BLOCKDAEMON

WHITEPAPER

Monad

A Guide for Institutions

Table of Contents

1 Introduction

Monad is a high-performance, EVM-compatible Layer 1 blockchain designed to address Ethereum's scalability limitations while maintaining full compatibility with existing smart contracts, tooling, and developer workflows. Developed by **Category Labs** and supported by the **Monad Foundation**, the network introduces low-latency consensus, parallel execution, and an optimized state database to deliver speed and reliability without compromising decentralization. Monad's founders are ex-high-frequency trading (HFT) quant engineers.

Monad targets 400-millisecond block times and two-round finality in approximately 800 milliseconds, achieving near-instant confirmation under normal network conditions. The protocol is engineered to support tens of thousands of transactions per second, depending on workload and gas composition, placing it among the most performant EVM-compatible Layer 1 networks currently in development.

The system's efficiency is driven by a coordinated technology stack:

- MonadBFT, a HotStuff-derived consensus protocol with tail-fork resistance and fast recovery mechanisms, introduced by **Category Labs**.
- Parallel execution, allowing transactions to process concurrently across CPU cores.
- **MonadDB**, a purpose-built storage engine optimized for SSDs and asynchronous reads and writes.

Monad's design makes it particularly suited for applications requiring consistent low latency and high throughput, including institutional DeFi, real-time trading, gaming, and tokenized asset markets.

Backed by major investors such as **Paradigm** and **Dragonfly Capital**, Monad's anticipated mainnet launch is Q4 2025.
This report provides a structured overview of Monad's architecture, consensus design, validator operations, and staking model. It also outlines Blockdaemon's institutional support for Monad, covering infrastructure, RPC connectivity, staking analytics, and wallet integration for institutions.

2 Monad Staking

Monad's consensus and leader rotation are governed by stake. Validators lock MON, the network's native token, to participate in consensus, while token holders can delegate additional stake to them. The total amount staked determines a validator's voting weight and how frequently it is selected to propose blocks. This system matches economic participation with operational responsibility, ensuring that healthy network performance and security are directly incentivized.

2.1 MonadBFT

At the centre of Monad's proof-of-stake architecture is **MonadBFT**, a consensus protocol built on the HotStuff lineage, designed to achieve speed, fairness, and deterministic finality at scale.

Every **400 milliseconds**, one validator becomes the leader and proposes a block. The remaining validators verify the proposal and send a single vote to the next leader in sequence. Those votes are aggregated into a **Quorum Certificate (QC)**, a compact cryptographic proof that a supermajority has agreed, which the next leader includes in its proposal.

Finality is both fast and predictable. Under ordinary conditions, a block becomes "voted" after one round and final after two rounds, totaling roughly **800 milliseconds**. Validators can speculatively execute blocks as soon as a quorum forms, and only a provable double-sign (a slashable offense) can revert results. Because each validator sends only one vote per round, communication remains linear, allowing Monad to scale efficiently without the quadratic message overhead that limits earlier BFT systems.

MonadBFT also includes **tail-fork resistance**, which ensures that valid blocks are not abandoned when a leader misses its slot. If a leader fails to propose, the next leader must repropose the last well-voted block unless it can present a **No-Endorsement Certificate** proving that a quorum never saw it. This keeps fairness and liveness even during partial outages.

Further **Fast Recovery** improvements allow validators to send votes to both the current and next leaders. Timeout messages include the latest QC and "tip" vote, enabling a new QC to form immediately when two-thirds of validators agree. This allows the protocol to recover from a missed round in a single view rather than multiple, keeping block production continuous.

For block propagation, Monad uses **RaptorCast**, an erasure-coded broadcast system that splits each block into small chunks distributed proportionally by validator stake. Each chunk is fanned out twice through the network, enabling full block reconstruction within two hops, even if up to one-third of stake is offline. This design maintains sub-second finality without overwhelming bandwidth capacity.

2.1.1 Transaction Lifecycle

When a user submits a transaction, it first reaches a Monad RPC node, the network's interface for transaction and state access. Instead of broadcasting to all validators, the RPC routes the transaction directly to the next three scheduled leaders, minimizing redundant traffic.
Each leader stores pending transactions in its local mempool until its assigned slot arrives. Transactions are ordered, typically by highest fee-per-gas, and assembled into a block proposal. Using RaptorCast, the proposal is distributed across the validator network for verification and voting. Once a Quorum Certificate is formed, the next leader carries that proof forward, finalizing the prior block. Within roughly 800 milliseconds, the transaction achieves permanent settlement.

2 Monad Staking

2.2 Monad Validators & Operations

Validators are the operational core of Monad's network. They produce blocks, verify transactions, and uphold consensus integrity. Participation is permissionless but performance-sensitive. Running a validator requires the ability to maintain high throughput and low latency within Monad's 400 millisecond block intervals.

