1 July 2025
ESMA50-481369926-29744

ESMA TRV Risk Analysis

Financial Innovation

Maximal Extractable Value
Implications for crypto markets

ESMA Report on Trends, Risks and Vulnerabilities Risk Analysis

ISBN 978-92-95235-13-7, DOI 10.2856/328752, EK-05-24-123-EN-N

European Securities and Markets Authority (ESMA)
Economics, Financial Stability and Risk Department
201-203 rue de Bercy
75012 Paris
FRANCE
risk.analysis@esma.europa.eu
ESMA – 201-203 rue de Bercy – CS 80910 – 75589 Paris Cedex 12 – France – www.esma.europa.eu

Financial Innovation

Maximal Extractable Value Implications for crypto markets

Contact: anne.chone@esma.europa.eu [1]

Summary

Maximal Extractable Value (MEV) commonly refers to the maximum amount of value a blockchain miner, validator or another agent, can make by changing the order of transactions within a block. ESMA started to look at MEV in the context of its contribution to the European Commission's report on recent developments in crypto-assets provided under Article 142 of the Markets in Crypto-Assets (MiCA) regulation. [2] This article leverages on this work to explore further the implications of MEV for Decentralised Finance (DeFi) users, protocols and the wider crypto system. The article is intended to advance a shared understanding of MEV and the concerns it raises, also with a view to inform possible future EU regulatory and supervisory discussions on the topic, while noting the need for more analysis grounded on robust evidence to comprehend the phenomenon more fully.

In summary, the article finds that MEV appears to be widespread on Ethereum and growing on some other chains, although available MEV data are sparse and come with important limitations. MEV is exclusive to blockchain systems and originates from the decentralized structure of blockchains. MEV can help addressing some of the inefficiencies found in DeFi protocols. Yet, it creates detriment to DeFi users to the extent that profits accrued to MEV extractors come in deduction to the wealth of users. It raises serious transparency concerns, because it is often not disclosed. In addition, MEV may go against the principles of fairness and integrity that underpin orderly markets in traditional finance. MEV counter-measures deployed so far fail to address these problems. More novel counter-measures look interesting but are still subject to ongoing research. There is an urgent need for crypto developers and researchers to develop relevant adequate solutions to address the negative consequences of MEV to support trust in DeFi and crypto markets.

[1] This article was written by Anne Chone and Max Diaz I Canals.

[2] See ESMA and EBA (2025).

Introduction

MEV as a concept is complex, as it requires a deep understanding of blockchain mechanics, the interactions between blockchain agents and the strategies used for MEV extraction. MEV is exclusive to blockchain systems and originates from the decentralized structure of blockchains, where transactions are not processed in a single, unified queue. This is in contrast with traditional financial markets, where central authorities enforce a fixed transaction order, often based on a first-come, first-served principle. Blockchain agents, such as block builders, proposers and validators, take advantage of the absence of a single queue to rearrange transactions in a way that maximizes profit for them. MEV extraction strategies effectively take many shapes, e.g., front-running or arbitrage, and evolve constantly, as blockchains and DeFi protocols innovate and new counter-measures are being introduced.

Scoping MEV and its outcomes is extremely challenging due to the technicalities involved and the frequent absence of a clear differentiation between 'mainstream' and MEV-related transactions. MEV has also received relatively limited regulatory and supervisory attention so far, as an issue that is mostly associated to DeFi, a small segment of crypto markets. In the EU, MiCA is not intended to directly address DeFi. Yet, MEV can have important consequences not only for DeFi but also the wider crypto system because of the links between the two and therefore warrants consideration.

This article is intended to advance a common understanding of MEV and the concerns it raises. It highlights the pressing need for crypto developers and firms to develop effective solutions to counter those forms of MEV that may be harmful. The article starts with (i) an introduction to MEV, from its origins to its main drivers and types; continues with (ii) the analysis of the scope of the phenomenon and (iii) the assessment of its consequences, notably for DeFi users and crypto markets integrity; touches briefly on (iv) regulatory considerations; before (v) concluding remarks.

What is MEV?

Definition and early development

Maximal Extractable Value is commonly defined as the value that blockchain agents, e.g., block builders, proposers or validators - called miners in Proof of Work (PoW) networks - can extract from a blockchain by using their ability to change the order, insert or censor transactions within a block.[3] The term was originally coined by Daian et al. (2020) as '*miner extractable value'*. It later evolved into '*maximal extractable value'* as a concept that applies not only to miners in PoW blockchains but also to validators and other agents in Proof of Stake (PoS) blockchains.

In essence, MEV is rooted in the absence of constraints on the precise ordering of transactions within a block in most blockchains. This is mainly due to the fact that it is virtually impossible in a decentralised system to ensure a precise enough and non-manipulable timestamp of transactions. Decentralisation means that there is **no pipeline creating a single queue** and no natural time-based ordering of transactions like in traditional finance. Blockchain agents therefore have latitude in the way they order transactions within a block. In addition, pending transactions in blockchains are visible in public pools or 'waiting rooms' called 'mempools'[4] This transparency means that blockchain agents can see and analyse transactions before they are included in a block and in turn strategically reorder them in a way that maximizes profit for them.

MEV has existed since the advent of blockchains. The ability of miners to use their priviliged position in transaction inclusion to extract profit was discussed as early as 2013. However, the issue did not garner much attention until **DeFi** protocols, including decentralised exchanges (DEXs), **started to gain traction** from 2018. MEV subsequently developed in two main phases. The first phase, in the months following the seminal paper on MEV by Daian et al. (2020),

[3] Gramlich et al. (2024) provide a useful overview of the different definitions of MEV in the current literature. Examples of transactions on blockchains include the transfer of crypto-asset A from user X to Y or the swap of crypto-asset A for B by user X. For further details on the role of block builders, proposers and validators on Ethereum, see box 1.

[4] The mempool, for memory pool, acts like a waiting room where unprocessed transactions are stored. On Ethereum, every node has its own mempool. The default mempool is public and accessible to everyone. However, there are private mempools too, like Flashbots Protect of Merkle Private Pool, which make transactions visible to specific validators only, thereby introducing a layer of confidentiality.

saw the boom of arbitrage bots competing for lucrative MEV opportunities. The second phase was marked by the deployment of MEV-Geth and its successor MEV-Boost from Flashbots, as a widespread MEV counter-measure introducing a separation between block proposers and builders on Ethereum.[5] We are now entering a new phase where a variety of novel counter-measures, including so-called Trusted Execution Environments (TEEs), are being actively explored as we discuss below.[6]

MEV drivers and agents

MEV is generated by **users** based on where, when and how they transact on blockchains. But the MEV extracted depends on the way in which blockchain agents re-order, insert or censor transactions within blocks.

