Espresso Network: A Base Layer for the Multi-Chain Future

General Whitepaper

Version 1.0
October 2025
Espresso Systems

Table of Contents

Abstract

Espresso Network is a decentralized layer-1 blockchain purpose-built as a base layer for the multi-chain future.

As new companies are launching their own rollups at an ever increasing rate, they've inadvertently broken the seamless composability users enjoy within a single chain and reintroduced single points of failure. This increases security risks and results in friction, especially when moving assets between chains. This also becomes apparent when trying to

deposit to a CEX from a rollup, which may take hours, as the CEX waits for the batch containing the deposit transaction to not only be posted by the rollup but also finalize on Ethereum.

The Espresso base layer fixes this. It's purpose-built to provide fast, secure finality, low cost data availability, and decentralized sequencing to applications such as rollups and other types of chains. This helps rollups avoid single points of failure where it counts, allows them to scale more, and grants users the seamless interoperability they expect.

The baselayer essentially acts as a nervous system for rollups, which they plug in to in order to securely communicate with one another. This works by processing rollup blocks through HotShot, a BFT consensus protocol with fast finality. Once a rollup's block has been confirmed by Espresso, it becomes impossible to revert, allowing other applications to read their finalized state with confidence and without delay. This speeds up bridging times and allows deposits from rollups to CEXs to process in seconds.

Espresso aims to provide subsecond confirmations, which would be **1000x faster** than waiting 12+ minutes for finality on the Ethereum L1. With Mainnet 0 launched November 2024, 20+ rollup integrations, and $60M+ in funding from a16z crypto and tier-1 investors, Espresso positions itself as critical base layer infrastructure that works alongside Ethereum—each optimized for different aspects of the multi-chain ecosystem.

1. The Vision: Universal Global Liquidity & Interoperability

Money should move like information

We imagine a world where all platforms for digital assets are interconnected, liquidity is unified, payments are seamless, and users experience the internet as a unified financial system rather than fragmented silos.

We've achieved this for information. The web allows any site to link to any other, APIs enable cross-platform data sharing, emails are sent and delivered across diverse clients, and users can navigate seamlessly between applications. But for value and assets, we remain trapped in walled gardens. Moving money between chains requires slow, expensive bridges. Crosschain applications are slow or brittle because of single points of failure. Users face friction at every interaction.

This fragmentation fundamentally limits what's possible. The power of Ethereum DeFi comes from composability: applications become money legos that builders use to create new products, protocols integrate permissionlessly, innovation compounds. As the ecosystem scales across many chains, we've lost that composability and returned to the fragmented world of traditional finance.

Every application becomes its own chain

No single blockchain can scale to handle the entire internet of value. The way Web3 scales is by every web application becoming its own L2 chain, not by every web application being rewritten as a smart contract on a single blockchain. This model is already emerging. Major web2 brands like Sony, Coinbase, Kraken, and Robinhood are launching rollups.

Any web application can become a blockchain application overnight. The requirements are simple: (1) post its data and transaction log to a base layer that provides fast finality and ensures data availability, and (2) open source its execution logic. That's it. The app is now verifiable, providing users with transparency and the ability to fork if something goes wrong.

This is how PayPal, Zelle, Nasdaq, or any fintech platform could go onchain without redesigning their entire stack. Post transactions to a base layer, derive state from that public log, and you've made your system verifiable and composable with the broader ecosystem. No need to rewrite everything for the EVM. No need to implement complex fault proof systems or ZK bridges—those are optional features for specific use cases like trustlessly bridging to Ethereum L1's EVM state.

The critical requirement: Fast finality

When applications shared a single blockchain, they could communicate synchronously—one smart contract calling another within the same block. Composability was instant. Ethereum's 12-15 minute finality didn't matter as much, because operations were atomic. If one of them happened to revert, the other did as well.

But when every application is its own chain, communication becomes asynchronous. A transaction on Chain A must finalize before Chain B can trust it (this is extra true in the case of L2s that operate centralized sequencers capable of equivocating). If finality takes 12 minutes, that's how long secure crosschain operations take. **There is no "interoperability solution" that can work around slow finality without adding risk for end users**. You simply need base layers that finalize quickly.

This is the architectural gap that prevents the multi-chain vision from realizing its potential. Fast finality isn't a nice-to-have optimization. It's the foundational requirement for composability across independent chains.

