Quaderni FinTech

Maximal extractable value as blockchain market microstructure:

Architectures, transaction handling, and strategy taxonomy

D.M. Di Nosse, A. Russo

20

novembre 2026

CONSOB
COMMISSIONE NAZIONALE
PER LE SOCIETÀ E LA BORSA

Nella collana dei Quaderni ***FinTech***

sono raccolti lavori di ricerca relativi

al fenomeno «FinTech» nei suoi molteplici aspetti

al fine di promuovere la riflessione e

stimolare il dibattito su temi attinenti

all'economia e alla regolamentazione

del sistema finanziario.

Comitato editoriale
Paola Deriu (responsabile)
Federico Picco (coordinatore)
Valeria Caivano
Daniela Costa

Segreteria di Redazione
Eugenia Della Libera

CONSOB

00198 Roma – Via G.B. Martini, 3
t +39.06.84771 centralino
f +39.06.8477612

20121 Milano - Via Broletto, 7
t +39.02.724201 centralino
f +39.02.89010696

h www.consob.it
e studi_analisi@consob.it

Tutti i diritti riservati. È consentita la riproduzione a fini didattici e non commerciali, a condizione che venga citata la fonte.

Il valore estraibile nei mercati delle cripto-attività:

Infrastrutture, gestione delle operazioni e strategie di negoziazione

D.M. Di Nosse, A. Russo *

Sintesi del lavoro

Nei mercati delle cripto-attività, il prezzo ottenuto da chi acquista o vende può dipendere anche dall'ordine con cui le operazioni vengono eseguite. Prima di essere registrata definitivamente su una blockchain, ossia un registro digitale condiviso, un'operazione attraversa diversi passaggi: viene trasmessa, può diventare visibile ad altri soggetti ed è inserita in una sequenza di esecuzione. Chi conosce in anticipo un'operazione o può influenzarne la posizione può sfruttare tale vantaggio per ottenere un guadagno. La letteratura indica questo fenomeno con l'espressione *Maximal Extractable Value*, traducibile come valore massimo estraibile. Il problema non riguarda soltanto il funzionamento della tecnologia, ma anche la qualità dell'esecuzione, la distribuzione dei guadagni e delle perdite e l'individuazione delle responsabilità.

Il lavoro esamina questi meccanismi mettendoli in relazione con problemi già noti nei mercati finanziari, quali le asimmetrie informative e il controllo sull'esecuzione degli ordini. Confronta diverse infrastrutture blockchain, tra cui Ethereum e Solana, e considera anche le operazioni che coinvolgono più reti. La domanda di fondo è la stessa per tutti i sistemi: chi può osservare un'operazione prima che sia eseguita, chi ne determina la posizione rispetto alle altre e quali informazioni consentono di ricostruire queste decisioni? Dal confronto emerge che limitare la visibilità pubblica delle operazioni non elimina necessariamente le opportunità di guadagno legate al loro ordinamento. Può invece trasferirle verso i soggetti che gestiscono i canali di accesso e l'organizzazione degli scambi.

Le conseguenze economiche dipendono dalla strategia adottata. Alcune operazioni di arbitraggio possono contribuire a riallineare i prezzi tra sedi di scambio diverse. Altre sfruttano un acquisto o una vendita di un utente, negoziando immediatamente prima e dopo

(*) Daniele Maria Di Nosse, Scuola Normale Superiore, Pisa (daniele.dinosse@sns.it);
Antonio Russo, CONSOB (a.russo@consob.it).

Le opinioni espresse nel lavoro sono attribuibili esclusivamente agli autori e non impegnano in alcun modo la responsabilità dell'Istituto. Errori e imprecisioni sono imputabili esclusivamente agli autori. Nel citare il presente lavoro, non è, pertanto, corretto attribuire le argomentazioni ivi espresse alla CONSOB o ai suoi Vertici.

di esso, e possono peggiorarne il prezzo di esecuzione. Un'ulteriore strategia consiste nel fornire, solo per il tempo necessario a una singola operazione, le cripto-attività utilizzate negli scambi, così da incassarne le commissioni. Questa attività può migliorare il prezzo ottenuto dall'utente, ma riduce la quota di commissioni destinata a chi mantiene stabilmente quelle risorse disponibili. Non tutte le forme di valore estraibile hanno quindi gli stessi effetti, né possono essere assimilate indistintamente a pratiche abusive.

Un'analisi delle operazioni osservate nel 2023 su uno specifico mercato di Uniswap, una piattaforma di scambio decentralizzata, affianca la ricostruzione dei meccanismi. Nel campione esaminato, le strategie differiscono per frequenza e distribuzione dei profitti: alcune producono molti guadagni contenuti, mentre altre sono meno frequenti ma associate a importi maggiori. I risultati hanno carattere descrittivo e riguardano le operazioni individuate con i criteri adottati, non l'intera attività potenzialmente riconducibile al fenomeno. I profitti sono inoltre misurati al lordo dei costi di esecuzione e dei pagamenti agli altri soggetti coinvolti; non rappresentano pertanto rendimenti netti effettivamente conseguiti.

Per la vigilanza, il punto centrale è che la trasparenza del registro finale non rende necessariamente trasparenti tutte le decisioni che precedono l'esecuzione. La registrazione pubblica consente di osservare le operazioni concluse, ma può non rivelare come siano state trasmesse, selezionate o ordinate. Occorre quindi considerare anche il ruolo degli intermediari e dei gestori delle infrastrutture attraverso cui gli utenti accedono agli scambi. Quando un intermediario regolamentato indirizza gli ordini dei clienti verso servizi decentralizzati, l'esposizione a questi meccanismi assume rilievo anche per la qualità dell'esecuzione e per le responsabilità nella relazione con il cliente. Il lavoro propone così di valutare i rischi non soltanto in base alla qualificazione di un sistema come centralizzato o decentralizzato, ma guardando a chi esercita concretamente il controllo sulle operazioni e alla possibilità di ricostruirne le scelte.

Maximal extractable value as blockchain market microstructure:

Architectures, transaction handling, and strategy taxonomy

D.M. Di Nosse, A. Russo *

Abstract

Maximal extractable value (MEV) arises when transaction inclusion, ordering, or execution can be used to capture surplus from pending or privately routed order flow. This paper treats MEV as a market-microstructure problem, not as a single Ethereum-specific anomaly. It compares transaction handling architectures across Ethereum, Solana, BNB Chain, rollups, and cross-chain execution, with attention to how each setting allocates visibility, sequencing authority, and accountability before settlement. It then organizes the main strategy families in the MEV literature, including arbitrage, sandwich attacks, just-in-time liquidity provision, and mixed JIT+sandwich bundles, and relates them to their closest traditional-market analogues. The central point is that MEV depends jointly on information asymmetry and ordering power: transparent state, programmable settlement, and concentrated sequencing rights make familiar microstructure motives executable in a distinct on-chain form.

(*) Daniele Maria Di Nosse, Scuola Normale Superiore, Pisa, Italy (daniele.dinosse@sns.it);
Antonio Russo, CONSOB, Rome, Italy (a.russo@consob.it).

The opinions expressed here are those of the authors and do not necessarily reflect those of CONSOB. Of course, the authors are the only responsible for errors and imprecisions.

Contents

Introduction **1**

1 Blockchain and Cryptoassets: A Primer for Non-Specialists **6**
1.1 From a ledger to a blockchain . . . 7
1.2 Cryptoassets, addresses, and wallets . . . 9
1.3 Smart contracts and decentralized finance . . . 10
1.4 How trading takes place on a decentralized exchange . . . 11
1.5 The path from a user instruction to settlement . . . 12

2 Blockchain Architectures and Transaction Handling **13**
2.1 Ethereum: Public Mempool, Private Order Flow, and PBS . . . 14
2.2 Solana: Leader Forwarding and Bundle Channels . . . 17
2.3 BNB Chain: Public Mempool with Restricted Builder Access . . . 19
2.4 Rollups: Private Sequencers and Explicit Ordering Auctions . . . 19
2.5 Cross-chain Execution: Fragmented Order Flow Across Domains . . . 20
2.6 DeFi compliance with European Regulation . . . 21

3 MEV strategies and traditional market analogues **22**
3.1 Flash loans as an execution primitive . . . 23
3.2 Back-running arbitrage . . . 24
3.3 Sandwich attacks . . . 24
3.4 Just-in-Time (JIT) liquidity . . . 25
3.5 Mixed JIT+sandwich bundles . . . 26
3.6 Empirical profit distributions . . . 27

4 Possible supervisory implications **30**

5 Conclusion **30**

References **33**

Glossary of on-chain terms **37**

Introduction

Cryptoassets are digital assets recorded and transferred through blockchain systems. Trading in these assets takes place through different types of venues.

The most common venues are centralized exchanges (CEXs), which are operated by a single organization and typically maintain customer accounts and internal trading systems. Alongside them, decentralized exchanges (DEXs) allow users to trade directly through blockchain-based software applications without relying on a conventional exchange operator.

More broadly, blockchain technology also supports decentralized finance (DeFi), a set of applications providing services such as trading, lending, derivatives, collateral management, and asset transfers.

Together, centralized exchanges, decentralized exchanges, wallets, lending protocols, and settlement infrastructures form a large and increasingly complex financial ecosystem.

Cryptoassets now form a large, multi-venue financial ecosystem, not a narrow experiment in peer-to-peer payments. Trading activity illustrates that scale. TokenInsight estimates total crypto exchange trading volume, including spot and derivatives across centralized and decentralized exchanges, at about USD 104.2 trillion in 2025, with quarterly volumes of USD 23.5 trillion, USD 22.6 trillion, USD 30.0 trillion, and USD 28.1 trillion from Q1 to Q4, respectively (TokenInsight Research, 2026). Centralized exchanges still dominated this activity, with an average 91.67% volume share, but decentralized exchanges accounted for an economically meaningful 8.33% share and briefly exceeded 25% during the late-2025 expansion of on-chain derivatives (TokenInsight Research, 2026) (Figure 1). CoinGecko reports a similar structural shift in spot markets: top spot DEX volumes doubled from USD 1.8 trillion in 2024 to USD 3.6 trillion in 2025, while the top spot DEX-to-CEX volume ratio rose from 10.3% to 19.3% (CoinGecko, 2026a) (Figure 2). The latest completed quarter indicates lower aggregate spot activity but a continuing DEX role: in the second quarter of 2026, total crypto market capitalization fell 12.6% (USD 304.8 billion) to USD 2.1 trillion, while the top ten spot CEXs recorded USD 1.95 trillion in trading volume and the top ten spot DEXs USD 408.9 billion, and the reported top-ten spot DEX-to-CEX volume ratio was 23.5% (CoinGecko, 2026b).

The crypto market is therefore best understood as a fragmented execution system spanning centralized exchanges, decentralized exchanges, derivatives venues, bridges, wallets, and blockchain settlement layers.

Figure 1: TokenInsight 2025 exchange-market measures.
Quarterly exchange volumes sum to USD 104.2 trillion; average venue shares remain CEX-dominated.

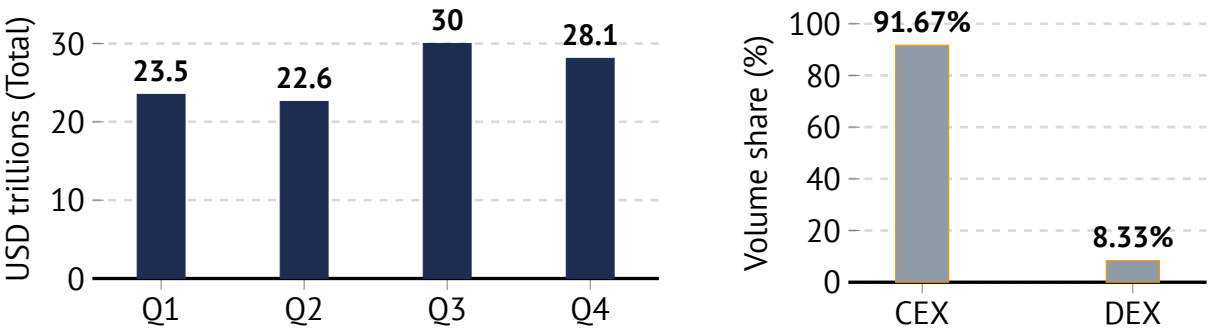
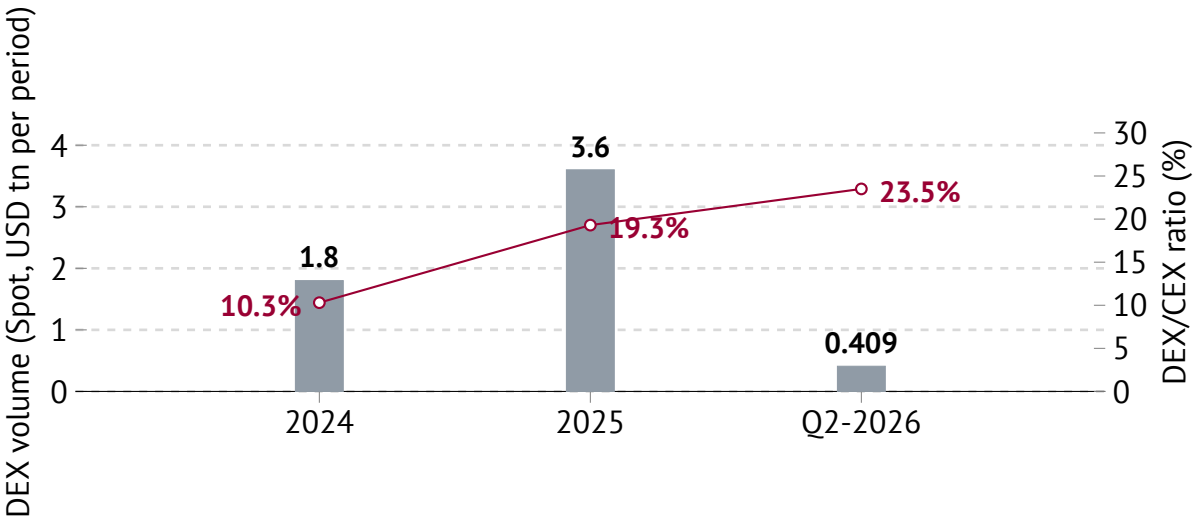


Figure 2: CoinGecko spot-DEX activity.
Annual top spot DEX volume doubled from USD 1.8 trillion in 2024 to USD 3.6 trillion in 2025, while the annual spot DEX-to-CEX volume ratio rose from 10.3% to 19.3%. In the second quarter of 2026, top spot DEX volume was USD 408.9 billion and the ratio was 23.5%. The quarterly total is shown separately and should not be compared directly with the annual totals.



