ethereum blockchain data, Flashbots API data, and other sources using a data-driven approach²³. They apply heuristics to detect and quantify MEV strategies like sandwiching, arbitrage, and liquidation. Based on the experimental analysis of Flashbots, there are several key findings. Firstly, Flashbots miners account for over 99.9% of hash power in Ethereum and make more than 2x the profit as compared to non-miners. Secondly, mining remains highly centralized, with over 90% of Flashbots blocks from just two miners. Thirdly, Flashbots disproportionately benefit miners over non-miners as 80% of MEV is extracted through Flashbots, as compared to 13.2% which comes from other private pools. Finally, Flashbots increases total MEV transactions while reducing gas prices, however, miners profit much more than searchers. It is concluded that Flashbots does not fully achieve its goals to illuminate MEV, democratize MEV access, and distribute benefits evenly. Similarly, Piet et al. [154] conduct an in-depth empirical analysis of MEV extraction on the Ethereum blockchain using Flashbots as an MEV relay²⁴. They develop a novel graph-based algorithm to detect various MEV strategies in historical blockchain data. Their findings reveal that the majority, i.e., 73% of private transactions conceal trading activity or redistribute miner rewards, while an overwhelming 87.6% of MEV collection occurs through privately submitted transactions. In addition, MEV accounts for a substantial 9.2% of miners' profits from transaction fees over a concise 12-day period. These findings together underscore the widespread influence of MEV, particularly within private transaction channels, emphasizing the urgent need for robust strategies to mitigate its impact on blockchain and DeFi ecosystems.

The emergence of MEV-boost as a dominant block construction mechanism in the Ethereum ecosystem has introduced a novel layer of complexity and dynamism to the MEV landscape. Hence, the inner workings of MEV-boost, its impact on block production, and its implications for user experience require a comprehensive empirical analysis. For instance, an in-depth study [67] analyzes the block construction of Ethereum from the Proposer Builder Separation (PBS) perspective. The authors use a data collection pipeline that combines Ethereum data²⁵ with API of the MEV-boost relay. In addition, they analyze the data using various metrics, such as MEV payments, market shares, block propagation, and timing attacks and introduce the MEV-Time Law, which quantifies the expected MEV revenue with respect to the time elapsed within an Ethereum slot. Their findings reveal that MEV-boost transferred a total of 160k ETH (>300 million US dollars) to proposers, with Flashbots holding a dominant 90% of the relay market share. Besides,

¹⁹<https://github.com/christoftorres/Frontrunner-Jones>

²⁰https://github.com/arthurgervais/pow_md5

²¹<https://defillama.com/hacks>

²²<https://github.com/SunWeb3Sec/DeFiHackLabs>

²³Flashbot in the Pan

²⁴Flashbots relay API

²⁵Ethereum Open Data

they demonstrate how MEV events amplify payments by 400-1000%, highlighting the market's sensitivity to MEV fluctuations. On the other hand, Grandjean et al. [163] present an in-depth analysis of the Ethereum PoS consensus layer, focusing on the implications of MEV and MEV-boost between 1 December 2020 and 15 May 2023. Datasets were collected from multiple sources (e.g., Etherscan, Rated Network²⁶, Beaconcha²⁷) to enable clustering for the validators. The authors report a 98.95% average proposal success rate over more than 6.4 million slots, partly due to MEV-boost and other factors. The study also highlights a steady increase in the number of active validators, with a total of 572,497 staking 15.23% of the total Ether supply. The distribution is dominated with 7,855 single-validator entities and a few large entities, such as Coinbase, controlling 81,165 validators. These large entities have a proposal success rate that is 0.5% higher and the ability to extract MEV across multiple blocks, increasing centralization risks. While the study offers useful insights, limitations exist around clustering methods, quantifying MEV impact, and understanding the influence of the consensus layer.

8.3. ML-based Analysis

ML techniques are increasingly being employed to detect MEV activities by utilizing sophisticated algorithms to identify and classify anomalous behaviors in blockchain transactions. The integration of big data analytics with artificial intelligence (AI) in blockchain provides enhanced capabilities for processing large-scale transaction data and implementing real-time MEV detection systems [66]. A range of studies [39, 60, 155, 164–167] demonstrate various ML-based methods designed to improve the detection of such activities. For instance, Park et al. [39] develop ArbiNet, a GNN-based model tailored for detecting arbitrage opportunities using ERC-20 token transfer data. The model is trained on a substantial dataset of labeled arbitrage and sandwich transactions to enhance detection precision. However, the GNN approach of ArbiNet introduces challenges in interpretability, making it difficult to understand the rationale behind the identification of certain transactions as arbitrage. Furthermore, its dependence on labeled training data²⁸ limits its ability to recognize new MEV strategies, which leads to false positives when faced with unfamiliar transaction patterns. Similarly, Li et al. [155] propose a method that combines representation learning with iterative clustering analysis to uncover new MEV activities in DeFi. This technique automates feature extraction from raw transaction bundles from Flashbots²⁹ and uses clustering to identify key features. Nevertheless, the iterative clustering process may cause computational strain if no new MEV activities are

detected, and the reliance on manual heuristic definition can constrain scalability and efficiency.

Babel et al. [60] introduce Lanturn, an adaptive learning framework that assesses the crypto-economic security of DeFi smart contracts. Unlike other methods, Lanturn does not rely on contract-specific heuristics; instead, it uses a simulation framework to execute transactions on-chain. However, Lanturn's effectiveness is contingent upon the assumption of consistent smart contract behavior based on historical data³⁰. Besides, the adaptive learning model in Lanturn struggles to keep pace with rapid market changes, potentially leading to less effective decisions in dynamic environments. Furthermore, Raun et al. [157] explore the bidding behavior-related analysis of MEV bots on Ethereum to predict winning bids and increase profitability in auctions. The authors develop ML models based on LGBMRegressor and linear regression to predict winning bids and optimize profits to their maximum. Two types of MEV extraction are considered: cyclic arbitrage [168] and sandwich attacks. They also employ a data-driven approach to collect and analyze transaction data from Flashbots' API and Ethereum-based archive nodes. Their findings highlight the effectiveness of ML for MEV extraction, with models achieving over a 50% success rate in arbitrage auctions and outperforming constant bidding strategies in sandwich auctions. The study's limitations include the use of readily available features, a static environment assumption, and a focus on specific MEV extraction techniques, suggesting opportunities for further exploration.

Generative AI (GenAI) approaches represent an advancement in MEV detection by (i) synthesizing realistic DeFi transaction sequences that expand the training domain and (ii) compressing long traces into latent representations that capture higher-order dependencies. For example, Rabieinejad et al. [169] develop a GAN whose discriminator separates malicious price manipulation traces from benign DEX activity. Likewise, Song et al. [170] combine a variational autoencoder with a lightweight transformer to detect liquidity-pool anomalies similar to sandwich attacks. Moreover, DeFiTrust [171] applies a transformer encoder to event logs and highlights scam tokens through attention-based outlier scoring. Additionally, Wu et al. [172] combine transformer embeddings with a GNN to enhance zero-shot detection of unseen DeFi attacks, while BlockFound [173] reports comparable gains on Ethereum and Solana datasets. Together, these GenAI studies demonstrate that sequence-level generative models adapt more readily to evolving DeFi behavior than fixed heuristics. Additionally, traditional ML approaches (e.g., GNNs, CNNs) partially address detection gaps by leveraging structural insights from on-chain data [60, 155]. However, these methods struggle to keep pace with real-time transaction throughput and are less effective against previously unseen MEV strategies.

²⁶<https://www.rated.network/>

²⁷<https://beaconcha.in/>

²⁸Arbinet Labeled Dataset

²⁹Flashbots Data Browser

³⁰Lanturn Historical Dataset

8.4. Time-based Analysis

A comprehensive time-based empirical analysis is studied to show the interplay between block proposal delays and MEV rewards in Ethereum [158]. The authors explore the impact of time-based strategies on PoS's stability and resilience by using an agent-based simulation model that includes dominant MEV-boost relays from Flashbots, Ultra Sound³¹, and Agnostic³². They combine extensive data collection from the Flashbots boost relay³³, focusing on block proposal timing dynamics and associated risks and rewards. Their study also acknowledges certain limitations, including its reliance on heuristic approaches to detect and quantify MEV and the omission of factors like network latency, communication failures, or adversarial behavior, which influence the waiting games and consensus outcomes.

8.5. Cross-chain Analysis

As the blockchain ecosystem diversifies, research has increasingly focused on MEV across various cross-chain environments [156]. For example, Bagourd and Francois [156] present an empirical analysis of MEV in Ethereum's L2 networks, such as Polygon [84], Optimism, and Arbitrum [83]. The authors highlight a significantly high MEV on Polygon, estimated at 213 million US dollars, which includes a substantial transaction involving USDC and IRON (Titan) tokens, contributing 165 million US dollars. Their research also shows that on Polygon, 16% of total profits arise from a single day, with the majority of profits coming from MATIC (63%), ETH (20%), and USDC (15%). Using a modified version of Flashbots' mev-inspect-py software and Uniswap's Price Oracle data, the study identifies a dominance of arbitrage opportunities in MEV on L2s, with liquidations being less frequent. In comparison to MEV on other networks, with Arbitrum at 0.25 million US dollars and Optimism at 0.12 million US dollars, Ethereum's MEV stands at 749 million US dollars, showing a clear contrast.

8.6. Stablecoin-based Analysis

In the context of MEV, stablecoin arbitrage has emerged as a focal area of research. Carrillo and Hu [159] conducted an analysis of approximately 2.8 million blocks from October 2021 to May 2022, covering over 117 million transactions³⁴. Their study identified around 188 thousand successful arbitrage transactions with a significant emphasis on the stablecoin UST. The findings reveal a shift toward shorter arbitrage paths characterized by 80% of transactions consisting of only two or three swaps. Additionally, the study reports a negative correlation between searchers' success rates and profitability, indicating higher profits typically associated with lower success rates. The notable failure rate of arbitrage attempts further highlights the intense competition and inherent challenges present in MEV-based stablecoin strategies.

8.7. Other Blockchain-based Analysis

While the majority of empirical MEV research has focused on Ethereum, a growing body of work examines MEV beyond Ethereum across both L1 and L2 platforms. These studies demonstrate how transaction visibility, ordering authority, execution environments, and fee-market design shape MEV extraction patterns and the associated mitigation infrastructure. Here, we first discuss L2 rollups as an architectural extension of Ethereum, then analyze Algorand and Solana as representative non-EVM L1 platforms with distinct design choices and DeFi ecosystems, and finally summarize emerging observations from other ecosystems.

L2 Rollups: L2 rollups inherit Ethereum for settlement while modifying the pre-inclusion pipeline through sequencer-mediated transaction intake and ordering. In many optimistic rollups, users submit transactions to a centralized sequencer via private RPC channels rather than through a public mempool. This design mitigates public-mempool-style front-running by external parties, but it simultaneously concentrates both ordering authority and order-flow visibility at the sequencer. Relative to Ethereum L1, MEV competition shifts away from gas-price priority races toward latency-sensitive back-running and arbitrage around DEX price updates, where execution advantage derives from earlier access to rollup-local state transitions and sequencing decisions [49, 156]. Fee economics further reshape extraction incentives on rollups. Lower transaction fees reduce the marginal cost of repeated probing and enable high-frequency cyclic-arbitrage attempts to consume substantial block space. Recent measurements show that cyclic-arbitrage bots can occupy a large fraction of rollup block space while paying considerably less gas than regular users, indicating that spam-like search may replace fee-auction-driven competition as a dominant mechanism on some L2s [89]. Moreover, the Dencun upgrade reduced the cost of posting rollup data to Ethereum, strengthening the economic viability of probing-intensive and spam-driven strategies by lowering the effective cost of failed or low-margin attempts [174]. Overall, L2 architectures relocate both extraction power and mitigation leverage toward sequencer governance and sequencing policy, including fair-ordering rules and sequencer-side auction mechanisms, rather than relying solely on L1-style mempool privacy and builder-market interventions.