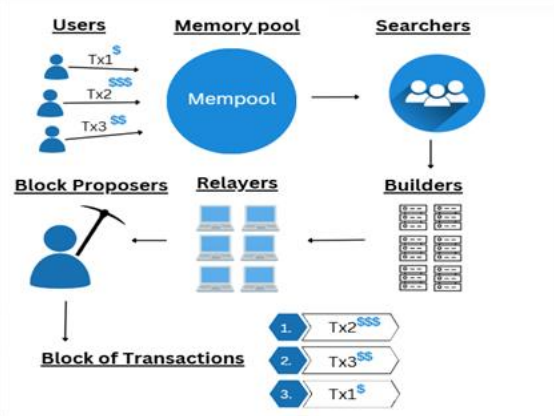
Blockchain agents act rationnally, which implies that there needs to be incentives, namely value to capture, for them to reorganise transactions. This explains why MEV is limited on the Bitcoin blockchain, which mainly supports 'basic' value transfers and prevalent on Ethereum and other chains that facilitate the deployment of smart contracts and sophisticated DeFi protocols. The growth of DeFi was effectively a key enabler of MEV. The development of automated market-making (AMMs) DEXs in particular introduced new possibilities for MEV extraction.[7]

Any blockchain agent with transaction ordering rights in the block-building process can in principle extract MEV. On Ethereum, **block proposers** have the direct authority to re-order, insert or delete transactions within the block they create and are therefore well-placed to extract MEV. Block proposers are a subset of **validators** who are specifically chosen to propose a new block at each slot.[8]

In practice, because of the level of complexity involved, block proposers rely on specialised **MEV searchers**. These searchers, sometimes just an individual, use sophisticated algorithms and bots to scan the mempool, identify MEV opportunities, and propose MEV strategies (what transactions to include and in which order) to the block proposers. Searchers often pay most of their MEV revenues (up to 90 % or even more) to proposers due to high competition.

Flashbots' MEV-Geth and its successor MEV-Boost, introduced two new agents in the Ethereum transaction chain, namely **block-builders and relays**.[9] In short, with MEV-Boost, proposers relinquish control over the contents of a block to block builders. The relays act as a communication layer between block builders and proposers (Box 1). The use of MEV-Boost is optional but currently widespread on Ethereum.[10]

Box 1 – Blockchain agents and the MEV-Boost supply chain



Note: Ethereum MEV-Boost supply chain.
Sources: Chainlink, ESMA.

(i) **Users** can submit their transactions publicly or through Flashbots' private transaction pool; (ii) **Searchers** compete to find the most profitable ordering of transactions, sequence them into bundles and bid for their inclusion in the next block using Flashbots' sealed-bid auction; (iii) **block builders** use the bundles received from the searchers to construct the most profitable block. Using MEV-Boost middleware, they then send an 'execution payload header' (i.e., a cryptographic commitment to the block's contents and total value) to validators via a relay for signing; (iv) **Relays** maintain the privacy of a block's contents until a validator commits to proposing it for inclusion in the network; (v) **Block proposers** communicate with relays to get the most profitable block header, which they attest to it by signing with their public key.

[5] Flashbots was formed in 2020 by Alexandre Obadia, Philip Daian and Stephane Gosselin as a non-profit organization with the objective to 'mitigate the negative externalities posed by MEV to stateful blockchains, starting with Ethereum'. It is effectively an MEV research and software developer. For further details on Flashbots' MEV-Boost system, see the section 'MEV counter-measures'.

[6] The concept of TEEs is not new and refers to a dedicated, secure area within a processor that guarantees the protection of sensitive data. In blockchains, TEEs provide a protected space where sensitive data and code (e.g., private keys and smart contracts) can operate without fear of tampering or observation from the outside world. For further details on TEEs, see CoinMarketCap (2025).

[7] For more background on DEXs and their design, see ESMA (2023).

[8] For further details on the role of proposers and validators in Ethereum's PoS, see Ethereum (2024).

[9] For further details on MEV-Boost, see Flashbots (2022).

[10] Heimbach et al (2023) estimate that the share of blocks built with MEV-Boost on Ethereum has varied between 85% and 95% since November 2022.

MEV types

Exploring the various types of MEV is useful to better understand their implications and the challenges involved in measuring them. A first approach distinguishes three main categories of MEV from the strategy used: (i) arbitrage, (ii) front-running and sandwich attacks, and (iii) liquidations.

Arbitrage MEV involves taking advantage of price discrepancies across exchanges, namely DEXs (on-chain arbitrage) or a mix of DEXs and CEXs (off-chain arbitrage). In short, arbitragers profit from purchasing one asset on the exchange offering the lower price and selling it on the exchange offering the higher price. In doing so, they contribute to closing the price gap between the two exchanges, while earning a profit.

Front-running MEV is a strategy where a validator or another blockchain agent place their own transaction ahead of a target transaction. The front-runner can send the same transaction as the target transaction with a higher fee, causing theirs to be processed first ('displacement' attack). Another type of front-running involves flooding the network with high-fee transactions, thereby preventing the execution from the target transaction ('suppression attack'). The latter is expensive though as a large amount of blockspace has to be used to reach the block capacity limit.

Sandwich attacks (sometimes also known as insertion attacks) are another variant of front-running. In the case of a sandwich attack, the exploiter places two transactions, one before the target transaction and one after. The front-running transaction manipulates the price in the attackers' interest. The back-running transaction reaps the profit of the manipulation. There are two main scenarios for a sandwich attack on DEXs, namely 'liquidity taker vs taker' attacks [11] and 'liquidity provider vs taker' attacks[12].

Liquidations consist in exploiting liquidations on DeFi lending protocols. The strategy involves identifying a borrower that is close to being liquidated, typically because the collateral value falls below a certain threshold. The attacker then sends a transaction to repay the borrowed position ahead of the liquidation taking place. In return they receive an amount of collateral larger than the amount repaid. The liquidation fee that users have to pay in case of liquidation also accrues to them.