---

2. Why Fast Finality Matters

The multi-chain composability problem

As of October 2025, there are 50+ production Layer-2 rollups with over $40 billion in total value locked. Arbitrum One, Optimism, Base, Polygon, Linea, Celo, zkSync, and dozens more process millions of transactions daily. The rollup-centric scaling approach is succeeding technically.

But these chains operate as islands. Moving assets requires waiting 12-15 minutes for Ethereum L1 finality before bridges release funds, or require users to take on additional risk.

Current approaches—traditional bridges, message-passing protocols, intent-based systems—all face the same bottleneck: **safe asynchronous communication requires fast finality.**

Ethereum wasn't designed for this

Ethereum is exceptional at what it was designed for: serving as a single, censorship-resistant smart contract platform capable of surviving World War III. Its architecture prioritizes security and decentralization above speed, achieving economic finality through Gasper after 2 epochs (~12 minutes).

This design made sense for Ethereum's original use case. When all applications share one execution environment, they don't need fast finality for cross-application communication. Smart contracts call each other instantly within the same blocks. The 12-minute finality delay affected only deposits to CEXs and similar operations where absolute certainty was required.

But this architecture doesn't serve the multi-chain future. Ethereum's limited throughput (constrained by every validator executing every transaction) and slow finality (constrained by extreme validator participation requirements) create bottlenecks for coordinating thousands of L2s.

This isn't primarily a criticism of Ethereum. It's recognition that different use cases require different architectures. Ethereum excels as a settlement layer and secure home for high-value assets. What the ecosystem needs is complementary infrastructure purpose-built for fast finality and L2 coordination.

---

3. Technical Architecture

What Espresso is

Espresso Network is a Layer-1 blockchain designed specifically as a base layer for L2s. It's important to understand what this means in practice:

What Espresso provides:

- 6-second finality today with a viable path to subsecond finality in 2026 provided by HotShot consensus.
- Highly scalable data availability layer baked into HotShot consensus.
- Espresso makes it easy for chains to decentralize their sequencer, and even share the same sequencer if they so wish, improving their decentralization and composability even further.
- Espresso can work with any type of chain, rollup stack, VM, or settlement layer

HotShot Consensus: BFT finality in seconds

Espresso's HotShot works as follows:

1. HotShot proceeds in a series of ‘views’.
    a. Views don’t have a fixed time frame. Instead, they can proceed as fast as the network allows.
2. Each view, one validator is randomly chosen to be the leader and propose a block during that view. The leaders for each view are chosen ahead of time.
3. The leader either:
    a. Forms a quorum certificate, or QC, from the highest view they’ve observed, ideally this is from the previous view.
        i. A QC can be formed when ⅔ of the stake-weighted validators vote that a valid block was proposed in a given view.
    b. If they can't form a QC from the highest observed view, they will form a timeout certificate, or TC, for that view instead. Additionally, they will include a QC for the highest view in which they could successfully form a QC.
        i. A TC can be formed when ⅔ of the stake-weighted validators vote that no valid block was proposed within a specific timeframe for a given view.
4. The leader bundles transactions into a block and broadcasts it to the network. For efficiency, the block is erasure-coded into shares, and validators receive shares proportional to their stake, as opposed to the full block. The shares are divided in such a manner that ⅔ of the stake-weighted validators can always reconstruct the block. This ensures data is always available. Additionally, as part of their proposal, the leader will:
    a. attach the QC for the highest view they’ve observed. Or;
    b. Attach the TC for the highest view they’ve observed, and additionally attach the QC from the highest view they’ve been able to obtain one from.
5. If a block is proposed during a view with a valid QC then it is certified. In this manner, the proposed block always extends the highest certified block as observed by the leader.
6. The validators will vote to accept the proposal if in their view the proposed block also builds on top of the highest certified block they have observed. To accomplish this, each validator keeps track of all votes for all blocks they have observed.
    a. Votes to form the QC are sent directly to the leader of the next view.

        i. Validators can be slashed for submitting conflicting votes on the same view.
    b. If the validator does not receive a valid proposal within a specified time following the last view, they will instead send a vote to form a TC to the next leader.
7. Once the leader collects ⅔ of the votes they can immediately form a new QC or TC and propose a new block.
8. In this manner we create a chain of certified blocks, where each block must refer to the previous certified block.
9. Once a chain of 2 certified blocks is formed, we can finalize the first certified block of the 2-chain as soon as we receive a subsequent QC.
    a. For example: Proposal(view = 10, QC(view = 7), TC(view = 9)) <- Proposal(view = 11, QC(view = 10)) <- Proposal(view = 12, QC(view = 11)). Following this, we know that at least ⅔ of stake agrees the block proposed in view 10 is correct and becomes finalized.