The scale and fragmentation of this ecosystem make transaction handling economically consequential. Before a transaction reaches final settlement, different actors may receive, inspect, route, or order it. This raises the central question addressed in the paper: who controls transaction execution before settlement, and what value can be extracted from that control? Maximal Extractable Value (MEV) provides the analytical lens through which this question is examined.

One important segment of this ecosystem is DeFi. Broadly speaking, DeFi refers to financial services that operate through software running on blockchain infrastructure rather than through traditional financial intermediaries. These services include trading, lending, collateral management, derivatives, and asset transfers. Although the terminology may appear unfamiliar, many of the underlying economic functions are analogous to those already performed within traditional financial markets.

In DeFi, software applications execute predefined rules directly on the blockchain. Rather than relying on centralized operators to maintain ledgers, match trades, or administer contracts, many operational functions can be performed automatically through code.

Its scale has expanded rapidly. A commonly used measure of DeFi activity is total value locked (TVL): the US-dollar value, at a stated observation time, of cryptoassets deposited in protocol smart contracts, for example as trading liquidity, collateral, or staked assets. TVL is therefore a stock of deposited assets, not a measure of trading volume, protocol revenue, or user numbers. Although TVL is an imperfect size metric whose computation is not fully standardized, it remains a common first proxy for ecosystem scale (Saggese *et al.*, 2025). Werner et al. report that TVL grew from about USD 700 million two years before April 2022 to about USD 150 billion in April 2022, while Zhou et al. document a peak above USD 253 billion (Werner *et al.*, 2021; Zhou *et al.*, 2022). As a current reference, CoinGecko reports that multichain TVL fell from USD 91.8 billion at the start of April 2026 to USD 70.3 billion at the end of June; a later DefiLlama observation reports USD 88.2 billion on 15 September 2026. DefiLlama's all-chain historical series excludes liquid-staking and double-counted TVL, so these measures should not be treated as interchangeable (CoinGecko, 2026b; DefiLlama, 2026). The expansion also appears in protocol development and usage data: Saggese et al. study 939 Ethereum DeFi projects, and Chemaya et al. analyze more than 50 million Uniswap transactions across Ethereum, Optimism, Arbitrum, and Polygon (Saggese *et al.*, 2025; Chemaya *et al.*, 2023). Automated-market-maker DEXs have become one of the core infrastructures of this system (Xu *et al.*, 2021), and recent empirical work suggests that shocks to centralized-exchange trust can reallocate activity toward decentralized venues (Wu *et al.*, 2024). Institutional attention has grown in parallel. Recent surveys describe DeFi as relevant for retail and institutional users, including central banks; in a survey of 109 experts, 43% expected at least high DeFi adoption by 2034, with convergence between traditional finance and DeFi viewed as more likely than outright displacement (Gogol *et al.*, 2024; Liebau, 2024).

The growth of crypto trading and DeFi usage makes the mechanics of on-chain execution economically important.

Unlike many traditional market infrastructures, blockchain-based trading systems often process transactions sequentially according to an order that is determined shortly before execution and settlement. Because execution outcomes may depend on that ordering, the ability to observe pending transactions or influence their position in the sequence can itself become economically valuable.

Transaction ordering is therefore not merely a technical feature. It can directly affect trading outcomes, execution quality, and the distribution of gains and losses among market participants.

As more liquidity, users, protocols, and institutional actors rely on programmable settlement, the value of seeing transactions before they settle and influencing how they are ordered becomes a central market-design problem. Maximal Extractable Value (MEV) names this problem: it is the surplus that can be captured by controlling transaction inclusion, ordering, and selective execution in blockchain systems. The term was originally introduced as *Miner Extractable Value* (Daian *et al.*, 2020), but the logic extends beyond mining. Whenever pending transactions can be observed, delayed, bundled, rerouted, or privately sequenced, the right to decide execution becomes economically valuable.

The specific actors involved differ across blockchain architectures. Some receive transactions from users, some determine how transactions are ordered before execution, and others validate and record the resulting state changes. Regardless of the terminology used by a particular system, the underlying economic logic is the same. Blockchain trading is executed through discrete state transitions, and value can arise whenever certain participants have privileged visibility into pending transactions or privileged influence over their ordering before settlement.

MEV is therefore best understood as a market-microstructure phenomenon. As in traditional financial markets, asymmetries in information and execution can create economic advantages. In blockchain systems, those advantages often arise from the ability to observe transaction intent before settlement or to influence the sequence in which transactions are executed. For market supervision, this creates two linked asymmetries. The first is an *information asymmetry*: some actors may observe transaction intent before final settlement. The second is a *power asymmetry*: some actors may influence inclusion, ordering, bundling, or censorship before the state transition becomes final. This differs from the standard traditional-finance front-running case, where the problematic signal is often confidential client order flow. In DeFi, the signal may come from public mempool visibility, private RPC routing, builder access, sequencer visibility, oracle timing, or cross-domain routing. The concern is not only non-public information, but also privileged visibility and privileged sequencing rights (European Securities and Markets Authority, 2025).

This framing does not imply that all MEV is harmful. Some forms, such as arbitrage, can restore price consistency across venues and may improve welfare. Others, such as sandwich attacks, are redistributive and worsen user execution. Just-in-time (JIT) liquidity is more ambiguous: it can improve execution for the immediate trader while diverting fee income away from passive liquidity providers (Capponi *et al.*, 2023).

The architecture of the chain determines how this game is played. Public mempools, private relays, leader-forwarding systems, centralized sequencers, and cross-chain settlement routes expose transactions to different actors and allocate ordering rights in different ways. MEV should be studied as a feature of how blockchains handle transactions before final settlement: who sees the order first, who can reorder it, whether priority is auctioned explicitly, and where monitoring or sanctions can be applied.

Readers unfamiliar with blockchain systems need not have prior technical knowledge. The next section introduces the core concepts required for the remainder of the paper, including blockchains, cryptoassets, wallets, smart contracts, decentralized exchanges, and transaction processing. The subsequent sections then examine how different blockchain architectures allocate visibility and ordering power, and how those design choices shape the forms of MEV that arise.

While a growing literature documents individual MEV strategies, protocol designs, and mitigation mechanisms, much of the evidence remains organized around specific blockchains or specific forms of extractable value. The contribution of this paper is to provide a unified market-microstructure perspective. Rather than treating Ethereum, Solana, rollups, and cross-chain systems as separate cases, the paper analyzes them through two common dimensions: transaction visibility and sequencing power. This perspective not only helps explain the emergence of different MEV strategies, but also highlights where accountability, execution discretion, and supervisory attention are likely to concentrate along the transaction chain.

The paper proceeds as follows. Section 1 provides essential background on blockchains, cryptoassets, smart contracts, and decentralized trading. Section 2 compares transaction handling on Ethereum, Solana, BNB Chain, rollups, and cross-chain systems. Section 3 then presents the main MEV strategy families and relates them to their closest traditional-market analogues.

1 Blockchain and Cryptoassets: A Primer for Non-Specialists

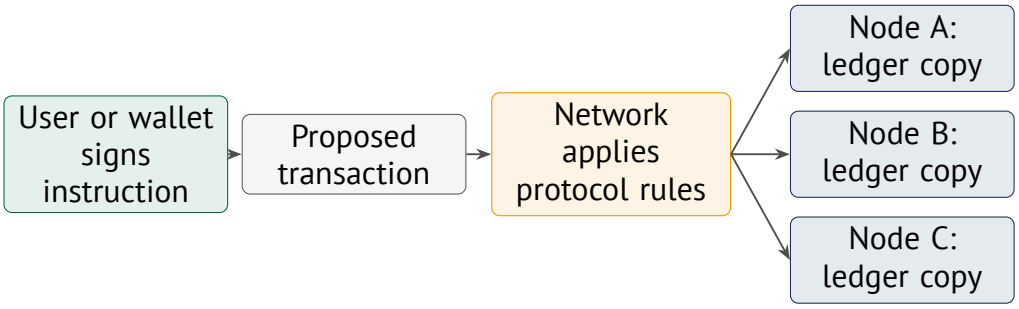
Readers already familiar with blockchain terminology may proceed directly to Section 2. This section is intended to provide a common conceptual background for readers approaching the topic from a market-regulation or supervisory perspective. Nonetheless, the definitions are not to be considered exhaustive.

This section provides the minimum conceptual background needed to follow the analysis. Readers familiar with traditional financial markets may find it helpful to think of a blockchain as a shared transaction register performing some of the record-keeping and settlement functions traditionally provided by institutions such as banks, central securities depositories, payment systems, or trading venues. The underlying economic functions are often familiar; what differs is the technological architecture through which they are performed. Importantly, a blockchain is not synonymous with cryptocurrency. A blockchain is the record-keeping infrastructure, whereas cryptocurrencies and other cryptoassets are applications built on top of that infrastructure. Unlike the ledger of a bank, broker, or central securities depository, its authoritative version is not maintained solely on one institution's database. Copies are held by multiple computers, called *nodes*, and a consensus protocol determines which updates are valid and in what order they become part of the accepted history. This arrangement changes the technical location of record-keeping and settlement; it does not, by itself, guarantee that a transaction is economically fair, legally compliant, or free from operational risk. Bitcoin was the first widely adopted application of this model for transferring a native digital asset. Ethereum and other programmable blockchains extend it by allowing general-purpose applications to modify the shared ledger according to rules expressed in code.

1.1 From a ledger to a blockchain

At any point in time, a blockchain represents a *state*: for example, the balances associated with addresses, the owner recorded for a token, and the data stored by applications. A transaction is a signed instruction that asks the network to change that state. It may transfer a cryptoasset, exchange one token for another, create a loan, or call a program deployed on the chain. Transactions are grouped into ordered batches called *blocks*. Each accepted block refers to the preceding one, producing the chronological chain from which the technology takes its name. Unlike most conventional databases, the order in which transactions are recorded can have direct economic consequences. In decentralized trading systems, changing transaction order may alter execution prices and redistribute value among participants. This feature becomes particularly important later when discussing Maximal Extractable Value (MEV).

Figure 3: A blockchain as a shared transaction register.
A signed instruction is checked under the protocol's rules and, when accepted, updates compatible copies of the ledger held by different nodes. Consensus determines technical validity and order; it does not establish the fairness of the trade or the truth of facts outside the chain.



The consensus mechanism selects or recognizes the participant entitled to propose the next block and allows the network to agree on the resulting history. Proof-of-work chains use computational competition among *miners*; proof-of-stake chains such as Ethereum rely on participants called *validators*, whose role is backed by assets committed to the protocol. Some high-throughput chains designate a scheduled validator as the next *leader*. A *rollup* is a secondary system, called layer 2, that executes transactions outside a base blockchain, usually Ethereum, and submits data or a proof back to it for settlement. In these cases, a *sequencer* may order transactions before submission. Mining is therefore only one possible method of block production, not a synonym for all blockchain operation. Consensus answers a technical question—which valid history the network accepts—rather than establishing the truth of an external fact. For example, consensus can confirm that a stablecoin transfer followed the program's rules; it cannot establish that the issuer holds the reserves it reports.

Once a transaction has sufficient confirmation or reaches the chain's specified finality condition, it is ordinarily treated as settled. The precise strength and timing of finality differ across systems. Earlier records are difficult to alter because doing so would require the network to replace an already accepted history. The common description of blockchains as "immutable" should therefore be understood as a strong technical resistance to unilateral modification, not as an absolute guarantee against software defects, governance interventions, compromised credentials, or exceptional chain reorganizations.

1.2 Cryptoassets, addresses, and wallets

A *cryptoasset* is a digitally represented asset whose creation, ownership, or transfer is recorded through this infrastructure. Some assets are native to a blockchain, such as ether on Ethereum. Others are *tokens* created by a smart contract. Tokens can serve different economic functions: they may be used for payment, provide access to a service, represent governance rights, track another asset, or seek to maintain a stable value. The fact that two instruments use the same token technology says little, by itself, about their legal classification, issuer obligations, or risk. In informal usage, "crypto" and "cryptocurrency" are often used for this ecosystem as a whole; *cryptoasset* is the broader term because not every token is designed to function as money.

Assets are associated on-chain with addresses, which can be thought of as publicly visible account identifiers. Users access and control those addresses through wallets. A wallet does not literally contain the assets. Instead, it stores or controls the cryptographic credentials needed to authorize transactions. The public key, or an address derived from it, can be shared in order to receive assets. The private key is the secret credential used to approve transactions. Control of that credential normally provides practical control over the associated assets. If it is lost, access may be irrecoverable; if it is stolen, an unauthorized transfer may nevertheless appear technically valid to the network. A useful analogy is online banking. Money is not stored inside the password used to access the account. Rather, the password allows the user to instruct the bank to perform certain actions. Similarly, a wallet stores or controls the credentials needed to authorize blockchain transactions, while the assets themselves remain recorded on the blockchain.

