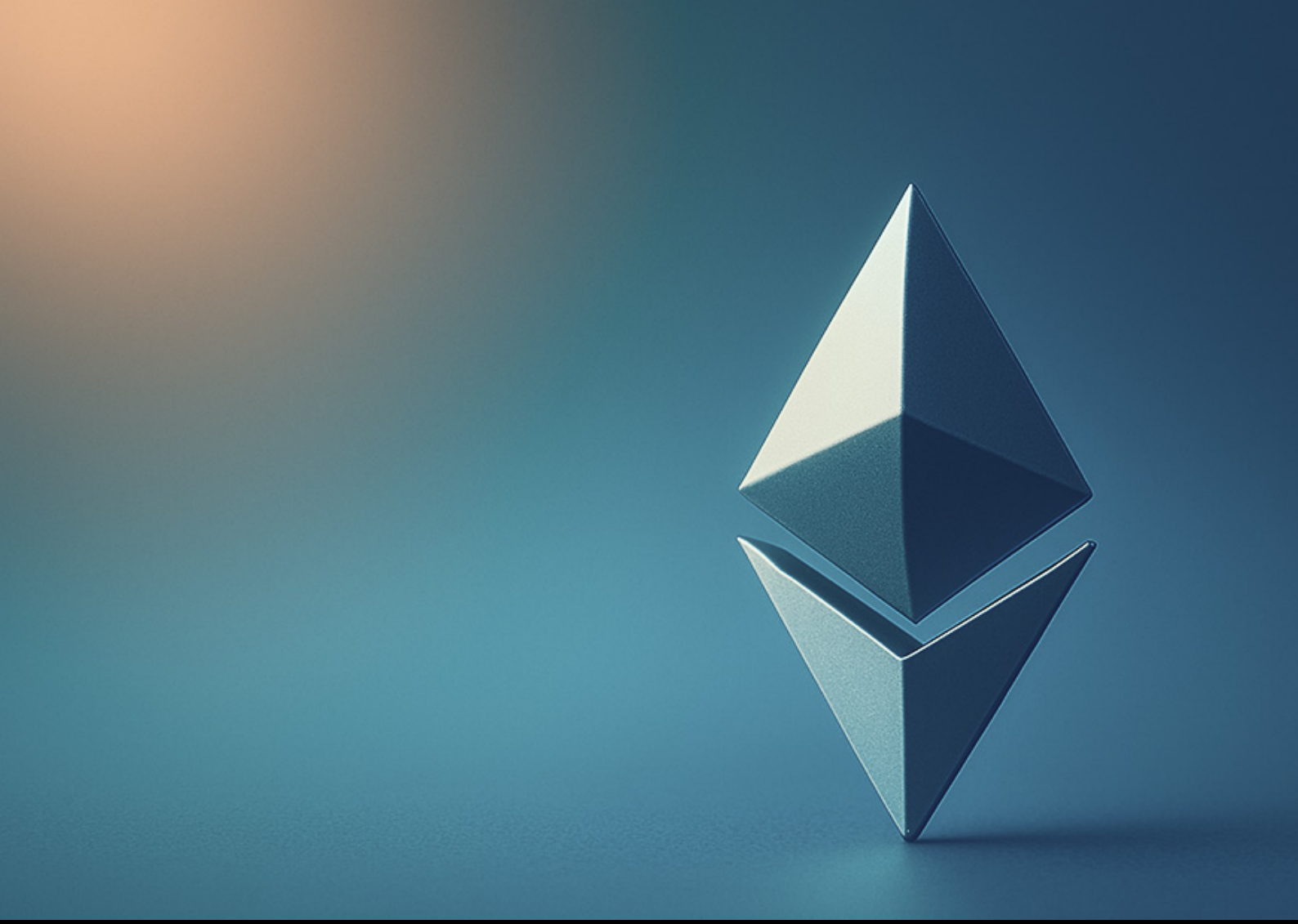


Whitepaper

From Wallet to Chain.
A Bridge of Two Worlds on an Ethereum Transaction

Nethermind & Deutsche Bank

May 2025

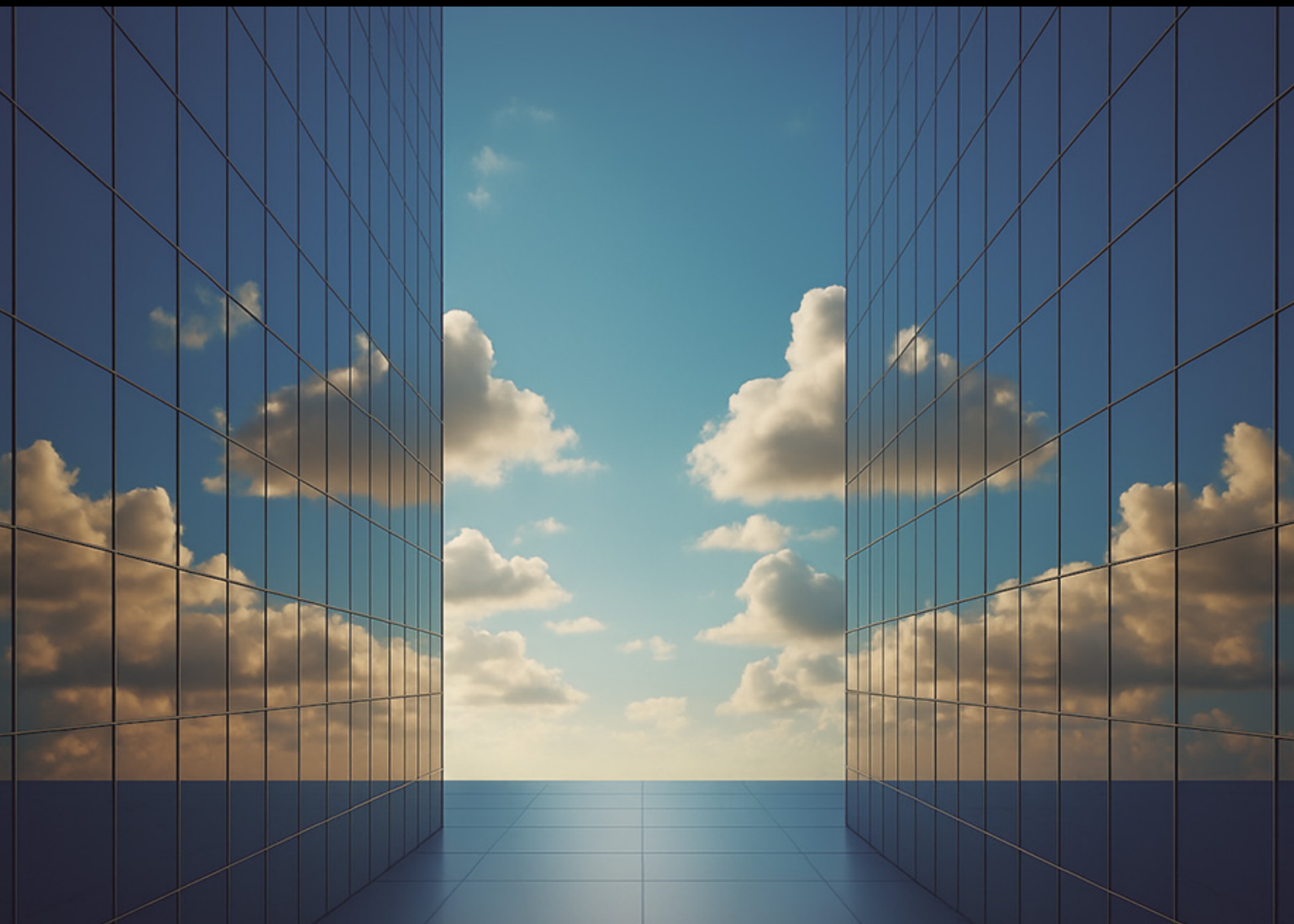
NETHERMIND

Deutsche Bank

Table of Content

01

Introduction & Executive Summary



1 - Introduction & Executive Summary

Blockchains are transforming the fintech landscape through fractionalization, transparency, and programmability, offering potential for fairness, equitable participation, growth, and reduced intermediation costs. While these technologies appeal to regulated financial sectors, blockchain's foundational principles - censorship resistance, decentralization, and open access - often appear to conflict with traditional finance's requirements for accountability, certainty, and centralized oversight.

Key Blockchain-Native Features

Key blockchain-native features exemplify both the promises and depth of public chain use in regulated environments:

- **Proposal-Builder Separation (PBS):** This mechanism separates the roles of block builders (who optimize transaction inclusion) and proposers/validators (who secure consensus), decentralizing block proposers for resilience in open environments and enhancing transparency and accountability.
- **Maximal Extractable Value (MEV):** Profit derived from transaction ordering and validation, often viewed solely negatively but playing important roles in blockchain economics.
- **Direct Private Order Flow:** Where transactions can be directed to whitelisted builders, avoiding the public Mempool where transactions are publicly visible and at risk of MEV attacks.
- **Trusted Execution Environments (TEEs):** Secure hardware environments allowing for verifiable, encrypted transaction computation.

Whitepaper Objectives - Functional Alignment

This joint whitepaper by Nethermind and Deutsche Bank bridges blockchain's decentralization ethos with the regulated industry's need for clarity in addressing shared challenges including fraud, inefficiencies, and mistrust. Using Ethereum as a reference public chain, it examines how blockchain attributes can align with compliance, governance, and operational resilience standards expected in regulated financial markets.

Ethereum's core principles include decentralization and resistance to censorship, collusion, and dominance which are essential elements of its operational resilience in a trustless public environment. These approaches should be viewed as complementary to, rather than opposing, traditional regulatory goals like market integrity and governance. Both worlds ultimately aim to create healthy, vibrant markets that serve users effectively. While their methods differ, they share similar objectives and visions of fairness.

Transaction Lifecycle, Mechanics and Finality

To demonstrate how comparable outcomes can be achieved through different means, this paper examines the complete transaction lifecycle on Ethereum—from initial user submission through to on-chain confirmation and finality. It explains how users can select various transaction submission channels, including public and private Remote Procedure Call (RPC) paths and mempool strategies. These choices influence the subsequent roles of third-party searchers, builders, and relayers within the Proposer-Builder Separation (PBS) model. Notably, private order relay channels enable financial institutions to direct transactions to specific validators, supporting important regulatory objectives such as market integrity, transaction privacy, and counter-terrorism financing measures.

The authors highlight Maximal Extractable Value (MEV) as a significant feature of Ethereum and similar public blockchains. MEV represents transaction fees paid to network validators for transaction ordering, serving as an economic incentive to secure the network. However, this mechanism can be exploited by sophisticated users, raising concerns about market manipulation, slippage, and potential harm to users. This whitepaper evaluates various countermeasures against MEV abuse, including encrypted mempools, fair ordering protocols, and curated builder ecosystems.

Transaction finality emerges as another critical factor for institutional adoption of blockchain technology. This whitepaper emphasizes how Ethereum achieves settlement finality through consensus backed by substantial economic security, making transaction reversal economically impossible - effectively creating an outcome similar to traditional financial systems but through different technical means. It also outlines Ethereum's existing ~13-minute finality mechanism and its progress towards Single Slot Finality (SSF), reducing this timeframe to roughly ~12 seconds while preserving consensus security via planned upgrades like Orbit.

Regarding infrastructure, the authors examine the growing centralization in block building and sequencing, analyzing its implications for operational resilience and market integrity. The whitepaper presents solutions like Trusted Execution Environments (TEEs) and BuilderNet as potential approaches to decentralized and verifiable block construction that ensure fair transaction inclusion without compromising confidentiality or builder performance.

Regulatory Perspective

From a regulatory perspective, the whitepaper introduces "functional outcome alignment," where different technological approaches can achieve equivalent regulatory objectives. In Ethereum's ecosystem, this alignment stems from the combination of technological architecture, financial incentives, community behavior, and commitment to decentralization and censorship resistance. The network has developed on-chain mechanisms supporting regulatory goals, including role separation (PBS), transaction irreversibility (slashing and staking models), and controlled transaction routing (private RPCs and permissioned builders). The concluding section examines public-permissioned blockchain architectures, which layer regulatory controls, permissioning, and privacy features onto open networks.