This first categorisation is interesting to the extent that it draws parallels with traditional finance. For example, arbitrage is widespread in traditional financial markets where it contributes to price discovery and efficient markets. Front running on the contray is considered unlawful, because it exploits non-public information and violates the duty of financial intermediaries to act in the best interests of their clients, which undermines market integrity and fairness.

Another way to look at MEV is to consider the **type and source of information** necessary for the extraction. For example, Frontier Research (2023) split MEV into 'EV_ordering' and 'EV_signal'. EV_ordering stems from reordering, inserting, or removing transactions within a block. Information on the blockchain state and public mempools is sufficient to extract MEV. DEX arbitrage or on-chain sandwiching fall in this category. EV_signal, on the contrary, requires a piece of information (a signal) that is external to the blockchain, e.g., the price of an asset on a centralized exchange, or transactions in private mempools. CEX-DEX arbitrage is the most well-known form of EV_Signal. This distinction comes close to the notion of public versus private information, which is an important concept in traditional markets, for example to qualify insider trading.

Another interesting distinction is whether MEV involves some **execution risk** or not. Atomic MEV refers to a situation where one 'leg' only is necessary for the extraction to be successful, e.g., a sandwich attack where the front- and back-running transactions are included in the same bundle of transactions. Because the leg is reverted if unsuccessful, MEV extractors face no

[11] An example is when a user (a taker) wants to trade a large amount of crypto-asset A for another crypto-asset B. The attacker places a front-running transaction (a swap order of B in exchange for A with a higher fee) before the large transaction is executed. This causes the price of B to increase for the original trader. The attacker profits by selling B at an increased price in a back-running transaction.

[12] In this case the attacker (the liquidity provider) manipulates the price of B relative to A by removing liquidity from the pool prior to the original transaction of the user (the taker) being executed. The lower liquidity translates into more slippage and therefore higher costs for the user. The attacker then re-adds liquidity to restore the original pool balance and swaps asset B for A at a more lucrative price. A related concept is Just-in-Time Liquidity (JIT) which involves liquidity providers adding liquidity to a pool just before a trade and withdrawing it immediately after, often exploiting MEV opportunities.

execution risk in this case. Non-atomic MEV in contrast requires the completion of different 'legs', like in the case of CEX/DEX arbitrage. If one of the legs fails, e.g., due to competition with other extractors, the extractor may face a loss. In other words, the expectation of a profit is not risk-free, which in turn has implications for the risk profile of the extractor.

Finally, **on-chain MEV** distinguishes MEV extracted from on-chain transactions only from **off-chain MEV** that straddles on-chain and off-chain activities. Off-chain MEV is generally considered more complex and risky than on-chain MEV, as it involves multiple steps across different platforms. Off-chain MEV is also likely to have broader implications on the wider crypto market compared to on-chain MEV which primarily (but not exclusively) affect the blockchain it occurs on. Off-chain MEV is effectively a form of **cross-domain MEV**, a concept introduced by Obadia et al (2021), who define a domain as 'a self-contained system with a globally shared state'. Layer-1 and Layer-2 solutions, side-chains, and CEXs are all examples of domains.[13] Cross-chain MEV is another form of cross-domain MEV where MEV is extracted across several blockhains and not just one.

MEV is widespread but difficult to quantify

Measuring MEV is a challenge

Measuring MEV is inherently difficult for several reasons. First, measuring MEV requires the reconciliation of vast amounts of transactional data and other data, e.g., oracles prices, which span multiple mempools, protocols and chains, and may not even be public.[14] This is both technically complex and computationally intensive.

Second, the pseudonymity attached to blockchains complicates the analysis of the information. For example, identifying sandwich attacks when the front- and back-running transactions are initiated from distinct wallets by one or multiple colluding (pseudonymous) users necessitates the use of advanced heuristic techniques, also bearing in mind that these attacks become increasingly sophisticated.[15]

Finally, measuring MEV begs complex questions like where to draw the line between MEV and 'mainstream' trading activities in blockchains. For example, bidding higher fees may be interpreted as a user's intention to have orders executed rapidly but not necessarily to front-run others.

Current measurement methods fall into two broad categories. The first category intends to measure variations in agents' account balances to assess their MEV revenues. The second category focuses on identifying likely MEV-related transactions to then infer the revenues derived from them.

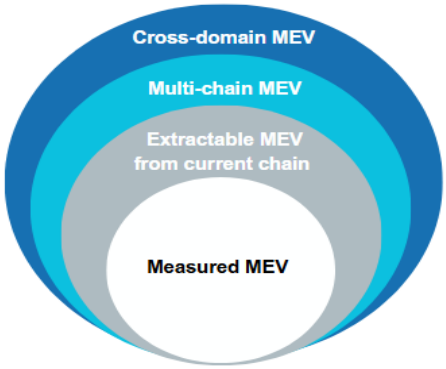
Available **MEV data are sparse**, mostly concern a single domain, namely Ethereum, which implies that they represent a fraction of the actual MEV (see Box 2) and come with important limitations, due to the challenges highlighted above. They need therefore to be considered with caution. Variations in the scoping definitions and measurement methods mean that data are often not comparable across sources. MEV techniques and counter-measures have also evolved through time, which limits the relevance of a historical data analysis. For what concerns Ethereum, the introduction of a separation between builders and proposers with MEV-Boost and the transition to a PoS consensus in September 2022, known colloquially as the 'Merge', significantly altered MEV schemes, hence the focus on post-Merge data in the following section.

[13] Layer-1 (L1s) serve as the base infrastructure on which DeFi protocols are built and operate. Examples of L1s are Ethereum, Binance Smart Chain (BSC), Polkadot, Avalanche, Cardano or Solana. Layer-2 (L2s) are secondary frameworks or protocols built on top of L1s to address scalability and efficiency issues. Examples of L2s include roll-ups, like Arbitrum, Optimism, zkSync, or Stark Net, state channels and side chains.

[14] Qin et al (2021) found that 32% of sandwich attacks were relayed to miners privately. Many of these attacks also involved transactions with more than 200 intermediate sub-transactions embedded within.

[15] On the growing sophisticatoin of the attacks, see for example: 'Jaredfromsubway.eth is back with a new MEV bot and new sandwich attacks', The Block, 20 August 2024.