Algorand: Algorand presents a distinctive MEV environment because its execution model and transaction-ordering rules diverge from the fee-driven priority mechanisms prevalent on EVM-compatible chains. Several studies [48, 71] conduct large-scale empirical analyses of MEV arbitrage opportunities on Algorand. These works employ a data collection pipeline that combines a self-hosted Algorand indexer, the AlgoNode service provider³⁵, and the Tinyman decentralized exchange³⁶. The analyses identify

³¹<https://relay.ultrasound.money/>

³²<https://aestus.live/>

³³Flashbots Boost Relay Data

³⁴Stablecoin Analysis

³⁵<https://nodely.io/>

³⁶<https://tinyman.org/>

more than 1.1 million arbitrage events across 13.7 million blocks comprising approximately 745.7 million transactions. In addition, over 265,000 instances of batch transaction issuances (BTIs) are documented, where individual addresses occupy more than 80% of a block with identical transaction types. This behavior reveals a spam-driven MEV strategy that is specific to FCFS-style ordering, in which searchers compete on network throughput rather than fee auctions. These findings underscore that while FCFS ordering suppresses classic gas-price-based front-running, it enables new MEV niches such as BTI-based congestion attacks.

Solana: Solana offers a contrasting setting, combining Proof-of-History (PoH) with Proof-of-Stake consensus, a highly parallelized execution environment, and localized fee markets. Recent empirical analyses investigate MEV on Solana in the presence of Jito, a validator client that introduces an out-of-protocol bundle auction market for transaction ordering [175, 176]. For example, Gerzon et al. [176] quantify both offensive sandwiching activity and defensive bundling strategies by using several months of Jito bundle data. The Solana MEV reports indicate that sandwich bots account for a non-trivial fraction of daily decentralized exchange volume, leveraging the determinism of Jito bundles relative to the probabilistic nature of native packet propagation [175]. Overall, these results suggest that Solana’s high throughput and localized fee markets concentrate MEV into a smaller set of high-intensity strategies, primarily sandwiching and back-running around concentrated-liquidity pools.

Other Platforms: Beyond Algorand and Solana, preliminary analyses of other ecosystems highlight additional design points. In the Cosmos ecosystem, app-chains such as Osmosis support AMM-based DEX activity while retaining substantial protocol-level flexibility [177]. For instance, the ProtoRev module automatically executes profitable routing trades and redirects the resulting revenue to the protocol treasury rather than to independent searchers [178]. Similarly, Avalanche’s C-Chain inherits Ethereum-like MEV mechanisms, although its Snowman consensus protocol influences the cost structure of spam and repeated probing [179]. Conversely, while empirical studies of TRON remain limited, its Delegated Proof-of-Stake (DPoS) consensus suggests that opportunistic extraction may arise through Super Representative (SR) ordering privileges rather than open gas auctions [180]. Collectively, these observations motivate treating MEV as a *multi-platform* phenomenon in which platform-level architectural choices determine the dominant extraction strategies.

8.8. Dynamics of MEV across Blockchains and DeFi

MEV is a multi-platform phenomenon whose dominant forms are shaped by platform architecture. Four determinants repeatedly govern both extraction feasibility and mitigation design: (i) transaction visibility before inclusion, (ii) the locus of ordering authority, (iii) the execution and fee-market model, and (iv) the availability of protocol-level

hooks that can internalize MEV. Table 6 provides a comparative view across six architectural dimensions. Visibility captures the pre-inclusion exposure of pending transactions and order flow to non-leader parties. Ordering authority identifies the entity that controls transaction inclusion and placement. Execution and fee model summarizes the cost structure and execution semantics that shape competition. MEV infrastructure denotes in-protocol or out-of-protocol mechanisms that mediate ordering or enable explicit MEV capture. Dominant MEV lists empirically prevalent extraction patterns associated with each design point, while mitigation surface highlights the design levers each platform exposes to reduce harm or redistribute value. This structured comparison clarifies why MEV mitigation does not transfer directly across platforms and why empirical measurements should interpret observed strategies in light of the underlying architecture.

Visibility and ordering authority: On Ethereum, a public mempool combined with fee-driven priority creates an environment in which searchers observe pending user order flow and compete for inclusion and positioning through gas bidding. With the introduction of MEV-Boost, ordering power shifts toward builders that aggregate order flow and win block auctions, altering both who captures MEV and where centralization pressures concentrate [181]. In contrast, many optimistic rollups rely on centralized sequencers and offer limited public visibility into transaction ordering. As a result, public-mempool-style races become less dominant, while sequencer-mediated ordering advantages and latency-sensitive arbitrage races grow more salient [49]. Solana represents a different design point altogether. Its base protocol lacks a global public mempool, and transaction ordering is leader-driven at high frequency. The emergence of Jito introduces an explicit bundle-and-tip market that reintroduces ordering control via out-of-protocol auctions, concentrating MEV around bundle-mediated strategies and validator extensions [175, 176]. Algorand provides a further contrast: its FCFS-like ordering suppresses fee-auction-driven races. Consequently, extraction shifts away from gas-price competition toward throughput-driven behaviors, including congestion-based tactics such as BTI [48, 71].

Execution model and fee-market design: Execution parallelism, block times, and fee granularity fundamentally reshape the cost structure of search. Low transaction fees on rollups reduce the marginal cost of repeated on-chain probing, and recent measurements show that speculative cyclic-arbitrage probing can dominate block space on some L2s [89]. Solana’s short slot times and localized fee markets sustain high-intensity competition for early block positions. Jito tips introduce an explicit channel for expressing ordering preferences, coupling MEV extraction to an infrastructure layer rather than relying solely on raw packet propagation [176].

Mitigation feasibility and redistribution: Platform architecture also determines which mitigation strategies are feasible. Ethereum-centric approaches typically target

Table 6: Architectural determinants of MEV across blockchain platforms.

Platform	Visibility	Ordering Authority	Execution/Fee Model	MEV Infrastructure	Dominant MEV	Mitigation Surface
Ethereum L1	Public mempool	Fee-driven; builders via MEV-Boost	Global fee market; sequential execution	MEV-Boost; relays; private orderflow	Sandwich, back-run, arbitrage, liquidation	Mempool privacy, builder auctions, PBS
L2 Rollups	Limited; sequencer-controlled	Centralized sequencer	Low fees; sequential; L1-inherited finality	Sequencer policy/auctions	Latency arbitrage, speculative probing	Sequencer ordering policy, auction design, shared sequencing
Solana	No global mempool; leader-driven	Leader+Jito bundle auction	Local fee markets; parallel execution; fast slots	Jito tips/bundles; validator extensions	Bundle-mediated sandwiching, back-run, DEX arbitrage	Validator-client governance, bundle-aware user protection
Algorand	Limited public; local pending tx	FCFS	Fixed or minimal fees; sequential execution	None standard	BTI spam, throughput-based clogging	Anti-spam, congestion controls, throughput limiting
Cosmos (Osmosis)	App-chain specific	Validators; protocol modules	App-chain configurable	ProtoRev module	Cyclic arbitrage	Protocol-owned capture and redistribution

mempool privacy, auction design, and builder market structure, reflecting the reliance of extraction on public pre-trade visibility and competitive block building [181]. Rollups expose a different mitigation surface centered on sequencer policy and protocol-level ordering rules, as the sequencer frequently becomes the focal point of ordering power [49, 89]. On Solana, mitigation efforts emphasize governance and accountability for validator extensions, together with bundle-aware user protections that reduce sandwich exposure in high-throughput environments [175]. Cosmos app-chains illustrate a further design point in which protocol modules can internalize a portion of MEV as protocol revenue. For instance, Osmosis ProtoRev captures cyclic arbitrage and redirects the proceeds away from external searchers, shifting the mitigation objective from elimination toward controlled redistribution [178].

Implications for empirical analysis: Cross-platform comparison necessitates platform-specific measurement interfaces. Ethereum provides public mempool data and MEV-Boost auction traces. Rollups instead require trace-based identification and long-horizon comparisons across heterogeneous sequencer designs [49]. Solana demands bundle-level visibility and validator-client telemetry because base-protocol mempool exposure is limited [176]. Algorand relies on indexer-based pipelines, as MEV manifests through chain-native ordering rules rather than gas-price auctions [71]. These differences motivate a comparative empirical methodology that conditions observed MEV patterns on the architectures that produce them, rather than treating Ethereum as the default reference point.

8.9. Real-world Case Scenarios

The severity of MEV exploitation manifests through documented incidents that have extracted billions from DeFi protocols and users, transforming theoretical vulnerabilities into substantial economic losses. These real-world cases demonstrate the systematic exploitation of transaction ordering mechanisms across multiple attack vectors. The following analysis presents verified incidents categorized by

their extraction methodologies and impact on decentralized financial infrastructure.

Direct value extraction through arbitrage and sandwich attacks has reached industrial scales, with sophisticated automated systems operating continuously across major DEXs. A prominent MEV operation³⁷ executed over 238,000 sandwich attacks affecting more than 100,000 users, extracting between 3.5 million USD and 34 million USD while consuming up to 142 ETH daily in gas fees during peak periods. Arbitrage bots have demonstrated significant efficiency, as evidenced by incidents in which automated systems extracted 800 ETH from pricing errors and by cross-chain operations generating 868.64 million USD in trading volume across 242,535 transactions. Back-running strategies on alternative chains have also yielded notable profits, with documented cases reporting 1.9 million USD from a single transaction through strategic positioning³⁸. Liquidation MEV has become systematized through operations earning millions via protocol liquidation mechanisms, with the MakerDAO Black Thursday incident standing as a watershed moment where 8.32 million USD in collateral was acquired through 1,462 zero-bid auctions, leaving 5.67 million DAI as bad debt³⁹. Recent validator-level exploits in 2024 demonstrated how malicious actors could manipulate MEV-boost infrastructure to extract approximately 25 million USD through coordinated attacks⁴⁰.

Infrastructure-level attacks and protocol manipulations demonstrate MEV’s capacity for systemic disruption across DeFi ecosystems. Oracle manipulation attacks have produced the most devastating single-incident losses, with the Mango Markets exploit draining 117 million USD through coordinated price manipulation that amplified token values by 2,000%⁴¹, while Cream Finance suffered

³⁷0xae2...e13

³⁸MEV Bot Analysis

³⁹Black Thursday Analysis

⁴⁰Halborn Security Analysis

⁴¹Chainalysis Report

\$130 million in losses through yUSD oracle exploitation⁴², and the Polter Finance incident resulted in 8.7 million USD losses through flash loan manipulation of oracle feeds⁴³. Network clogging attacks have systematically disrupted blockchain operations, exemplified by the Otherdeed NFT launch burning 176 million USD in gas fees with transaction costs reaching 8,000 gwei⁴⁴, the Status.im ICO where mining pools leveraged hash power to monopolize token allocation through transaction censorship⁴⁵, and sustained spam campaigns on Polygon generating 6,800 USD daily profit while consuming substantial network capacity⁴⁶. Cross-chain MEV has intensified through incidents such as the Wormhole bridge exploit extracting 320 million USD through signature verification bypass⁴⁷, while specialized arbitrage on Solana extracted 30 million USD within two months through cross-protocol MEV⁴⁸. These attacks collectively demonstrate the exploitation of MEV in threatening the operational integrity of blockchain and cross-chain DeFi protocols.

Insights: Empirical analysis across diverse blockchain ecosystems reveals that MEV extraction has evolved from opportunistic behavior into a sophisticated, systematized industry with predictable patterns and dominant market participants. Real-world data demonstrates significant concentration among MEV extractors with sophisticated relay mechanisms fundamentally altering validator economics. Besides, the evolution toward ML-based MEV detection methods and cross-chain analysis reveals that protocol design choices significantly influence both MEV prevalence and the adequacy of traditional heuristic approaches. These empirical findings collectively demonstrate that MEV represents a fundamental economic force within blockchain rather than a temporary inefficiency, necessitating protocol-level interventions that account for the persistent and evolving nature of value extraction behaviors observed across multiple blockchain platforms and time periods.

9. Research Challenges and Future Directions

Building on our analysis of MEV strategies, mitigation solutions, theoretical implications, and empirical studies, we outline the key research challenges and future directions for MEV. We organize this discussion along four axes that follow the core technical analysis: (i) MEV strategy evolution and detection, (ii) future MEV mitigation mechanisms and deployment, (iii) cross-chain and cross-domain MEV in interoperable DeFi architectures, and (iv) socio-technical and data-centric foundations for MEV research.