Synthesis of Approaches - Bridging the Two Worlds

Ethereum's evolving technical capabilities, combined with industry collaboration and thoughtful regulatory engagement, can create viable pathways for regulated institutions to adopt public blockchains while meeting risk management requirements. The future of financial infrastructure need not present a zero-sum choice between decentralization and control. Instead, it can synthesize strengths from both approaches: resilience and openness from public chains with safety and accountability of traditional systems.

By integrating these complementary strengths rather than treating them as contradictory forces, the digital asset ecosystem can achieve greater benefits for all participants.

This whitepaper was co-written by Nethermind and Deutsche Bank, exploring technological advancements in the Ethereum protocol and their contributions to on-chain risk management. Ethereum is used as a reference for public chains, with no implied endorsements.

1.1 - Main Insights: How Ethereum Meets Institutional Needs and Regulatory Requirements

1. MEV is a Structural Incentive for Economic Security

Maximal Extractable Value (MEV) incentivizes and rewards validators for proposing blocks honestly. However, it has attracted attention due to user strategies such as frontrunning, sandwich attacks, and Centralized Exchange - Decentralized Exchange (CEX-DEX) arbitrage, which have introduced systemic inefficiencies, market abuse elements and user-level risks (including increased gas costs and transaction failure). With the DEX being understood as a peer-to-peer marketplace where transactions occur directly between crypto traders.

The whitepaper explains MEV and outlines technical and architectural mitigants against intentional abuse of this structural attribute, e.g. private order flow, MEV sharing, encrypted mempools, which balance builder incentives with user fairness and avoid market abuse practices.

2. Proposer-Builder Separation (PBS) Enables Role Specialisation and Reduces Conflicts of Interest

Proposer-Builder Separation (PBS) mitigates centralization risks and conflicts of interest by separating the roles of block building (performed by specialized entities) and validation (carried out by decentralized nodes). By separating the roles of block builders, who optimize transaction inclusion and ordering, and proposers/ validators, who secure consensus, PBS creates accountability and operational neutrality. This separation also introduces the ability to whitelist builders, implement censorship policies, and reduce opportunities for validator self-dealing - crucial for institutions concerned with governance and auditability. Additionally, Trusted Execution Environments (TEEs) provide secure hardware environments that enable effective block construction without requiring mutual trust, further addressing centralization or collusion concerns.

3. Orbit and Single Slot Finality Are Critical for Institutional Confidence in Settlement

Current Ethereum finality is about ~13 minutes and when paired with a Layer 2 for settlement finality, near instant finality can be reached on the Layer 2. The whitepaper presents Orbit SSF, a proposed upgrade using validator capping for Ethereum to achieve finality within a single slot (~12 seconds) while preserving consensus and security-by-economics. This development is an equivalent of the traditional securities T+0 or instant settlement expectations, albeit without requiring centralized trusted intermediaries.

4. TEEs and Collaborative Builder Networks Reduce Centralisation Risks in Block Construction

Today's MEV ecosystem is dominated by specialized block builders. TEEs, such as those deployed in BuilderNet (Flashbots, Nethermind, BeaverBuild), create secure, verifiable, and censorship-resistant environments where multiple parties can co-build blocks without mutual trust. This distributed approach to infrastructure governance aligns with the Web3 ethos, mitigates dominance and hence collusion risks, while also avoiding single points of failure.

5. L2 Solutions Bring Scalability with Accountability of Centralized Sequencers

While Layer 2 (L2) networks offer scalability and cost-efficiency, currently, they tend to rely on centralized sequencers with full control over transaction ordering. As a result, mechanisms such as forced inclusion have been developed to mitigate malicious sequencer's wilful derisking of transactions and thereby uphold inclusiveness and mitigate abuse of power in Web3. However, from a regulated financial industry perspective where the sequencer is reputed to uphold regulatory sanction lists, forced inclusion could be perceived as an attempt by a participant to bypass established compliance and risk controls.

6. Censorship resistance upgrades are on Ethereum's Roadmap

Ethereum's ongoing development includes upgrades such as enshrined PBS (ePBS, a potential future version of PBS), encrypted mempools, and inclusion lists. These advancements are designed to evolve Ethereum with more sophisticated features to support growing demands while maintaining core blockchain values like decentralisation, censorship resistance and user protection. This also reflects responsive, outcome-and-evidence based governance as a way to evaluate public chain innovations.

7. Regulatory Alignment Can Be Achieved Through Functional Outcomes as Equivalence

Ethereum and other public chains can satisfy regulatory outcomes through technological mechanisms (e.g. staking for finality, economic slashing for misbehavior, private RPCs for transaction traceability), even if they lack centralized governance structures. This "functional outcomes over design conformity" approach is essential to ensure dynamic adaptable alignments between future technological progress, such as Enshrined PBS, with time-honoured safety and soundness goals.

02

A Blockchain Transaction

2 - A Blockchain Transaction

A blockchain transaction is a request to update what's known as the "state" of the blockchain (the current record of all information stored on it, such as account balances and data), which must be digitally signed by the account owner. Common transaction types include ETH transfers, token transfers, smart contract interactions (like token swaps or NFT mints), and smart contract deployments.

Each transaction contains several key components:

- **From:** The sender's address
- **To:** The recipient address (account or contract)
- **Value:** Amount of ETH transferred
- **Data:** Optional calldata for contract interactions
- **Signature:** Cryptographic proof of authorization
- **Gas parameters:** Maximum (base) gas, priority fee, and max fee per gas
- **Nonce:** A sequential counter preventing transaction replay

In the following sub-sections, we will walk through the lifecycle of a blockchain transaction, from:

1. Creation in the wallet (Section 2.1), to
2. Propagation and validation of the transaction (Section 2.2), to
3. Transaction confirmation and finality (Section 2.3)

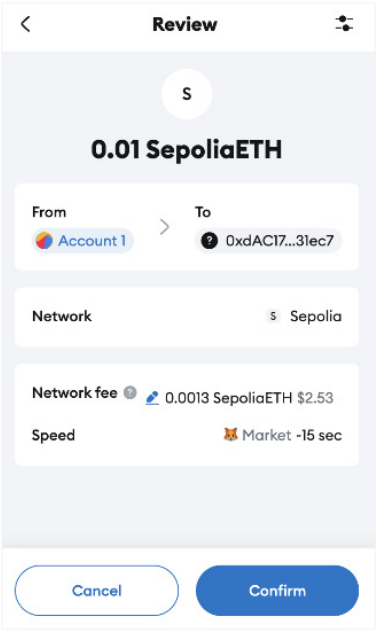


Figure 2: A wallet screen (Source: Metamask)

2.1 - In The Wallet: Transaction Creation

The transaction lifecycle begins in a user's wallet when they initiate an action. The wallet software:

1. Constructs the transaction with appropriate parameters;
2. Signs the transaction with the user's private key; and
3. Sends transaction to the remote procedure call (RPC) endpoint configured on the user's wallet, which can be switched between:

S/N	RPC endpoint configurations
3a)	Default RPC endpoint of the node-as-a-service used by the wallet that interacts with the public mempool ("Public RPC"). For this configuration, users do not have direct control over the path of their transactions, whether or not they will be processed through the Proposer-Builder Separation (PBS) mechanism. This is elaborated in Section 2.3.
3b)	Custom RPC endpoint that interacts with private infrastructures ("Private RPC"). Specifically, users may choose to connect to private mempool solutions that implement PBS like Flashbots Protect. This is elaborated in Section 2.3.2.

Figure 2.1: RPC configuration options in the wallet

2.2 - In the Mempool: Maximal Extractable Value (MEV)

When initiating a transaction, users can set priority fees to incentivise block proposers or builders to include their transactions, as they receive these fees directly. The base fee, which is determined by network congestion, is burned to effectively remove a portion of ETH from circulation to potentially increase its value to all ETH holders. This mechanism creates a market for block space, where users compete through priority fees for faster inclusion. New ETH is minted as a reward to block proposers for each block proposed.

Figure 2.2: Performance of MEV Types (Source: EigenFi)

MEV represents an economic feature of transaction ordering where PBS participants can earn fees via optimal sequencing of the transactions. It is a natural economic outcome where different sequence of transaction orders – with each transaction having their own fees – can create value differentials.

This is typically termed as "MEV extraction" and it has several economic and efficiency implications:

- **User Cost:** The transaction fees paid by users are distributed to builders and validators
- **Higher Gas Fees:** Bidding competition for MEV opportunities by specialized validators can drive up gas prices for themselves and spills over to other users. However, the fee increase represents a redistribution mechanism where general users are effectively paying more for the network's efficiency and security through higher transaction fees. The higher fees paid by users during those times are an important incentive for network maintenance and security provision. There is an effective mitigant to self-servicing high bids by validators in the form of accessible interoperability with other compatible chains that users can migrate to if high fees on the source chain persist unreasonably.
- **Centralization Pressure:** Advantages accrue to those with superior infrastructure and capital.

More validators can join, attracted by the possibilities to earn reasonable gas fees and in doing so, the diverse validator pool mitigates concerns about market fairness and long-term network health that could arise as a result of concentration of MEV extraction capability among a small set of builders and searchers.

The relationship between MEV extraction and gas fees demonstrates how the blockchain network's economic structure seeks to balance operational sustainability with user costs paid via dynamic market-based mechanisms, rather than periodic administrative fees determination or fee cards.

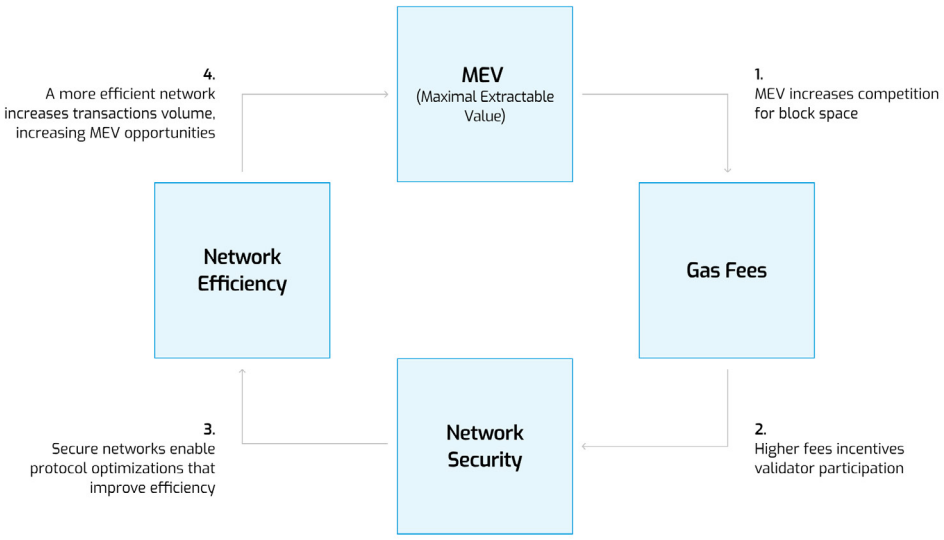


Figure 2.2b: A relationship diagram between MEV, Security, Efficiency and Gas

To extract or earn MEVs, block builders and specialized MEV searchers employ several common strategies:

2.2.1 – Frontrunning

Frontrunning occurs when builders see a pending transaction in the public mempool and quickly insert their own transactions ahead of it to gain an advantage. Common types include:

- **DEX Frontrunning:** When a large swap is detected, frontrunners place their own swap first, causing price slippage for the user and profiting from the price movement.
- **NFT Frontrunning:** Outbidding others for NFTs by paying higher gas fees after spotting their pending purchase transactions.
- **Contract Deployment Frontrunning:** Copying and deploying someone's contract code before they can deploy it themselves.

These practices harm users through higher costs, failed transactions, and missed opportunities. Frontrunning is particularly problematic because it unfairly extracts value from users who initiated legitimate economic activity in the first place.