Box 2 – Measured versus actual MEV



Note:Graphical comparison of different definitions for MEV.
Sources: ESMA, Galaxy Research.

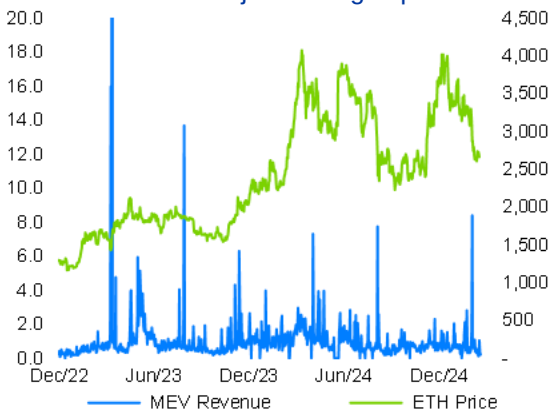
Sizeable MEV on Ethereum

Flashbots estimated the realised extractable value (REV) on Ethereum to 526,207 Ether in total between September 2022 and early June 2024[16], which is equivalent to around USD 1.1bn. This figure corresponds to the total value accrued to validators for the entirety of the blocks that they produce, bearing in mind that a portion only of the transactions in the blocks may qualify as MEV transactions. [17] Another MEV data specialist, EigenPhi, provides estimates for MEV revenues and MEV profits of USD 963mn and USD 417mn respectively for the period from December 2022 to January 2025 on Ethereum but little information is available on the methodology used to infer those figures.[18] Another source, Sorella Labs, estimated that since September 2022, total revenues from MEV on Ethereum totalled USD 1.26bn when including MEV from arbitrage between DEXs and CEXs but again details on the methodology and scope of analysis are lacking.

The above figures look relatively small when compared to the trading volumes. For instance, the above REV estimates from Flashbots represent approximately 0.12% of the volume traded on DEXs deployed on Ethereum over the same period.[19] However, these estimates are not necessarily reflective of the actual MEV revenues because of the important limitations highlighted above. Looking at the trading volumes and not only the revenues generated by MEV is useful to better understand the scope of the phenomenon. As an illustration, according to a post from EigenPhi, MEV seemingly generated almost half of the volumes of Ethereum's DEXs in 2022, namely USD 328bn out of a total of USD 666bn.[20]

MEV vary widely through time and operations. Available data show that MEV revenues tend to increase with valuation levels and are subject to sudden spikes at times of market stress when price volatility is high (Chart 1). For example, Silicon Valley bank's collapse, which caused a temporary de-peg of the USD Coin stablecoin, led to a boom in MEV revenues in March 2023 (+8,000% over three days compared to the baseline of the month). More recently, the market sell-off of August 2024 triggered a surge in MEV revenues (+700% over three days). The same happened again when Ether's price lost almost 20% in a few days in February 2025.

Chart 1
MEV revenues and daily Ether price
MEV revenues subject to large spikes



Note:Daily MEV revenues on Ethereum (USD mn) from arbitrage and sandwich attacks. Daily spot price of ETH cryptocurrency (USD, rhs).
Sources: Eikon, EigenPhi, ESMA.

A few MEV operations are significantly more lucrative than others, which increases

[16] See Flashbots Transparency Dashboard, last update as of 9 June 2024, Flashbots discontinued the dashboard after that date.

[17] More specifically, Flashbots estimates REV from the difference in the proposer balance before and after the block is proposed. The figure therefore includes not only the net MEV profits but also the tips and priority fees accrued to validators for the blocks they produce using MEV-Boost. Conversely, it does not include REV accrued to builders, searchers and other agents in the transaction lifecycle, although Flashbots estimates that validator retain the largest portion of the MEV revenues (more than 90%, up to 99% in certain cases).

[18] EigenPhi: MEV Daily Report data include arbitrage MEV and sandwich MEV, ESMA computations.

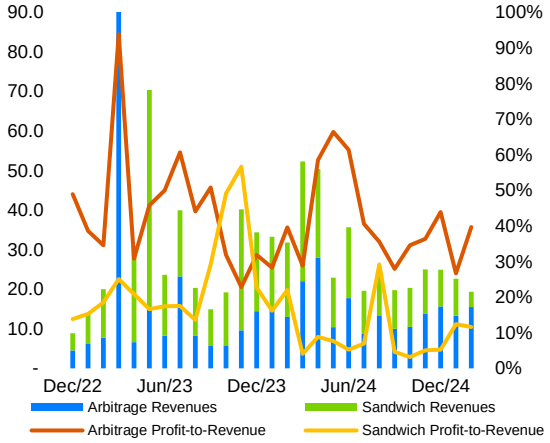
[19] According to DefiLlama data, the cumulative traded volumes on DEXs on Ethereum totalled around USD 930bn between mid-September 2022 and early June 2024.

[20] See https://x.com/EigenPhi/status/1630266577894375425

competition to capture them. Wahrstätter et al. (2023) found that 20% of MEV operations accounted for 72% of the total revenues between September 2022 and May 2023.

Looking at the different types of MEV, arbitrage MEV on average yielded higher revenues than sandwich MEV (USD 20.2mn versus USD 16.8mn per month) and at a lower cost, although with higher variations through time (Chart 2).

Chart 2
Revenues and profits by MEV type
Downward trend for sandwiching

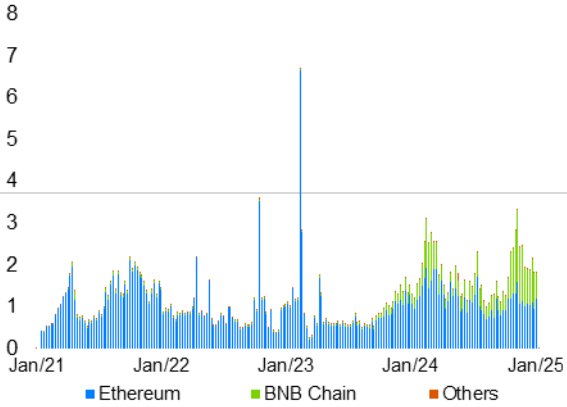


Note: Monthly revenues (USD mn) and profit-to-revenue ratios (in %, rhs) for arbitrage MEV and sandwiching MEV.
Sources: EigenPhi, ESMA.