9.1. MEV Strategy Evolution and Detection

MEV strategies evolve together with DeFi infrastructure, trading tools, and user behavior. They already extend beyond simple arbitrage or sandwich attacks and involve complex multi-hop paths, interactions with multiple protocols, and adaptive use of infrastructure such as private order flow. The central challenge is to track this evolution at the level of individual strategies and at the scale of the full MEV supply chain. This subsection focuses on open problems around recognizing new MEV patterns early and building adaptive detection pipelines that remain effective as DeFi changes.

9.1.1. Detection of Newer MEV Strategies

With the rapid growth and advances of DeFi, new MEV patterns (e.g., Lazarus, gas-leeching) are also constantly evolving [60]. For example, Li et al. [155] introduce 17 variants of MEV strategies in DeFi actions. To underscore the adaptive and multifaceted nature of MEV activities, it becomes inevitably important to come up with novel detection and mitigation solutions. On the other hand, standard MEV detection methods (e.g., Flashbots) largely rely on static (or heuristic) transaction analysis. Such analysis often becomes ineffective against rapidly evolving MEV strategies due to their complex and time-sensitive transaction patterns. As a result, the development of adaptive detection methods is essential for the growing DeFi landscape. Furthermore, emerging MEV strategies often entail interlinked contracts, multi-hop trades, and dynamic order placements that interact with different layers of protocols (consensus, base, and application). Future research should incorporate time-series analysis and streaming data pipelines to identify MEV patterns as they evolve rather than only recognizing static behaviors. For instance, graph-based models combined with real-time anomaly detection can capture new MEV strategies that dynamically alter transaction flows and exploit time-dependent market conditions (e.g., sudden liquidity shifts or pricing discrepancies).

9.1.2. LLM-based MEV Detection and Mitigation

Existing heuristic-based MEV detection methods often fail to adapt swiftly to newly emerging attacks, which necessitates more robust and flexible learning frameworks. Large language models (LLMs) represent a paradigm shift in MEV detection by learning a joint distribution over transaction semantics and contract logic. This enables unified reasoning across heterogeneous on-chain inputs. Several specialized LLMs have emerged for direct MEV transaction classification. For example, BlockGPT [182] is trained on 68 million Ethereum execution traces, allowing it to process about 2,000 transactions per second. It routinely ranks front-running and sandwich exploits among its highest-risk alerts. OwLLM, developed by Sec3, is another 100-million-parameter model trained on millions of blockchain transactions. It demonstrates chain-agnostic

⁴²[0x0fe...1c92](#)

⁴³[Rivanorth Analysis](#)

⁴⁴[DappRadar Report](#)

⁴⁵[DSHR Analysis](#)

⁴⁶[Cointelegraph Report](#)

⁴⁷[Rekt News](#)

⁴⁸[Solana MEV Analysis](#)

Table 7: Summary of key challenges and future directions.

Challenges	Key Enablers	Research Gap	Future Direction
Theory & Practice	- Game-theoretic models - Open-source testbeds	Limited real-world validation	i) Deploy mitigation pilots ii) Evaluate on production chains
Newer MEV	- Dynamic & graph analytics - Streaming pipelines	No adaptive multi-chain detectors	i) Real-time monitoring ii) Adaptive pattern recognition
Interoperability	- Cross-chain correlation - Bridge analytics	Complex ordering across heterogeneous chains	i) Standardized analytics ii) Robust bridging standards
GenAI and LLMs	- VAEs & GANs - Transformers	Bias, opacity, compute cost	i) Explainable GenAI detectors ii) Resource-efficient inference
AI Agents	- Decentralized agent - On-chain governance	Scalable coordination	i) Large-scale agent orchestration ii) Incentive-aligned cooperation
Scalability	- Online learning - Distributed compute	High throughput and resource limits	i) Lightweight algorithms ii) Sharded detection
Explainability	- SHAP, LIME - Domain ontologies	Limited user-friendly insights	i) Consistent explanation layers ii) Visualization dashboards
Interpretability	- Model-agnostic attribution - Feature importance ranking	Opaque deep-model logic	i) Global attribution methods ii) Transparent rule extraction
Ethical	- User consent frameworks - Transparent disclosures	Empirical welfare assessments	i) Develop ethical evaluation ii) Enhance user consent
Regulatory	- Protocol-level transparency - Legal definitions	Undefined legal framework	i) Establish regulatory criteria ii) Cross-jurisdictional cooperation

MEV classification with 94% accuracy⁴⁹. On the other hand, DeFiScope [183] adapts GPT-3.5 and GPT-4 to parse arbitrary price-calculation code, achieving 80% recall on historical price-manipulation incidents.

LLMs are also advancing MEV detection through sophisticated vulnerability analysis and exploit generation capabilities, thus demonstrating their dual-use nature in the MEV ecosystem. AiRacleX [184] employs three LLMs in sequence to detect price-oracle manipulation MEV patterns. This approach improves recall by 2.58x over GPTScan while maintaining similar precision. The LLM-BSCVM framework [185] provides comprehensive vulnerability management, which includes detection, cause analysis, repair suggestions, and patch generation. It achieves an >91% F1 score. Recent advances in smart contract decompilation, using fine-tuned Llama 3.2-3B models [186], enable analysis of unverified MEV bot contracts. These models successfully reverse-engineer vulnerabilities in bots that suffered 221,600 USD losses. However, the dual-use nature of LLMs presents significant challenges. For example, InstAI’s framework generates MEV strategies on Solana using a custom LLM trained on 2.3 million profitable MEV transactions⁵⁰. The A1 system [187] demonstrates autonomous exploit generation, with a 63% success rate on vulnerable contracts. This system could potentially extract up to 8.59 million USD per exploit. Despite these promising developments, LLM-based MEV approaches face limitations. These include cross-chain generalization challenges, accuracy degradation on new datasets, computational overhead limiting real-time

deployment, and the need for ethical frameworks governing responsible disclosure and deployment practices.

9.2. Future MEV Mitigation Mechanisms and Deployment

Mitigation mechanisms must reshape incentives instead of only hiding order flow or shifting MEV into opaque execution channels. Designs require clear economic guarantees, robustness under strategic behavior, and practical deployment paths in production DeFi systems. A key challenge is to connect theoretical models of MEV with protocol, infrastructure, and application design while preserving scalability and decentralization. This subsection highlights research directions for mechanism design, deployment, and evaluation that bridge this gap.

9.2.1. Bridging Gap between Theory and Practice

The inherent information asymmetry between validators and users often results in unfair outcomes, where validators disproportionately profit from user transactions. Addressing this issue requires the adaptation of new algorithms to ensure equitable wealth distribution from coordinated actions [188]. Furthermore, implementing mechanisms for transparent information sharing and fair profit distribution among all participants is crucial for building trust and ensuring the long-term viability of DeFi. Additionally, exploring game-theoretic frameworks and multi-agent reinforcement learning techniques could contribute to the development of MEV-resistant protocols that incentivize cooperation and prevent exploitation, thereby enhancing the sustainability of the DeFi ecosystem. Bridging the gap between theoretical advancements and practical applications is essential for mitigating MEV.

⁴⁹<https://www.sec3.dev/blog/owlmm>

⁵⁰<https://www.instai.dev/learn>

Integrating MEV dynamics into formal blockchain system models provides a foundational framework for systematic analysis and protocol design. Consequently, developing robust frameworks that can withstand adversarial attacks and operate effectively in real-world scenarios is critical for realizing the full potential of MEV mitigation [189]. To support this, the use of open-source platforms, the establishment of standardized interfaces, and the promotion of collaborative research efforts are vital for translating academic research into practical and effective solutions.

9.2.2. Scalability, Explainability, and Interpretability

The continuous evolution of DeFi platforms introduces new assets, routes, and participants at an accelerating pace. MEV detection and mitigation algorithms must be adaptable enough to keep up with these changes, dynamically adjusting strategies to maintain coordination and efficiency. Approaches such as online learning [190], dynamic network adaptations [191], and real-time feedback [192] are essential for staying responsive to the shifting DeFi landscape while accurately identifying MEV activities. Moreover, scalability is another key concern. As blockchain networks grow in size and complexity, algorithms must remain computationally efficient to process the increasing volume of transactions and data. Lightweight algorithms and distributed computing techniques are promising solutions that can help scale detection systems to handle large datasets and high-frequency transaction flows. These advancements are critical to ensure that MEV strategies can be identified and mitigated without sacrificing performance or responsiveness. Despite advances in MEV detection, the explainability and interpretability of AI have become some of the emerging areas in regard to identifying malicious or anomalous transactions [193]. For example, the blackbox nature of deep-learning or ensemble-based systems reduces user trust, as stakeholders (e.g., liquidity providers, traders, protocol developers) typically cannot see the reasoning behind flagged activity. Furthermore, the high-dimensional data (e.g., real-time transaction histories, liquidity pool states, and conditional states of smart contracts) make it difficult to produce concise and human-readable justifications. This complexity is amplified by rapidly evolving DeFi protocols and market conditions, which may invalidate pre-defined explanation templates or static rule sets.

Integrating Explainable AI (XAI) into MEV detection can be a notable direction to overcome some limitations [194]. XAI models (e.g., SHAP, LIME) can be adapted into blockchain data structures to generate localized and human-readable versions of specific transaction attributes or historical factors that would trigger an MEV alert. In conjunction, model-agnostic interpretability approaches can help ensure explanations remain consistent across multiple detection algorithms or evolving protocol versions. Moreover, domain-specific ontologies (e.g., standard labels for transaction types, contract states, or pool behaviors) will enhance the data layer to produce uniform and comprehensible justifications [140].

9.2.3. Cooperative AI Agents

Cooperative AI marks a transformative approach to address the inherent complexities in DeFi by leveraging the collective intelligence of multiple AI systems [195–199]. Within this framework, AI agents become crucial as they collaboratively enhance the system’s capabilities. These agents are autonomous systems that process information and execute actions to achieve specific goals [200, 201]. In terms of MEV, AI agents monitor, detect, and neutralize malicious behaviors in order to enhance the overall fairness, efficiency, and security of DeFi. However, it is challenging to deploying the cooperative AI agent in real-world DeFi settings due to several reasons. Firstly, current multi-agent approaches assume agents to pre-agree on cooperative strategies. However, adversarial actors in permissionless environments are motivated to defect and maximize MEV. Second, real-time cooperation among multiple agents in blockchains involves significant computational overhead, complex consensus rules, and evolving smart contracts.

To address these challenges, on-chain governance models should be explored where agent-driven mechanisms can be designed to adapt to the dynamic market conditions [202]. Moreover, agent-based monitoring and forecasting tools can help DeFi stakeholders anticipate and preempt sophisticated MEV schemes [165, 203]. Furthermore, we should explore the AI agents in decentralized commitment devices to coordinate actions and prevent adversarial behaviors associated with MEV [196].

9.3. Cross-chain and Cross-domain MEV in Interoperable DeFi

Interoperable DeFi introduces MEV opportunities that extend across bridges, rollups, and heterogeneous L1 platforms. Value extraction is no longer confined to a single chain and depends on settlement guarantees, latency, liquidity distribution, and bridge design across domains. The main challenge is to characterize and control cross-domain MEV while preserving legitimate cross-chain activity and capital mobility. This subsection outlines future research directions for MEV-aware interoperability protocols and cross-domain risk management.

9.3.1. Interoperability between Protocols and Domains

With the increasing interoperability of DeFi platforms and the rise of cross-chain bridges, MEV opportunities are no longer confined to a single blockchain or protocol. Cross-protocol and cross-chain MEV exploits involve taking advantage of discrepancies in asset prices, liquidity, or arbitrage opportunities across multiple ecosystems. However, tracking cross-chain MEV strategies introduces several challenges: (1) Transaction ordering complexity, as malicious actors sequence trades across different networks to maximize gains; (2) heterogeneous security assumptions due to the chain variety in consensus mechanisms and finality guarantees; (3) inconsistent data availability makes it difficult to monitor and correlate transactions in real

time; and (4) protocol-specific bugs or vulnerabilities within bridging mechanisms affect cross-chain arbitrage or front-running.