2.2.2 – Backrunning

Backrunning occurs when blockchain participants strategically place their transactions immediately after a target transaction is processed to capitalize on its effects on the network. Common types include:

- **Liquidation Backrunning:** Racing to execute profitable liquidations immediately after collateral prices change, allowing backrunners to claim liquidation bonuses.
- **AMM Rebalancing:** Exploiting price imbalances in automated market makers after large swaps have altered token ratios in liquidity pools.
- **Failed Transaction Opportunities:** Capturing value opportunities that are revealed when another user's transaction fails to execute properly.

While backrunning can contribute to market efficiency, it nevertheless diverts value that might otherwise remain with regular users.

2.2.3 - Sandwich Attacks

Sandwich Attacks combine both frontrunning and backrunning techniques to extract value from users' transactions. In this strategy, attackers position their own transactions both before and after a target transaction. Common process:

- **First Transaction:** The attacker places a transaction ahead of a detected large swap, moving the market price in the direction that will disadvantage the user.
- **User's Transaction:** The original user's swap then executes at a worse price due to the increased slippage caused by the first attack transaction.
- **Second Transaction:** The attacker quickly places another transaction after the user's, reversing their initial position and capturing profit from the temporary price distortion.

These attacks have been observed in DEXes with predictable pricing algorithms and limited liquidity pools, where price movements can be more pronounced and easily manipulated.

2.2.4 - CEX-DEX Arbitrage

CEX-DEX Arbitrage involves capitalizing on price differences between centralized exchanges (CEX) and decentralized exchanges (DEX) to generate returns without directly targeting specific user transactions. This is akin to traditional relative arbitrage trading strategy. The CEX-DEX Arbitrage process tends to be as follows:

- **Price Discovery:** Identifying significant price discrepancies for the same asset between centralized and decentralized trading platforms.
- **Coordinated Execution:** Purchasing the asset on whichever venue offers the lower price while simultaneously selling on the venue with the higher price.
- **Profit Extraction:** Capturing the price differential as profit, minus the transaction fees and gas costs required for execution.

Unlike other MEV strategies, arbitrage can benefit the broader market by improving price consistency across different trading venues. However, the value captured still represents an opportunity cost for other market participants who might otherwise benefit from these inefficiencies.

2.2.5 - MEV Mitigation Approaches

Before discussing the many MEV mitigation approaches, it's important to understand that most negative MEV mechanisms result from adverse selection, where a searcher can simulate transactions and then choose an ordering of transactions that benefits themself while negatively affecting a user. The key insight into many MEV mitigation strategies is that they aim to either remove the searcher's ability to choose the transaction ordering, or to charge the searcher a fee for doing so - the consequence of which is improved end user welfare. Several approaches have been proposed to mitigate the impacts of harmful MEV:

- **Fair Ordering Protocols:** Implementing time-based or randomised transaction ordering
- **MEV Sharing:** Redistributing extracted MEV to affected users or the broader network
- **Encrypted Mempools:** Preventing transaction contents from being visible before inclusion
- **Application Design:** Creating DEX mechanisms resistant to sandwich attacks
- **Protocol-Level Solutions:** Implementing consensus-layer protections against harmful extraction

As blockchain ecosystems evolve, the balance between efficient markets, builder incentives, and user protection remains an active area of research and development.

2.3 - In The Nodes: Transaction Propagation and Validation

In Ethereum, an epoch, which is comprised of 32 slots of 12 seconds each, is the time period during which every validator attests once. There are multiple ways and types of entities that perform these activities in a given slot:

<table>
<tr><th rowspan="2">Activity</th><th colspan="3">Entity Performing the Activity for Each Transaction Path</th></tr>
<tr><th>Transaction Path a) – Public Order Flow, Default on Ethereum (Without PBS) OR</th><th>Transaction Path b) – Public Order Flow with PBS Opt-in OR</th><th>Transaction Path c) – Private Order Flow with PBS Opt-in</th></tr>
<tr><td>1. Bundle transactions from a public/private mempool to construct a block</td><td rowspan="3">Activities performed by the randomly selected block proposer from the entire validator set for the slot</td><td>Activity outsourced to the entire set of specialized third-party searchers and builders with sophisticated MEV extraction expertise</td><td>Activity outsourced to selected verified and trusted builders</td></tr>
<tr><td>2. Validate the block</td><td colspan="2">Activity outsourced to third-party relayers that would relay the most profitable validated block to the elected block proposer/ validator</td></tr>
<tr><td>3. Sign and submit the block to a subset of validators known as attesters for further validation</td><td colspan="2">Activity performed by randomly selected block proposer/validator</td></tr>
<tr><td>4. Vote for the validity of the block. When 2/3 votes are attained, the block becomes “justified” i.e. unlikely to be re-ordered</td><td colspan="3">Attesters (rest of validators)</td></tr>
</table>

Table 2.3a: Mapping of transaction validation activities & participants for each transaction path

As a result, this creates 3 **mutually exclusive** transaction paths as depicted in the diagram:

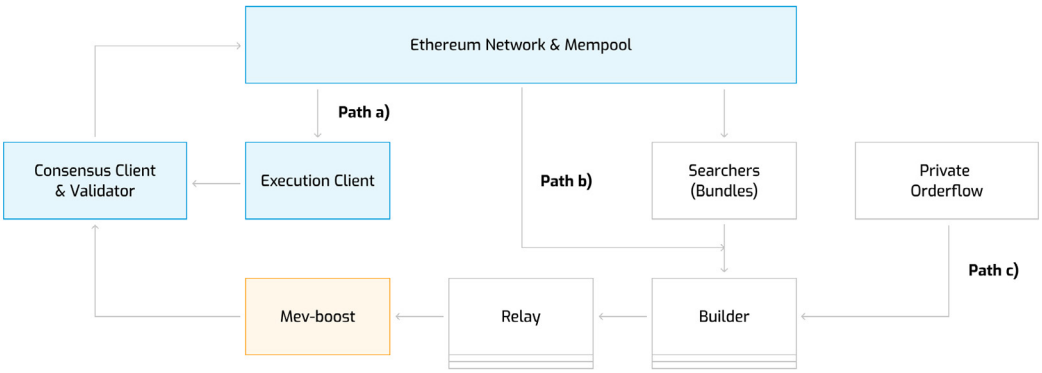


Figure 2.3b: Illustration of 3 mutually exclusive transaction paths on Ethereum

Below is a summarised overview of the 3 transaction paths:

Characteristics	**Transaction Path a)** Public Order Flow, Default on Ethereum (Without PBS) OR	**Transaction Path b)** Public Order Flow with PBS Opt-in OR	**Transaction Path c)** Private Order Flow with PBS Opt-in
1. Transaction Entry Point	**Public** RPC	**Public** RPC	**Private** RPC
2. Participating Entities for Transaction Processing	Block proposer / validator only	1. **Entire** set of PBS searchers & builders 2. Relayers 3. Block proposer/ validator	1. **Selected** searcher(s) & builder(s) 2. Relayers 3. Block proposer/ validator
3. User Choice of Participating Entities in 2)	No	No	Yes
4. Potential to Whitelist Entities in 2)	No	Yes	Yes
5. Transaction Privacy	No	Yes	Yes
6. MEV Abuse Protection	No	No	Yes
7. Suitable for:	General users / Small orders		Regulated users / Large orders

Table 2.3c: Summarised comparison of 3 transaction paths

For the purpose of this paper, the authors will focus on the following transaction paths in the subsequent sections:

- **Section 2.3.1 on Transaction Path b): Public Order Flow with PBS**
- **Section 2.3.2 on Transaction Path c): Private Order Flow with PBS**

2.3.1 – Public Order Flow With PBS

A block of transactions, routed through the PBS transaction path from the public mempool (transaction path b), was first selected and bundled by third-party intermediaries (searchers and builders) before reaching block proposers/validators that have opted into PBS mechanisms like MEV boost.

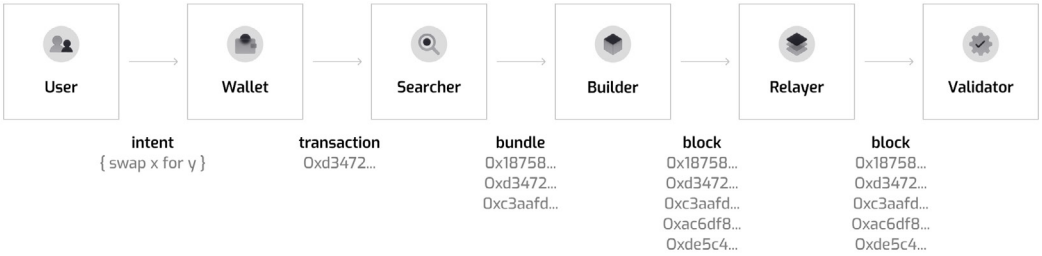


Figure 2.3.1: Public Order Flow with PBS

By separating block proposing from block building, PBS creates a clear separation between:

- Builders that compete on their ability to construct a block with the highest value/MEV rather than the amount of ETH staked; and
- The more decentralized proposers/validators that focus on consensus security, that receive, sign and publish the most profitable block without needing to possess specialized block building capabilities.

The process works as follows:

1. **Searchers:**
   - Monitor public mempool and on-chain state for MEV opportunities
   - Create transaction bundles to capture value
   - Submit bundles to block builders

2. **Block builders:**
   - Maintain sophisticated transaction ordering algorithms
   - Receive and evaluate searcher bundles
   - Bundle transactions to capture MEV opportunities
   - Include their address as fee recipient for priority fees
   - Submit sealed block proposals to relayers

3. **Relayers:**
   - Validate submitted blocks
   - Run auctions between multiple builders
   - Forward the most profitable valid blocks to proposers
   - Act as trusted intermediaries ensuring fair play

4. **Block proposers/validators:**
    - Connect to multiple relayers for redundancy
    - Receive the highest-value valid block header
    - Sign the winning block header without seeing its contents
    - Receive the full block and publish it

By separating these roles, PBS allows the builder market to be anchored on technical expertise and resource-capital efficiency, while maintaining a diverse and decentralized validator set focused on consensus security. This architectural decision trades builder centralisation for validator decentralisation, in favour of **overall network security, resilience and resistance to any large well-resource groups trying to gain dominance to influence things their way.**

Furthermore, this natural role specialization creates a market-based check and balance mechanism that mirrors the separation of duties. This ensures no single entity controls both the proposal of transactions to be included in a block and the verification of the transactions within that block.

In this case, block builders handle transaction bundling and validators would provide independent verification on transactions that are proposed by a 3rd party and not by themselves. **From a financial industry regulatory standpoint, this reduces the conflict of interests in transaction inclusion and verification, and enables accountability since builders can be whitelisted and enforce a level of valid filtering** – or 'censorship' as the term is used in Web3 – of known or suspected undesirable transactions or parties.

However, despite the possibility to whitelist searchers, builders, relayers and proposers in the PBS architecture, users do not have control over how their transactions in the public mempool will be processed, with or without PBS. Private Order Flow with PBS is a method that provides this required control.

2.3.2 – Private Order Flow with PBS

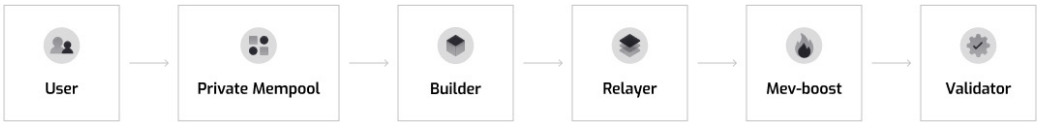


Figure 2.3.2: Private Order Flow with PBS

Several services offer specialized RPC endpoints to private mempools, which offers control and frontrunning protection.

The transaction path via such specialized RPCs is as follows:

- Transactions are sent directly from the wallet to the connected private infrastructure
- Transactions do not appear in the public mempool
- The provider routes transactions directly to verified and trusted builders
- Users can avoid frontrunning without technical complexity
- Some services offer "no revert, no pay" guarantees for failed transactions
- Users can often specify parameters to limit extractable value

Modern Private RPCs, such as Flashbots Protect[1] and Cow Finance's MEV Blocker[2], share order flow with builders under certain conditions. Common conditions include no front-running and rebating the user's

transaction if it creates an arbitrage opportunity. Some Private RPCs like Bloxroute ETH Protect RPC[3] also implement compliance checks at the RPC level and filter out sanctioned transactions.