Very limited data for other chains but MEV seemingly growing

Assessing MEV on other chains is even more challenging than for Ethereum, because of the extremely limited data available. Data pertaining to EVM-chains [21] from Dune, a crypto data provider, indicate that the volume of transactions from MEV sandwich bots is growing on the BNB Chain from Binance, while it is slightly receding on Ethereum (Chart 3). Several elements may contribute to this trend, including increasingly crowded MEV extraction and more sophisticated and in turn more difficult to detect MEV techniques on Ethereum, but also the growth of meme coins deployed on the BNB Chain. [22] Meme coins traders are targets of choice for MEV, because they typically set high price slippage tolerance for their transactions and the meme coins themselves are extremely volatile.

Chart 3
MEV sandwich bots volume across EVM chains
Sandwich transactions growing on BNB Chain



Note: Volume for single-block MEV sandwich bots (in USD bn) across a selection of protocols for selected EVM-compatible chains.
Sources: Dune, ESMA.

Non-EVM-chains are not exempt from MEV either. For example, a recent report highlighted that much of Solana's sandwiching originated from a private mempool operated by a single entity.[23] Over 30 days between 7 December 2024 and 5 January 2025, the program executed 1.55 million sandwich transactions for a profit of 65,880 SOL equivalent to USD 13.4mn. However, here again we lack relevant MEV data to really assess the scope of the phenomenon.

Layer-2 and cross-domain MEV largely unexplored so far

Layer-2[24] and cross-domain MEV[25] have received limited attention so far but require consideration, because of the growing popularity of Layer-2 solutions and concurrent chains to Ethereum. Ferreira Torres et al. (2024) found widespread MEV on the most popular rollups in the form of arbitrage and liquidations, with transactions volume comparable to Ethereum but with lower associated costs and significantly lower revenues. They did not identify instances of sandwiching on any of the roll-ups under consideration, which suggests that the sequencer

[21] EVM-chains are chains that use the Ethereum Virtual Machine (EVM) as their computation engine. Examples include the BNB chain from Binance, Avalanche and Arbitrum.

[22] For additional background as to why the BNB Chain is a hotspot for meme coins, see Bitget Wallet (2025).

[23] See Helius (2025).

[24] Ibid 13.

[25] Cross domain MEV refers to MEV extracted across several blockchain domains. Obadia et al (2021) define a domain as 'a self-contained system with a globally shared state'. Layer-1 and Layer-2 solutions, side-chains, and CEXs are all examples of domains.

behave as intended and do not sandwich users.[26] However, they highlighted the potential for cross-layer sandwich attacks. Oz et al. (2025) looking at two cross-chain arbitrage strategies across nine blockchains found that they generated a profit of USD 9.5mn from a total traded volume of USD 465mn over a year between September 2023 to August 2024, which is still fairly small but again requires consideration as it may evolve quickly.

Important negative externalities

MEV addresses some inefficiencies of DeFi protocols

Arbitrage MEV, like arbitrage in traditional markets, helps closing gaps in prices across trading venues, in this case across DEXs and between DEXs and CEXs, which should in principle contribute to reducing market fragmentation and enhancing market efficiency.

Most DEXs today operate as Automated Market Makers (AMMs).[27] A limitation that is inherent to AMMs' design in their current stage of development is the capacity of a large transaction to move the price of a trading pair in a given liquidity pool, which can in turn generate meaningful price differences with other liquidity pools and also centralised exchanges. Arbitrage contributes to closing these price differences and in turn enhancing market liquidity.

Similarly, liquidation MEV contributes to the efficiency of DeFi lending protocols by accelerating liquidations when they become necessary, which should in principle benefit users overall. Yet, these benefits come with important negative externalities.

MEV benefits extractors at the expense of ordinary users

Because MEV is a zero-sum game, profit accrued to MEV extractors is at the cost of another agent, which in most cases is the individual transacting with DeFi protocols. In short, MEV shifts wealth from ordinary users to MEV extractors, often without providing tangible benefits to the users and occurring without their awareness, as we discuss below. MEV generates millions in profits for MEV extractors, as discussed above. In some cases, when MEV is atomic, MEV extractors do not even bear any risks to generate those profits, which means that this is a free lunch for them.

MEV inflates trading volumes and exacerbates competition for block space. Extractors bid higher priority fees to have their transactions included in the next block, which often translates into higher execution costs for ordinary users. This happened in 2021 when MEV extraction ballooned with the development of arbitrage bots and priority gas auctions. The high trading volumes can also create congestion and latency issues in the execution of transactions, which again can be detrimental to ordinary users.

Important market integrity issues

As an introductory remark, it is important to highlight that this section is not intended to provide a comprehensive assessment of the implications of MEV for the orderly functioning of crypto markets, as this would require an in-depth analysis based on robust evidence. Rather it provides a preliminary overview of the key risks that MEV poses from a market integrity perspective.

Discussions around harmful forms of MEV often revolve around the distinction between (i) arbitrage (and liquidations) MEV, often considered benign as it helps promote market efficiency; and (ii) front-running MEV considered toxic, in the same way as front running in traditional markets where it typically qualifies as unlawful. Yet, we believe that a more granular and encompassing approach to those forms of MEV that are harmful is necessary, considering the specificities of blockchains. As a first approach, we believe that a focus on information and power asymetries is useful to identify detrimental MEV. Information and power asymetries undermine transparency and fairness, two core principles that underpin market integrity.

[26] Each rollup has its own ordering mechanism, a service called a sequencer. In most cases, this is a centralized server operated by the rollup developer following a first-come, first-served strategy.

[27] Ibid 7.