To address the aforementioned challenges, multiple avenues can be explored. For example, cross-chain analytics platforms (e.g., CryptoQuant⁵¹) can be deployed to aggregate and normalize transaction data from diverse blockchains and DeFi ecosystems. Another direction could be unified standards or interoperable smart contract interfaces (e.g., ERC-20, ERC-721), which have the potential to reduce the risk of mismatched finality or exploit-prone bridging solutions. On-chain governance platforms (e.g., Tezos⁵²) are another promising avenue to enforce stricter bridging protocols to mitigate vulnerabilities from asset transfers. These governance frameworks provide systematic decision-making processes and community-driven oversight mechanisms to mitigate vulnerabilities from asset transfers [204].

9.4. Socio-technical and Data-centric Foundations for MEV Research

MEV research sits at the intersection of protocol design, markets, and policy. Technical approaches depend on assumptions about acceptable forms of value extraction, on the availability and quality of on-chain and off-chain data, and on the behavior of infrastructure providers and users. At the same time, regulators, platforms, and communities hold different views on fairness, privacy, and accountability. This subsection highlights ethical, regulatory, and data-centric questions that need to evolve in parallel with technical work on MEV.

9.4.1. Ethical, Regulatory, and Jurisdictional Implications

The ethical debate around MEV increasingly centers on the distinction between extractive and productive strategies introduced in Section 5.5. MEV strategies like sandwich attacks and front-running exploit informational asymmetries, imposing indirect costs on ordinary users [205]. Although certain MEV activities such as arbitrage might improve market efficiency, distinguishing beneficial from harmful practices remains challenging, as even seemingly benign methods can impact network fairness and congestion [56]. Centralization of MEV rewards among sophisticated entities also threatens decentralization principles. Moreover, monetizing user intent without explicit consent, particularly through selling transaction data, raises significant privacy concerns [56, 206]. A critical research gap persists regarding the empirical evaluation of MEV's overall welfare impact. Future research should develop frameworks emphasizing user intent as a core ethical principle, clearly define exploitative behaviors, and foster transparency to facilitate informed user consent. Addressing these ethical concerns is essential for maintaining user trust and promoting sustainable adoption.

The regulatory landscape surrounding MEV remains largely underdeveloped, posing significant challenges to policymakers and blockchain participants [34]. Existing laws struggle to address blockchain-specific manipulation effectively, lacking clear definitions or enforcement frameworks for MEV-related activities [205, 206]. Regulatory bodies, including BIS, IOSCO, CFTC, and SEC have begun recognizing MEV, but clarity and coherence in the legal treatment of MEV are still lacking [30, 34]. Enforcement difficulties arise due to challenges in proving intent and market impact, although recent regulatory actions indicate increasing scrutiny [30, 207]. Future regulatory approaches should integrate accountability and transparency at the protocol level, establish clear criteria for detecting MEV exploitation, and support empirical assessments of MEV's welfare implications before imposing prescriptive measures [34, 56]. Emphasis should be placed on prosecuting clear instances of fraudulent or manipulative behavior, thus creating a regulatory environment conducive to both innovation and fairness [205, 206].

The jurisdictional challenges also pose particularly significant obstacles to effective MEV enforcement across international boundaries. The decentralized and borderless nature of blockchain networks creates situations where MEV activities occur globally without clear legal nexus, making it difficult for regulators to determine applicable jurisdiction and establish oversight [208]. This technological architecture enables regulatory arbitrage, where MEV participants can relocate operations to exploit more permissive jurisdictions while continuing to affect markets elsewhere [56]. The resulting patchwork of local regulations creates a "race to the bottom", encouraging jurisdiction shopping and undermining enforcement efforts of more regulated nations [209]. The pseudonymous nature of blockchain participants exacerbates these challenges, as identifying parties involved in illicit MEV activities becomes extremely difficult for regulators attempting to trace and prosecute cross-border violations. International coordination efforts have emerged to address these challenges: ESMA's MiCA guidelines emphasize the need for EU-wide supervisory culture and cross-border cooperation to address third-country crypto-asset service providers that may elude regulatory reach [210], while IOSCO's DeFi recommendations stress the importance of international coordination given the interconnectedness between DeFi and traditional finance [211]. However, successful enforcement requires unprecedented levels of collaborative solutions and information sharing between national authorities to combat the inherent advantages that bad actors gain from exploiting regulatory differences [212, 213].

9.4.2. Platform Inclusivity and Analysis Constraints

The concept of inclusive blockchain platforms designed to provide equitable access and fair transaction ordering mechanisms represents a critical consideration in MEV research. However, the selection of blockchain platforms for MEV studies inherently introduces systematic biases that

⁵¹<https://cryptoquant.com/>

⁵²<https://tezos.com/>

limit the generalizability of findings [214]. Current research predominantly focuses on established chains like Ethereum and Polygon due to their substantial DeFi activity and mature data infrastructure, yet this concentration overlooks emerging platforms with innovative MEV-resistant designs. Future research must develop chain-agnostic methodologies that can analyze MEV patterns across heterogeneous blockchain architectures [85]. Additionally, research efforts should extend to non-EVM platforms requiring custom tooling and chains without public mempools where traditional detection methods fail to capture MEV activity.

Beyond platform selection biases, MEV data collection faces significant technical and temporal constraints that further undermine analytical accuracy and completeness [33]. Price normalization methodologies using block-timestamp exchange rates may deviate from actual execution prices by 5-10% during volatile periods, introducing systematic error into value calculations [49]. Additionally, detection methodologies suffer from high false-negative rates for novel strategies, API rate limits constrain real-time analysis capabilities, and the absence of ground truth labels limits validation accuracy. These constraints collectively indicate that current empirical estimates represent only a lower bound of true MEV extraction, with actual values potentially exceeding reported totals by 20-40% when accounting for undetected strategies, private mempool transactions, and cross-chain activities that elude current analytical tools.

10. Conclusion

We presented a comprehensive survey of MEV within the DeFi and blockchain ecosystem. By systematically categorizing existing and emerging MEV strategies, we highlighted the intricate interactions between digital tokens, DeFi protocols, and the evolving tactics of adversaries. This addressed the need to understand how malicious behaviors adapt to new platforms, solutions, and consensus protocols. Furthermore, we provided a multifaceted representation of MEV mitigation strategies across different layers of blockchain, i.e., consensus, base, and application layer. This outlined how each mitigation strategy targets different parts of the blockchain stack. Moreover, we combined theoretical insights and empirical analysis to explore MEV's dynamics comprehensively. Furthermore, theoretical frameworks (e.g., game theory, optimization) and empirical analysis were explored through the lens of the economic incentives and strategic behaviors of users, searchers, and adversaries.

Future research must address the adaptive and multifaceted nature of emerging MEV strategies, such as those leveraging interlinked contracts, multi-hop trades, and dynamic order placements. Existing static detection methods fall short of handling the evolving complexities of MEV. Advanced methods incorporating time-series analysis, graph-based models, and real-time anomaly detection are crucial

for capturing dynamic transaction flows and layered protocol interactions. Furthermore, cross-protocol monitoring and AI-driven approaches will play an essential role in detecting sophisticated MEV activities as DeFi systems grow more intricate. To ensure a sustainable and equitable digital financial landscape, interdisciplinary efforts across protocol design, smart contract engineering, and regulatory frameworks are vital. This holistic perspective will enable DeFi to evolve while maintaining fairness, security, and inclusivity for all stakeholders.

Acknowledgments

This work is supported by the National Key Research and Development Program of China (No. 2020YFA0909100) and the Basic and Applied Basic Research Foundation of Guangdong Province (No. 2023TQ07A264).

Authors Contribution Statement

Md Monjurul Karim: Conceptualization, Methodology, Formal analysis, Visualization, Software, Writing – Original Draft.

Dong Hoang Van: Visualization, Writing – Review & Editing.

Qiang Qu: Conceptualization, Validation, Supervision, Project administration, Funding acquisition, Writing – Review & Editing.

Declaration of Interest Statement

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

The author is an Editorial Board Member/Editor-in-Chief/Associate Editor/Guest Editor for this journal and was not involved in the editorial review or the decision to publish this article.

References

- [1] P. Schueffel, What colors are the bricks? unboxing the defi model-a literature survey, empirical study, and taxonomy of decentralized finance, *Journal of Banking and Financial Technology* (2025) 1–29.
- [2] D. Stroukal, P. Peterka, Tokenization as a pathway to anonymity in central bank digital currencies, *Research in International Business and Finance* 75 (2025) 102769.
- [3] J. Gan, J. Su, K. Lin, Z. Zheng, Financefuzz: Fuzzing smart contracts with financial properties, *Blockchain: Research and Applications* (2025) 100301.
- [4] S. Hagele, Centralized exchanges vs. decentralized exchanges in cryptocurrency markets: A systematic literature review, *Electronic Markets* 34 (1) (2024) 33.
- [5] M. Kirişci, An integrated decision-making process for risk analysis of decentralized finance, *Neural Computing and Applications* (2025) 1–31.
- [6] P. A. Bongini, F. Mattassoglio, A. Pedrazzoli, S. Vismara, Crypto ecosystem: navigating the past, present, and future of decentralized finance, *The Journal of Technology Transfer* (2025) 1–22.