Custodial service providers hold or manage keys for clients, whereas self-hosted wallets leave this responsibility with the user.

Most public blockchains are *pseudonymous*, not necessarily anonymous. Transactions and addresses are publicly observable, but an address does not automatically disclose the natural or legal person controlling it. Attribution may require information held by trading platforms, wallet providers, other intermediaries, or investigative data providers. Conversely, once an address is reliably linked to a person, its historical activity may be unusually transparent.

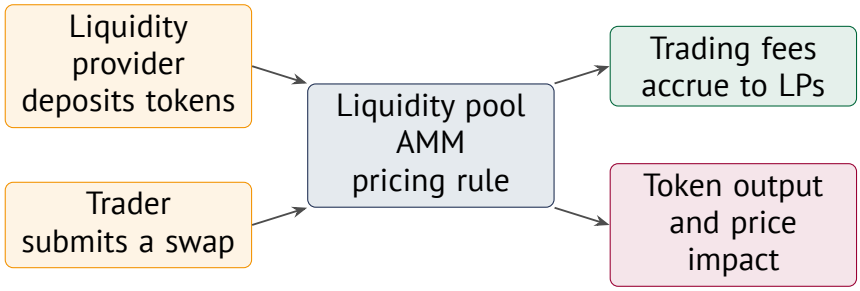
1.3 Smart contracts and decentralized finance

A *smart contract* is a program stored on a blockchain. When a transaction calls it, the network executes the same rules and records the resulting state change. The word "contract" can be misleading: it describes executable code and does not necessarily imply a legally enforceable agreement. Smart contracts can hold assets and combine several actions without a conventional back office. If any required step fails, an Ethereum-style transaction can *revert*, undoing its state changes, although the user may still incur a transaction fee. A vending machine offers a useful intuition. Once a customer inserts money and selects a product, the machine automatically verifies the relevant conditions, applies predefined rules, and determines the outcome without requiring a human operator. If the conditions are satisfied, the product is delivered; otherwise, the transaction fails. Smart contracts operate according to the same general principle. When invoked by a transaction, they automatically evaluate predetermined conditions and execute the corresponding actions. For example, a decentralized trading application may use a smart contract to verify available liquidity, calculate an execution price, transfer assets between users, and update the blockchain's shared record, all without the intervention of a centralized administrator.

Decentralized finance (DeFi) uses smart contracts to provide services such as trading, lending, collateral management, derivatives, and asset transfers. In functional terms, these services resemble familiar financial activities such as exchanging assets, granting credit, or managing collateral. The main difference is that many operational processes are executed through software directly on the blockchain rather than through centralized institutions and back-office systems. DeFi applications can interact with one another, so a single transaction may borrow funds, trade across several venues, repay the loan, and distribute the residual proceeds. This *composability* permits rapid innovation and can reduce some settlement and counterparty exposures when the programmed conditions work as intended. It also creates dependencies through which errors and incentives can propagate across protocols within one transaction.

"Decentralized" does not mean that every component is dispersed or that no identifiable intermediary exists. A protocol may depend on a concentrated development team, governance body, administrator key, website, wallet interface, price oracle, transaction router, bridge, or block-production service. These components may determine which users gain access, which information is observed before settlement, and how transactions reach the chain. The allocation of control must therefore be assessed function by function rather than inferred from a label.

Figure 4: AMM trade.
Liquidity providers supply the pool and earn fees; a trader swaps against it. The pool rule determines the output and price impact.



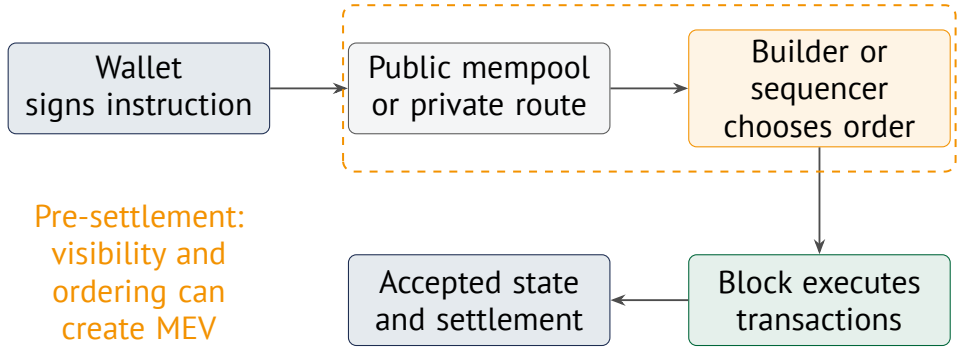
1.4 How trading takes place on a decentralized exchange

A decentralized exchange (DEX) performs a role broadly comparable to that of a trading venue. The key difference is that trading and settlement are typically executed through smart contracts rather than by a centralized operator. On a centralized exchange, the operator typically maintains client accounts and matches orders in an internal order book. Settlement on the blockchain, if any, may occur only when assets are deposited or withdrawn. A decentralized exchange (DEX), by contrast, executes trades through smart contracts and records the resulting transfers on-chain. Some DEXs use order books, but many important venues use an *automated market maker* (AMM).

An AMM can be thought of as a pool of assets that is permanently available for trading. Instead of matching buyers and sellers directly, users trade against the pool itself. An AMM replaces the conventional matching engine with one or more *liquidity pools*. A pool is a smart contract that holds quantities of two tokens. Liquidity providers deposit the tokens and receive a share of trading fees. A trader submits a *swap* to exchange one token for the other. The program calculates the amount received from the pool's current reserves and its pricing rule. A larger trade relative to available liquidity moves the pool price more and therefore has greater *price impact*. The difference between an expected quote and the eventual execution can also reflect intervening transactions; users normally set a slippage limit beyond which the swap must fail. A useful traditional-market analogy is a thinly traded security. A large order tends to move prices more when available liquidity is limited. AMMs exhibit a similar effect through their pricing formula.

AMM prices need not coincide continuously with prices on other pools or centralized exchanges. Arbitrageurs trade when a difference is large enough to cover fees and execution costs, and their transactions tend to bring prices back into alignment. This activity can improve price consistency, but it also illustrates a central feature of on-chain markets: every trade changes a shared state that the next transaction will encounter. Transaction order is consequently part of the economic outcome, not merely a technical detail.

Figure 5: Path from user instruction to settlement.
Before a block is accepted, a public or restricted route may expose the transaction and a builder or sequencer can select its position.



1.5 The path from a user instruction to settlement

In traditional financial markets, investors are often concerned with the price at which an order executes. In blockchain-based markets, execution price may depend not only on market conditions but also on the relative ordering of transactions waiting to be processed. As a result, the question of who sees a transaction first and who can influence its position in the execution queue can have direct economic consequences.

Consider a user who wishes to exchange one token for another on a DEX. First, the wallet constructs the transaction, including the target smart contract, the proposed input, the minimum acceptable output, and an offer to pay the required computational and priority fees, commonly described as *gas* on Ethereum. Second, the user signs the instruction. Third, the wallet submits it either to a public waiting area, commonly called a *mempool*, or through a restricted route operated by an RPC provider, router, relay, or sequencer. Submission is not yet execution.

Before settlement, a block producer or specialized builder selects transactions and chooses their order. The network then executes them sequentially. If an earlier transaction changes a pool's reserves, a later swap receives a different price even if the later user's signed instruction has not changed. When the block is accepted, the successful state changes become part of the shared ledger. The user can inspect the final transaction, but may not be able to observe every private message, rejected candidate block, routing decision, or commercial agreement that influenced its position.

This interval between submission and settlement is where MEV arises. Actors that can see a pending instruction may trade before or after it; actors that build or sequence blocks may sell priority, insert their own transactions, or choose among competing bundles. The closest traditional-market intuition is that knowledge of incoming order flow and control over queue position can have economic value. On-chain systems add two distinctive features: transactions can be simulated before inclusion, and multiple actions can succeed or fail as one atomic package.

For supervisory analysis, public ledger data are therefore necessary but not always sufficient. They provide a detailed record of transactions that settled, but do not automatically identify the controlling persons, reveal transactions that were withheld or rejected, or reconstruct decisions taken through private infrastructure. The practical questions are: who first received the instruction; who could inspect it; who determined inclusion and ordering; what fee, auction, or routing rule allocated priority; and which entity can be held accountable for the resulting execution.

The discussion in this chapter highlights three conditions that often co-exist in blockchain-based trading systems:

- Transactions may become visible before final settlement.
- Certain actors may influence whether and when those transactions are included.
- Transaction order can affect execution outcomes and economic value.

Whenever these three conditions are present simultaneously, opportunities emerge to extract value from transaction handling and ordering. The next section examines how different blockchain architectures allocate visibility and ordering power, and how those design choices shape the forms of MEV that arise.

2 Blockchain Architectures and Transaction Handling

The introduction framed MEV as a joint problem of visibility and sequencing power. This section makes that claim specific to each architecture. Four questions are especially useful: how users submit transactions, which actors can inspect them before settlement, who has authority to choose their relative ordering, and whether that ordering authority can be monitored or sold through an explicit auction. Table 1 summarizes the contrasts most relevant for this study.

Table 1: How transaction handling shapes MEV across major blockchain architectures.

Chain	Transaction handling before execution	Ordering architecture	Dominant MEV channel	Governance / accountability surface
Ethereum	Users can broadcast to the public mempool or send flow privately through order-flow auctions, relays, and builders.	Off-chain PBS via builders, relays, and proposers.	Sandwiching, back-running, JIT and builder capture of private order flow.	Builders, relays, validators, and private order-flow intermediaries.
Solana	Transactions are forwarded from RPC nodes to current and upcoming leaders; Jito adds private bundle routing.	Leader-based sequencing with validator-client extensions and block-engine routing.	Bundle arbitrage, tip auctions, and validator-mediated sandwiching.	Block-engine operators, validators, and stake-pool governance.
BNB Chain	Users can use a public EVM-style mempool or protected builder routes that bypass open competition.	PBS-style builder bidding to the in-turn validator through sentries.	Sandwiching, builder filtering, and protected routing.	Smaller validator set, builders, wallets, and coordinated ecosystem governance.
Rollups	Transactions are typically submitted to a private sequencer mempool and revealed publicly only after sequencing.	Centralized sequencers; Arbitrum adds an express-lane auction, Base adds Flashblocks.	Internalized arbitrage and ordering advantages; less classic public-mempool sandwiching.	Sequencers, auction operators, and chain governance.
Cross-chain	Execution is split across chains, bridges, and routers, often with inventory pre-positioned on several domains.	Multi-domain execution with no single global sequencer.	Inventory-based and bridge-based arbitrage across domains.	Bridges, routers, solvers, sequencers, and large arbitrageurs spanning multiple domains.

2.1 Ethereum: Public Mempool, Private Order Flow, and PBS

Ethereum remains the canonical reference point because a public gossip mempool now coexists with a large private-order-flow sector and a mature proposer–builder separation stack. In a study covering October 2023 to March 2024, MEV-Boost produced about 90% of Ethereum blocks and three builders produced about 80% of MEV-Boost blocks. In a separate study covering January 2023 to May 2024, private order flow accounted for 54.59% of block value (Öz *et al.*, 2024; Wang *et al.*, 2024). On Ethereum, the central issue is not only whether a swap is visible in the public mempool, but also who internalizes valuable order flow before block construction (Ethereum Foundation, 2024; Gupta *et al.*, 2023; Wang *et al.*, 2024).

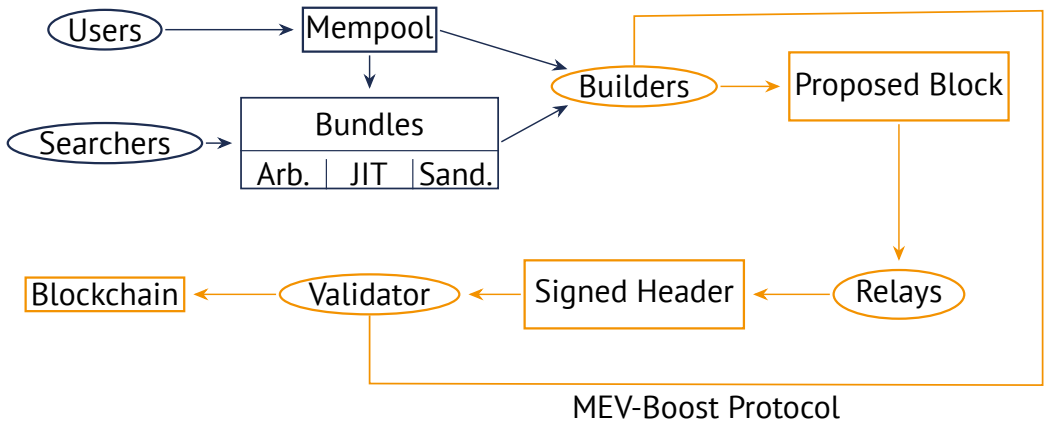
An Ethereum user transaction can follow two broad paths. If it is broadcast publicly, it propagates across nodes, sits in the mempool, and can be simulated by searchers before inclusion. If it is sent privately through a wallet router, an order-flow auction, or a relay, it may never become visible to the public mempool at all. In that case, builders internalize the opportunity and compete for it at the block level. In both cases, the transaction is ultimately embedded in a candidate block assembled off-chain and sold to the proposer selected by the consensus protocol.

In traditional electronic markets, orders are matched nearly continuously, and the main microstructure frictions are latency, queue position, and fragmentation across venues. On Ethereum, by contrast, transactions are executed in discrete blocks. After submission, a transaction propagates across nodes and may remain pending until a proposer includes it in a block. When order flow is public, a large swap can be simulated before execution, making the interval between submission and inclusion the natural arena in which MEV strategies are designed.