Blockchains are intended to be transparent and decentralised by design. However, some agents have an information advantage over users' transactions on Ethereum. Barczentewicz (2023) identifies at least three such groups, namely (i) operators of Ethereum nodes or private relays to which users submit their transactions; (ii) operators of Ethereum nodes used to query the blockchain; and (iii) operators of off-chain applications who facilitate the use of on-chain applications. These groups are in a privileged position to extract MEV because of an earlier or better information on pending or intended users' transactions. The argument sometimes used that the traditional concept of front-running is nullified in blockchains because the transactions are public is flawed in that respect. In addition, some agents have a power advantage on users transactions, which they can also use at their advantage for MEV extraction. For example, block proposers in Ethereum have a (temporary) monopoly of transaction selection and ordering for the block they submit.[28]

Because the lifecycle of transactions on blockchains is technically complex, many users may not understand the risk and cost implications for them fully. Users may not be aware of the existence of a public mempool that exposes their transactions to the view of others and facilitate front-running attacks. There is also potential for conflicts of interest situations. Some service providers, e.g., private relays, wallet providers or off-chain applications, may establish privileged relationships with certain agents and channel their users' transactions to those agents in exchange for a fee, without the users necessarily knowing. More generally, the implied costs of MEV are typically unknown to users, which goes against the principle of transparency. The very limited available data to scope the phenomenon as highlighted above is another illustration of the lack of transparency that prevails.

These information and power assymetries have the potential to distort price discovery mechanisms, and exacerbate price volatility for crypto-assets in times of stress.

All the above combined could create serious distrust towards DeFi protocols and crypto markets more widely, because of the interconnections between the two. A classic example is the issue of price formation on DEXs, which may be affected by MEV activities, and in turn spill over on price formation on CEXs. The rising share of DEXs relative to CEXs in crypto-asset trading volumes exacerbates this issue.

MEV threatens blockchain security

MEV has the potential to act as a force for centralisation, which is at odds with the value proposition of blockchain technology. MEV techniques have become increasingly sophisticated and resources intensive. This favours big players in a self-reinforcing mechanism, whereby the largest extractors are able to re-invest more resources into MEV strategies, crowding out smaller players. This could ultimately raise censorhip issues and undermine the network security, e.g., in case validation power concentrates in the hands of a few players. A dominant validator could decide to delay or block the execution of certain transactions or several validators may collude to manipulate the blockchain's consensus.

Another risk to the security of the network stems from the incentives that MEV creates for validators to re-write the history of blocks, undermining blockchain integrity. Daian et al. (2020) for example argue that if the available MEV exceeds block rewards, validators would have an interest in reorganising previous blocks to extract past MEV in what is known as a 'time-bandit attack'.

MEV counter-measures

Mitigating the negative externalities of MEV is an ongoing and evolving research field for crypto developers and academics. A variety of tools and approaches are being explored but they all have limitations in their current state of development.

Flashbots' MEV-Boost appears as the most widely used MEV counter-measure on Ethereum today, with a usage ratio of 85% to 95% for the produced blocks. MEV-Boost is the closest instantiation of the proposer-builder-separation (PBS) framework proposed by the Ethereum Foundation. PBS introduces a mechanism to decouple block-proposing from block-building, mainly with a view to address network security and centralisation issues.[29] PBS achieves these

[28] For more on this, see for example Schwarz-Schilling et al., (2023); Bonneau et al. (2015). In the case of MEV-Boost the power asymetry shifts from proposers to builders.

[29] As mentioned by Buterin (2021), "Instead of the block proposer trying to produce a revenue-maximizing block by

objectives in two ways: (i) time bandit attacks are less likely because validators are not directly focused on optimising MEV; (ii) centralisation risk is reduced at validators' level because even smaller validators can accrue MEV revenues.

An important difference between PBS and MEV-Boost is the need for a trusted relay with MEV-Boost, because it is not enshrined in the Ethereum protocol. Ultimately, the intention is to have PBS enshrired in the Ethereum protocol, namely e-PBS. However, e-PBS remains a distant prospect at this point, as it would require changes to the fork choice rule on the consensus layer and involves several critical research and design questions. Meanwhile, one of the main observed drawbacks of MEV-Boost is the centralisation that it introduces at the relays and block builders levels. [30] Centralisation raises censorship but also operational risk issues. Capponi et al. (2024) also observe that PBS transforms incentives in the builder market towards generating and securing more MEV. This leads to an overall increase in the total MEV and in turn potentially greater harm to ordinary users.

Another category of MEV-measures aim at enforcing a **fair ordering** of transactions, with the primary objective to protect users. Some propose to re-introduce a time-based ordering, e.g., Kelkar et al. (2020) propose to preserve the ordering of transactions (or by default blocks) received by a sufficiently large fraction of honest nodes. Another method proposes that nodes maintain synchronised local clocks to confirm a common timestamp for all incoming transactions. Still other methods leverage on the concept of batch auctions, whereby all orders within a time interval are aggregated and receive the same price.

The second type, known as **blind ordering**, leverages on the idea that ordering should be independent on the contents of the transactions. Blind ordering typically involves a commit-and-reveal protocol, which receives user commitments (a request to include a transaction in a block) along with some metadata (e.g., the transaction fee). The commit-and-reveal function can be instantiated through a trusted layer such as time-lock encryption or a hardware-based 'trusted execution environment' (TEE). Once this step is achieved, validators determine an ordering based on the commitments, then the protocol opens the commitments, and the transactions are executed.

Blind ordering does not fully eliminate the risk of front-running, e.g., the leakage of metadata such as gas price or address may still be sufficient to run an attack, and is therefore considered weaker than time-based ordering. However, timed-based ordering can have negative externalities, e.g., co-location as it creates a speed race between users. Fair-ordering solutions can also introduce centralisation and raise latency issues depending on the exact framework used to order transactions. The same centralisation and latency challenges also arise when users choose to send their transactions to a private mempool to keep their transactions hidden from the public mempool.

Other MEV counter-measures, e.g., Flashbots' MEV-Share, aim at re-distributing MEV profits accured by extractors to users. Still others, e.g., the Protected Order Flow proposed by Babel et al. (2024), are designed to tackle the main root cause of MEV, namely the publicity of transactions, by enhancing privacy. Yet, these novel counter-measures have seen limited uptake at the moment or are still at an early stage of development.

Regulatory approach

Regulatory and supervisory attention to MEV has been relatively limited so far, mainly because DeFi is still very small in size. For example, MEV is not legally defined and there have been very few enforcement actions or litigations specifically targeted at MEV activities.

In the EU, the new Markets in Crypto Assets Regulation (MiCA), does not directly address DeFi and makes no explicit reference to MEV. However, MiCA provides for the obligation to report "any reasonable suspicion regarding an order or transaction, including any cancellation or

themselves, they rely on a market where outside actors that we call block-builders produce bundles consisting of complete block contents and a fee for the proposer, and the proposer chooses the bundle with the highest fee. The proposer's choice is reduced to picking the highest-fee bundle […]" .