- [7] P. Zheng, Z. Jiang, J. Wu, Z. Zheng, Blockchain-based decentralized application: A survey, *IEEE Open Journal of the Computer Society* 4 (2023) 121–133.
- [8] J. Chen, M. Huang, Z. Lin, P. Zheng, Z. Zheng, To healthier ethereum: A comprehensive and iterative smart contract weakness enumeration, *Blockchain: Research and Applications* 6 (2) (2025) 100258.
- [9] S. Chaliasos, M. A. Charalambous, L. Zhou, R. Galanopoulou, A. Gervais, D. Mitropoulos, B. Livshits, Smart contract and defi security tools: Do they meet the needs of practitioners?, in: *Proceedings of the 46th IEEE/ACM International Conference on Software Engineering*, 2024, pp. 1–13.
- [10] F. Wu, A. Ye, Y. Diao, Y. Zhang, J. Chen, C. Huang, Trustchain: A privacy protection smart contract model with trusted execution environment, *Blockchain: Research and Applications* (2025) 100296.
- [11] A. Shrestha, S. S. Mohammed Abdul, J. Yong, Crossdefi: A novel cross-chain communication protocol, *Future Internet* 16 (9) (2024).
- [12] W. Li, Z. Liu, J. Chen, Z. Liu, Q. He, Towards blockchain interoperability: A comprehensive survey on cross-chain solutions, *Blockchain: Research and Applications* (2025) 100286.
- [13] Llama Corp. [DefiLlama DeFi Dashboard](#) [online]. (Accessed 20 March 2025).
- [14] EigenPhi. [Daily MEV Data Reports](#) [online]. (Accessed 20 March 2025).
- [15] Dune Analytics. [Uniswap V3 MEV Activity](#) [online]. (Accessed 20 March 2025).
- [16] CoinGecko. [The Beginner's Guide to MEV](#) [online]. (Accessed 20 March 2025).
- [17] L. Zhou, X. Xiong, J. Ernstberger, S. Chaliasos, Z. Wang, Y. Wang, K. Qin, R. Wattenhofer, D. Song, A. Gervais, Sok: Decentralized finance (defi) attacks, in: *2023 IEEE Symposium on Security and Privacy (SP)*, IEEE, 2023, pp. 2444–2461.
- [18] L. Zhou, K. Qin, C. F. Torres, D. V. Le, A. Gervais, High-Frequency Trading on Decentralized On-Chain Exchanges, in: *2021 IEEE Symposium on Security and Privacy (SP)*, 2021, pp. 428–445. doi:10.1109/SP40001.2021.00027.
- [19] K. Qin, L. Zhou, P. Gamito, P. Jovanovic, A. Gervais, An empirical study of defi liquidations: Incentives, risks, and instabilities, in: *Proceedings of the 21st ACM Internet Measurement Conference*, 2021, pp. 336–350.
- [20] L. Zhou, K. Qin, A. Cully, B. Livshits, A. Gervais, On the Just-In-Time Discovery of Profit-Generating Transactions in DeFi Protocols, in: *2021 IEEE Symposium on Security and Privacy (SP)*, 2021, pp. 919–936. doi:10.1109/SP40001.2021.00113.
- [21] K. Qin, L. Zhou, A. Gervais, Quantifying Blockchain Extractable Value: How dark is the forest?, in: *2022 IEEE Symposium on Security and Privacy (SP)*, 2022, pp. 198–214. doi:10.1109/SP46214.2022.9833734.
- [22] P. Daian, S. Goldfeder, T. Kell, Y. Li, X. Zhao, I. Bentov, L. Breidenbach, A. Juels, Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability, in: *2020 IEEE Symposium on Security and Privacy (SP)*, 2020, pp. 910–927. doi:10.1109/SP40000.2020.00040.
- [23] Y. Zhao, X. Kang, T. Li, C.-K. Chu, H. Wang, Toward trustworthy defi oracles: past, present, and future, *IEEE Access* 10 (2022) 60914–60928.
- [24] S. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, W. Knottenbelt, SoK: Decentralized Finance (DeFi), in: *Proceedings of the 4th ACM Conference on Advances in Financial Technologies, AFT '22*, Association for Computing Machinery, New York, NY, USA, 2023, pp. 30–46. doi:10.1145/3558535.3559780.
- [25] A. Alamsyah, G. N. W. Kusuma, D. P. Ramadhani, A review on decentralized finance ecosystems, *Future Internet* 16 (3) (2024) 76.
- [26] J. Xu, K. Paruch, S. Cousaert, Y. Feng, SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols, *ACM Computing Surveys* 55 (11) (2023) 238:1–238:50. doi:10.1145/3570639.
- [27] J. Xu, Y. Feng, Reap the Harvest on Blockchain: A Survey of Yield Farming Protocols, *IEEE Transactions on Network and Service Management* 20 (1) (2023) 858–869. doi:10.1109/TNSM.2022.3222815.
- [28] C. Baum, J. Hsin-yu Chiang, B. David, T. K. Frederiksen, L. Gentile, Sok: Mitigation of front-running in decentralized finance, in: *International Conference on Financial Cryptography and Data Security*, Springer, 2022, pp. 250–271.
- [29] D. Xiang, Y. Lin, L. Nie, Y. Zheng, Z. Xu, Z. Ding, Y. Liu, An empirical study of attack-related events in defi projects development, *Empirical Software Engineering* 29 (2) (2024) 49.
- [30] S. Yang, F. Zhang, K. Huang, X. Chen, Y. Yang, F. Zhu, Sok: Mev countermeasures, in: *Proceedings of the Workshop on Decentralized Finance and Security*, 2024, pp. 21–30.
- [31] L. Heimbach, R. Wattenhofer, SoK: Preventing Transaction Reordering Manipulations in Decentralized Finance, in: *Proceedings of the 4th ACM Conference on Advances in Financial Technologies, AFT '22*, Association for Computing Machinery, New York, NY, USA, 2023, pp. 47–60. doi:10.1145/3558535.3559784.
- [32] Z. Alipanahloo, A. S. Hafid, K. Zhang, Maximum extractable value (mev) mitigation approaches in ethereum and layer-2 chains: A comprehensive survey, *IEEE Access* 12 (2024) 185212–185231.
- [33] H. Materwala, S. M. Naik, A. Taha, T. A. Abed, D. Svetinovic, Maximal extractable value in decentralized finance: Taxonomy, detection, and mitigation, *IEEE Transactions on Services Computing* 18 (6) (2025) 4386–4407.
- [34] V. Gramlich, D. Jelito, J. Sedlmeir, Maximal extractable value: Current understanding, categorization, and open research questions, *Electronic Markets* 34 (1) (2024) 49.
- [35] H.-A. Pham, C. T. Nguyen, T. C. Lam, Blockchain adoption for authentication: A survey, *Blockchain: Research and Applications* (2025) 100383.
- [36] S. Rizal, D.-S. Kim, Enhancing blockchain consensus mechanisms: A comprehensive survey on machine learning applications and optimizations, *Blockchain: Research and Applications* (2025) 100302.
- [37] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, *Decentralized Business Review* (2008) 21260.
- [38] V. Buterin, et al., *Ethereum white paper*, GitHub repository 1 (22-23) (2013) 5–7.
- [39] S. Park, W. Jeong, Y. Lee, B. Son, H. Jang, J. Lee, Unraveling the MEV enigma: ABI-free detection model using Graph Neural Networks, *Future Generation Computer Systems* 153 (2024) 70–83. doi:10.1016/j.future.2023.11.014.
- [40] M. Hanif, E. U. Munir, M. M. Rehan, S. G. Ahmad, I. Khan, R. Setchi, Tiered blockchain framework: A secure, trustworthy, and cost-efficient solution for the digital rights protection, *Blockchain: Research and Applications* (2025) 100308.
- [41] M. Blum, N. Crimi, P. Emmenegger, F. Spychiger, C. J. Tessone, Governance and maintenance for daos with physical assets—the case of no1s1, *Blockchain: Research and Applications* (2025) 100357.
- [42] W. Li, J. Bu, X. Li, H. Peng, Y. Niu, Y. Zhang, A survey of defi security: Challenges and opportunities, *Journal of King Saud University-Computer and Information Sciences* 34 (10) (2022) 10378–10404.
- [43] M. Bartoletti, J. H.-y. Chiang, A. Lluch Lafuente, Maximizing Extractable Value from Automated Market Makers, in: I. Eyal, J. Garay (Eds.), *Financial Cryptography and Data Security*, Lecture Notes in Computer Science, Springer International Publishing, Cham, 2022, pp. 3–19. doi:10.1007/978-3-031-18283-9_1.
- [44] J. H. Sijursen, W. Meng, W.-Y. Chiu, Towards Quantifying Cross-Domain Maximal Extractable Value for Blockchain Decentralisation, in: D. Wang, M. Yung, Z. Liu, X. Chen (Eds.), *Information and Communications Security*, Lecture Notes in Computer Science, Springer Nature, Singapore, 2023,

- pp. 627–644. doi:10.1007/978-981-99-7356-9_37.
- [45] J. Chen, Y. Wang, Y. Zhou, W. Ding, Y. Tang, X. Wang, K. Li, Understanding the Security Risks of Decentralized Exchanges by Uncovering Unfair Trades in the Wild, in: 2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P), 2023, pp. 332–351. doi:10.1109/EuroSP57164.2023.00028.
- [46] S. Hossain, A. Altarawneh, Unraveling ethereum’s mempool: The impact of fee fairness, transaction prioritization, and consensus efficiency, arXiv preprint arXiv:2506.07988 (2025).
- [47] W. Ding, Y. Tang, Y. Wang, Asymmetric mempool dos security: Formal definitions and provable secure designs, in: 2025 IEEE Symposium on Security and Privacy (SP), IEEE, 2025, pp. 1584–1602.
- [48] Oz, Burak and Rezabek, Filip and Gebele, Jonas and Hoops, Felix and Matthes, Florian, A study of mev extraction techniques on a first-come-first-served blockchain, in: Proceedings of the 39th ACM/SIGAPP Symposium on Applied Computing, 2024, pp. 288–297.
- [49] C. Ferreira Torres, A. Mamuti, B. Weintraub, C. Nita-Rotaru, S. Shinde, Rolling in the shadows: Analyzing the extraction of mev across layer-2 rollups, in: Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security, 2024, pp. 2591–2605.
- [50] H. Adams, N. Zinsmeister, M. Salem, R. Keefer, D. Robinson, Uniswap v3 Core, Uniswap Technical Report (2021).
- [51] M. Egorov, Stableswap – efficient mechanism for Stablecoin liquidity, Tech. rep., Curve StableSwap Whitepaper (2019). URL <https://classic.curve.fi/files/stableswap-paper.pdf>
- [52] E. Hertzog, G. Benartzi, G. Benaratzi, Bancor Protocol – Continuous Liquidity for Cryptographic Tokens through their Smart Contracts, Tech. rep., Bancor Whitepaper (Mar. 2018). URL <https://docs.bancor.network/about-bancor-network/faqs/resources>
- [53] F. Calandra, F. P. Rossi, F. Fabris, M. Bernardo, Learning from terra-luna: A simulation-based study on stabilizing algorithmic stablecoins, Blockchain: Research and Applications (2025) 100364.
- [54] D. Li, D. Han, T.-H. Weng, Z. Zheng, H. Li, K.-C. Li, On Stablecoin: Ecosystem, architecture, mechanism and applicability as payment method, Computer Standards & Interfaces 87 (2024) 103747. doi:10.1016/j.csi.2023.103747.
- [55] M. M. Karim, Q. Qu, Y. Cai, T. Liu, X. Meng, Bitcoin reimaged: A comprehensive study of ordinals and inscriptions protocols for web3 asset innovation, Blockchain: Research and Applications (2025) 100379.
- [56] M. Barcentewicz, Mev on ethereum: A policy analysis, ICLE White Paper (2023) 01–23.
- [57] European Securities and Markets Authority (ESMA), Maximal extractable value: Implications for crypto markets, TRV Risk Analysis ESMA50-481369926-29744, European Securities and Markets Authority, Paris, France, published 1 July 2025 (July 2025). URL https://www.esma.europa.eu/sites/default/files/2025-07/ESMA50-481369926-29744_Maximal_Extractable_Value_Implications_for_crypto_markets.pdf
- [58] S. Ramos, J. Ellul, The MEV Saga: Can Regulation Illuminate the Dark Forest?, in: M. Ruiz, P. Soffer (Eds.), Advanced Information Systems Engineering Workshops, Lecture Notes in Business Information Processing, Springer International Publishing, Cham, 2023, pp. 186–196. doi:10.1007/978-3-031-34985-0_19.
- [59] P. Poux, P. De Filippi, B. Deffains, Maximal extractable value and the blockchain commons, Available at SSRN 4198139 (2022).
- [60] K. Babel, M. Javaheripi, Y. Ji, M. Kelkar, F. Koushanfar, A. Juels, Lanturn: Measuring economic security of smart contracts through adaptive learning, in: Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, 2023, pp. 1212–1226.
- [61] A. Antonovici, MEV Bot Guide for Beginners: Ethereum Arbitrage in 2024 (Sep. 2023). URL <https://www.tastycrypto.com/defi/mev-bots/>
- [62] Uniswap Protocol. Swap, Earn, and Build on the Leading Decentralized Crypto Trading Protocol [online]. (Accessed 20 March 2025).
- [63] PancakeSwap. The Most Popular AMM on BSC by User Count [online]. (Accessed 20 March 2025).
- [64] D. Mancino, A. Leporati, M. Viviani, G. Denaro, Exploiting Ethereum after "The Merge": The Interplay between PoS and MEV Strategies, in: F. Buccafurri, E. Ferrari, G. Lax (Eds.), Proceedings of the Italian Conference on Cyber Security (ITASEC 2023), Bari, Italy, May 2-5, 2023, Vol. 3488 of CEUR Workshop Proceedings, CEUR-WS.org, 2023, pp. 1–14.
- [65] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, L. Shamseer, J. M. Tetzlaff, E. A. Akl, S. E. Brennan, et al., The prisma 2020 statement: an updated guideline for reporting systematic reviews, bmj 372 (2021).
- [66] S. A. Abed, M. Gök, Big data and artificial intelligence on the blockchain: a review, Babylonian Journal of Artificial Intelligence 2023 (2023) 1–4.
- [67] A. Wahrstätter, L. Zhou, K. Qin, D. Svetinovic, A. Gervais, Time to Bribe: Measuring Block Construction Market (Jun. 2023). arXiv:2305.16468, doi:10.48550/arXiv.2305.16468.
- [68] K. Qin, S. Chaliasos, L. Zhou, B. Livshits, D. Song, A. Gervais, The Blockchain Imitation Game, in: 32nd USENIX Security Symposium (USENIX Security 23), 2023, pp. 3961–3978. URL <https://www.usenix.org/conference/usenixsecurity23/presentation/qin>
- [69] W. Zhang, L. Wei, S.-C. Cheung, Y. Liu, S. Li, L. Liu, M. R. Lyu, Combatting Front-Running in Smart Contracts: Attack Mining, Benchmark Construction and Vulnerability Detector Evaluation, IEEE Transactions on Software Engineering 49 (6) (2023) 3630–3646. doi:10.1109/TSE.2023.3270117.
- [70] D. M. Doe, J. Li, N. Dusit, L. Wang, Z. Han, Incentive Mechanism Design for Mitigating Frontrunning and Transaction Reordering in Decentralized Exchanges, IEEE Access 11 (2023) 96014–96028. doi:10.1109/ACCESS.2023.3236891.
- [71] B. Öz, J. Gebele, F. Rezabek, F. Hoops, F. Matthes, A First Study of MEV on an Up-and-Coming Blockchain: Algorand (Aug. 2023). arXiv:2308.06513, doi:10.48550/arXiv.2308.06513.
- [72] L. Heimbach, R. Wattenhofer, Eliminating Sandwich Attacks with the Help of Game Theory, in: Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security, ASIA CCS ’22, Association for Computing Machinery, New York, NY, USA, 2022, pp. 153–167. doi:10.1145/3488932.3517390.
- [73] Y. Wang, Y. Chen, H. Wu, L. Zhou, S. Deng, R. Wattenhofer, Cyclic Arbitrage in Decentralized Exchanges, in: Companion Proceedings of the Web Conference 2022, WWW ’22, Association for Computing Machinery, New York, NY, USA, 2022, pp. 12–19. doi:10.1145/3487553.3524201.
- [74] I. Makarov, A. Schoar, Trading and arbitrage in cryptocurrency markets, Journal of Financial Economics 135 (2) (2020) 293–319. doi:10.1016/j.jfineco.2019.07.001.
- [75] H. Jin, C. Li, J. Xiao, T. Zhang, X. Dai, B. Li, Detecting Arbitrage on Ethereum Through Feature Fusion and Positive-Unlabeled Learning, IEEE Journal on Selected Areas in Communications 40 (12) (2022) 3660–3671. doi:10.1109/JSAC.2022.3213335.
- [76] M. Hansson, Arbitrage in crypto markets: An analysis of primary ethereum blockchain data, Available at SSRN 4278272 (2022).
- [77] K. Li, S. Guan, D. Lee, Towards Understanding and Characterizing the Arbitrage Bot Scam In the Wild, Proceedings of the ACM on Measurement and Analysis of Computing Systems 7 (3) (2023) 52:1–52:29. doi:10.1145/3626783.
- [78] K. Qin, L. Zhou, B. Livshits, A. Gervais, Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit, in: N. Borisov, C. Diaz (Eds.), Financial Cryptography and Data