Furthermore, solutions such as Flashbots Protect, Titan[4] and BeaverBuild[5] are directly integrated into several wallet applications, making private order flow accessible to average users who might otherwise lack the technical knowledge to protect their transactions from MEV attacks.

2.4 - In Consensus: Transaction Confirmation and Finality

When users submit transactions to Ethereum, they need confidence that those transactions won't be reverted or altered after the transactions have settled. This property is called finality. While traditional financial systems achieve finality through legal frameworks and trusted intermediaries, blockchains must create this guarantee of irreversibility through technical and economic mechanisms.

User Perspective on Transaction Finality

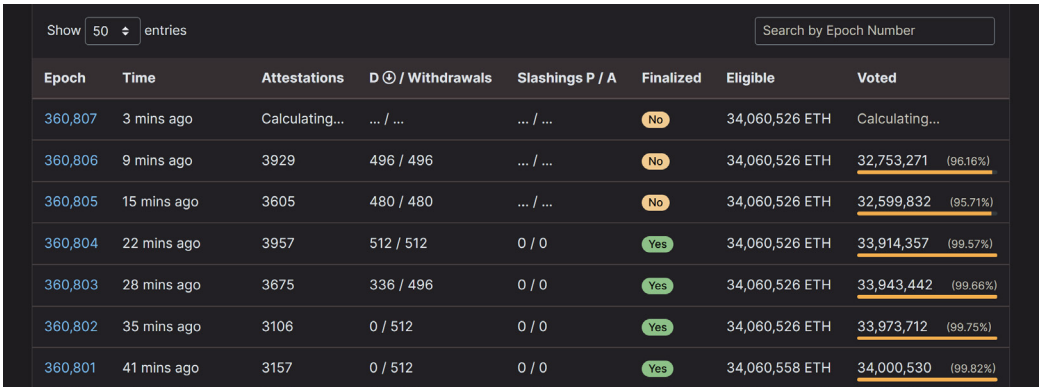


Figure 2.4: View of transaction finality status on public block explorer (Source: beaconcha.in)

Blockchain finality represents the point at which a transaction can be considered irreversible.

2.4.1 - Technical Definition of Finality

In Ethereum's proof-of-stake consensus, finality has a precise technical definition:

- **A block is considered finalised when at least 2/3 of the total validator stake has attested to it through two consecutive checkpoints.**
- **Finalization typically occurs every 2 epochs (approximately 12.8 minutes)**
- **Attempting to revert a finalised block would require at least 1/3 of the stake to be slashed**
- **This economic guarantee makes finality effectively irreversible under normal conditions**

This definition creates a cryptoeconomic security threshold: an attacker would need to sacrifice at least 33% of the total staked ETH (which in today's range of price, would be valued at billions of dollars) to be in a position to revert finality.

2.4.2 - Factors Resulting in Non-Finality

While finality is the normal operating state, Ethereum's consensus could also enter periods of non-finality under certain edge probability conditions that are akin to outages in traditional market infrastructures. These are:

- **Network Issues:** Severe global connectivity problems preventing validator communication, which can also impact broader areas other than blockchain.
- **Client Bugs:** Software errors causing validators to disagree on chain state. This is rare given the extensive testings performed in testnets and the depth of community expertise to proactively identify bugs.
- **Validator Inactivity:** Mass validator offline events reducing active participation.

During non-finality periods:

- No new blocks reach finalised status
- The chain continues to produce blocks that remain in "justified" state
- Users face increased uncertainty about transaction permanence
- Applications may pause operations requiring finality guarantees

2.4.3 - Liveness

Ethereum's consensus design has already considered the factors that could result in non-finality. It prioritizes liveness (continued operation). Hence, even during non-finality periods, the chain continues producing blocks and processing transactions, though these could carry increased reorganization risks since settlement finality is affected. Once network conditions improve, the chain would resume its normal finality process. This design choice reflects the prioritization of keeping the network operational even under adverse conditions, avoiding mass panic while signaling to the users that the chain is in a sub-optimal situation so that users can manage their transactions better. Finality will return on normal operations.

Finalization should eventually be restored through automated mechanisms that remove inactive validators, or through coordinated action by the validators, for example, by updating to patched clients.

2.4.4 - Reorganization

A blockchain reorganization (reorg) occurs when one chain unfinalized of blocks is replaced by another, potentially removing previously confirmed transactions. Reorgs can happen for several reasons:

- **Network Latency:** When blocks propagate slowly, validators may build on different chain tips
- **Late Block Arrivals:** Valid blocks that arrive after others have already built on an alternative
- **Validator Partitions:** Network splits causing validators to see different chain states

Most reorgs that happen on Ethereum are very shallow, for example only reorging the most recent block; it is rare to have deeper reorgs of many blocks. This means that for most applications waiting for a couple of blocks is enough to be confident of transaction inclusion.

2.4.5 - Economic incentives for Finalization

Ethereum's security and the irreversibility of transactions rely on a system where validators, who have a stake in the system, vote on blocks of transactions. When two-thirds of these validators agree on a block, it's finalized, making it extremely difficult to change or reverse.

This works because validators have a strong economic incentive to act honestly. If they try to cheat by voting for two conflicting blocks, they risk losing a significant portion of their staked Ethereum as a penalty. This is known as slashing, and makes it highly unlikely that a validator would attempt to disrupt the finality process, as the potential cost is too high.

2.4.6 - Implications for Users and Applications

The finality mechanism has several practical implications:

- **Tiered Security Models:** Applications can implement different security thresholds based on transaction value.
- **Finality Oracles:** Services that monitor and report finality status to dependent systems
- **Optimistic Operations:** Protocols that act on non-final data with fallback mechanisms
- **Cross-chain Bridges:** Systems that must wait for finality before releasing funds on other chains

---

2.5 - Future Directions

We observe how delayed finality creates suboptimal user experience: users must either accept the risk of unfinalized blocks (which could be reorganized), or wait for finality with delay of approximately 13 mins.

One approach that is being developed to mitigate such risk is to finalize transactions with almost zero-delay, (i.e. in a single slot). Ethereum refers to this emerging paradigm as Single Slot Finality (SSF). In this context, a key challenge is reaching consensus agreement across an extremely large set of validators (for Ethereum, approximately 1 million validators at the time of writing) in such a short time period. This is a non-trivial task as consensus complexity scales with the number of participants (albeit with great levels of robustness).

A straightforward approach that is gaining traction in academic discussions is the use of consensus committees[6], where subsets of validators are periodically selected to propose and finalize blocks on behalf of the full validator set. This technique is known in the Ethereum community as validator capping (or validator committees).

- **Validator capping** in PoS systems is non-trivial and requires careful consideration of the economic implications. When the protocol chooses a smaller subset of validators to vote on the validity of new blocks, it reduces economic security.
- **Economic Security** refers to the amount of stake locked in to secure a consensus decision—the total stake behind the validators attesting to a block's finality. With a smaller validator committee, economic security decreases, potentially making it easier for an attacker to corrupt or bribe the committee.

An approach for validator capping with maximum economic security under SSF paradigm has been recently proposed in the Ethereum ecosystem with the protocol Orbit SSF.

2.5.1 - Orbit: Validator capping with maximum economic security

Orbit SSF[7] is a research effort from Ethereum's community that proposes a protocol with three main goals:

1. **Validator capping:** Select a subset of validators to propose blocks, ensuring acceptable communication complexity for single slot finality.
2. **Solo staking viability:** Maintain a fair staking ecosystem where solo stakers can compete effectively with larger staking pools.
3. **High economic security:** Maximize the committee's stake to ensure strong resistance against attacks.

Orbit selects weighted committees based on validators' stakes - the higher the stake, the more likely a validator is to be selected. This approach ensures the active validator set maintains substantial economic security, providing stronger finality guarantees. The committee rotates gradually, allowing most validators to participate in block attestation.

At the core of Orbit are two components: the EIP-7251 (MaxEB)[8], which allows validators to stake more than 32 ETH, and consolidation incentives that encourage wealthy validators to concentrate their stake rather than fragment it. These mechanisms reduce the likelihood of small-stake committees while increasing the total stake held by the active validator set. MaxEB will be on Ethereum Mainnet in May 2025.

2.5.2 - Active Validator Set

The Orbit committee selection has two critical components:

1. **Committee selection:** Orbit defines two critical parameters - the stake of a validator and an inclusion threshold. Validators with stake equal to or greater than the threshold are guaranteed to participate in the committee. Validators with less stake have a smaller chance of being selected.
2. **Committee reward function:** Validators in the committee earn rewards proportional to their stake for securing the network and participating in consensus via attestations. Validators with stake below the threshold receive a base reward, while those with higher stake receive additional rewards based on their stake; the more stake above threshold they have, the higher the rewards.

2.5.3 - Validator Consolidation

In the Ethereum context, consolidation refers to the ability of entities controlling multiple 32 ETH validators to concentrate their stake into fewer validators with larger balances (with EIP-7251 allowing up to 2048 ETH per validator).

For Orbit, this means encouraging large stakers to operate fewer validators with higher stakes, providing optimal economic security without increasing the committee size in the single slot finality protocol. By incentivizing consolidation, Orbit maximizes the fraction of total system stake (D) that gets committed to the validator committee (D_a). The protocol achieves this by offering rewards to entities that consolidate their validators.

The following image visualizes this concept. It shows a set of validators, with each validator's size representing its stake. The fully consolidated scenario clearly demonstrates how this approach maximizes the stake in the selected committee, obtaining a total stake $D''_a > D'_a$