When competition is resolved in the public mempool, searchers bid for priority mainly through higher gas tips. This generates priority-gas auctions and raises execution costs for ordinary users.[1] Proposer–Builder Separation (PBS) was proposed to reduce these externalities and to mitigate incentives for validators to vertically integrate the block-building function (Buterin, 2021). PBS separates the *proposer* role, which belongs to the validator selected by the consensus protocol, from the *builder* role, which assembles a block and decides transaction ordering. Although PBS is currently implemented through third-party infrastructure, protocol-level designs remain an active research direction (Ethereum Foundation, 2024).

The most widely adopted implementation of PBS is Flashbots' MEV-Boost (Wahrstätter, Toni, 2025). Searchers submit bundles and bids to builders. Builders construct candidate blocks and send only block headers and payment offers to relays. Proposers then select the most profitable header, sign it, and receive the full payload only afterward. Figure 6 summarizes this workflow. Off-chain auctions reduce the need for public gas bidding, but they also create new bottlenecks and new points where failure or policy-driven filtering can affect execution (Marzec *et al.*, 2024; D'Amato *et al.*, 2023; Öz *et al.*, 2024).

Figure 6: PBS schema.



1 Under EIP-1559 the transaction fee is split into a base fee (burned) and a priority fee (paid to the block producer).

At the same time, a growing share of high-value order flow bypasses the public mempool altogether. Wallets, aggregators, and bots may submit transactions directly to builders through private RPC endpoints or order-flow auctions, creating *exclusive order flow* (EOF). This can protect the sender from mempool-based attacks, but it also changes the bargaining problem: the party with first access to the order may internalize part of the associated MEV or rebate some of it back to the user.[2]

In practice, the resulting market is concentrated. As a current point of reference, seven-day RelayScan snapshots show that only three builders can account for close to 90% of MEV-Boost blocks in a weekly window.[3] Off-chain auctions reduce public gas wars, but they also add layers of intermediation that matter for both competition and censorship risk.

For this paper, PBS matters because it turns MEV into an explicit market for inclusion and ordering. A searcher does not simply ask whether a strategy is profitable in gross terms. She asks how much of that gross profit can be passed on to the builder or proposer while still leaving a positive net return. To fix notation, we decompose the per-block profits of the three main actors as follows. Table 2 collects the corresponding symbols.

$$\textbf{Searcher:} \quad \pi_s = M - (C_{\text{gas}} + D_{\text{sb}} + C_{s,\text{infra}}), \tag{1}$$

$$\textbf{Builder:} \quad \pi_b = R - (1+\rho)B - R_{\text{refund}} - C_{b,\text{infra}}, \tag{2}$$

$$\textbf{Validator:} \quad \pi_v = B + R_{\text{consensus}} - C_{v,\text{infra}}. \tag{3}$$

$$R_{\text{refund}} = \varphi D_{\text{sb}}, \qquad 0 \le \varphi \le 1.$$

$$R = \sum_{\text{transactions}} C_{\text{gas}} + \sum_{\text{searchers}} D_{\text{sb}}.$$

From the perspective of the framework proposed in this paper, Ethereum combines broad transaction visibility in the public mempool with a competitive but increasingly intermediated market for sequencing rights. MEV opportunities therefore arise from both informational access and the commercial allocation of ordering authority through builders, relays, and private order-flow channels.

2 In some arrangements the builder is explicitly allowed to insert complementary transactions (for example, back-runs) around the private order.

3 For updated builder shares, see `https://www.relayscan.io/overview?t=7d`.

Table 2: Notation for PBS payoffs.

Symbol	Meaning
R	Raw block value (priority-fee tips + direct transfers)
B	Builder $\longrightarrow$ proposer payment (coinbase transfer)
M	MEV revenue realised in the searcher's bundle(s)
C_{gas}	Gas actually paid by the searcher's bundle
D_{sb}	Direct ETH transfer (tip) from searcher to builder
φ	Refund ratio (0--1) set by MEV-Share or similar
R_{refund}	On-chain rebate to user: φD_{sb}
ρ	Relay-fee fraction on the builder's bid ($\in [0, 1]$)
$C_{s,\text{infra}}$	Off-chain infrastructure costs of the searcher
$C_{b,\text{infra}}$	Builder infrastructure & order-flow costs
$C_{v,\text{infra}}$	Validator infrastructure costs
$R_{\text{consensus}}$	Protocol-level block-proposal reward

2.2 Solana: Leader Forwarding and Bundle Channels

Solana handles pending transactions differently from Ethereum, so the relevant terms need careful definition. On Ethereum, a transaction often sits first in a public mempool: a broadly visible waiting area in which many market participants can observe pending order flow before execution. Solana's *Gulf Stream* design tries to avoid such a public waiting room. A user typically sends a transaction to an RPC node, a server that receives the user's request and relays it into the network. Instead of leaving the transaction in a widely shared mempool, Gulf Stream forwards it toward the validators expected to produce the next blocks (Solana Foundation, 2019).

These scheduled block producers are called *leaders*. More generally, a *validator* is a node that participates in consensus and helps confirm the chain; the *leader* is the validator whose turn it is to assemble the next block. This distinction matters for MEV because the leader sees pending transactions before final settlement and can influence their relative ordering. The absence of a public mempool therefore does not mean that transactions are invisible before execution. It means that visibility is concentrated among a narrower set of actors: RPC operators, the current and upcoming leaders, and specialized routing services.

Jito adds another layer to this transaction path. Jito's block engine is an off-chain service that accepts transaction bundles and forwards them to participating validators (Jito Labs, 2026). A *bundle* is an ordered set of transactions that should execute together and in the submitted order, or not at all. Searchers use bundles when they want a multi-step strategy—for example, a front-run, a victim trade, and a back-run—to survive as a single package. To persuade validators to prefer one bundle over another, searchers attach *tips*, which are explicit side payments for priority. From this perspective, Jito's goal is similar to that of MEV-Boost.

This routing model changes how MEV is produced. Since many ordinary users do not expose their transactions in a public queue that everyone can inspect, the classic picture of any outside observer spotting a pending trade and reacting to it is less accurate on Solana. MEV instead depends more heavily on privileged access to transaction flow and on infrastructure that can reach leaders quickly. Searchers who can construct profitable bundles and deliver them through Jito or comparable channels are therefore better positioned than users who rely on ordinary RPC routing alone.

Measurement evidence shows that harmful MEV still survives in this environment. Over four months of early-2025 Jito data, Gerzon et al. identify 521,903 sandwich attacks causing more than $7.7 million in user losses (Gerzon *et al*., 2025). A sandwich attack on Solana follows the same economic logic as on Ethereum: the attacker trades before and after a visible user trade to worsen the user's execution and capture the resulting price movement. The architectural difference is not the economic mechanism, but the route through which the attacker gains the necessary visibility and ordering power.

Jito governance has also moved toward blacklist-based enforcement against validators associated with harmful MEV (Jito Foundation, 2025). That response matters because it makes Solana unusual in placing routing, sequencing, and sanctions close to one another: the same ecosystem actors that help intermediate bundle flow can also influence which forms of MEV are tolerated. For this paper, the main lesson is that a mempool-less design does not eliminate pre-trade asymmetries. It relocates them from an open public queue to a more selective infrastructure layer centered on leader forwarding, private bundle channels, and validator-side routing.

Within the framework of this paper, Solana reduces public transaction visibility but concentrates pre-settlement information and sequencing influence among a narrower set of infrastructure actors. MEV therefore depends less on open mempool observation and more on privileged access to routing, leaders, and bundle channels.

2.3 BNB Chain: Public Mempool with Restricted Builder Access

BNB Chain is closer to Ethereum at the execution level, since users can still submit transactions to a public EVM-style mempool. The difference is that its PBS design routes builder bids through sentries and restricts builders to sending bids only to the in-turn validator (BNB Chain, 2024b; BNB Chain, 2024a). Transactions can also be routed through protected builder channels, so order flow is split between open mempool competition and more controlled private execution paths. Relative to Ethereum, the validator surface is much smaller and the route from user flow to final ordering is easier to attribute.

That narrower control surface has made collective mitigation more feasible. The Goodwill Alliance launched in March 2025 to coordinate wallets, builders, and validators around anti-sandwich filters, and BNB Chain reported by July 2025 that sandwich volume had fallen by more than 95% after common filtering rules were deployed (BNB Chain, 2025a; BNB Chain, 2025b). BNB Chain therefore illustrates a design in which public order flow still exists, but MEV handling is shaped by a more concentrated set of intermediaries and by a greater capacity for ecosystem-level intervention.

BNB Chain combines public transaction visibility with a relatively concentrated sequencing and governance surface. This configuration preserves mempool-based MEV opportunities while making coordinated mitigation and attribution comparatively more feasible.

2.4 Rollups: Private Sequencers and Explicit Ordering Auctions

Rollups change transaction handling more radically because users usually do not submit transactions to a public L1-style mempool. Instead, they send them to a centralized sequencer that maintains a private mempool, orders transactions internally, executes them, and only later posts data to Ethereum. On OP Stack chains, this means that pre-trade visibility sits primarily with the sequencer. On Base, block construction is further subdivided through 200 ms Flashblocks and a dynamic mempool managed by the builder (Optimism, 2026; Base, 2026). Arbitrum makes the sale of ordering rights explicit through Timeboost, which auctions an express lane on top of the centralized sequencer (Arbitrum Foundation, 2024).

The consequence is not the disappearance of MEV, but its internalization. A 2026 study finds that sustained economically meaningful sandwiching is largely absent on major private-mempool rollups (Gogol *et al.*, 2026). At the same time, the first large-scale Timeboost study finds strong concentration, with two entities winning more than 90% of auctions between April and July 2025 (Messias *et al.*, 2025). Rollups therefore suppress the classic public-mempool form of MEV while increasing the importance of sequencer discretion and auction design.

Rollups reduce public visibility while concentrating ordering authority within sequencers or express-lane mechanisms. MEV consequently shifts away from open mempool competition and toward sequencer governance, auction design, and the conditions under which priority is allocated.

2.5 Cross-chain Execution: Fragmented Order Flow Across Domains

Cross-chain MEV no longer fits within a single chain's transaction queue. A trader or solver may need to route across several blockchains, bridges, and liquidity venues, so each leg is exposed to a different local sequencer or validator set. In practice, profitable execution often depends on pre-positioned inventory across multiple domains, because waiting for a bridge can eliminate the opportunity. Transaction handling is therefore fragmented: there is no single mempool, no single block builder, and no single point of ordering authority (Öz *et al.*, 2025; McMenamin, 2023).

This fragmentation produces a different form of MEV. A year-long study covering September 2023 to August 2024 identifies 242,535 executed cross-chain arbitrages totaling $868.64 million in volume, with 66.96% using pre-positioned inventory and settling in 9 seconds on average, versus 242 seconds for bridge-based trades (Öz *et al.*, 2025). The advantage here is not only faster local ordering, but also the ability to coordinate capital, routing, and execution across heterogeneous domains.

Across these architectures, private channels do not eliminate MEV; they reassign informational advantage and sequencing power. The privileged actor may be a builder, block engine, validator, sequencer, wallet route, or cross-chain solver, but the source of extraction remains control over transaction handling before final settlement (European Securities and Markets Authority, 2025; Ji *et al.*, 2025).

Cross-chain execution fragments both visibility and sequencing authority across domains. The relevant advantage is therefore not located in a single mempool or sequencer, but in the capacity to coordinate information, inventory, routing, and execution across multiple infrastructures.

2.6 DeFi compliance with European Regulation

The previous sections showed that blockchain architectures differ primarily in the way they allocate transaction visibility and ordering authority before settlement. These architectural choices are also relevant from a regulatory perspective, because they help identify where effective control over execution resides and where accountability and supervisory responsibilities may emerge. Against this background, Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCAR) (European Parliament and Council of the European Union, 2023) can be read not only as a framework governing crypto-assets and crypto-asset services, but also as a framework for identifying accountable actors along the transaction path. DeFi challenges this approach because a single execution path may involve a smart contract, liquidity pool, front end, wallet, router, sequencer, and validator, several of which may not be regulated entities.

MiCAR is built around identifiable actors: issuers, offerors, persons seeking admission to trading, and crypto-asset service providers (CASPs). This mismatch is why DeFi sits at the boundary of MiCAR rather than cleanly inside or outside it.

Existing DeFi compliance debates often start from identity. That is understandable. Pseudonymity, the absence of a traditional intermediary, and the difficulty of assigning responsibility all push regulators toward KYC and permissioning models. Those tools matter for compliance and enforcement, but they are not the main lens for this paper. For MEV, the central question is not who the end user is. It is who sees the order, who routes it, who can influence its position, and who executes it before settlement.

MiCAR does not displace identity-based compliance, but its most relevant hook here is order execution. Services provided in a "fully decentralised manner without any intermediary" fall outside the Regulation's direct scope. Activities performed, provided, or controlled, directly or indirectly, by identifiable undertakings remain in scope even when they use decentralised infrastructure. The decisive issue is therefore not whether settlement takes place on a decentralised protocol. It is whether a professional intermediary controls access, routing, ordering, or execution somewhere along the transaction path.

MiCA Q&A 2711 makes this concrete for order execution. Article 78(5) MiCAR requires CASPs executing client orders to make specific disclosures and obtain explicit consent when execution may occur outside a trading platform. The Q&A states that, for this purpose, a "trading platform" means a platform authorised under MiCAR. Execution on a DEX or another DeFi protocol therefore counts as execution outside a trading platform and brings the associated conduct-of-business obligations into play.