[30] For example, while Wahrstatter et al. (2023) found that no builder held more than 20% of the market share between September 2022 and May 2023, in October 2024, two builders, namely Beaverbuild and Titan Builder, seemingly produced 88% of Ethereum blocks, see 'Two builders produce 88% of Ethereum blocks in October, raising concerns', Cointelegraph, 17 October 2024. For more recent data, see MEV-Boost Pics (2024).

modification thereof, and other aspects of the functioning of the distributed ledger technology such as the consensus mechanism."[31] In addition, under MiCA's proposed technical standards, entities subject to the regulation may need to detect and report instances of MEV through comprehensive "suspicious transaction or order reports" (STORs).

In the US, the recently launched crypto task force from the SEC was tasked with developing a clear and comprehensive regulatory framework for crypto-assets. Whether and how this framework might address MEV is unclear at this point. Of note, in May 2024, the US Department of Justice opened a first of its kind lawsuit allegedly involving facts pertaining to MEV (see textbox 1).

Textbox 1

Two brothers arrested for manipulating Flashbots private mempool

In May 2024, the US Department of Justice charged two brothers, Anton and James Peraire-Bueno, for wire fraud and conspiracy to commit wire fraud and money laundering. The DoJ accused the two brothers for 'tampering and manipulating the protocols relied upon by millions of Ethereum users' and 'exploiting the very integrity of the Ethereum blockchain'. The fraud allegedly yielded USD 25mn of gains to the two brothers within 12 seconds.

While the exact details of the fraud remain unknown at this point, a common understanding is that the two brothers exploited a vulnerability in a Flashbots' private mempool to gain access to the pending transactions bundles, break these bundles and extract MEV from their parts at their own benefit.

Ironically, because the original bundles were designed to extract MEV from users' transactions, the attack can be likened to a sandwich attack on a sandwich attack. This may effectively question the merits of the case, as it could unintentionally give a rub of respectability to a phenomenon that has many negative externalities as highlighted above. Indeed, the case does not incriminate the original MEV extractors but only those who tricked them to extract MEV at their own advantage.

It will therefore be interesting to see the outcomes of the trial which is set for October 2025.

In the UK, the Financial Conduct Authority in a 2024 research note highlighted that MEV is a multifaceted and evolving concept and that perspectives on whether MEV raises market manipulation concerns vary across the industry and academia. The note elaborated further that a fundamental understanding of the context, behaviours, incentives, and outcomes associated with MEV is helpful to determine whether some MEV types may constitute market abuse.

At international level, the International Organization of Securities Commissions ("IOSCO") in its 2023 Final Report with Policy Recommendations for Decentralized Finance (DeFi) recommended that regulators evaluate the ability for a 'Responsible Person'[32] to identify and disclose, and, to the extent practicable, manage and mitigate the impact of MEV strategies. The report further noted the potential for MEV-related conflicts of interest and the need to address them.

Conclusion

MEV is a widespread phenomenon in blockchains. Some MEV can contribute to address some inefficiencies found in DeFi protocols. However, MEV often comes with important negative outcomes for users and market integrity that need to be addressed and warrant regulatory and supervisory attention. A variety of counter-measures are currently being explored by crypto researchers and developers but the topic remains an area of ongoing research because of the many challenges involved. Effective MEV counter-measures should consider as the priority the protection of DeFi users and crypto-assets market integrity, while providing the right incentives to maintain the efficiency of blockchains.

[31] 2024 ESMA Final Report, Draft technical standards specifying certain requirements in relation to the detection and prevention of market abuse under MiCA.

[32] Responsible person(s) is meant broadly, to encompass, for example, natural persons, groups of persons, entities and organizations, whether formally or informally constituted. There may be more than one Responsible person for any particular DeFi product, service, or activity. These Responsible Person(s) include those exercising control or sufficient influence over a financial product offered, financial service provided, or financial activity engaged in (or over products, services, and activities that behave like, or have been substituted by investors for, financial products, services, and activities) by the DeFi arrangement.

Glossary

This Glossary applies to this article only. It uses technical, non-legal definitions.

Automated Market Maker (AMM) DEX: A type of Decentralised Exchange (DEX) that utilizes liquidity pools and determines prices by mathematical formulas based on the ratio of the crypto-assets in the pools.

Blockchain: A form of distributed ledger in which details of transactions are held in the ledger in the form of blocks of information. A block of new information is appended to the chain of pre-existing blocks via a computerised process by which transactions are validated.

Crypto-asset: A digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology.

Decentralised Finance (DeFi): A set of alternative financial markets, products and systems that operate using crypto-assets and 'smart contracts' (software) built using distributed ledger or similar technology.

DeFi protocols: A specialised autonomous system of rules that creates a program designed to perform financial functions. Examples of DeFi protocols include Decentralised Exchanges (DEXs), which facilitate peer-to-peer trading using smart contracts.

Layer-1 (L1): The base layer or foundation of a blockchain on which DeFi protocols are built and operate. Examples of L1s are Ethereum, BNB Chain, Solana, Avalanche or Polkadot.

Layer-2 (L2): A secondary framework or protocol built on top of L1s to address scalability and efficiency issues. Examples of L2s include roll-ups, like Arbitrum, Optimism, zkSync, or Stark Net, state channels and side chains

Proof of Work (PoW) and Proof of Stake (PoS): Two distinct forms of consensus mechanism used for processing transactions and creating new blocks on a blockchain. Both are intended to incentivise good behaviour and make it difficult and expensive to act maliciously. In PoW systems, miners secure the blockchain network by solving complex computational puzzles, which is energy-intensive. PoS systems are secured by participants who stake an amount of crypto-assets on the network in order to activate their ability to create new blocks.

References

Babel, K., Jean-Louis, N., Ji, Y., Misra, U., Kelkar, M., Yapa Mudiyanselage, K., Miller, A. and Juels, A. (2024), 'PROF: Protected Order Flow in a Profit-Seeking World', *Cryptology ePrint Archive*, https://eprint.iacr.org/2024/1241.

Barczentewicz, M. (2023), 'MEV on Ethereum: A Policy Analysis', *ICLE White Paper*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4332703.