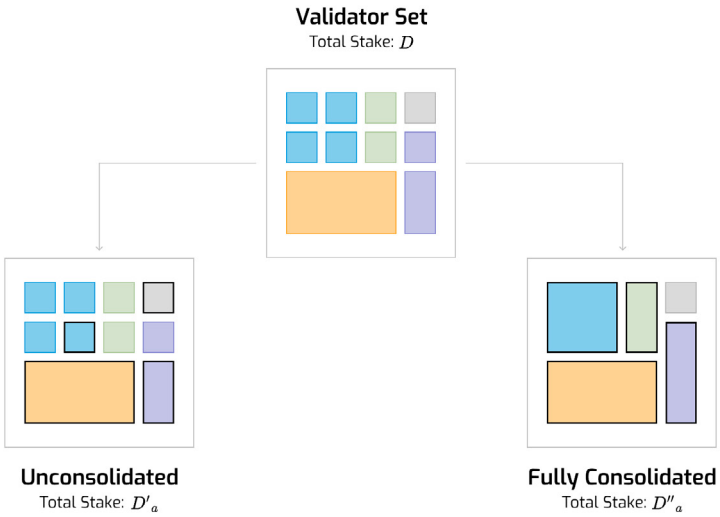


Figure 2.5.3: Validator consolidation

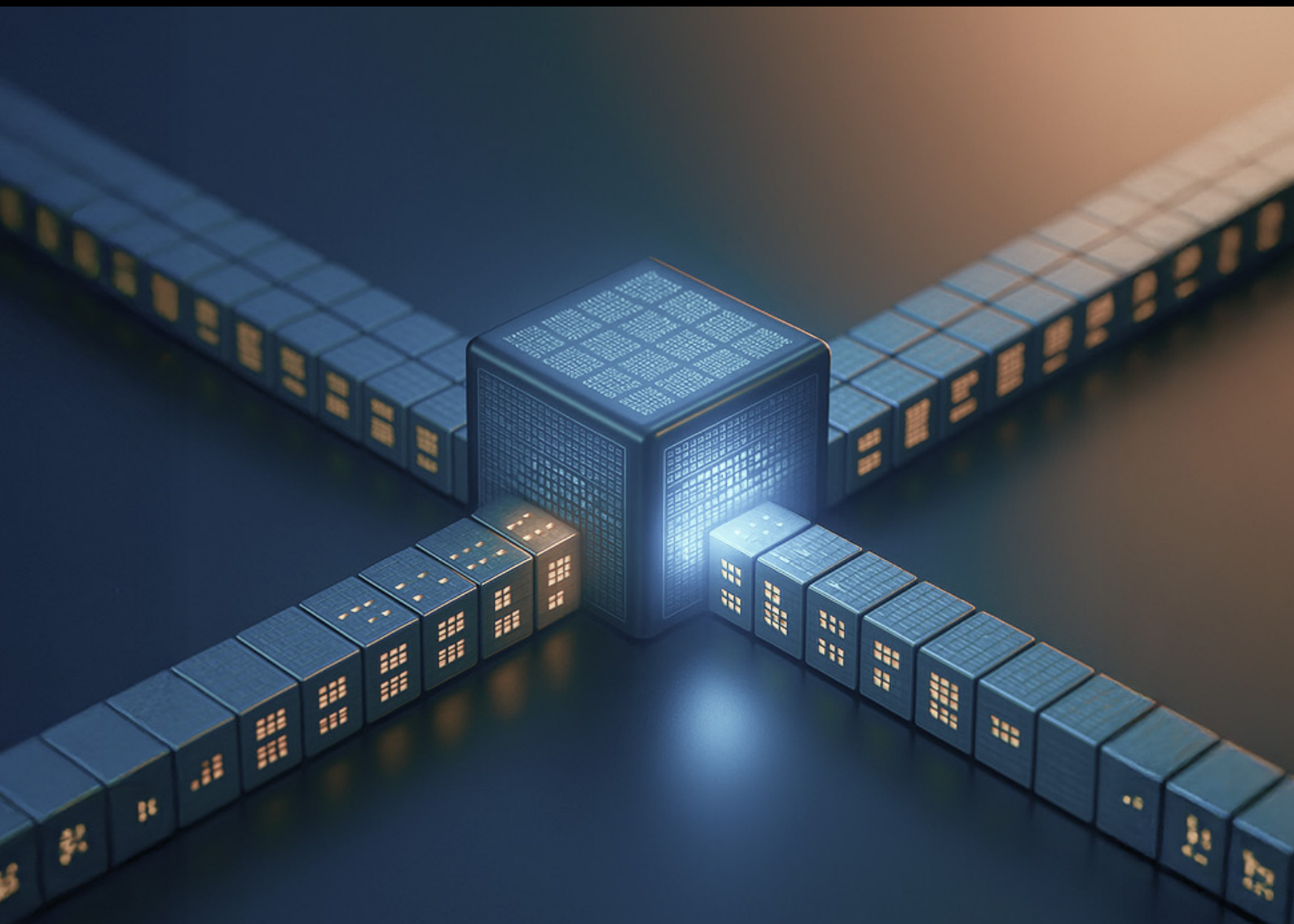
Committee selection in Orbit for a validator set with five entities (pink, green, purple, blue, and yellow). The committee (highlighted with red lines) includes 4 validators in both the unconsolidated and fully consolidated scenarios.

While full consolidation is desirable, it **risks excluding solo stakers**. This is evident in the example above, where the purple validator (a solo staker) has minimal chances of participating in the committee. Orbit addresses this through an incentive mechanism that balances both objectives by maximizing consolidation incentives up to a desired equilibrium. The incentives are divided into two categories:

1. **Collective consolidation incentives:** Rewards are proportional to the amount of stake deposited in the committee—the protocol compensates validators based on the economic security they provide.
2. **Individual consolidation incentives:** Rewards for consolidated entities become saturated once a certain consolidation threshold is reached in the system. Beyond this point, further consolidation becomes unprofitable, preserving opportunities for smaller validators.

03

Centralization and Censorship Concerns



3 - Centralization and Censorship Concerns

Proposer Builder Separation (PBS) introduces new considerations. If block building power is concentrated in a few major entities, this can introduce potential central points of failure. Furthermore, these large group of builders could also threaten network neutrality through "censorship" filtering of transactions.

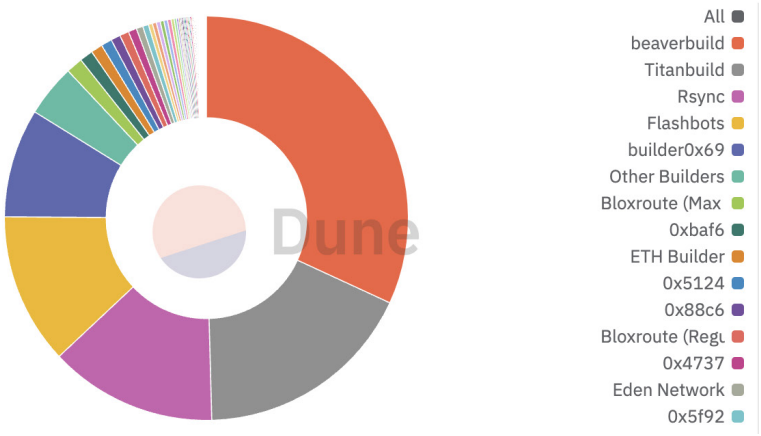


Figure 3a: Block builder ecosystem by daily success rate (%) (Source: Dune)

Censorship in PBS can occur at three levels - builders, relayers, and attesters. Based on this, it can be grouped into two broad categories:

- **Hard Censorship:** When **attesters** refuse to select blocks containing specific transactions, addresses, or contract interactions, regardless of their profitability. Since attesters have final say over block selection, their coordinated censorship can effectively block transactions even if some builders include them.
- **Soft Censorship:** When some **builders or relayers** filter out specific transactions but others still include them. This is the more common scenario today with non-private order flows, where OFAC-compliant builders and relayers reject transactions involving sanctioned addresses and contracts while non-compliant ones continue including them. Since most attesters don't censor, these transactions eventually get included but are subject to longer confirmation times or require higher fees.

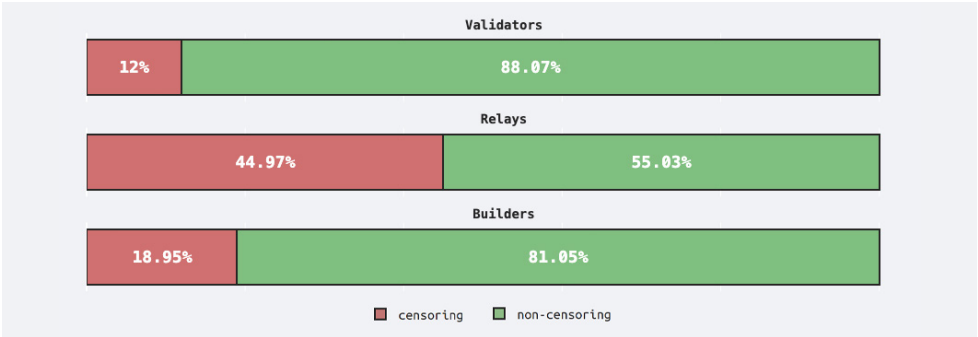


Figure 3b: Percentage of censoring vs non-censoring participants in PBS. (Source: Ethereum Censorship Dashboard)

3.1 - Impact on Users

The concerns about censorship are about their impacts to users access to the chain, which can undermine

network neutrality through the following methods:

- Basic transfers and withdrawals can be completely blocked
- User funds may become effectively frozen if interactions are censored
- Privacy-preserving protocols can become inaccessible
- A blockchain network neutrality is compromised when one jurisdiction's regulations are enforced globally via blockchain mechanisms
- Users in certain regions can also lose access

While centralization of trust and transaction filtering/censorship may not be favoured in Web3, directed private order flows with PBS mirrors current traditional setups where users can enter into contractual agreements with their service providers to mitigate counterparty risks, agree on robust risk management standards, and to apply an industry standard level of transaction filtering rules on suspected, undesirable transactions or parties. Therefore, this can achieve similar outcomes that the regulated financial industry are familiar with.

3.2 - Existing Solutions to Mitigate Censorship Concerns

3.2.1 - Decentralized Block Building via Trusted Execution Environments (TEEs)

TEEs represent a promising approach to decentralized block building to address concerns with PBS implementations today. TEEs are secure hardware enclaves that provide:

- **Confidential Computation:** Code and data remain encrypted during processing
- **Attestation:** Cryptographic proof that specific code is running unmodified
- **Isolation:** Protection from interference by the host system or operator
- **Integrity Verification:** Guarantees that the execution hasn't been tampered with

When applied to block building, TEEs enable a single logical builder to be operated by multiple independent entities without requiring trust between them. The process works as follows:

1. Block building logic is deployed within the TEE
2. Multiple operators run instances of the same TEE-protected builder
3. Each operator receives transactions and searcher bundles
4. The TEE ensures consistent execution, producing identical block proposals across all operators
5. Operators cannot modify the block building algorithm or extract sensitive information

This architecture creates a "trust-minimised" block builder where users don't need to trust individual operators, only the TEE technology and the code running within it.

3.2.1.1 - Benefits of TEEs

1. **Improved MEV Protection:** Decentralized builders can implement fair ordering policies that protect users from harmful MEV extraction:

    - Transaction ordering rules are transparent and consistently applied
    - No single entity can manipulate ordering for profit

- Frontrunning protection can be built into the builder's core logic
- MEV extraction can be redistributed to users or the protocol
- Builders can compete on fairness guarantees rather than MEV extraction capability

These protections are more credible when enforced by TEE technology rather than relying on trust in a centralized builder.

2. **Enhanced Censorship Resistance:** With multiple independent operators running the same builder:

   - Diverse operator policies support regulatory diversity
   - Users have multiple submission paths via different operators to reach the same builder
   - No single entity can unilaterally implement dominant exclusion policies

   This diversity significantly raises the transaction inclusiveness. From a financial regulatory view, there are multiple layers of safeguards to filter sanctioned or blacklisted transactions including PBS participants who adhere to regulatory lists of such transactions. Traceability of all transactions for investigations of related criminal parties remain possible in the event that undesirable transactions are validated.

3. **Reduced Trust Requirements for Searchers** who discover MEV opportunities benefit from decentralized building through:

   - Protection of proprietary strategies from builder theft
   - Consistent and fair bundle evaluation across operators
   - Reduced risk of builders stealing or front-running their opportunities
   - More predictable inclusion based on economic merit rather than relationships
   - Greater competition among builders leading to better revenue sharing

   This creates a more level playing field where searchers can focus on finding opportunities rather than managing builder relationships, and in turn, a fairer environment for users.

Case Study on TEEs
BuilderNet: A Collaborative Approach

BuilderNet[9] is an initiative to counteract the current centralizing trend of blockbuilding. In its first release, BuilderNet is operated jointly by Flashbots, Nethermind and BeaverBuild, BuilderNet demonstrates how competing entities can cooperate to create a more neutral building infrastructure through collaborative blockbuilding.

Key features of BuilderNet include:

- Multiple independent operators running the same builder logic
- TEE-based protection ensuring consistent execution
- Shared block building algorithms with transparent ordering rules
- Distributed infrastructure across different jurisdictions
- Collaborative governance with multiple stakeholders

This approach combines the efficiency of specialized block building with the censorship resistance of a distributed system. By bringing together multiple established builders, BuilderNet creates a more neutral alternative to single-entity builders while maintaining competitive block construction capabilities.

3.2.1.2 - Challenges and Limitations of TEEs

Despite its promise, decentralized block building faces several challenges:

- **TEE Security:** Reliance on hardware security that may have undiscovered vulnerabilities
- **Performance Tradeoffs:** Potential efficiency losses compared to fully optimized centralized builders
- **Coordination Overhead:** Increased complexity in managing multiple operators
- **Hardware Requirements:** Dependence on specific TEE-capable hardware
- **Update Management:** Complexity in coordinating software updates across operators

These challenges highlight that decentralized building remains an evolving technology with nascent adoption.

3.3 - Future Directions of Block Building Decentralization

The block building ecosystem continues to evolve toward greater decentralisation through:

- **Open-Source Building Algorithms:** Publicly available block building logic
- **Permissionless Operator Participation:** Allowing anyone to run builder instances
- **Cross-Builder Collaboration:** Standardised interfaces between different builders
- **Protocol-Level Support:** Consensus layer changes to better support decentralized building
- **Hybrid Approaches:** Combining centralized efficiency with decentralized security guarantees

As these technologies mature, they promise to create a more open, neutral, diverse and resilient block building ecosystem.