The practical consequence is that MiCAR obligations follow the order, not the venue label. If a MiCA-authorised CASP receives, transmits, or executes a client order and routes it to decentralised liquidity, the CASP remains responsible for compliance. Automation at the settlement layer does not remove that responsibility. Disclosure duties, client consent requirements, and best-execution obligations still apply when the final leg settles on permissionless infrastructure.

This reading narrows the practical meaning of "fully decentralised". A DEX pool may be autonomous at the smart-contract level, but many access points are not. Wallets with embedded swaps, aggregators, routers, custody providers, and hybrid trading platforms may qualify as CASPs when they arrange client order flow professionally or exercise discretion over execution. In those cases, DeFi is not a separate unregulated market. It is execution infrastructure used inside a regulated service.

That matters for MEV. Once a regulated intermediary routes a client order into decentralised liquidity, slippage, routing choices, liquidity depth, and exposure to MEV become execution-quality issues within the client relationship. They cannot be treated only as protocol-level facts. The CASP must manage, disclose, and monitor them in the same way it must account for other features of the execution process.

MiCAR therefore shows one way an entity-based regime can affect decentralised markets without imposing identity checks at the protocol level. It regulates the intermediary's handling of the order rather than the user's direct access to the smart contract. The supervisory problem is architectural, not categorical: it requires identifying where control, ordering authority, and execution discretion sit along the transaction path, and where responsibility for market outcomes, including MEV-related effects, can realistically be enforced even when settlement remains decentralised.

3 MEV strategies and traditional market analogues

This section introduces the strategy families that recur in MEV discussions and relates them to their closest analogues in traditional finance. While these strategies are executed at the protocol level, their relevance for market integrity and regulation increases materially when the underlying order flow is routed, bundled, or executed by intermediated access points. The goal is not to force a one-to-one mapping between DeFi and TradFi institutions. Instead, for each on-chain strategy we ask which familiar market function it most closely resembles—cross-venue arbitrage, trading ahead of predictable order flow, or opportunistic liquidity supply—and then identify where the analogy breaks down because of atomic execution, public observability, or protocol design. For a broad survey of the MEV landscape, see Materwala *et al.* (2025).

A compact taxonomy is therefore necessary. Extractable value may come from ordering itself, denoted here as $EV_{ordering}$, or from an external or privileged signal, denoted EV_{signal}. It may be atomic, when all relevant legs execute or revert together, or non-atomic, when inventory, latency, or failed-execution risk remains. It may also be fully on-chain, or it may span off-chain and cross-domain venues such as centralized exchanges, rollups, bridges, and multiple chains.

We restrict attention to four patterns that are central to AMM execution: back-running arbitrage, sandwich attacks, just-in-time liquidity provision, and mixed JIT+sandwich bundles. Flash loans are discussed first because they are an important execution primitive, but they are better treated as financing technology than as a separate strategy. Similarly, protocol exploits based on oracle failures, governance attacks, or liquidation races are important parts of the broader MEV landscape, but they depend on vulnerabilities external to the transaction-ordering mechanisms emphasized here. The following subsections provide a separate schematic for each strategy class.

3.1 Flash loans as an execution primitive

A flash loan allows an Ethereum user to borrow a potentially large amount of on-chain liquidity without posting collateral, provided that the borrowing, use of funds, and repayment all occur within the same transaction. If repayment fails, the entire transaction reverts. From the lender's perspective, there is therefore no residual credit exposure once the transaction is finalized.

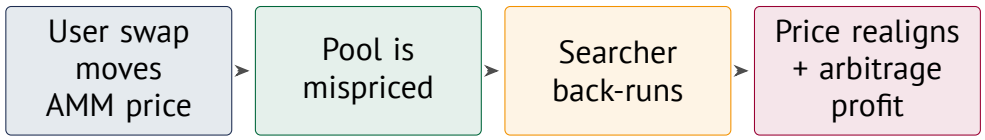
Flash loans matter because they relax capital constraints. They can finance arbitrage, sandwiching, and more complex multi-leg bundles without requiring the searcher to hold the relevant inventory ex ante or to post collateral. In that sense, they are better understood as a *financing technology* than as a distinct MEV strategy. They are also frequently used in exploit-driven attacks that manipulate a thin on-chain price and then monetize the distortion against a protocol that treats that price as informative. Those episodes, however, depend on oracle design or contract vulnerabilities rather than on the AMM execution game studied here.

There is no exact analogue in traditional finance. The closest comparison would be pre-arranged intraday funding or margin credit, but the analogy is imperfect. TradFi credit is neither permissionless, nor unsecured in the same sense, nor atomically contingent on the success of a complete multi-leg strategy. This difference is central: in DeFi, financing, execution, and settlement can be collapsed into one transaction.

3.2 Back-running arbitrage

Back-running arbitrage exploits the price dislocation created when a large swap pushes an AMM away from the broader market. After the user trade executes, the searcher submits an offsetting transaction that brings the on-chain price closer to an external reference, such as another DEX or a centralized exchange. When both legs are on-chain, the strategy can often be bundled atomically; when one leg is off-chain, the arbitrage becomes non-atomic and the searcher bears latency and inventory risk.

Figure 7: Sequence of actions in back-running arbitrage.
The user trade first moves the pool price; the searcher then back-runs to restore the price and capture arbitrage.



This is closest to *cross-venue arbitrage* in fragmented equity, FX, or ETF markets. In both settings, arbitrageurs enforce price consistency across trading venues and are rewarded for speed, routing efficiency, and access to capital. The important difference is implementation. In TradFi, arbitrage typically requires pre-funded balances, exchange memberships, credit lines, and exposure to execution risk during the latency window. In DeFi, by contrast, a smart contract can route across venues and may use a flash loan to finance the trade, compressing both capital requirements and settlement risk.

It is useful to distinguish this repricing activity from exploit-driven "arbitrages" that first manufacture a price distortion and only then monetize it. Those episodes are better classified as *price manipulation* than as ordinary arbitrage. Their closest analogue in traditional markets is benchmark manipulation or the exploitation of a thin, illiquid reference venue, not routine price alignment. Since their profitability depends on vulnerabilities external to the swap itself, they are not the object of our theoretical analysis.

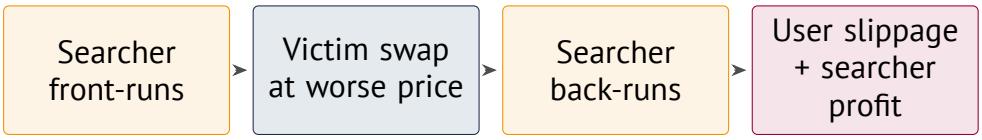
3.3 Sandwich attacks

A sandwich attack targets a user swap that is visible before inclusion. The searcher first trades in the same direction as the user, moving the AMM price against the user. The user trade then executes at this worse price, after which the searcher unwinds in the opposite direction. The attacker's profit comes from appropriating part of the price impact that the user would otherwise have imposed on the pool.[4]

4 There may of course be multiple user swaps inside the bundle, but the economic logic is the same.

The user's slippage tolerance is a crucial constraint. If the front-run is too large, the user's transaction violates its minimum-output condition and reverts, causing the bundle to fail. For this reason, sandwiching is not simply a question of "trading as much as possible" before the victim; it is an optimization problem constrained by the user's own transaction parameters.

Figure 8: Sequence of actions in a sandwich attack.
The searcher front-runs the victim swap and back-runs afterward, extracting value from the price movement around the victim trade.



The closest TradFi analogue is *trading ahead of predictable order flow*. This includes the classic case of broker front-running, but also some forms of latency-sensitive order anticipation in fragmented markets. The economic similarity is straightforward: in both cases, a faster intermediary extracts value from information about imminent demand and worsens the execution obtained by the slower trader. A related analogy is *quote stuffing*, where a malicious trader sends many orders and cancellations to saturate a venue's matching engine and create exploitable artificial latency. The institutional difference is equally important. In traditional markets, the relevant information is often confidential customer flow, and the practice is therefore heavily regulated or prohibited. In DeFi, by contrast, the signal may come from public mempool data rather than entrusted client information. The tactic is therefore technologically transparent, but not economically harmless: the loss still materializes as adverse execution for the user.

3.4 Just-in-Time (JIT) liquidity

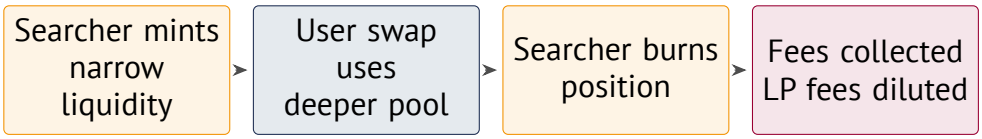
JIT liquidity exploits the concentrated-liquidity design implemented, for example, in Uniswap v3 and v4. After observing a large pending swap, a searcher mints liquidity in a very narrow price range around the current price, remains active only for the targeted trade, collects a large share of the fees generated by that trade, and then burns the position immediately afterward. This strategy is also referred to as *LP sandwich* or *active liquidity provision*[5] (Capponi *et al.*, 2023). Unlike a sandwich, JIT does not profit by worsening the user's execution. By deepening the pool during the swap, it can instead reduce price impact for the transacting user. The rent is extracted from fee income that would otherwise accrue to passive liquidity providers (Capponi *et al.*, 2023).

5 This should not be confused with the broader notion of *active liquidity*, namely the total liquidity whose range contains the current price.

There is no exact TradFi counterpart. The closest analogy is *opportunistic market making* or fleeting liquidity provision that appears only when execution is especially attractive and adverse selection is limited. But the parallel remains incomplete. In regulated markets, quoting obligations, queue priority, minimum resting requirements, and surveillance constrain how transient liquidity can be. In Uniswap, a concentrated position can be inserted and removed around a single trade with atomic finality. The result is a distinctly DeFi form of selective intermediation.

This also explains why the welfare assessment of JIT is more subtle than that of sandwiching. Relative to the user, JIT may be beneficial because it improves execution. Relative to passive LPs, it is rent-extractive because it dilutes the fee income that compensates them for providing standing liquidity.

Figure 9: Sequence of actions in just-in-time (JIT) liquidity provision.
The searcher mints concentrated liquidity before the swap, earns fees during execution, and burns the position afterward.

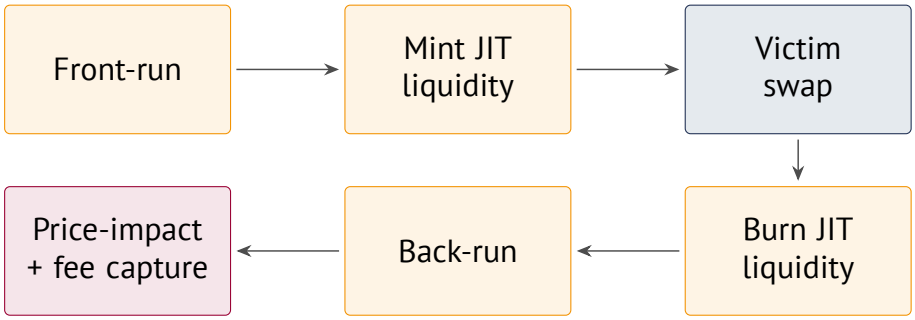


3.5 Mixed JIT+sandwich bundles

Large swaps can also be exploited through a mixed bundle that combines aggressive and passive legs: the searcher front-runs the user, mints JIT liquidity, lets the user trade, burns the position, and then back-runs. This construction captures both the fee income generated during the user trade and part of the price displacement created by the front-run. Because the temporary liquidity position makes the book deeper during the user leg, the user's slippage constraint becomes less restrictive, allowing a larger feasible front-run than in a pure sandwich. Recent evidence suggests that such patterns do occur on-chain (Di Nosse *et al.*, 2025).

The closest TradFi comparison is a hybrid of order anticipation and opportunistic market making, but there is no clean one-to-one equivalent. In conventional markets, the aggressive and passive components are typically separated by venue rules, inventory constraints, and non-atomic execution. In DeFi, by contrast, they can be composed into a single bundle and resolved within one block. This is why mixed strategies are especially interesting analytically: they are not merely the sum of two familiar tactics, but a genuinely blockchain-native form of intermediation.

Figure 10: Sequence of actions in a mixed JIT+sandwich bundle.
The searcher combines a sandwich with temporary JIT liquidity inside one atomic bundle.



3.6 Empirical profit distributions

While the proposed strategy taxonomy provides a useful theoretical framework, it requires empirical validation against actual transaction data. To this end, we deploy an MEV event collector on the Uniswap v3 USDC/WETH 0.05% pool over the 2023 block window. The input consists of the pool's temporally ordered stream of Swap, Mint, and Burn events, extracted from the Uniswap v3 subgraph and enriched with on-chain pool state data where necessary (Uniswap Labs, 2026). Our detector scans each block for strict, single-pool, contiguous event sequences: *mint–victim-swap–burn* for pure JIT liquidity; *front-run–victim-swap–back-run* for classical sandwiches; *front-run–mint–victim-swap–burn–back-run* for mixed JIT-sandwiches; and an immediate opposite-direction swap following a victim swap for reverse back-runs.