- Security, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 2021, pp. 3–32. doi:10.1007/978-3-662-64322-8_1.
- [79] R. McLaughlin, C. Kruegel, G. Vigna, *A Large Scale Study of the Ethereum Arbitrage Ecosystem*, in: 32nd USENIX Security Symposium (USENIX Security 23), 2023, pp. 3295–3312. URL <https://www.usenix.org/conference/usenixsecurity23/presentation/mclaughlin>
- [80] M. Bartoletti, J. H.-y. Chiang, A. L. Lafuente, Sok: lending pools in decentralized finance, in: Financial Cryptography and Data Security, FC 2021 International Workshops: CoDecFin, DeFi, VOTING, and WTSC, Virtual Event, March 5, 2021, Revised Selected Papers 25, Springer, 2021, pp. 553–578.
- [81] C. McMenamin, Sok: Cross-domain mev, arXiv preprint arXiv:2308.04159 (2023).
- [82] B. Oz, C. F. Torres, C. Schlegel, B. Mazorra, J. Gebele, F. Rezabek, F. Matthes, Cross-chain arbitrage: The next frontier of mev in decentralized finance, Proceedings of the ACM on Measurement and Analysis of Computing Systems 9 (3) (2025) 1–33.
- [83] Bousfield et al., Arbitrum nitro: A second-generation optimistic rollup (2022).
- [84] M. Bjelic, S. Nailwal, A. Chaudhary, W. Deng, Pol: One token for all polygon chains, Polygon Technology (2021).
- [85] B. Öz, C. F. Torres, J. Gebele, F. Rezabek, B. Mazorra, F. Matthes, Pandora’s box: Cross-chain arbitrages in the realm of blockchain interoperability, arXiv preprint arXiv:2501.17335 (2025).
- [86] D. Mancino, H. O. Sevim, O. S. Gonzalez, Bunny hops and blockchain stops: Cross-chain mev detection with n-hops, arXiv preprint arXiv:2511.17527 (2025).
- [87] X. Lao, S. Chen, Q. Wang, Fluxlayer: High-performance design for cross-chain fragmented liquidity, in: 2025 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2025, pp. 1–3.
- [88] C. Li, Z. Sun, J. X. Yu, X. Wang, The walls have ears: Unveiling cross-chain sandwich attacks in defi, arXiv preprint arXiv:2511.15245 (2025).
- [89] O. Solmaz, L. Heimbach, Y. Vonlanthen, R. Wattenhofer, Optimistic mev in ethereum layer 2s: Why blockspace is always in demand, arXiv preprint arXiv:2506.14768 (2025).
- [90] J. H. Sijrsen, W. Meng, W.-Y. Chiu, A Closer Look at Cross-Domain Maximal Extractable Value for Blockchain Decentralisation, in: 2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2023, pp. 1–3. doi:10.1109/ICBC56567.2023.10174971.
- [91] D. Wang, S. Wu, Z. Lin, L. Wu, X. Yuan, Y. Zhou, H. Wang, K. Ren, Towards a first step to understand flash loan and its applications in defi ecosystem, in: Proceedings of the Ninth International Workshop on Security in Blockchain and Cloud Computing, 2021, pp. 23–28.
- [92] T. Chitra, K. Kulkarni, Improving Proof of Stake Economic Security via MEV Redistribution, in: Proceedings of the 2022 ACM CCS Workshop on Decentralized Finance and Security, DeFi’22, Association for Computing Machinery, New York, NY, USA, 2022, pp. 1–7. doi:10.1145/3560832.3564259.
- [93] thefett, *On Oracle Extractable Value* (Sep. 2021). URL <https://medium.com/@nfett/on-oracle-extractable-value-f6c7a0d64af5>
- [94] M. Xie, M. Hu, Z. Kong, C. Zhang, Y. Feng, H. Wang, Y. Xue, H. Zhang, Y. Liu, Y. Liu, Defort: Automatic detection and analysis of price manipulation attacks in defi applications, in: Proceedings of the 33rd ACM SIGSOFT International Symposium on Software Testing and Analysis, 2024, pp. 402–414.
- [95] T. Mackinga, T. Nadahalli, R. Wattenhofer, TWAP Oracle Attacks: Easier Done than Said?, in: 2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2022, pp. 1–8. doi:10.1109/ICBC54727.2022.9805499.
- [96] N. Ruan, H. Sun, Z. Lou, J. Li, A General Quantitative Analysis Framework for Attacks in Blockchain, IEEE/ACM Transactions on Networking 31 (2) (2023) 664–679. doi:10.1109/TNET.2022.3201493.
- [97] P. McCorry, A. Hicks, S. Meiklejohn, Smart Contracts for Bribing Miners, in: Financial Cryptography and Data Security: FC 2018 International Workshops, BITCOIN, VOTING, and WTSC, Nieuwpoort, Curaçao, March 2, 2018, Revised Selected Papers, Springer-Verlag, Berlin, Heidelberg, 2018, pp. 3–18. doi:10.1007/978-3-662-58820-8_1.
- [98] A. Judmayer, N. Stifter, A. Zamyatin, I. Tsabary, I. Eyal, P. Gazi, S. Meiklejohn, E. Weippl, Pay to win: cheap, crowdfundable, cross-chain algorithmic incentive manipulation attacks on pow cryptocurrencies, Cryptology ePrint Archive (2019).
- [99] V. Mohan, P. Khezr, Blockchains, mev and the knapsack problem: a primer, arXiv preprint arXiv:2403.19077 (2024).
- [100] C. Atada, *Inside the mempool: Where front-running, sandwiching, and fairness collide*, Mitosis University Blog, accessed: December 15, 2025 (July 2025). URL <https://university.mitosis.org/inside-the-mempool-where-front-running-sandwiching-and-fairness-collide/>
- [101] B. Mazorra, M. Reynolds, V. Daza, Price of MEV: Towards a Game Theoretical Approach to MEV, in: Proceedings of the 2022 ACM CCS Workshop on Decentralized Finance and Security, DeFi’22, Association for Computing Machinery, New York, NY, USA, 2022, pp. 15–22. doi:10.1145/3560832.3563433.
- [102] S. M. Shareef, R. F. Hassan, Improved blockchain technique based on modified slim algorithm for cyber security, Mesopotamian Journal of CyberSecurity 5 (1) (2025) 147–164.
- [103] A. Vedula, S. B. Venkatakrishnan, A. Gupta, Masquerade: Simple and Lightweight Transaction Reordering Mitigation in Blockchains (Aug. 2023). arXiv:2308.15347, doi:10.48550/arXiv.2308.15347.
- [104] D. Malkhi, P. Szalachowski, Maximal Extractable Value (MEV) Protection on a DAG, in: 4th International Conference on Blockchain Economics, Security and Protocols (Tokenomics 2022), Vol. 110 of Open Access Series in Informatics (OASICS), Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 2023, pp. 6:1–6:17. doi:10.4230/OASICS.Tokenomics.2022.6.
- [105] P. Zarbafian, V. Gramoli, Lyra: Fast and Scalable Resilience to Reordering Attacks in Blockchains, in: 2023 IEEE International Parallel and Distributed Processing Symposium (IPDPS), 2023, pp. 929–939. doi:10.1109/IPDPS54959.2023.00097.
- [106] J. Piet, V. Nair, S. Subramanian, MEVade: An MEV-Resistant Blockchain Design, in: 2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2023, pp. 1–9. doi:10.1109/ICBC56567.2023.10174966.
- [107] J. Bebel, D. Ojha, *Ferveo: Threshold Decryption for Mempool Privacy in BFT Networks* (2022). URL <https://eprint.iacr.org/2022/898>
- [108] H. Zhang, L.-H. Merino, V. Estrada-Galiñanes, B. Ford, Flash Freezing Flash Boys: Countering Blockchain Front-Running, in: 2022 IEEE 42nd International Conference on Distributed Computing Systems Workshops (ICDCSW), 2022, pp. 90–95. doi:10.1109/ICDCSW56584.2022.00026.
- [109] K. Babel, P. Daian, M. Kelkar, A. Juels, Clockwork Finance: Automated Analysis of Economic Security in Smart Contracts, in: 2023 IEEE Symposium on Security and Privacy (SP), 2023, pp. 2499–2516. doi:10.1109/SP46215.2023.10179346.
- [110] C. McMenamin, V. Daza, M. Fitzi, P. O’Donoghue, Fair-TraDEX: A Decentralised Exchange Preventing Value Extraction, in: Proceedings of the 2022 ACM CCS Workshop on Decentralized Finance and Security, DeFi’22, Association for Computing Machinery, New York, NY, USA, 2022, pp. 39–46. doi:10.1145/3560832.3563439.
- [111] B. Nasrulin, G. Ishmaev, J. Decouchant, J. Pouwelse, LO: An Accountable Mempool for MEV Resistance, in: Proceedings of the 24th International Middleware Conference, Middleware ’23, Association for Computing Machinery, New York, NY, USA,