3.3.1 - Enshrined PBS (ePBS)

Enshrined Proposer-Builder Separation (ePBS)[10] is a proposed Ethereum protocol upgrade that would integrate PBS directly into the consensus layer. Currently being discussed by Ethereum researchers, ePBS aims to address key trust and centralisation concerns in the existing MEV-Boost architecture.

Key enhancements include:

- **Elimination of Trusted Relays:** The builder auction would be conducted directly within the protocol, removing relays as trusted intermediaries.
- **Protocol-Level Builder Registration:** Builders would need to operate validators and stake ETH, creating accountability and skin-in-the-game
- **Standardised Builder Interface:** The protocol would define standard APIs for builder-proposer communication.
- **Transparent Auction Mechanics:** Block auctions would follow protocol-defined rules visible to all participants.
- **Decentralized Builder Selection:** The protocol would manage builder selection and payment distribution.

These changes would:

- Reduce centralisation risk from trusted relays
- Enforce greater builder accountability through staking requirements
- Improve transparency in block markets
- Implement protocol-enforced fairness in block auctions
- Simplify infrastructure requirements for participants

While ePBS remains under active research and development, it represents a significant step toward a more trustless and decentralized block building ecosystem.

3.3.2 - Encrypted Mempools

Encrypted mempools offer a technological solution to transaction exclusion and frontrunning by encrypting transactions for a short period until they are on-chain. This accomplishes several things:

- Hiding transaction contents until inclusion using encryption
- Preventing builders from censoring based on addresses or contract interactions
- Requiring builders to commit to transaction inclusion before seeing contents
- Preventing frontrunning by forcing builders to commit to ordering on encrypted transactions

An early implementation of an encrypted mempool is Shutter[11], which uses threshold cryptography. This approach divides the decryption key for user transactions over a decentralized set of "Keypers", trusting that a 2/3 majority of the set are honest and will not collude to frontrun user transactions.

3.3.3 - Inclusion Lists

Fork-choice enforced Inclusion Lists (FOCIL)[12] is a research proposal under discussion, which aims to introduce a protocol-level anti-censorship mechanism that leverages the decentralized validator set to force the Block Proposer or Builder to include transactions from the public mempool.

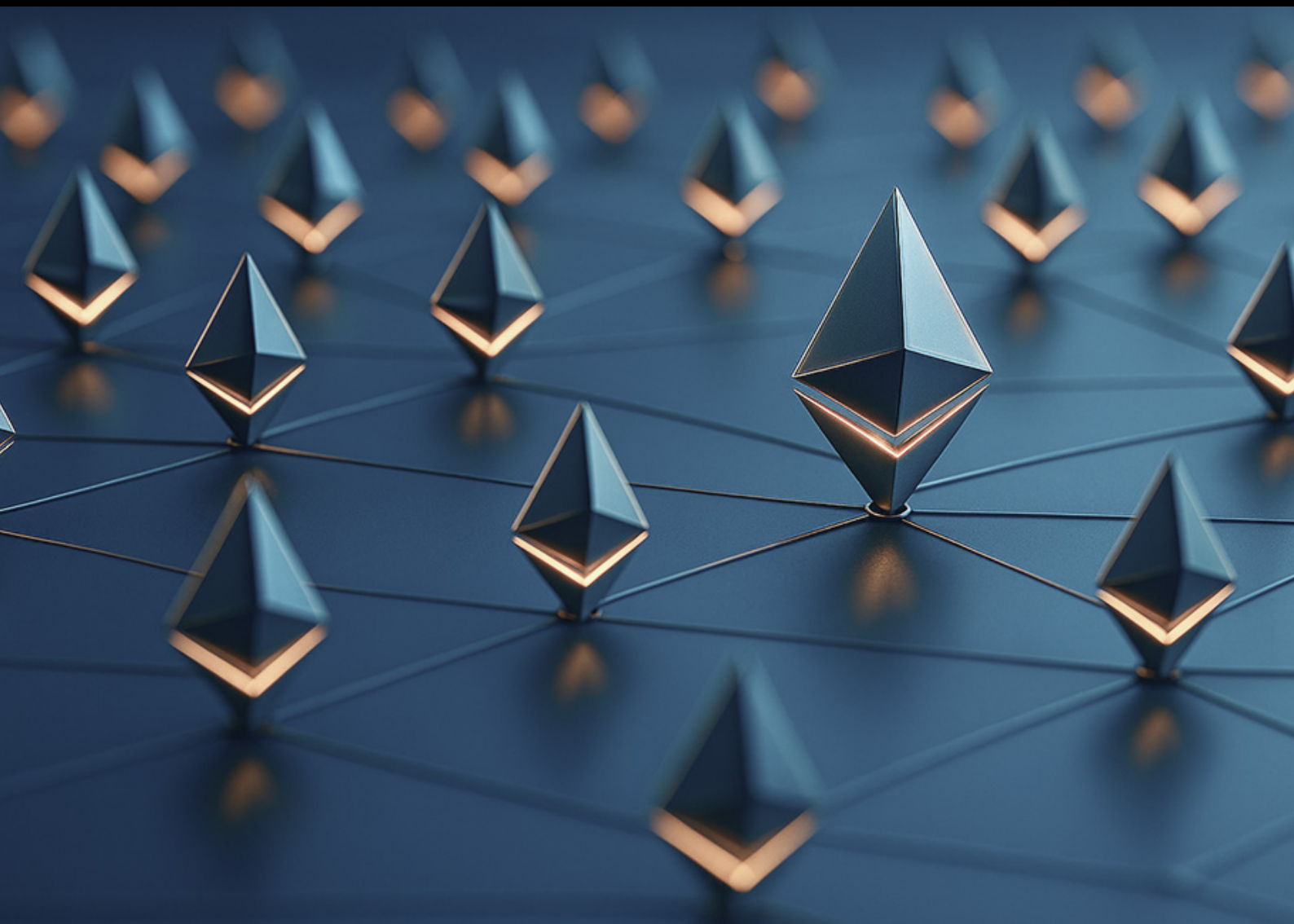
The main mechanism behind the FOCIL proposal relies on using the validator set and forming a committee composed of randomly selected validators responsible for constructing Inclusion Lists (ILs) that Block Builders must include in their block or risk their block being rejected by the attestors, who will verify that the final block proposed includes transactions from the Inclusion Lists. **However, Block Builders still retain some degree of control under the FOCIL proposal:**

- **Transaction Ordering:** Builders retain the ability to decide the sequence of all transactions included within the block.
- **Inclusion of Additional Transactions:** They are free to add other valid transactions from the public or private sources to fill the block.
- **Skipping Invalid Transactions:** If a transaction on the required list is invalid (e.g., due to insufficient funds or other errors), the builder must exclude it to ensure the overall block remains valid.
- **Conditional Inclusion (Block Full):** Builders may omit a required transaction, even if valid, if adding it would cause the block to exceed its capacity limits (like the gas limit).

How FOCIL details can lead to similar regulatory outcomes should be part of cross-industry discussions to further public chain uses.

04

Centralization and Censorship Concerns on Layer 2



4 - Centralization and Censorship Concerns on Layer 2

4.1 - Overview of Layer 2

Layer 2 (L2)[13] solutions are chains that (in theory) inherit Ethereum's security to scale the amount of blockspace.

Unlike L1 where multiple block builders compete and block proposers/validators are randomly chosen from the entire validator set, L2s currently operate with a single or few entity(ies) known as a sequencer with complete control over transaction inclusion, responsible for:

- Receiving user transactions
- Determining transaction ordering
- Batching transactions for L1 submission
- Publishing state updates and validity proofs

Even if a transaction would be profitable to include, the sequencer can reject it for policy or compliance reasons. For example, the sequencer can:

- Selectively exclude transactions from specific addresses
- Censor interactions with particular contracts
- Implement jurisdiction-specific compliance policies
- Prioritize transactions based on non-economic factors
- Completely block certain users from network access

Many L2 solutions currently operate with the following characteristics:

- **Upgradeable Contracts:** Admin keys can modify protocol rules or pause operations
- **Multisig Governance:** Small groups control critical protocol parameters
- **Missing Forced Inclusion:** Some L2s lack fully implemented bypass mechanisms
- **Unproven Proof Systems:** Novel cryptographic systems without long-term security validation
- **Sequencer Centralisation:** Single entities control transaction ordering
- **Limited Exit Windows:** Restricted timeframes for challenging invalid state transitions
- **Incomplete Fault Proofs**: Systems where invalid state transitions cannot yet be challenged

The current state of L2 security can be viewed on L2Beat[14].

From a regulated financial industry standpoint, the role of centralized sequencers on L2 bears great resemblance with those of traditional financial market infrastructures, that can be licensed and governed to ensure financial market integrity and resilience while benefiting from the security of Layer 1 Ethereum.

Therefore, a Layer 1-2 architecture for example, a zk-rollup Layer 2 on Ethereum as the Layer 1 could present promising potentials for the tokenised financial market, optimising ease of accessibility, transaction scalability, cost-effectiveness, speed and converging compliance needs.

4.2 - Existing Mitigating Solutions

4.2.1 - Forced Inclusion Mechanisms

To mitigate L2 sequencer censorship, many L2 designs incorporate forced inclusion mechanisms that allow users to bypass the sequencer after a delay:

- **Direct L1 Submission:** Users can submit transactions directly to the L1 contract governing the L2
- **Inclusion Timeout:** After a predefined period (typically hours or days), the L2 protocol forces sequencers to process these L1-submitted transactions.
- **Canonical Ordering Rules:** The protocol defines how these forced transactions must be ordered relative to sequencer-submitted transactions.
- **Censorship Evidence:** Some designs allow users to provide proof of sequencer censorship to accelerate inclusion.

While these mechanisms provide an eventual guarantee of transaction inclusion, they come with significant drawbacks:

- Long waiting periods (often 24+ hours)
- Higher costs due to L1 gas fees
- Potential for transaction staleness
- Complex user experience requiring L1 interaction
- Possible MEV extraction during the forced inclusion

These limitations make forced inclusion a last-resort exception option rather than a practical daily alternative to sequencer submission. The good news is that these drawbacks are actively being addressed by the Ethereum development community today through new and upcoming upgrades.

05

Functional Outcomes Meeting Regulatory Goals

5 - Functional Outcomes Meeting Regulatory Goals

The convergence of finance and digital assets should be a question of "when" and not "if". The advances in blockchain technologies are creating enhanced capabilities with new compliance capabilities and security features that converge with other momenta of greater on-chain activities with new operating models – led by asset managers, digital money, tokenized funds and collateral management – amidst regulatory expectations and a more relaxed operating environment.

From a global perspective, US agencies and the public sector have significantly pivoted their stance to encourage blockchain-based finance including public chains and stablecoin for capital market and retail uses1. The EU is actively exploring public-permissioned blockchains for tokenised financial instruments. Other jurisdictions are or would be consulting on prudential treatment requirements for cryptoassets – that include tokenised financial instruments issued on public chains – in preparation to implement such rules by 1 Jan 2026.

Between all these forces is a balance point that the market is seeking – an equilibrium between public chains for innovation, inclusiveness and cost-effective growth, with concerns for necessary market and consumer protection which if unresolved, could see punitive balance sheet treatment for banks.