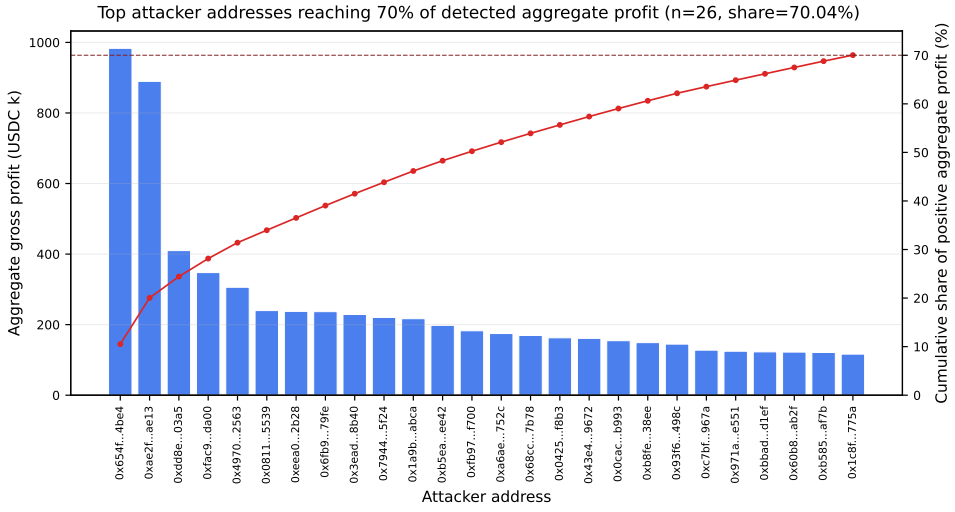
Given the noisy nature of the reverse back-run heuristic, we filter for candidates that are economically feasible and return the execution price to within 1% of the optimal no-arbitrage bound, approximated as $(1-f)\,P_0$ or $\frac{P_0}{(1+f)}$ depending on the direction of the victim's swap and where f is the pool fee and P_0 is the pre-victim price. Throughout this section, we report observed gross profits valued in USDC, derived from token cash flows, fee accruals, and pool prices. These figures strictly exclude gas costs, validator bribes, and builder payments.

We emphasize that our detection heuristics are designed for precision rather than exhaustive recall. Consequently, these results delineate the empirical profit distributions of the identified strategies rather than providing definitive frequency bounds. The strict pattern-matching may yield false negatives or, particularly in the case of back-runs, occasional false positives. A second caveat is that the reported values are gross profits: they do not net out gas fees, validator bribes, builder payments, or other execution costs, and therefore should not be read as realized net returns.

This limitation naturally extends to our coverage metrics. Within our 2023 sample, the pool recorded 43,216 Mint and 1,937,268 Swap events. Pure JIT accounts for 18,013 temporary mint legs (41.68% of all Mint events), while mixed JIT-sandwich bundles contribute an additional 499 (1.15%). Combined, JIT-style liquidity provision covers 42.84% of total Mint events. For swaps, measuring only victim-side trades (excluding attacker legs), classical sandwiches encompass 2,297 events (0.119% of total swaps. Some sandwiches contain multiple victim swaps within the same bundle), and mixed JIT-sandwiches add 585 events, bringing the total sandwich-type victim flow to 0.149%. Reverse back-run candidates account for 20,379 victim swaps (1.052%). We note that these proportions are highly specific to the 5 bps fee tier; because fee levels dictate the economic viability of front-running, back-running, and temporary liquidity provision, the observed strategy mix cannot be mechanically extrapolated to other pools (for a broader cross-tier analysis, see Di Nosse *et al.* (2025)).

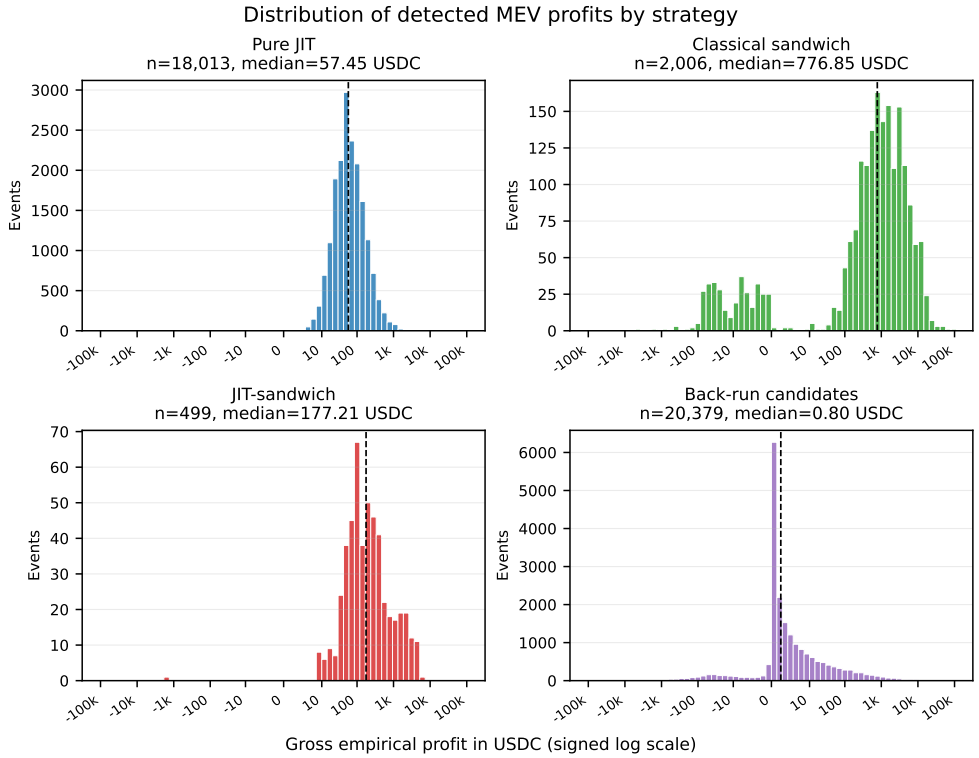
Figure 11 illustrates the address-level concentration of these activities. Ranking attackers by aggregate observed gross profit, the smallest prefix accounting for 70% of the total positive aggregate profit comprises only 26 addresses.

Figure 11: Rank plot of the top attacker addresses.
Bars show address-level aggregate observed gross profit in USDC thousands; the red line shows the cumulative share of positive aggregate attacker profit. The plotted addresses are the smallest ranked prefix reaching 70% of the detected positive aggregate profit. X-axis labels are shortened attacker addresses.



As shown in Figure 12, the profit distributions across all strategies are strongly right-skewed. Pure JIT is the most frequently detected strategy (18,013 events), yielding a modest per-event profit profile (median: USD 57.45; mean: USD 102.78; 95th percentile: USD 320.91) and an aggregate gross profit of USD 1.85 million. In contrast, classical sandwiches are much less frequent (2,006 events) but dominate total profitability, generating USD 4.70 million in aggregate gross profit. Their per-event profits are substantially larger (median: USD 776.85; mean: USD 2,343.87; 95th percentile: USD 10,207.71), with 83.2% of classical sandwiches being strictly positive before gas and bribes. Mixed JIT-sandwiches, while rare (499 events), remain economically significant (median: USD 177.21; mean: USD 533.01; aggregate: USD 0.27 million). Candidate reverse back-runs present a distinctly different topology: they are highly prevalent (20,379 events) but overwhelmingly composed of micro-arbitrage opportunities (median: USD 0.80; 75th percentile: USD 7.06). Their aggregate gross profit nonetheless reaches USD 2.46 million, driven by a heavy right tail (99th percentile: USD 2,095.62; maximum $>$ USD 218,000).

Figure 12: Empirical gross profit distributions by detected MEV strategy.
Back-runs are restricted to detector-labelled candidate rows. Profits are observed gross token-flow profits valued in USDC and exclude gas costs, bribes, and builder payments.



Overall, the empirical data does not indicate a single dominant MEV strategy at all scales. Instead, we observe a fragmented landscape: pure JIT is frequent but low-margin; classical sandwiches are infrequent but highly lucrative; mixed bundles are rare but consistently profitable; and reverse back-runs consist of abundant near-zero events punctuated by severe outlier realizations.

4 Possible supervisory implications

The analysis developed in this paper may suggest some implications for market supervisors. First, transparency at the settlement layer does not necessarily imply transparency in transaction handling. Critical decisions concerning routing, sequencing, and execution may occur before a transaction becomes visible on-chain. Second, supervisory attention should extend beyond the final venue of execution to the actors that control transaction flow before settlement, including routers, builders, sequencers, block engines, and aggregators. Third, different blockchain architectures generate different combinations of informational and ordering asymmetries. Supervisory risks should therefore be assessed at the level of transaction handling rather than solely at the level of the underlying protocol. Finally, accountability is likely to concentrate around actors that exercise effective discretion over routing, sequencing, and execution, even where final settlement occurs through decentralized infrastructure.

These implications also affect the evidence available to supervisors. Public-ledger data provide a detailed record of settled transactions, but may not reveal private routing decisions, rejected bundles, withheld transactions, or the commercial arrangements through which priority was allocated. Effective supervision may therefore require information from intermediaries and infrastructure providers in addition to on-chain analysis.

5 Conclusion

This review has framed Maximal Extractable Value (MEV) as a market-microstructure phenomenon arising from the interaction between transaction visibility and ordering authority before settlement. The relevant asymmetry is therefore not purely informational, but architectural: public mempools, private routing channels, builder markets, sequencers, and cross-domain execution paths determine who sees transactions, who can influence their ordering, and how execution outcomes are shaped.

The architectural comparison presented in this paper shows that design choices in transaction handling do not eliminate MEV in a simple sense. Rather, they reassign it across different layers of the execution stack. Public mempools expose users to open searcher competition and classic sandwiching strategies; private routing reduces that exposure while concentrating execution advantages in wallets, builders, relays, or sequencers; explicit ordering auctions make priority rights visible but commodify them; and cross-chain execution shifts the advantage toward inventory placement and routing control. The central question is therefore not whether MEV exists, but where along the transaction path visibility and ordering authority are concentrated, contested, or internalised.

The strategy taxonomy reinforces this conclusion. Back-running arbitrage, sandwich attacks, just-in-time liquidity provision, and mixed bundles all reflect familiar microstructure motives—such as arbitrage, order anticipation, and selective liquidity provision—translated into a programmable, atomic execution environment. While these strategies are executed at the protocol level, their economic and regulatory relevance increases materially when user order flow is routed, bundled, or executed through intermediated access points. In such settings, MEV becomes a dimension of execution quality rather than a purely protocol-internal phenomenon.

From a regulatory perspective, this execution-centric framing aligns with the logic of the European crypto-asset regulatory framework. Rather than relying on identity-based compliance or access-focused regulatory solutions, MiCAR anchors responsibility at the level of regulated intermediaries and ensures that conduct-of-business and execution obligations follow the order when decentralised liquidity is used. In this way, routing decisions, ordering authority, and exposure to MEV become relevant not because of who the user is, but because of how a client order is executed when it is routed by a regulated intermediary toward decentralised execution infrastructure.

The broader implication is that supervision of decentralised finance cannot rely on categorical distinctions between centralised and decentralised systems. Effective oversight requires attention to execution architectures: who has pre-settlement visibility, who controls sequencing, how routing choices are made, and where accountability for execution outcomes can be enforced. A realistic policy objective is therefore not to promise MEV-free blockchains, but to design execution environments in which extractable value is more transparent, more constrained, and easier to attribute.

In this sense, MEV serves as a useful diagnostic lens. It reveals how economic rents emerge from transaction handling and how regulatory responsibility intersects with execution design when decentralised systems are accessed through intermediated channels. Understanding these interactions is essential not only for market integrity, but for the future integration of decentralised execution infrastructures into regulated financial markets.

From a regulatory perspective, the key lesson is that MEV should not be understood solely as a technological phenomenon. It is fundamentally a question of market design and transaction governance. The relevant supervisory question is therefore not simply whether a market is centralized or decentralized, but who can observe transaction intent, who can influence routing and execution, and who can ultimately be held accountable for the resulting outcomes.

References

Arbitrum Foundation (2024), Constitutional AIP: Proposal to Adopt Timeboost, a New Transaction Ordering Policy, *https://forum.arbitrum.foundation/t/constitutional-aip-proposal-to-adopt-timeboost-a-new-transaction-ordering-policy/25167*, Accessed: 2026-04-22, URL: https://forum.arbitrum.foundation/t/constitutional-aip-proposal-to-adopt-timeboost-a-new-transaction-ordering-policy/25167.

Base (2026), Block Building, *https://docs.base.org/base-chain/network-information/block-building*, Accessed: 2026-04-22, URL: https://docs.base.org/base-chain/network-information/block-building.

BNB Chain (2024a), Integration Guide for Builder - BSC MEV, *https://docs.bnbchain.org/bnb-smart-chain/validator/mev/builder-integration/*, Accessed: 2026-04-22, URL: https://docs.bnbchain.org/bnb-smart-chain/validator/mev/builder-integration/.

BNB Chain (2024b), Overview - BSC MEV, *https://docs.bnbchain.org/bnb-smart-chain/validator/mev/overview/*, Accessed: 2026-04-22, URL: https://docs.bnbchain.org/bnb-smart-chain/validator/mev/overview/.

BNB Chain (2025a), BNB Good Will Alliance, *https://www.bnbchain.org/en/blog/bnb-good-will-alliance*, Accessed: 2026-04-22, URL: https://www.bnbchain.org/en/blog/bnb-good-will-alliance.

BNB Chain (2025b), How the Goodwill Alliance Slashed Sandwich Attacks by 95%, *https://www.bnbchain.org/en/blog/how-the-goodwill-alliance-slashed-sandwich-attacks-by-95*, Accessed: 2026-04-22, URL: https://www.bnbchain.org/en/blog/how-the-goodwill-alliance-slashed-sandwich-attacks-by-95.

Buterin, V. (2021), Proposer/block builder separation-friendly fee market designs, *https://ethresear.ch/t/proposer-block-builder-separation-friendly-fee-market-designs/9725*, URL: https://ethresear.ch/t/proposer-block-builder-separation-friendly-fee-market-designs/9725.