Bitget Wallet (2025), 'BNB Chain Meme Coins Are Surging! Here's Why & What to Watch', *Bitget Wallet Academy*, https://web3.bitget.com/en/academy/bnb-chain-meme-coins-are-surging-here-is-why-and-what-to-watch.

Bonneau, J., Miler, A., Clark, J., Narayanan, A., Kroll, J. and Felten, E. (2015), 'SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies', *Cryptology ePrint Archive,* https://eprint.iacr.org/2015/261.

Buterin, V. (2021), 'Proposer/block builder separation-friendly fee market designs', *EthResearch*, https://ethresear.ch/t/proposer-block-builder-separation-friendly-fee-market-designs/9725.

Capponi, A., Jia, R. and Wang, Y. (2024), 'MEV and Allocative Inefficiencies in Public Blockchains', https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3997796#paper-citations-widget.

Chen, E., Toberoff, A., Srinivasan, S. and Chiplunkar, A. (2023), 'A Tale of Two Arbitrages', *Frontier Research*, https://frontier.tech/a-tale-of-two-arbitrages.

CoinMarketCap (2025), 'Ethereum Community Debates TEE Technology: A Foundational Revolution in Blockchain Privacy and Security', https://coinmarketcap.com/academy/article/f9bc3622-977b-4d8f-b0ff-2ef964abd060.

Daian, P., Goldfelder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L. and Juels, A. (2020), 'Flash Boys 2.0: Frontrunning in decentralized exchanges, miner

extractable value, and consensus instability', in Kellenberger, P. (ed.), *IEEE Symposium on Security and Privacy (SP),* San Francisco, United States, pp. 910–927, https://ieeexplore.ieee.org/document/9152675.

EigenPhi (last update in 2024), Market Overview: MEV Scan Daily Report, https://eigenphi.io/mev/ethereum/dailyReport.

ESMA (European Securities and Markets Authority) and EBA (European Banking Authority) (2025), *Joint Report - Recent Developments in Crypto-Assets (Article 142 of MiCAR)*', https://www.esma.europa.eu/sites/default/files/2025-01/ESMA75-453128700-1391_Joint_Report_on_recent_developments_in_crypto-assets__Art_142_MiCA_.pdf.

ESMA (European Securities and Markets Authority) (2023), *TRV Risk Analysis - Decentralised Finance in the EU: developments and risks*, https://www.esma.europa.eu/sites/default/files/2023-10/ESMA50-2085271018-3349_TRV_Article_Decentralised_Finance_in_the_EU_Developments_and_Risks.pdf.

Ethereum (2024), 'Proof-of-stake (PoS)', *Ethereum Developers*, https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/.

Ethereum (2024), 'Proposer-builder Separation', *Ethereum Roadmap,* https://ethereum.org/en/roadmap/pbs/.

Ferreira Torres, C., Mamuti, A., Weintraub, B., Nita-Rotaru, C. and Shinde, S. (2024), 'Rolling in the Shadows: Analyzing the Extraction of MEV Across Layer-2 Rollups', *arXiv preprint,* https://arxiv.org/abs/2405.00138.

Financial Conduct Authority (2024), 'Research Note – Review of Maximal Extractable Value & Blockchain Oracles'*, FCA research notes in financial regulation,* https://www.fca.org.uk/publication/research-notes/research-note-review-and-maximal-extractable-value-blockchain-oracles.pdf.

Flashbots (2022), 'Flashbots Builders', *Flashbots Docs,* https://docs.flashbots.net/.

Flashbots (last update in 2024), *Flashbots Transparency Dashboard,* https://transparency.flashbots.net/.

Galaxy (2023). 'Distribution of MEV Surplus', *Galaxy Insights Research*, https://www.galaxy.com/insights/perspectives/distribution-of-mev-surplus/.

Gramlich, V., Jelito, D. and Sedlmeir, J. (2024), 'Maximal extractable value: Current understanding, categorization, and open research questions', *Electronic Markets,* volume 34, article number 49, https://link.springer.com/article/10.1007/s12525-024-00727-x.

Helius (2025), 'Solana MEV Report: Trends, insights, and Challenges', *Helius Research*, https://www.helius.dev/blog/solana-mev-report.

Heimbach, L., Kiffer, L., Ferreira Torres, C. and Wattenhofer, R. (2023), 'Ethereum's Proposer-Builder Separation: Promises and Realities'*, arXiv preprint,* https://arxiv.org/pdf/2305.19037.

IOSCO (2023), *Final Report with Policy Recommendations for Decentralized Finance (DeFi)*, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD754.pdf.

Kelkar, M., Zhang, F., Goldfeder, S. and Juels, A. (2020), 'Order-Fairness for Byzantine Consensus'*, Cryptology ePrint Archive*, https://eprint.iacr.org/2020/269.pdf.

MEV-Boost Pics (2024), *MEV-Boost Dashboard,* https://mevboost.pics/.

Obadia, A., Salles A., Sankar L., Chitra T., Vaibhav C. and Daian P. (2021), 'Unity is Strength: A Formalization of Cross-Domain Maximal Extractable Value', *arXiv Preprint*, https://arxiv.org/abs/2112.01472.

Öz, B., Ferreira Torres, C., Gebele, J., Rezabek, F., Mazorra, B. and Matthes, F. (2025), 'Pandora's Box: Cross-Chain Arbitrages in the Realm of Blockchain Interoperability', https://arxiv.org/abs/2501.17335.

Qin, K., Zhou, L. and Gervais, A. (2021), 'Quantifying Blockchain Extractable

Value: How dark is the forest?', *arXiv preprint, https://arxiv.org/pdf/2101.05511*.

Schwarz-Schilling, C., Saleh, F., Thiery, T., Pan, J., Shah, N. and Monnot, B. (2023), 'Time is Money: Strategic Timing Games in Proof-of-Stake Protocols', *arXiv preprint,* https://arxiv.org/abs/2305.09032*.*

Sorella Labs (last update in 2024), 'MEV over time', *Sorella Labs Dashboard,* https://sorellalabs.xyz/dashboard.

Wahrstätter, A., Zhou, L., Qin, K., Svetinovic, D. and Gervais, A. (2023), 'Time to Bribe: Measuring Block Construction Market', *arXiv preprint*, https://arxiv.org/pdf/2305.16468.

Publications Office
of the European Union