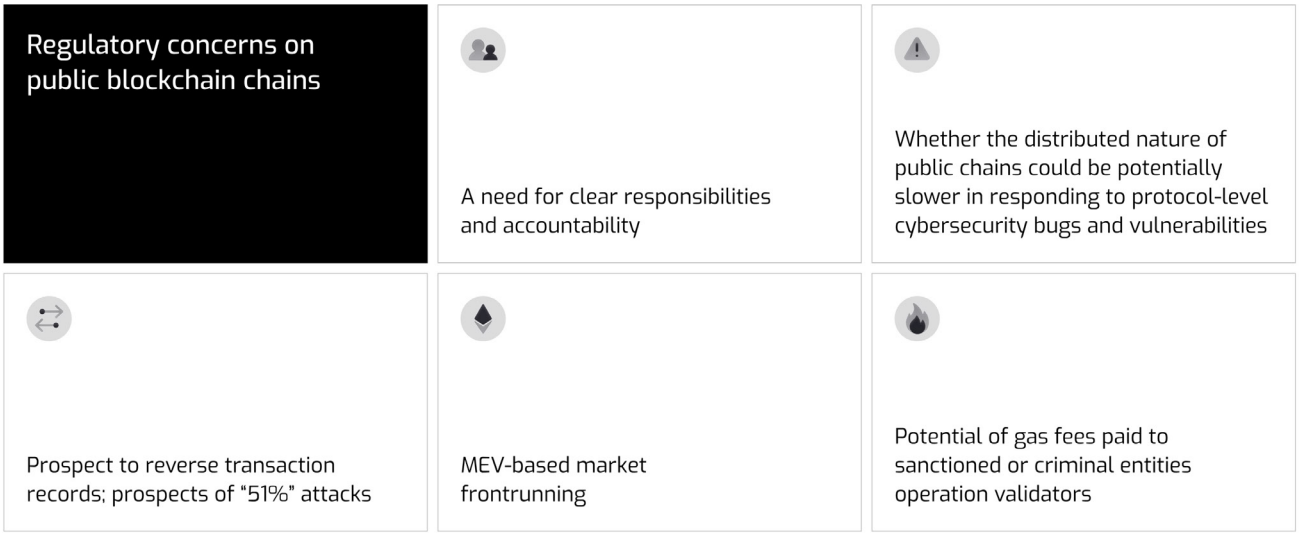


Figure 5a: Select regulatory concerns on public blockchain chains

Industry debates have centered on three main approaches: private blockchains, which address regulatory concerns but fragment liquidity and reduce accessibility; public blockchains, which offer cost-effectiveness and better liquidity formation but require alignment with regulatory goals; and public-permissioned systems, which represent a compromise between these competing priorities.

Establishing consensus on acceptable standards is crucial for the financial industry's advancement towards digital assets, unlocking new growth and operational methods. Furthermore, it offers an opportunity to modernize outdated sequential workflows that have persisted since the introduction of computers following Wall Street's "Paperwork Crisis" in the 1960s[15].

Blockchain	Pros	Cons
Public Chain	• Cost-effective • Fair and equitable access • Better liquidity formation and product access • Promote broad-base innovation	• Unidentifiable validators • Concerns about probabilistic settlement • Robustness and "51%" Attack • Market abuse/front running • Lack of on-chain privacy[16]
Private Chain	• Identified validators • Readily meets regulatory goals • No front-running • Could have technical confidentiality • Product access • Promote broad-base innovation	• High investment hurdle • Access only for collaborators and clients • Anti-competitive concerns • Dominant partner-driven innovation • Fragments product and liquidity
Public-Permissioned chain / Layer 1-2 architecture or permissioned via smart contracts	• More cost effective than private chain but less than public chain • Able to meet regulatory safety and soundness goals with more effort • Can still facilitate liquidity formation and product access • Availability of privacy-preserving L2 platforms	• Security inherited from Layer 1 (based on a L1-2 architecture) • More complex permissioning (based on a smart-contract architecture) • L2 transaction confidentiality does not extend to underlying L1 chain • More maintenance than a public chain-only setup

Table 5b: Comparative analysis of public, private and public-permissioned blockchains

Any comparative analysis of public, private and public-permissioned blockchains would readily highlight these trade-offs. Probing further would uncover different anchoring paradigms for each type of chain and how they could align with current regulatory frameworks. Importantly, it is not about which is the most optimal blockchain, but rather about how the chains can effectively meet adoption, cost-effectiveness, safety and soundness goals.

Traditional financial regulatory frameworks typically require centralized entities and organizational-based controls to achieve their goals. However, blockchain networks, especially public ones, can achieve similar protective outcomes, albeit typically through technological and behavioral means rather than design or organizational-based ones.

These different basis, encapsulated as a "design versus functional outcomes" contrast, can challenge the evaluating public blockchains' effectiveness in satisfying regulatory objectives.

Exploring this question requires the considerations of such blockchain attributes that the earlier sections have highlighted, and how they align to regulated outcomes.

5.1 – Outcomes versus Design Approach

The technical innovations in public blockchain networks described in previous chapters represent significant advancements in blockchain infrastructure with possibilities to also act as mitigants to some regulatory concerns about public chains.

A focus on similar regulatory outcomes despite different methods in achieving these outcomes, can ensure adaptability between technological advances with safety and soundness. The following table summarises how such a focus on outcomes can effectively align with governance goals.

A) Transaction Processing on Ethereum
Blockchain Attribute: Proposer-Builder Separation
Description • Separation of responsibilities between block builders and proposers • Block proposers are relatively concentrated while validators are widely decentralized • MEV-Boost auction to encourage competition between proposers for optimal revenue **Functional Outcomes** • Separation of responsibilities and duties • Market-based competition • Market competition begets operational resilience. Inadequate validators or proposers are quickly replaced through natural market competition **Alignment with Safety & Soundness Goals** Mitigants to collusion and conflict of interests in the open access environment by aligning behaviors via economic incentives **Design-based Equivalent** Designation of specific parties and definition of roles to separate scope of work, with regulatory reporting and fines as monitoring and penalty respectively
Blockchain Attribute: Encrypted Mempool
Description Encrypted Mempool prevent frontrunning by encrypting transactions until they are included on-chain **Functional Outcomes** Prevents frontrunning and MEV-Attacks like Sandwich Attacks **Alignment with Safety & Soundness Goals** Prevents market abuse and frontrunning **Design-based Equivalent** After the fact monitoring and reporting

Blockchain Attribute: Direct Private Order Flow and MEV Boost

Description
- Wallet configurable remote procedure call endpoints can route transactions through specific channels
- Transactions are privately routed to builders' private mempool, bypassing Ethereum's public mempool
- Specialized block builders competitively assemble transactions
- Relayers validate blocks submitted by builders
- Block proposers/validators select most profitable blocks through MEV-Boost protocol to finalise transactions on-chain
- Finalised blocks are broadcasted into the open chain for record purposes

Functional Outcomes
- Each participant in the transaction, from user wallet to PRC provider, builder, relayers and validators, are identifiable
- Transactions remain traceable from submission through to block finalization
- Transactions are written public chain for transparency
- Services are available to ensure transparency by disclosing the transactions they have routed to reinforce end-to-end responsibility
- A leading group of builders are already voluntarily adhering to filtering of transactions based on OFAC lists

Alignment with Safety & Soundness Goals
- Mitigants to concerns that validators are unidentifiable and risks if validators are state-actors or organised crime bypassing AML and sanctions
- Possibilities for the industry to engage with select participants to agree on a set of practical robust risk management standard that can satisfy regulatory goals for proportionate resilience and robustness
- Behavior to uphold goodness is already present
- Allows open market competitiveness to continue without unnecessary burden while ensuring core safety outcomes

Blockchain Attribute: Inclusion List

Description
Inclusion list leverage the more decentralized validator set to force the builder set to include transactions. This is also governed by transparent implementation rules

Functional Outcomes
- Natural check-and-balance that leverages mathematical robustness for consensus from a diverse set of participants
- An inherent check against manipulation
- Ethereum's Liveness criteria ensures that every valid submitted transaction would eventually make it on-chain

Alignment with Safety & Soundness Goals
- Financial inclusion, free competition and prevention of unfair and inequitable derisking practices.
- Anti-market manipulation

Design-based Equivalent
- Gather evidence of unfair derisking, industry discussions, write rules, consult and implement; monitor for effectiveness

B) Transaction Finality on Ethereum

Blockchain Attribute: Settlement Finality on Ethereum

Description
- Current ~13 minutes finality after which blocks cannot be reverted without burning 33% of total staked ether
- "Inactivity Leaks" that allow the chain to continue even when 1/3 validators are offline

Functional Outcomes
Prospect of transaction reversal after finalization is very low, policed by significant economic penalties

Alignment with Safety & Soundness Goals
- Market integrity
- On-chain record trustworthiness

Design-based Equivalent
Centralized entity with rulebook to define point of finality (delivery-versus-payment) and scope for transaction reversals

Blockchain Attribute: Finality Risks
- Transaction Reversals
- Reorganization of blocks
- Finality Delay
- "51%" Attack

Description
Amass enough staked ether for "51%" attack that will require off-chain social coordination for the scale of capital involved

Functional Outcomes
- Active and watchful community for mature chains like Ethereum to respond and neuter a developing attack
- Very expensive economic loss of staked ether
- Makes it highly unprofitable for the attacker

Alignment with Safety & Soundness Goals
Goals of resilience, robustness, ownership and fiduciary duties albeit not mandated

Design-based Equivalent
- Formal fiduciary duties, roles and responsibilities
- Centralized entities and reporting procedures

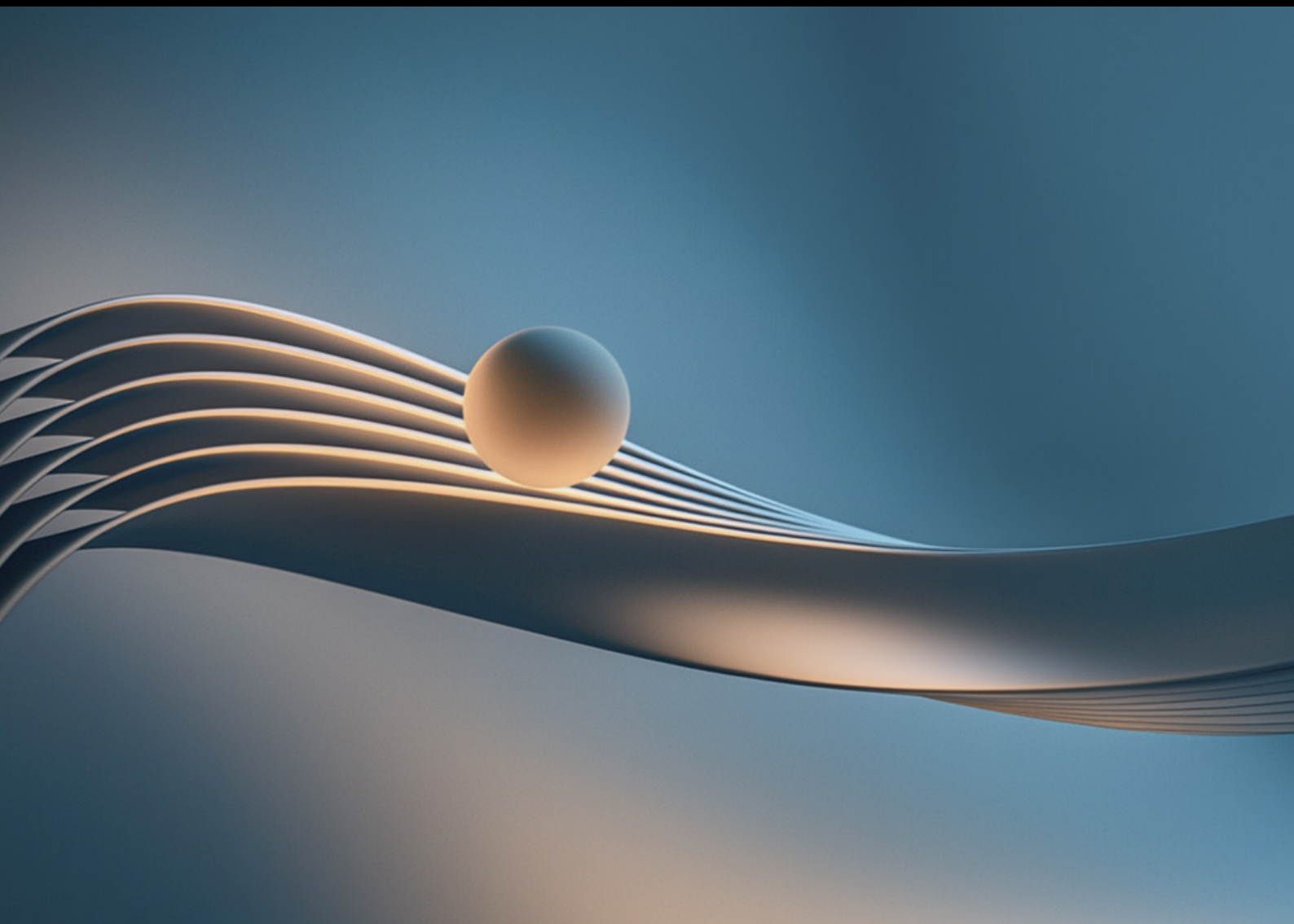
C) Transaction Processing on Layer 2
Blockchain Attribute: Single Sequencer
Description Single sequencer, and concentration of trust in this single entity **Functional Outcomes** Organically fits traditional regulatory design to have a designated, accountable central entity. If the Layer 2 is a private layer, this attribute can be preserved **Alignment with Safety & Soundness Goals** • Centralized trust • Ability to apply industry standard level of transaction filtering on suspected, undesirable transactions or parties **Design-based Equivalent** • Central entity that can be licensed and held accountable • Contractual agreements to mitigate counterparty risks and agree on robust risk management standards

Table 5.1: Blockchain Functional Outcome-Safety Goals-Design Equivalent

06

Conclusion

Bridging the Two Worlds



6 – Bridging the Two Worlds

Public chains represent a cost-effective, innovative and readily accessible choice of a digital asset infrastructure for the regulated financial and banking industry. Layer 1-2 constructions can balance decentralized operations with a higher degree of accountability, and feature other benefits like privacy with appropriate transparency, operational resilience and scalability. Their technical innovations and features, as highlighted in this whitepaper and exemplified by Ethereum public chain, are not incompatible with regulatory objectives. They achieve these objectives instead, through a different route that uses technological and economical means.