Capponi, A., Jia, R., Zhu, B. (2023), The paradox of just-in-time liquidity in decentralized exchanges: More providers can sometimes mean less liquidity, *arXiv preprint arXiv:2311.18164*.

Chemaya, N., Cong, L.W., Jorgensen, E., Liu, D., Zhang, L. (2023), A Dataset of Uniswap Daily Transaction Indices by Network, *arXiv preprint arXiv:2312.02660*, DOI: 10.48550/arXiv.2312.02660.

CoinGecko (2026a), 2025 Annual Crypto Industry Report, *https://www.coingecko.com/research/publications/2025-annual-crypto-report*, Accessed: 2026-05-08, URL: https://www.coingecko.com/research/publications/2025-annual-crypto-report.

CoinGecko (2026b), 2026 Q2 Crypto Industry Report, *https://assets.coingecko.com/reports/2026/CoinGecko-2026-Q2-Crypto-Industry-Report.pdf*, Accessed: 2026-09-15, URL: https://assets.coingecko.com/reports/2026/CoinGecko-2026-Q2-Crypto-Industry-Report.pdf.

D'Amato, F., Neuder, M. (2023), Equivocation attacks in mev-boost and ePBS, *https://ethresear.ch/t/equivocation-attacks-in-mev-boost-and-epbs/15338*, Accessed: 2025-07-10, URL: https://ethresear.ch/t/equivocation-attacks-in-mev-boost-and-epbs/15338.

Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., Juels, A. (2020), ``Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability'', in 2020 IEEE Symposium on Security and Privacy (SP), 910–927, DOI: 10.1109/SP40000.2020.00040.

DefiLlama (2026), Historical DeFi TVL, all chains, *https://api.llama.fi/v2/historicalChainTvl*, Accessed: 2026-09-15. The series excludes liquid-staking and double-counted TVL., URL: https://api.llama.fi/v2/historicalChainTvl.

Di Nosse, D.M., Gatta, F., Lillo, F., Jaimungal, S. (2025), Deviations from Tradition: Stylized Facts in the Era of DeFi, arXiv: 2510.22834 [q-fin.TR], URL: https://arxiv.org/abs/2510.22834.

Ethereum Foundation (2024), Proposer-Builder Separation, *https://ethereum.org/en/roadmap/pbs/*, Accessed: 2025-07-09, URL: https://ethereum.org/en/roadmap/pbs/.

European Parliament and Council of the European Union (2023), Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32023R1114*, Official Journal of the European Union, L 150, 9 June 2023.

European Securities and Markets Authority (2025), TRV Article: Maximal Extractable Value Implications for Crypto Markets, *https://www.esma.europa.eu/document/trv-article-maximal-extractable-value-implications-crypto-markets*, ESMA50-481369926-29744. Accessed: 2026-04-22, URL: https://www.esma.europa.eu/document/trv-article-maximal-extractable-value-implications-crypto-markets.

Gerzon, N., Weintraub, B., In, J., Mislove, A., Nita-Rotaru, C. (2025), ``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, 937–943, DOI: 10.1145/3730567.3764493.

Gogol, K., Killer, C., Schlosser, M., Bocek, T., Stiller, B., Tessone, C. (2024), SoK: Decentralized Finance (DeFi) -- Fundamentals, Taxonomy and Risks, *arXiv preprint arXiv:2404.11281*, DOI: 10.48550/arXiv.2404.11281.

Gogol, K., Schneider, M., Gorzny, J., Tessone, C. (2026), How to Serve Your Sandwich? MEV Attacks in Private L2 Mempools, *arXiv preprint arXiv:2601.19570*, DOI: 10.48550/arXiv.2601.19570.

Gupta, T., Pai, M.M., Resnick, M. (2023), The Centralizing Effects of Private Order Flow on Proposer-Builder Separation, *arXiv preprint arXiv:2305.19150*, DOI: 10.48550/arXiv.2305.19150.

Ji, Y., Grimmelmann, J. (2025), Regulatory Implications of MEV Mitigations, in Financial Cryptography and Data Security 2024 Workshops, *Lecture Notes in Computer Science*, *Springer*, 14746, 335–363, DOI: 10.1007/978-3-031-69231-4_21.

Jito Foundation (2025), JIP-22: Establish a Mechanistic MEV Blacklist & Blacklist Operations Committee, *https://forum.jito.network/t/jip-22-establish-a-mechanistic-mev-blacklist-blacklist-operations-committee/839*, Accessed: 2026-04-22, URL: https://forum.jito.network/t/jip-22-establish-a-mechanistic-mev-blacklist-blacklist-operations-committee/839.

Jito Labs (2026), Low Latency Transaction Send, *https://docs.jito.wtf/lowlatencytxnsend/*, Accessed: 2026-04-22, URL: https://docs.jito.wtf/lowlatencytxnsend/.

Liebau, D. (2024), Decentralized Finance (Literacy) Today and in 2034: Initial Insights from Singapore and Beyond, *arXiv preprint arXiv:2410.14173*, DOI: 10.48550/arXiv.2410.14173.

Marzec, D., Thibault, L. (2024), Subverting the Total Eclipse (of the Heart), *https://hackmd.io/@dmarz/total-eclipse-of-the-relay*, Accessed: 2025-07-10, URL: https://hackmd.io/@dmarz/total-eclipse-of-the-relay.

Materwala, H., Naik, S.M., Taha, A., Abed, T.A., Svetinovic, D. (2025), Maximal extractable value in decentralized finance: Taxonomy, detection, and mitigation, *IEEE Transactions on Services Computing*, *IEEE*.

McMenamin, C. (2023), SoK: Cross-Domain MEV, *arXiv preprint arXiv:2308.04159*, DOI: 10.48550/arXiv.2308.04159.

Messias, J., Ferreira Torres, C. (2025), The Express Lane to Spam and Centralization: An Empirical Analysis of Arbitrum's Timeboost, *arXiv preprint arXiv:2509.22143*, DOI: 10.48550/arXiv.2509.22143.

Optimism (2026), OP Stack Differences from Ethereum, *https://docs.optimism.io/op-stack/protocol/differences*, Accessed: 2026-04-22, URL: https://docs.optimism.io/op-stack/protocol/differences.

Öz, B., Ferreira Torres, C., Schlegel, C., Mazorra, B., Gebele, J., Rezabek, F., Matthes, F. (2025), Cross-Chain Arbitrage: The Next Frontier of MEV in Decentralized Finance, *arXiv preprint arXiv:2501.17335*, DOI: 10.48550/arXiv.2501.17335.

Öz, B., Sui, D., Thiery, T., Matthes, F. (2024), Who wins ethereum block building auctions and why?, *arXiv preprint arXiv:2407.13931*.

Saggese, P., Fröwis, M., Kitzler, S., Haslhofer, B., Auer, R. (2025), Towards Verifiability of Total Value Locked (TVL) in Decentralized Finance, *arXiv preprint arXiv:2505.14565*, DOI: 10.48550/arXiv.2505.14565.

Solana Foundation (2019), Gulf Stream: Solana's Mempool-less Transaction Forwarding Protocol, *https://solana.com/news/gulf-stream--solana-s-mempool-less-transaction-forwarding-protocol*, Accessed: 2026-04-22, URL: https://solana.com/news/gulf-stream--solana-s-mempool-less-transaction-forwarding-protocol.

TokenInsight Research (2026), Crypto Exchange Report: 2025 Annual Report, *https://tokeninsight.com/en/research/reports/crypto-exchange-2025-annual-report*, Accessed: 2026-05-08, URL: https://tokeninsight.com/en/research/reports/crypto-exchange-2025-annual-report.

Uniswap Labs (2026), Uniswap Subgraph Overview, *https://developers.uniswap.org/docs/ecosystem/subgraphs/overview*, Accessed: 2026-05-13.

Wahrstätter, Toni (2025), MEV-Boost Dashboard, *https://mevboost.pics/*, Accessed: 2025-07-09, URL: https://mevboost.pics/.

Wang, S., Huang, Y., Zhang, W., Huang, Y., Wang, X., Tang, J. (2024), Private Order Flows and Builder Bidding Dynamics: The Road to Monopoly in Ethereum's Block Building Market, *arXiv preprint arXiv:2410.12352*, DOI: 10.48550/arXiv.2410.12352.

Werner, S.M., Perez, D., Gudgeon, L., Klages-Mundt, A., Harz, D., Knottenbelt, W.J. (2021), SoK: Decentralized Finance (DeFi), *arXiv preprint arXiv:2101.08778*, DOI: 10.48550/arXiv.2101.08778.

Wu, X., Deng, W., Quan, Y., Cong, L.W., Zhang, L. (2024), Trust Dynamics in Cryptocurrency Markets: Centralized vs. Decentralized Exchanges, *arXiv preprint arXiv:2404.17227*, DOI: 10.48550/arXiv.2404.17227.

Xu, J., Paruch, K., Cousaert, S., Feng, Y. (2021), SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols, *arXiv preprint arXiv:2103.12732*, DOI: 10.48550/arXiv.2103.12732.

Zhou, L., Xiong, X., Ernstberger, J., Chaliasos, S., Wang, Z., Wang, Y., Qin, K., Wattenhofer, R., Song, D., Gervais, A. (2022), SoK: Decentralized Finance (DeFi) Attacks, *arXiv preprint arXiv:2208.13035*, DOI: 10.48550/arXiv.2208.13035.

Glossary of on-chain terms

Table 3: Plain-language glossary for core on-chain terminology used in the paper.

Term	Simple meaning
Active liquidity	Liquidity whose chosen price range currently contains the pool price. Only active liquidity affects swap execution and earns swap fees.
Address	An alphanumeric identifier to which cryptoassets and on-chain activity are associated. An address is publicly visible but does not, by itself, identify the person or entity controlling it.
Atomic execution	All steps inside a transaction happen together as one indivisible operation: either every step succeeds, or the whole transaction is cancelled and the blockchain state goes back to what it was before.
Automated market maker (AMM)	A trading protocol that prices swaps with a rule based on the pool's token reserves instead of matching buyers and sellers through a traditional order book. Uniswap is the canonical example.
Arbitrum	An Ethereum layer-2 rollup ecosystem in which users submit transactions to a sequencer before data is posted back to Ethereum. In this paper, Arbitrum is relevant because Timeboost makes part of ordering priority explicit through an auction.
Back-run	A transaction placed immediately after another transaction or set of transactions. In this paper, a back-run often trades in the opposite direction after a user swap has moved the pool price.
Base (layer 2)	An Ethereum layer-2 rollup built on the OP Stack. In this paper, Base is relevant because its Flashblocks design subdivides block construction and affects pre-settlement visibility and ordering.
Base fee	The part of an Ethereum transaction fee that is set by the protocol under EIP-1559 and burned rather than paid to the block producer.
Block	A batch of transactions that is ordered, executed, and added to the blockchain as one update to the shared state.
Blockchain	A shared transaction register whose accepted history is replicated across nodes and updated according to a consensus protocol.
Block builder	A specialized actor that assembles candidate Ethereum blocks, chooses transaction ordering, and bids to have its block accepted by the selected proposer.
Block engine	An off-chain routing service, such as Jito's infrastructure on Solana, that receives bundles from searchers and forwards profitable or policy-compliant bundles to participating validators.
Bridge	Infrastructure that moves assets or messages between blockchains. Bridge delays and risks matter for cross-chain MEV because price opportunities can disappear while assets are in transit.
Bribe / tip	A payment offered for priority, inclusion, or a preferred ordering. In Ethereum PBS this can be a direct transfer or priority-fee payment; on Solana bundle systems it is often called a tip.
Bundle	A group of transactions that is submitted as a coordinated package with a chosen internal order, so the transactions are intended to be executed together in the same block.
Burn	A Uniswap liquidity action that removes all or part of an LP position and returns the underlying tokens plus accrued fees. Burns do not move the pool price by themselves.
Calldata	The input data attached to an Ethereum transaction. For swaps, calldata can encode router choices, token paths, recipient addresses, deadlines, and minimum-output or maximum-input constraints.
Centralized exchange (CEX)	A trading venue operated by a company or intermediary, such as Binance or Coinbase. CEX prices are often used as external references for on-chain arbitrage or hedging.
Coinbase transfer	A direct payment to the block producer's fee recipient address. Despite the name, this is unrelated to the Coinbase exchange and is commonly used as an explicit MEV payment.
Concentrated liquidity	The Uniswap v3 design in which liquidity providers choose a price range instead of supplying liquidity across all prices. This makes liquidity more capital efficient but creates tick-specific execution effects.
Consensus	The protocol process by which validators agree on the next valid block and the canonical chain history.
Constant-product rule	The AMM pricing rule in which the product of the two reserves is preserved after accounting for fees. Within one Uniswap v3 tick, virtual reserves follow this rule.