- 2023, pp. 98–110. doi:10.1145/3590140.3629108.
- [112] A. Kavousi, D. V. Le, P. Jovanovic, G. Danezis, *BlindPerm: Efficient MEV Mitigation with an Encrypted Mempool and Permutation* (2023).
URL <https://eprint.iacr.org/2023/1061>
- [113] D. Yakira, A. Asayag, G. Cohen, I. Grayevsky, M. Leshkowitz, O. Rottenstreich, R. Tamari, *Helix: A Fair Blockchain Consensus Protocol Resistant to Ordering Manipulation*, IEEE Transactions on Network and Service Management 18 (2) (2021) 1584–1597. doi:10.1109/TNSM.2021.3052038.
- [114] M. Kelkar, F. Zhang, S. Goldfeder, A. Juels, *Order-Fairness for Byzantine Consensus*, in: D. Micciancio, T. Ristenpart (Eds.), *Advances in Cryptology – CRYPTO 2020, Lecture Notes in Computer Science*, Springer International Publishing, Cham, 2020, pp. 451–480. doi:10.1007/978-3-030-56877-1_16.
- [115] Y. Zhang, S. Setty, Q. Chen, L. Zhou, L. Alvisi, *Byzantine Ordered Consensus without Byzantine Oligarchy*, in: 14th USENIX Symposium on Operating Systems Design and Implementation (OSDI 20), 2020, pp. 633–649.
URL <https://www.usenix.org/conference/osdi20/presentation/zhang-yunhao>
- [116] K. Kursawe, Wendy, the Good Little Fairness Widget: Achieving Order Fairness for Blockchains, in: *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, AFT '20, Association for Computing Machinery, New York, NY, USA, 2020, pp. 25–36. doi:10.1145/3419614.3423263.
- [117] K. Kursawe, Wendy Grows Up: More Order Fairness, in: *Financial Cryptography and Data Security. FC 2021 International Workshops: CoDecFin, DeFi, VOTING, and WTSC*, Virtual Event, March 5, 2021, Revised Selected Papers, Springer-Verlag, Berlin, Heidelberg, 2021, pp. 191–196. doi:10.1007/978-3-662-63958-0_17.
- [118] C. Cachin, J. Micić, N. Steinhauer, L. Zanolini, *Quick Order Fairness*, in: *Financial Cryptography and Data Security: 26th International Conference, FC 2022, Grenada, May 2–6, 2022, Revised Selected Papers*, Springer-Verlag, Berlin, Heidelberg, 2022, pp. 316–333. doi:10.1007/978-3-031-18283-9_15.
- [119] M. Kelkar, S. Deb, S. Long, A. Juels, S. Kannan, *Themis: Fast, Strong Order-Fairness in Byzantine Consensus* (2021).
URL <https://eprint.iacr.org/2021/1465>
- [120] Y. Li, M. Zhang, J. Li, E. Chen, X. Chen, X. Deng, *MEV Makes Everyone Happy under Greedy Sequencing Rule*, in: *Proceedings of the 2023 Workshop on Decentralized Finance and Security, DeFi '23*, Association for Computing Machinery, New York, NY, USA, 2023, pp. 9–15. doi:10.1145/3605768.3623543.
- [121] P. Momeni, S. Gorbunov, B. Zhang, *Fairblock: Preventing blockchain front-running with minimal overheads*, in: *International Conference on Security and Privacy in Communication Systems*, Springer, 2022, pp. 250–271.
- [122] M. Castro, B. Liskov, *Practical byzantine fault tolerance and proactive recovery*, ACM Transactions on Computer Systems (TOCS) 20 (4) (2002) 398–461.
- [123] V. Buterin, D. Hernandez, T. Kamphofner, K. Pham, Z. Qiao, D. Ryan, J. Sin, Y. Wang, Y. X. Zhang, *Combining GHOST and Casper* (May 2020). arXiv:2003.03052, doi:10.48550/arXiv.2003.03052.
- [124] L. Heimbach, L. Kiffer, C. Ferreira Torres, R. Wattenhofer, *Ethereum's Proposer-Builder Separation: Promises and Realities*, in: *Proceedings of the 2023 ACM on Internet Measurement Conference, IMC '23*, Association for Computing Machinery, New York, NY, USA, 2023, pp. 406–420. doi:10.1145/3618257.3624824.
- [125] A. Yaish, K. Qin, L. Zhou, A. Zohar, A. Gervais, *Speculative Denial-of-Service Attacks in Ethereum* (2023).
URL <https://eprint.iacr.org/2023/956>
- [126] G. Wood, et al., *Ethereum: A secure decentralised generalised transaction ledger*, Ethereum project yellow paper 151 (2014) (2014) 1–32.
- [127] M. I. Alnajjar, M. S. Kiraz, A. Al-Bayatti, S. Kardas, *Mitigating MEV Attacks with a Two-Tiered Architecture Utilizing Verifiable Decryption* (2023).
URL <https://www.researchsquare.com/article/rs-3311434/v1>
- [128] M. Pai, M. Resnick, *Structural advantages for integrated builders in mev-boost*, in: *International Conference on Financial Cryptography and Data Security*, Springer, 2024, pp. 128–132.
- [129] E. Kokoris-Kogias, E. C. Alp, L. Gasser, P. Jovanovic, E. Syta, B. Ford, *CALYPSO: Private data management for decentralized ledgers*, *Proceedings of the VLDB Endowment* 14 (4) (2020) 586–599. doi:10.14778/3436905.3436917.
- [130] L. Zhou, K. Qin, A. Gervais, *A2MM: Mitigating Frontrunning, Transaction Reordering and Consensus Instability in Decentralized Exchanges* (Jun. 2021). arXiv:2106.07371, doi:10.48550/arXiv.2106.07371.
- [131] H. Adams, E. Williams, W. Pote, Z. Yang, N. Zinsmeister, X. Wan, A. Lin, R. Campbell, D. Robinson, M. Toda, M. Leibowitz, E. Zhong, A. Karys, *Uniswapx*, Tech. rep., Uniswap Labs (jul 2023).
URL <https://app.uniswap.org/whitepaper-uniswapx.pdf>
- [132] A. Bukov, S. Kunz, M. Melnik, G. Alekseev, M. Snow, X. Shape, *linch fusion+: Intent-based atomic cross-chain swaps*, Tech. rep., linch Network (sep 2024).
URL https://linch.com/assets/linch_fusion+_atomic_swaps_september_12_2024.pdf
- [133] A. S. Yin, *An introduction to intents and intent-centric architectures* (sep 2023).
URL <https://anoma.net/blog/an-introduction-to-intents-and-intent-centric-architectures>
- [134] Y. Mo, J. Chen, Y. Wang, Z. Zheng, *Toward automated detecting unanticipated price feed in smart contract*, in: *Proceedings of the 32nd ACM SIGSOFT International Symposium on Software Testing and Analysis*, 2023, pp. 1257–1268.
- [135] L. Breidenbach, C. Cachin, B. Chan, A. Coventry, S. Ellis, A. Juels, F. Koushanfar, A. Miller, B. Magauran, D. Moroz, et al., *Chainlink 2.0: Next steps in the evolution of decentralized oracle networks*, *Chainlink Labs 1* (2021) 1–136.
- [136] C. McMenamin, V. Daza, *Dynamic, Private, Anonymous, Collateralizable Commitments vs. MEV* (2023). arXiv:2301.12818.
- [137] K. Qin, J. Ernstberger, L. Zhou, P. Jovanovic, A. Gervais, *Mitigating Decentralized Finance Liquidations with Reversible Call Options* (Mar. 2023). arXiv:2303.15162, doi:10.48550/arXiv.2303.15162.
- [138] M. Capiński, E. Kopp, *The Black-Scholes Model*, Cambridge University Press, 2012.
- [139] R. Gan, L. Wang, X. Lin, *Why Trick Me: The Honeypot Traps on Decentralized Exchanges*, in: *Proceedings of the 2023 Workshop on Decentralized Finance and Security, DeFi '23*, Association for Computing Machinery, New York, NY, USA, 2023, pp. 17–23. doi:10.1145/3605768.3623546.
- [140] G. Ali, A. Samuel, S. P. Kabiito, Z. Morish, A. Thomas, W. Robert, A. Denis, M. Sallam, M. M. Mijwil, J. Ayad, et al., *Integration of artificial intelligence, blockchain, and quantum cryptography for securing the industrial internet of things (iiot): Recent advancements and future trends*, *Applied Data Science and Analysis* 2025 (2025) 19–82.
- [141] K. Babel, L. Baker, *Strategic Peer Selection Using Transaction Value and Latency*, in: *Proceedings of the 2022 ACM CCS Workshop on Decentralized Finance and Security, DeFi'22*, Association for Computing Machinery, New York, NY, USA, 2022, pp. 9–14. doi:10.1145/3560832.3563440.
- [142] G. Angeris, T. Chitra, T. Diamandis, K. Kulkarni, *The Specter (and Spectra) of Miner Extractable Value* (Oct. 2023). arXiv:2310.07865, doi:10.48550/arXiv.2310.07865.
- [143] A. Judmayer, N. Stifter, P. Schindler, E. Weippl, *Estimating (miner) extractable value is hard, let's go shopping!*, in: *International Conference on Financial Cryptography and Data Security*, Springer, 2022, pp. 74–92.
- [144] C. Jin, T. Wang, Z. Wang, L. Shi, S. Zhang, *First-Price Sealed-Bid Auction for Ethereum Gas Auction Under Flashbots*, in:

- 2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom), 2023, pp. 449–457. doi:10.1109/MetaCom57706.2023.00085.
- [145] M. Bartoletti, R. Zunino, A theoretical basis for Blockchain Extractable Value (May 2023). [arXiv:2302.02154](#), doi:10.48550/arXiv.2302.02154.
- [146] B. Mazonra, N. Della Penna, Towards Optimal Prior-Free Permissionless Rebate Mechanisms, with applications to Automated Market Makers & Combinatorial Orderflow Auctions (Jun. 2023). [arXiv:2306.17024](#), doi:10.48550/arXiv.2306.17024.
- [147] K. Kulkarni, T. Diamandis, T. Chitra, Towards a Theory of Maximal Extractable Value I: Constant Function Market Makers (Apr. 2023). [arXiv:2207.11835](#), doi:10.48550/arXiv.2207.11835.
- [148] C. Hughes, Reducing Disorder: An Information-Theory Formulation of MEV (Nov. 2023). [arXiv:2311.05367](#), doi:10.48550/arXiv.2311.05367.
- [149] M. Bartoletti, R. Marchesin, R. Zunino, DeFi composability as MEV non-interference (Sep. 2023). [arXiv:2309.10781](#), doi:10.48550/arXiv.2309.10781.
- [150] E. Winter, The shapley value, Handbook of game theory with economic applications 3 (2002) 2025–2054.
- [151] E. Lehrer, An axiomatization of the banzhaf value, International Journal of Game Theory 17 (1988) 89–99.
- [152] C. F. Torres, R. Camino, et al., Frontrunner jones and the raiders of the dark forest: An empirical study of frontrunning on the ethereum blockchain, in: 30th USENIX Security Symposium (USENIX Security 21), 2021, pp. 1343–1359.
- [153] B. Weintraub, C. F. Torres, C. Nita-Rotaru, R. State, A flash(bot) in the pan: Measuring maximal extractable value in private pools, in: Proceedings of the 22nd ACM Internet Measurement Conference, IMC '22, Association for Computing Machinery, New York, NY, USA, 2022, pp. 458–471. doi:10.1145/3517745.3561448.
- [154] Julien Piet and Jaiden Fairuze and Nicholas Weaver, Extracting Godl [sic] from the Salt Mines: Ethereum Miners Extracting Value, in: 21st Annual Workshop on the Economics of Information Security, WEIS 2022, Tulsa, USA, 21–22 June, 2022, 2022, pp. 1–20.
- [155] Z. Li, J. Li, Z. He, X. Luo, T. Wang, X. Ni, W. Yang, X. Chen, T. Chen, Demystifying DeFi MEV Activities in Flashbots Bundle, in: Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, CCS '23, Association for Computing Machinery, New York, NY, USA, 2023, pp. 165–179. doi:10.1145/3576915.3616590.
- [156] A. Bagourd, L. G. Francois, Quantifying MEV On Layer 2 Networks (Aug. 2023). [arXiv:2309.00629](#), doi:10.48550/arXiv.2309.00629.
- [157] C. Raun, B. Estermann, L. Zhou, K. Qin, R. Wattenhofer, A. Gervais, Y. Wang, Leveraging Machine Learning for Bidding Strategies in Miner Extractable Value (MEV) Auctions (2023). URL <https://eprint.iacr.org/2023/1281>
- [158] B. Öz, B. Kraner, N. Vallarano, B. S. Kruger, F. Matthes, C. J. Tessone, Time Moves Faster When There is Nothing You Anticipate: The Role of Time in MEV Rewards (Jul. 2023). [arXiv:2307.05814](#), doi:10.48550/arXiv.2307.05814.
- [159] F. Carrillo, E. Hu, MEV in fixed gas price blockchains: Terra Classic as a case of study (Mar. 2023). [arXiv:2303.04242](#), doi:10.48550/arXiv.2303.04242.
- [160] Z. Zhang, Z. Lin, M. Morales, X. Zhang, K. Zhang, Your exploit is mine: instantly synthesizing counterattack smart contract, in: 32nd USENIX Security Symposium (USENIX Security 23), 2023, pp. 1757–1774.
- [161] L. Ankile, M. X. Ferreira, D. Parkes, I see you! robust measurement of adversarial behavior, in: Multi-Agent Security Workshop@ NeurIPS'23, 2023, pp. 1–20.
- [162] A. Yaish, M. Dotan, K. Qin, A. Zohar, A. Gervais, Suboptimality in defi, Cryptology ePrint Archive (2023).
- [163] D. Grandjean, L. Heimbach, R. Wattenhofer, Ethereum Proof-of-Stake Consensus Layer: Participation and Decentralization (Sep. 2023). [arXiv:2306.10777](#), doi:10.48550/arXiv.2306.10777.
- [164] G. Palaiokrassas, S. Scherrers, I. Ofeidis, L. Tassioulas, Leveraging machine learning for multichain defi fraud detection, in: 2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), IEEE, 2024, pp. 678–680.
- [165] T. Niedermayer, P. Saggese, B. Haslhofer, Detecting financial bots on the ethereum blockchain, in: Companion Proceedings of the ACM on Web Conference 2024, 2024, pp. 1742–1751.
- [166] S. Ren, T. Tu, J. Liu, D. Wu, K. Ren, Lookahead: Preventing defi attacks via unveiling adversarial contracts, arXiv preprint arXiv:2401.07261 (2024).
- [167] Z. Yao, F. Huang, Y. Li, W. Duan, P. Qian, N. Yang, W. Susilo, Mecon: A gnn-based graph classification framework for mev activity detection, Expert Systems with Applications 269 (2025) 126486.
- [168] J. A. Berg, R. Fritsch, L. Heimbach, R. Wattenhofer, An Empirical Study of Market Inefficiencies in Uniswap and SushiSwap, in: Financial Cryptography and Data Security. FC 2022 International Workshops, Lecture Notes in Computer Science, Springer International Publishing, Cham, 2023, pp. 238–249. doi:10.1007/978-3-031-32415-4_16.
- [169] E. Rabeinejad, A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Generative adversarial networks for cyber threat hunting in ethereum blockchain, Distributed Ledger Technologies: Research and Practice 2 (2) (2023) 1–19.
- [170] A. Song, E. Seo, H. Kim, Anomaly VAE-Transformer: A Deep Learning Approach for Anomaly Detection in Decentralized Finance, IEEE Access 11 (2023) 98115–98131.
- [171] M. Gunathilaka, S. Wickramanayake, H. D. Bandara, Defitrust: A transformer-based framework for scam defi token detection using event logs and sentiment analysis, Expert Systems with Applications 251 (2024) 123913.
- [172] Z. Wu, J. Wu, H. Zhang, Z. Zheng, W. Wang, Hunting in the dark forest: A pre-trained model for on-chain attack transaction detection in web3, in: Proceedings of the ACM on Web Conference 2025, 2025, pp. 4519–4530.
- [173] J. Yu, X. Wu, H. Liu, W. Guo, X. Xing, Blockfound: Customized blockchain foundation model for anomaly detection, arXiv preprint arXiv:2410.04039 (2024).
- [174] K. Gogol, M. Schneider, C. Tessone, First-spammed, first-served: Mev extraction on fast-finality blockchains, arXiv preprint arXiv:2506.01462 (2025).
- [175] Lostin, Solana MEV report: Trends, insights, and challenges (jan 2025). URL <https://www.helius.dev/blog/solana-mev-report>
- [176] N. Gerzon, B. Weintraub, J. In, A. Mislove, C. Nita-Rotaru, Quantifying the threat of sandwiching mev on jito: A measurement of solana's leading validator client, in: Proceedings of the 2025 ACM Internet Measurement Conference, 2025, pp. 937–943.
- [177] D. Cunningham, Approaches to MEV: Ethereum vs. cosmos (jun 2021). URL <https://www.reverie.ooo/post/approaches-to-mev-ethereum-vs-cosmos>
- [178] Osmosis Labs, Protorev (2023). URL <https://docs.osmosis.zone/overview/features/protorev/>
- [179] Avalanche, Apricot phase four: Snowman++ and reduced c-chain transaction fees (aug 2021). URL <https://medium.com/avalancheavax/apricot-phase-four-snowman-and-reduced-c-chain-transaction-fees-1e1f67b42ecf>
- [180] TRON Foundation, Advanced decentralized blockchain platform (dec 2018). URL https://tron.network/static/doc/white_paper_v_2_0.pdf
- [181] B. Oz, D. Sui, T. Thiery, F. Matthes, Who wins ethereum block building auctions and why?, arXiv preprint arXiv:2407.13931 (2024).
- [182] Y. Gai, L. Zhou, K. Qin, D. Song, A. Gervais, Blockchain large

- language models, arXiv preprint arXiv:2304.12749 (2023).
- [183] J. Zhong, D. Wu, Y. Liu, M. Xie, Y. Liu, Y. Li, N. Liu, Defiscope: Detecting various defi price manipulations with llm reasoning, arXiv preprint arXiv:2502.11521 (2025).
- [184] B. Gao, Y. Wang, Q. Wei, Y. Liu, R. S. M. Goh, D. Lo, Airaclex: Automated detection of price oracle manipulations via llm-driven knowledge mining and prompt generation, arXiv preprint arXiv:2502.06348 (2025).
- [185] Y. Jin, C. Li, P. Fan, P. Liu, X. Li, C. Liu, W. Qiu, Llmbscv: An llm-based blockchain smart contract vulnerability management framework, arXiv preprint arXiv:2505.17416 (2025).
- [186] I. David, L. Zhou, D. Song, A. Gervais, K. Qin, Decompiling smart contracts with a large language model, arXiv preprint arXiv:2506.19624 (2025).
- [187] A. Gervais, L. Zhou, Ai agent smart contract exploit generation, arXiv preprint arXiv:2507.05558 (2025).
- [188] N. Songsom, J. Suaboot, W. Werapun, Fsa: A framework for analyzing secondary preimage attacks on merkle proof-based airdrops, Blockchain: Research and Applications (2025) 100368.
- [189] B. Luo, Z. Zhang, Q. Wang, A. Ke, S. Lu, B. He, Ai-powered fraud detection in decentralized finance: A project life cycle perspective, ACM Computing Surveys 57 (4) (2024) 1–38.
- [190] Y. Bar-On, Y. Mansour, Uniswap liquidity provision: An online learning approach, arXiv preprint arXiv:2302.00610 (2023).
- [191] A. Leivadeas, M. Falkner, A Survey on Intent-Based Networking, IEEE Communications Surveys & Tutorials 25 (1) (2023) 625–655. doi:10.1109/COMST.2022.3215919.
- [192] D. Alsagheer, L. Xu, W. Shi, Decentralized Machine Learning Governance: Overview, Opportunities, and Challenges, IEEE Access 11 (2023) 96718–96732. doi:10.1109/ACCESS.2023.3311713.
- [193] M. M. Karim, S. Khan, D. H. Van, X. Liu, C. Wang, Q. Qu, Transforming data annotation with ai agents: A review of architectures, reasoning, applications, and impact, Future Internet 17 (8) (2025) 353.
- [194] S. U. Hamida, M. J. M. Chowdhury, N. R. Chakraborty, K. Biswas, S. K. Sami, Exploring the landscape of explainable artificial intelligence (xai): A systematic review of techniques and applications, Big Data and Cognitive Computing 8 (11) (2024) 149.
- [195] W. Cai, Z. Liu, M. Zhang, C. Wang, Cooperative artificial intelligence for underwater robotic swarm, Robotics and Autonomous Systems 164 (2023) 104410.
- [196] X. Sun, D. Crapis, M. Stephenson, B. Monnot, T. Thiery, J. Passerat-Palmbach, Cooperative AI via Decentralized Commitment Devices (Nov. 2023). arXiv:2311.07815, doi:10.48550/arXiv.2311.07815.
- [197] A. Torreno, E. Onaindia, A. Komenda, M. Štolba, Cooperative multi-agent planning: A survey, ACM Computing Surveys (CSUR) 50 (6) (2017) 1–32.
- [198] N. Bitansky, R. Canetti, A. Chiesa, S. Goldwasser, H. Lin, A. Rubinfeld, E. Tromer, The hunting of the snark, Journal of Cryptology 30 (4) (2017) 989–1066.
- [199] G. B. Mensah, M. M. Mijwil, M. Abotaleb, S. M. Tawfeek, G. Ali, K. Dhoska, I. Adamopoulos, The era of ai: The impact of artificial intelligence (ai) and machine learning (ml) on financial stability in the banking sector, EDRAAK (2024) 43–48.
- [200] Z. Durante, Q. Huang, N. Wake, R. Gong, J. S. Park, B. Sarkar, R. Taori, Y. Noda, D. Terzopoulos, Y. Choi, et al., Agent ai: Surveying the horizons of multimodal interaction, arXiv preprint arXiv:2401.03568 (2024).
- [201] M. M. Karim, D. H. Van, S. Khan, Q. Qu, Y. Kholodov, Ai agents meet blockchain: A survey on secure and scalable collaboration for multi-agents., Future Internet 17 (2) (2025).
- [202] Y. Li, B. Luo, Q. Wang, N. Chen, X. Liu, B. He, Cryptotrade: A reflective llm-based agent to guide zero-shot cryptocurrency trading, in: Proceedings of the 2024 Conference on Empirical Methods in Natural Language Processing, 2024, pp. 1094–1106.
- [203] K. Saurabh, N. Rani, P. Upadhyay, Towards novel blockchain decentralised autonomous organisation (dao) led corporate governance framework, Technological Forecasting and Social Change 204 (2024) 123417.
- [204] H. H. Ekal, S. N. Abdul-Wahab, Defi governance and decision-making on blockchain, Mesopotamian Journal of Computer Science 2022 (2022) 10–17.
- [205] A. Vadlamani, The (questionable) legality of" maximal extractable value": A securities law perspective, Journal of Law, Technology, and Policy (2024) 85.
- [206] Y. Ji, J. Grimmelmann, Regulatory implications of mev mitigations, in: International Conference on Financial Cryptography and Data Security, Springer, 2024, pp. 335–363.
- [207] A. Wahrstatter, J. Ernstberger, A. Yaish, L. Zhou, K. Qin, T. Tsuchiya, S. Steinhorst, D. Svetinovic, N. Christin, M. Barczentewicz, et al., Blockchain censorship, in: Proceedings of the ACM Web Conference 2024, 2024, pp. 1632–1643.
- [208] N. S. Uzougbo, C. G. Ikegwu, A. O. Adewusi, International enforcement of cryptocurrency laws: Jurisdictional challenges and collaborative solutions, Magna Scientia Advanced Research and Reviews 11 (01) (2024) 068–083.
- [209] X. Xiong, J. Luo, Global trends in cryptocurrency regulation: An overview, in: The International Conference on Mathematical Research for Blockchain Economy, Springer, 2024, pp. 71–92.
- [210] European Securities and Markets Authority, Guidelines on supervisory practices for competent authorities to prevent and detect market abuse under the markets in crypto-assets regulation, accessed: 2025-08-16 (2025). URL https://www.esma.europa.eu/sites/default/files/2025-04/ESMA75-453128700-1408_Final_Report_MiCA_Guidelines_on_prevention_and_detection_of_market_abuse.pdf
- [211] Financial Stability Board, Policy recommendations for decentralized finance (defi), accessed: 2025-08-16 (2023). URL <https://www.fsb.org/2023/12/policy-recommendations-for-decentralized-finance-defi/>
- [212] Y.-P. Yang, When jurisdiction rules meet blockchain: Can the old bottle contain the new wine?, Stan. J. Blockchain L. & Pol'y 6 (2023) 137.
- [213] H. M. Salih, A. M. Mahmood, et al., A electric vehicle blockchain: Problems and opportunities, Babylonian Journal of Networking 2024 (2024) 18–24.
- [214] B. Guidi, A. Michienzi, Linking mev attacks to further maximise attackers' gains: evidence from the ethereum blockchain, Blockchain: Research and Applications (2025) 100340.