Each validator's total stake, its self-bonded MON plus any delegated tokens, determines its voting power and how frequently it serves as leader. The leader schedule is computed deterministically at the start of each epoch, allowing all participants to derive the same sequence independently.

Validators must maintain continuous uptime, precise time synchronization, and stable network connectivity to ensure smooth block progression. The network currently operates with approximately 186 validators on testnet, scaling to 200 at mainnet launch.

2.2.1 Block Rewards

Each block currently offers 25 MON in rewards, automatically distributed among a validator's delegators according to their share of stake, minus the validator's commission (0 - 100%). Validators that remain online and sign consistently maximize returns, while inactivity or protocol faults (such as double-signing) lead to slashing or removal from the active set.

2.3 Monad Network Constants

Validators are the operational core of Monad's network. They produce blocks, verify transactions, and uphold consensus integrity. Participation is permissionless but performance-sensitive. Running a validator requires the ability to maintain high throughput and low latency within Monad's 400 millisecond block intervals.

Each validator's total stake, its self-bonded MON plus any delegated tokens, determines its voting power and how frequently it serves as leader. The leader schedule is computed deterministically at the start of each epoch, allowing all participants to derive the same sequence independently.

Validators must maintain continuous uptime, precise time synchronization, and stable network connectivity to ensure smooth block progression. The network currently operates with approximately 186 validators on testnet, scaling to 200 at mainnet launch.

Constant	Description	Value
Epoch Length	Total number of blocks in a single epoch.	**50,000** Blocks
Epoch Delay Period	Consensus rounds between the boundary block and epoch end.	**5,000** Rounds
Withdrawal Delay	Epochs required before unstaked tokens become withdrawable	**1** epoch
Minimum Self-Stake	Minimum MON a validator must self-delegate.	**100,000** MON
Minimum Total Stake	Combined (self + delegated) MON required for active participation.	**10,000,000** MON
Active Validator Set Size	Number of validators in each epoch.	**200** Validators
Block Reward	Reward distributed per finalized block.	**25** Mon per block

Source: Monad (2025)

3 Tokenomics

The MON token serves as Monad's native utility and governance asset, underpinning all economic activity within the network.

3.1 Supply & Distribution

The initial supply of MON is **approximately 100 billion tokens**, with an estimated **10 percent circulating post-TGE**. Token allocations include **community airdrops**, **ecosystem and developer grants exceeding $100 million**, **staking rewards**, and a **foundation treasury** dedicated to long-term protocol development.

Initial airdrop distributions targeted roughly **5,500 core community members** as well as to nearly 225,000 members of the wider crypto community.

3.2 Supply & Distribution

MON powers the network through multiple roles:

- Payment of **gas fees** for transactions and smart contract execution.
- **Staking collateral** securing the proof-of-stake mechanism and validator set.
- **Governance rights** for onchain proposals and protocol upgrades.
- **Incentives** via ecosystem programs such as Monad Momentum, which funds user and developer growth.

3.3 Governance

Governance will be community-driven, with MON holders able to propose and vote on upgrades. The model emphasizes decentralization, ensuring no central authority controls core parameters or treasury functions.

4 Blockdaemon's Monad Offerings

Blockdaemon offers a unified stack of validator management, RPC connectivity, and staking services, built for both performance and security across both Monad mainnet and testnet.

4.1 Monad RPC

The **RPC layer** is Monad's primary gateway for developers and institutions, providing reliable, low-latency access to the network. As mentioned in section 2.1.1, rather than broadcasting transactions across all nodes, the RPC delivers them directly to the **next three leaders** in the schedule. This reduces bandwidth usage while maintaining rapid propagation.

Blockdaemon operates both **shared** and **dedicated RPC endpoints** for institutions seeking scalable access to Monad.

4.1 Monad Staking

Blockdaemon will provide institutional-grade staking and validator infrastructure for the Monad network, enabling secure participation in proof-of-stake consensus. Validator services include delegated staking, automated deployment, monitoring, and reward reporting, offering institutions confidence in Monad staking with Blockdaemon's 99.9% uptime and compliance.

4.3 Wallet Integration

Blockdaemon will be integrating Monad into the Blockdaemon's institutional wallet infrastructure, allowing clients to securely manage MON tokens.

This integration enables:

- **MPC-based custody** for secure key management and transaction signing.
- **Policy-controlled operations** for institutional governance and compliance.
- **Full network visibility**, including balances across accounts.

5 Conclusion

Monad overcomes the traditional scaling challenges faced by Ethereum, offering an infrastructure capable of sustaining institutional-scale activity while remaining accessible to the broader developer ecosystem.

With **Blockdaemon's institutional support**, including validator operations, high-performance RPC infrastructure, staking, and wallet integration, institutions gain the ability to participate securely and efficiently in Monad's network from day one. Together, Monad's technical foundation and Blockdaemon's operational expertise form a coherent pathway for institutions seeking exposure to performant, standards-aligned blockchain infrastructure.