Continued on next page

Term	Simple meaning
Cross-chain MEV	MEV that depends on execution across multiple blockchains, bridges, or liquidity venues rather than on a single chain's transaction queue.
Cryptoasset / token	A digitally represented asset recorded through blockchain infrastructure. A native asset belongs to the base protocol; a token is generally created and managed by a smart contract.
Decentralized exchange (DEX)	An on-chain trading venue implemented with smart contracts. Users trade directly against the protocol's liquidity rather than through a centralized operator.
DeFi protocol	A smart-contract application that provides financial services on-chain, such as trading, lending, borrowing, or derivatives, without relying on a traditional centralized intermediary.
Direct transfer	An explicit on-chain payment included in a transaction or bundle, often used to pay a builder, proposer, or validator for inclusion.
Event-level diagnostic	An empirical check that evaluates each detected on-chain event using its own observed parameters rather than comparing all observations to one common calibration.
Exclusive order flow (EOF)	Transaction flow that is sent privately to a limited set of wallets, builders, relays, or auctions instead of being broadcast to the public mempool. The first party to see it may be able to internalize its MEV.
Fee tier	The swap fee charged by a Uniswap pool, such as 0.01%, 0.05%, 0.3%, or 1%. Higher fee tiers make some strategies more expensive and give liquidity providers more fee income.
Fee accrual	The process by which swap fees are assigned to LP positions in proportion to their share of active liquidity. Accrued fees are realized when the position is collected or burned.
Fee-on-input	A fee convention in which the pool withholds the fee from the trader's input token before updating the price. The formulas write the effective input as r times the raw input, where $r = 1 - f$.
Finality	The condition after which a blockchain transaction is treated as settled and reversal becomes impossible under the protocol's normal operation or sufficiently unlikely under the chain's security assumptions.
Flash loan	An uncollateralized loan that must be borrowed, used, and repaid inside the same transaction. If repayment fails, the whole transaction reverts, so the lender is not left with credit exposure.
Flashblocks	A Base block-building design that subdivides block construction into very short intervals, changing who sees and orders transactions before final publication.
Front-run	A transaction placed immediately before a target transaction. In a sandwich, the front-run moves the pool price against the user before the user's swap executes.
Gas	The resource unit used to pay for computation and storage in Ethereum-style chains. Higher gas payments can make a transaction more attractive for inclusion but reduce the searcher's net profit.
Gulf Stream	Solana's transaction-forwarding design, in which transactions are routed toward upcoming leaders instead of waiting in a broadly visible public mempool.
Hedging	Taking an offsetting position, often on another venue, to reduce the price risk created by an on-chain strategy. JIT liquidity providers may hedge because they temporarily take the other side of the user's swap.
Inclusion	The act of placing a transaction or bundle into a block. MEV profits are only realized if the relevant transactions are included in the intended order.
Inventory	The tokens or assets a trader already holds on a venue or chain. Cross-chain arbitrage often requires inventory to be pre-positioned because bridge transfers are too slow.
Jito	A Solana infrastructure stack that provides a block engine and bundle-routing channel used by searchers and validators.
Just-in-Time (JIT) liquidity	A strategy in which a searcher adds concentrated liquidity immediately before a large swap, collects a share of the swap fees, and removes the liquidity immediately afterward.
Layer 1 / Layer 2	A layer-1 chain, such as Ethereum mainnet, provides base settlement and consensus. A layer-2 system, such as a rollup, executes transactions elsewhere and posts data or proofs back to the layer 1.
Leader	The Solana validator scheduled to produce an upcoming block. Leaders have privileged visibility and ordering power over transactions routed to them.
Liquidity pool	A smart contract holding two or more tokens that traders can swap against. In an AMM, the pool's reserves determine the execution price.
Liquidity multiple	The model's measure of how large a temporary JIT position is relative to existing active liquidity. For example, $\alpha = 1$ means the searcher doubles active liquidity and owns half of the active range.

Continued on next page

Term	Simple meaning
Liquidity provider (LP)	A user or bot that deposits tokens into a liquidity pool and earns fees from trades that use that liquidity. Passive LPs keep liquidity available over time; JIT LPs provide it briefly around a target trade.
Liquidity taker (LT)	A trader whose swap consumes liquidity from a pool. In this paper the large user swap targeted by MEV strategies is the liquidity-taking trade.
Maximal Extractable Value (MEV)	The surplus that can be captured by controlling transaction inclusion, ordering, or execution around other users' transactions.
Mempool	The waiting area where not-yet-confirmed transactions sit before they are included in a block. Actors who can observe this flow may try to reorder or react to those transactions.
MEV-Boost	The widely used Ethereum PBS middleware in which builders send candidate block headers and bids through relays, and proposers choose among them.
Mint	A Uniswap liquidity action that creates or increases an LP position by depositing the required tokens for a chosen price range.
Mixed JIT+sandwich bundle	A bundle that combines a sandwich front-run/back-run with temporary JIT liquidity, allowing the searcher to capture both price-impact profit and part of the victim swap's fee income.
Node	A computer running blockchain software that stores, relays, or verifies network data. Node roles and access to transaction flow differ across architectures.
Oracle	A mechanism that supplies external data to a smart contract, most often a price. If the oracle is slow, manipulable, or based on a thin market, it can create profitable attack opportunities.
OP Stack chains	Layer-2 rollups built with the Optimism OP Stack software stack. They usually route transactions through a sequencer before posting data back to Ethereum, so pre-trade visibility is concentrated in the sequencing layer.
Order flow	The stream of user transactions or trading requests before they are executed. Who sees order flow first is central to MEV.
Order-flow auction	A mechanism that sells or allocates access to transaction flow, often letting builders or searchers compete for the right to execute around it.
Passive liquidity	Liquidity that remains in a pool over time and is exposed to ordinary trading, price movements, and adverse selection, unlike JIT liquidity that appears only around a target trade.
Pool reserves	The token balances available inside an AMM pool. In the simplified constant-product view, reserves determine how much output a swap receives.
Price impact	The change in the execution price caused by a trade consuming liquidity from a pool. Larger trades and thinner liquidity create larger price impact.
Priority fee	The part of an Ethereum transaction fee paid to the block producer as a tip for inclusion. Searchers can use priority fees to compete for ordering.
Priority-gas auction	Competition in the public mempool where searchers raise gas tips to obtain earlier inclusion or a preferred transaction position.
Private mempool	A transaction queue visible only to a restricted actor, such as a sequencer or builder, rather than to the whole network.
Private key	The secret cryptographic credential used to authorize transactions from an address. Whoever controls it can normally control the associated on-chain assets.
Private RPC endpoint	An RPC submission route that sends transactions directly to a private intermediary, builder, or protection service instead of broadcasting them through the public mempool.
Proposer	The Ethereum validator selected by consensus to propose the next block. Under PBS, the proposer usually chooses among blocks built by specialized builders.
Proposer--Builder Separation (PBS)	An Ethereum architecture that separates the validator who proposes a block from the builder who constructs the block and chooses transaction ordering.
Relay	An intermediary in MEV-Boost that receives candidate blocks from builders, checks them, and passes bids or headers to proposers.
Revert	A failed Ethereum-style transaction outcome in which state changes are undone. Users may still pay gas for the failed attempt, but the intended swap or contract action does not settle.
Rollup	A layer-2 blockchain that executes transactions off Ethereum mainnet and later posts data or proofs back to Ethereum. Rollups often have centralized or restricted sequencers.
Router	A smart contract or wallet service that chooses how to route a user's trade across pools, aggregators, or private execution paths.

Continued on next page

Term	Simple meaning
RPC node	A server that exposes a blockchain's remote procedure call interface, so wallets, bots, and applications can read chain data and submit transactions to the network. RPC operators may see transaction flow before it reaches block producers or public routing channels.
Sandwich attack	A strategy in which the searcher trades before and after a user's visible swap, worsening the user's execution and capturing part of the induced price movement.
Searcher	A bot operator or trading firm that scans order flow and blockchain state for profitable MEV opportunities, then submits transactions or bundles to capture them.
Sequencer	The actor, common on rollups, that receives user transactions, orders them, executes them, and later posts the result or data to a settlement chain.
Settlement	The point at which executed transactions become part of the accepted chain state. Before settlement, ordering and inclusion can still be contested.
Single-tick approximation	A simplifying assumption that every relevant swap leg stays inside one Uniswap v3 tick, so active liquidity is constant and the formulas reduce to constant-product updates.
Slippage tolerance	The maximum execution deterioration a user allows before her transaction reverts, often implemented through a minimum-output or maximum-input condition.
Smart contract	A program stored on the blockchain that executes automatically when called. DeFi protocols are built from smart contracts that enforce trading, lending, and settlement rules in code.
Solver	An off-chain actor that finds and executes a route for a user intent or cross-chain trade, often using its own inventory and execution infrastructure.
Square-root price	The Uniswap v3 price variable $S = \sqrt{P}$. It is useful because token amounts and liquidity changes have simple formulas in terms of S within a tick.
Swap	A trade that exchanges one token for another through a pool, router, or exchange. In Uniswap, swaps are the actions that move the pool price.
Tick boundary	The edge of a Uniswap v3 price interval. When price reaches a boundary, active liquidity can change before execution continues in the next tick.
Tick / tick range	A discrete price interval in Uniswap v3. Liquidity is active only when the current price lies inside the LP's chosen tick range.
Tick crossing	A swap moving the price across one or more tick boundaries. Crossing a tick can change active liquidity, so single-tick formulas become only an approximation.
Timeboost	Arbitrum's express-lane auction for ordering priority on top of the sequencer, making part of transaction ordering an explicit auction.
Transaction	A signed instruction submitted to a blockchain, such as a token transfer, swap, mint, burn, or smart-contract call.
Uniswap v3	A decentralized exchange protocol whose pools use concentrated liquidity and fee tiers. Its tick structure is central to the paper's JIT and sandwich analysis.
Validator	A node participating in consensus by checking blocks and, when selected, proposing or producing blocks. Validators can receive MEV payments directly or through intermediaries.
Virtual reserves	The reserve-like quantities implied by Uniswap v3's active liquidity and square-root price inside a tick. They allow within-tick execution to be treated like a constant-product AMM.
Victim swap	The user swap targeted or used by a searcher. The term indicates the swap around which a bundle is built, although in pure JIT the user may receive better execution rather than being harmed.
Wallet	Software or a service that constructs and signs blockchain transactions by controlling cryptographic keys. The assets remain recorded on the blockchain rather than being stored literally inside the wallet.

Quaderni FinTech

20 – novembre 2026 **Maximal extractable value as blockchain market microstructure:**
Architectures, transaction handling, and strategy taxonomy
D.M. Di Nosse, A. Russo

19 – luglio 2026 **Sperimentazione dell'IA nell'azione di contrasto della CONSOB agli abusivismi finanziari**
M. Trerotola, A. Boghi, P. Deriu, G. Frega

18 – giugno 2026 **La comunicazione finanziaria tramite il canale digitale**
Profili di rischio per l'investitore retail
A. Canepa, M. Caratelli, D. Colonnello, A. Ottavianelli, P. Soccorso

17 – dicembre 2025 **L'aggregazione di dati finanziari nella prospettiva dell'*open finance***
Profili di mercato e regolatori
A. Burchi, S. Mezzacapo, P. Musile Tanzi, T.N. Poli, G. Quaresima, V. Troiano

16 – dicembre 2025 **Sustainable Development Goals omission and environmental sentiment metric for greenwashing and ESG controversies alert in green bonds**
A. Nicolodi, S. Paterlini, M. Gentile, V. Foglia Manzillo, G. Vittorioso

15 – agosto 2025 **Riflessioni in tema di intelligenza artificiale e attività di vigilanza**
P. Deriu, S. Racioppi; con presentazione a cura di A. Lalli

14 – luglio 2025 **Greenwashing alert system for EU green bonds**
The CONSOB–University of Trento prototype
S. Paterlini, A. Nicolodi, M. Gentile, V. Foglia Manzillo, M.R. Sancilio, P. Deriu

13 – luglio 2024 **Il crowdinvesting made in Italy**
Un'indagine conoscitiva
V. Caivano, C. Lucarelli, F.J. Mazzocchini, P. Soccorso

12 – febbraio 2024 **Dimensionality reduction techniques to support insider trading detection**
CONSOB - Scuola Normale Superiore di Pisa

11 – dicembre 2022 **A machine learning approach to support decision in insider trading detection**
CONSOB - Scuola Normale Superiore di Pisa

10 – luglio 2022 **How Covid mobility restrictions modified the population of investors in Italian stock markets**
CONSOB - Scuola Normale Superiore di Pisa

9 – giugno 2022 **L'intelligenza artificiale nell'*asset* e nel *wealth management***
N. Linciano, V. Caivano, D. Costa, P. Soccorso, T.N. Poli, G. Trovatore; in collaborazione con Assogestioni

8 – aprile 2021 **La portabilità dei dati in ambito finanziario**
A cura di
A. Genovese e V. Falce

7 – settembre 2020 **Do investors rely on robots?**
Evidence from an experimental study
B. Alemanni, A. Angelovski, D. Di Cagno, A. Galliera, N. Linciano, F. Marazzi, P. Soccorso

6 – dicembre 2019 **Valore della consulenza finanziaria e *robo advice* nella percezione degli investitori**
Evidenze da un'analisi qualitativa
M. Caratelli, C. Giannotti, N. Linciano, P. Soccorso

5 – luglio 2019 **Marketplace lending**
Verso nuove forme di intermediazione finanziaria?
A. *Sciarrone Alibrandi, G. Borello, R. Ferretti, F. Lenoci, E. Macchiavello, F. Mattassoglio, F. Panisi*

4 – marzo 2019 **Financial Data Aggregation e Account Information Services**
Questioni regolamentari e profili di business
A. Burchi, S. Mezzacapo, P. Musile Tanzi, V. Troiano

3 – gennaio 2019 **La digitalizzazione della consulenza in materia di investimenti finanziari**
Gruppo di lavoro CONSOB, Scuola Superiore Sant'Anna di Pisa, Università Bocconi, Università di Pavia, Università di Roma 'Tor Vergata', Università di Verona

2 – dicembre 2018 **Il FinTech e l'economia dei dati**
Considerazioni su alcuni profili civilistici e penalistici
Le soluzioni del diritto vigente ai rischi per la clientela e gli operatori
E. Palmerini, G. Aiello, V. Cappelli G. Morgante, N. Amore, G. Di Vetta, G. Fiorinelli, M. Galli

1 – marzo 2018 **Lo sviluppo del FinTech**
Opportunità e rischi per l'industria finanziaria nell'era digitale
C. Schena, A. Tanda, C. Arlotta, G. Potenza