By focusing on blockchain's attributes for functional outcomes to meet safety and soundness goals rather than seeking specific design requirements, practical paths can be found to enable responsible innovation that maintains the essential protections to ensure financial stability, trust and integrity that benefits all.

A way forward requires collaboration between the two worlds and multiple stakeholders to develop shared understanding. Through shared understanding, alignment with regulatory goals can be forged, which can then lead to practical implementable frameworks that align innovation, technology outcomes and current regulatory design principles.

One step would be to develop key functional mappings that can show how public blockchain features – both current and being developed – can create outcomes that would satisfy regulatory requirements with this paper as a catalyst. Proportionate complementary controls can then be considered where blockchain mechanisms do not fully satisfy regulatory needs. Financial industry associations and blockchain foundations can play leading roles in these endeavours. Regulators can open their private-public sector sandbox environments to develop acceptable standards that facilitate the adoption of mature public chains and to opine on how on-chain characteristics can meet regulatory conditions and criteria to facilitate adoption and minimise unnecessary costs in the industry.

With these and other steps, the industry can progress past the debates on public versus private chains, liquidity and product fragmentation, and move towards a future of digital finance where blockchain technology readily enhances the financial system's resilience, efficiency and inclusivity with new robust moats against risks.

07

Glossary of Terms

Ethereum Transaction Lifecycle and Compliance

Attesters – Validators responsible for confirming that proposed blocks follow consensus rules. They "vote" on the correct chain and help finalise blocks.

Auction (Block) – A process in which multiple block builders compete to construct and propose the most profitable block to validators.

Base Fee – A dynamically adjusted network fee that is burned rather than paid to block proposers. It regulates Ethereum's gas pricing mechanism.

Beneficiary (Coinbase Address) – The Ethereum address designated to receive block rewards and transaction fees for a proposed block.

Block Builder – An entity responsible for selecting, ordering, and structuring transactions into a block before submission to a proposer.

Block Inclusion – The process by which transactions move from the mempool to being part of a confirmed block.

Block Proposer – The validator selected to propose a new block during a slot in Ethereum's proof-of-stake consensus.

Censorship – The act of preventing or delaying certain transactions from being included in blocks due to compliance, regulatory, or centralisation risks.

Centralized Sequencer – A single entity responsible for ordering and bundling transactions on Layer 2 networks.

Consensus Layer – The part of the Ethereum protocol responsible for ensuring agreement on the blockchain's state among validators.

Data (Transaction Field) – Optional information included in transactions, often used for smart contract interactions.

Decentralized Block Building – A model where multiple independent participants contribute to block construction to reduce centralisation risks.

Decentralized Sequencer – A sequencing model where multiple independent nodes order Layer 2 transactions instead of a single centralized operator.

ePBS (Enshrined Proposer-Builder Separation) – A proposed Ethereum upgrade integrating proposer-builder separation directly into the consensus protocol to eliminate the need for trusted third parties.

Encrypted Mempool – A transaction pool where transaction contents are encrypted until block inclusion to prevent frontrunning and censorship.

Ethereum Validators – Network participants who stake at least 32 ETH to participate in transaction validation and block proposal.

Finality – The state in which a block is confirmed and cannot be reverted unless a significant portion of validators are slashed.

Frontrunning – An MEV strategy where a trader or bot submits transactions ahead of a user's to exploit price changes.

Gas Parameters – Settings in a transaction that define gas limits, priority fees, and max fees per gas.

Gossip Network – A peer-to-peer mechanism used by Ethereum nodes to propagate transactions and blocks across the network.

Inclusion List – A protocol proposal requiring validators to include specified transactions in blocks, reducing censorship risk.

Intents – User-defined desired outcomes for blockchain interactions, leaving execution details flexible for solvers to determine the best path.

Layer 2 (L2) Solutions – Networks built on Ethereum that aim to increase scalability while inheriting Ethereum's security.

Liquidation Backrunning – An MEV strategy where bots profit by quickly executing liquidations of undercollateralised positions.

Mempool – A temporary storage area where pending transactions wait before being included in a block.

MEV (Maximal Extractable Value) – Profit that can be extracted by block producers through optimized transaction ordering.

Nonce – A sequential number assigned to each transaction from an account to prevent replay attacks.

OFAC Compliance – Adherence to sanctions lists issued by the Office of Foreign Assets Control, which can impact transaction inclusion by major block builders.

PBS (Proposer-Builder Separation) – A mechanism that divides responsibilities between block proposers and block builders to optimize transaction ordering and MEV capture.

Priority Fee – An optional tip paid by users to incentivise faster transaction inclusion by block proposers.

08

Reference Sources

1. Flashbots. “Flashbots Protect Overview.” https://docs.flashbots.net/flashbots-protect/overview
2. CoW Protocol. “MEV Blocker.” https://cow.fi/mev-blocker
3. bloXroute. “Protect RPCs.” https://docs.bloxroute.com/bsc-and-eth/protect-rpcs
4. Titan Builder. https://www.titanbuilder.xyz/
5. Beaver Build. https://beaverbuild.org/
6. Daian, P., et al. “Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges.” ACM, 2019. https://dl.acm.org/doi/abs/10.1145/3318041.3355458
7. Ethereum Research. “Orbit SSF: Solo Staking Friendly Validator Set Management for SSF.” https://ethresear.ch/t/orbit-ssf-solo-staking-friendly-validator-set-management-for-ssf/19928
8. Ethereum Improvement Proposals. “EIP-7251: Single-Slot Finality.” https://eips.ethereum.org/EIPS/eip-7251
9. BuilderNet. https://buildernet.org/

10. Ethereum Improvement Proposals. “EIP-7732: Wildcard Precompile Registration.” https://eips.ethereum.org/EIPS/eip-7732

11. Gnosis Chain. “Shutter: High-Level Specifications.” https://github.com/gnosischain/specs/blob/master/shutter/high-level.md

12. Ethereum Improvement Proposals. “EIP-7805: Secret Single Leader Election for Block Proposers.” https://eips.ethereum.org/EIPS/eip-7805

13. Ethereum Foundation. “Layer 2.” https://ethereum.org/en/layer-2/

14. L2BEAT. “Layer 2 Ethereum Scaling Solutions.” https://l2beat.com/

15. Lexology. “Digital Asset Regulation Overview.” https://www.lexology.com/library/detail.aspx?g=1f852fff-a3f8-475b-96c2-6badec65358a

16. Bank for International Settlements. “Working Paper No. 44.” https://www.bis.org/bcbs/publ/wp44.pdf

General References

- White House. “Strengthening American Leadership in Digital Financial Technology.” Presidential Action, January 2025. https://www.whitehouse.gov/presidential-actions/2025/01/strengthening-american-leadership-in-digital-financial-technology/

- European Union. “Digital Finance Package.” Publications Office of the European Union, 2024. https://op.europa.eu/en/publication-detail/-/publication/cab54e8e-ad3b-11ef-acb1-01aa75ed71a1/language-en

- Bank for International Settlements. “Basel Committee on Banking Supervision Publications No. D579.” https://www.bis.org/bcbs/publ/d579.htm

- Wood, G. “Ethereum: A Secure Decentralized Generalized Transaction Ledger.” Ethereum Project Yellow Paper, 2014. https://ethereum.github.io/yellowpaper/paper.pdf

- Beiko, T., et al. “Ethereum 2.0 Book: Capella Edition.” https://eth2book.info/capella/

09

About us

Nethermind

Nethermind is a blockchain research and software engineering company empowering enterprises and developers worldwide to work with and build on decentralized systems. Our work touches every part of the blockchain ecosystem, from fundamental cryptography research through security to application-layer protocol development. As a core contributor to the development of Ethereum and active builders of the Starknet ecosystem, we leverage our expertise to provide strategic support to our institutional and enterprise partners in blockchain, digital assets, and DeFi.

Deutsche Bank

Deutsche Bank provides retail and private banking, corporate and transaction banking, lending, asset and wealth management products and services as well as focused investment banking to private individuals, small and medium-sized companies, corporations, governments and institutional investors. Deutsche Bank is the leading bank in Germany with strong European roots and a global network.

Authors

Boon-Hiong Chan
Asia Pacific Head of Securities & Technology Advocacy and Industry Applied Innovation Lead, Deutsche Bank, Singapore

Jaelynn Lee
Digital Product Manager, Deutsche Bank, Singapore

Marc Harvey-Hill
Ethereum Core Developer, Nethermind
marc.harvey-hill@nethermind.io

Swapnil Raj
Head of Innovation, Nethermind
swp@nethermind.io

Aikaterini-Panagiota Stouka
Blockchain Researcher, Nethermind
aikaterini-panagiota@nethermind.io

Stefano De Angelis
Consensus Researcher, Nethermind
stefano@nethermind.io

Delane Foo
APAC Regional Managing Director, Nethermind
delane.foo@nethermind.io

Tomasz Kurowski
Head of DeFi & Enterprise Business, Nethermind
tomasz.kurowski@nethermind.io

Acknowledgements

The authors extend their sincere appreciation to Julia Laganowska, Lesa Moné, and Melannie Manrique, for their significant contributions to this work.

Non-Investment Disclaimer

This whitepaper has been prepared for the general information and understanding of the readers. No representation or warranty, express or implied, is given by Deutsche Bank and/or Nethermind as to the quality, accuracy, reliability, adequacy, or completeness of any of the information, material or opinions contained in the above whitepaper. Deutsche Bank and Nethermind expressly disclaim any liability for errors or omissions in such information and material.

This whitepaper is meant for informational purposes only. It is not meant to serve as investment advice. Both past performance and yield may not be a reliable guide to future performance. All information provided by Deutsche Bank and Nethermind is impersonal and not tailored to any subscriber's needs.

Nethermind is not a securities broker/dealer, cryptoasset broker/dealer, investment adviser, commodity trading advisor, or financial adviser, analyst, or planner of any kind. Nethermind is neither licensed nor qualified to provide investment or trading advice, and Nethermind does not explicitly or implicitly recommend or suggest an investment strategy of any kind. Readers should conduct their own research and consult an independent financial, tax or legal advisor before making any investment decision.

Any individual who chooses to invest in cryptoassets should do so with caution. Investing in cryptoassets is speculative and carries a high degree of risk; you may lose some or all of the money that is invested, and if you engage in margin transactions, your loss may exceed the amount invested.

No third party should rely on this whitepaper in any way, including without limitation as financial, investment, tax, regulatory, legal, or other advice, or interpret this whitepaper as any form of recommendation.

Let's build a compliant and innovative future **together.**

nethermind.io

db.com