In practical terms, this process enables Espresso to finalize blocks as fast as the network allows. Additionally, because finalized blocks include a QC that proves that ⅔ of stake voted on it, it's possible to slash up to ⅓ of the stake in the event that a second, conflicting block is finalized, as they'll have voted on both blocks. This means Espresso has strong cryptoeconomic security backing its finality. And by erasure coding each block, Espresso reduces bandwidth constraints, providing a highly scalable DA layer to integrated chains.

Light client verification

To ensure that rollups can check whether a block was finalized by Espresso, a light client smart contract that tracks HotShot consensus has been developed. This contract is currently deployed on Ethereum and Arbitrum One, and provides the following functionality:

1. Maintains the current set of Espresso validators and their stake distribution
2. Uses BLS signature aggregation to cryptographically verify that 2/3+ of those validators signed off on a specific block
3. Thereby enables L2 settlement contracts to verify that specific blocks were finalized by Espresso

Trusted Execution Environment (TEE) attestation

An alternative approach leverages secure hardware through Trusted Execution Environments. In this model, the L2's batch poster—the component responsible for publishing blocks to the settlement layer—runs inside a TEE such as Intel SGX or AMD SEV. The TEE provides cryptographic attestation that specific code is running unmodified within the secure environment. In this case, it ensures that the batch poster only publishes blocks that exactly match the blocks that were finalized by Espresso's HotShot consensus.

Caffeinated Nodes: State derivation interface

Besides light clients and smart contracts, full nodes also need to be able to derive the rollup's finalized state. Caffeinated Nodes (Caff Nodes) serve as this interface. Traditional rollup nodes wait for L1 finality (12+ minutes) before deriving state. A Caff Node is a modified rollup full node that instead uses the Espresso Network to derive the finalized rollup state within seconds.

Caff Nodes download transaction data from EspressoDA and re-execute transactions locally to verify state transitions. They are identical to traditional full nodes, but using Espresso as the canonical source. They maintain standard JSON-RPC interfaces for compatibility with existing tooling.

The state derived by Caff Nodes is guaranteed to match eventual L1 settlement because:

1. Espresso's BFT consensus finalizes transaction ordering with 2/3+ validator signatures
2. The settlement contract enforces only blocks finalized by Espresso are accepted in the canonical rollup chain.

External parties can read from Caff Nodes to access fast, reliable rollup states without waiting for L1 settlement. This is useful for many different types of third parties:

- Bridges: Reduce bridge times from 12-15 minutes to ~10 seconds by trusting Espresso confirmations
- Exchanges: CEXs reduce deposit confirmation times, improving capital efficiency and user experience
- Other rollups: Fast visibility into integrated chains' states enables crosschain composability within seconds
- Messaging protocols: Faster message verification without additional trust assumptions
- Solver networks: Reduced capital requirements and risk premiums through reliable fast confirmations
- DeFi protocols: Build crosschain financial products leveraging subsecond finality
- End users: For stronger guarantees that high value transactions won't revert.

Integrating with Espresso

Now to consider a practical example, here's how an Ethereum rollup would integrate with Espresso:

1. Transactions for the rollup are sent to a sequencer.
2. The sequencer determines an ordering for these transactions and turns them into blocks.
3. The sequencer forwards their blocks to Espresso.
4. Espresso will quickly finalize the rollup's block.
5. The blocks finalized by Espresso will be batched and forwarded to Ethereum.
6. Ethereum includes these batches in an Ethereum block.
7. Ethereum eventually finalizes the block that includes the rollup's transaction batch.

8. The canonical rollup blockchain is determined by the batches that were finalized on Espresso and Ethereum. If a block wasn't finalized by Espresso, it won't be accepted as part of the rollup's final state.

This process ensures that the rollup can't reorg after a block has been finalized by Espresso, allowing anyone to quickly derive the rollup's finalized state simply by reading from Espresso. This also makes it easier for rollups to decentralize their sequencer, as they are no longer strictly reliant on a trusted sequencer to provide soft-confirmations to improve UX for end users.

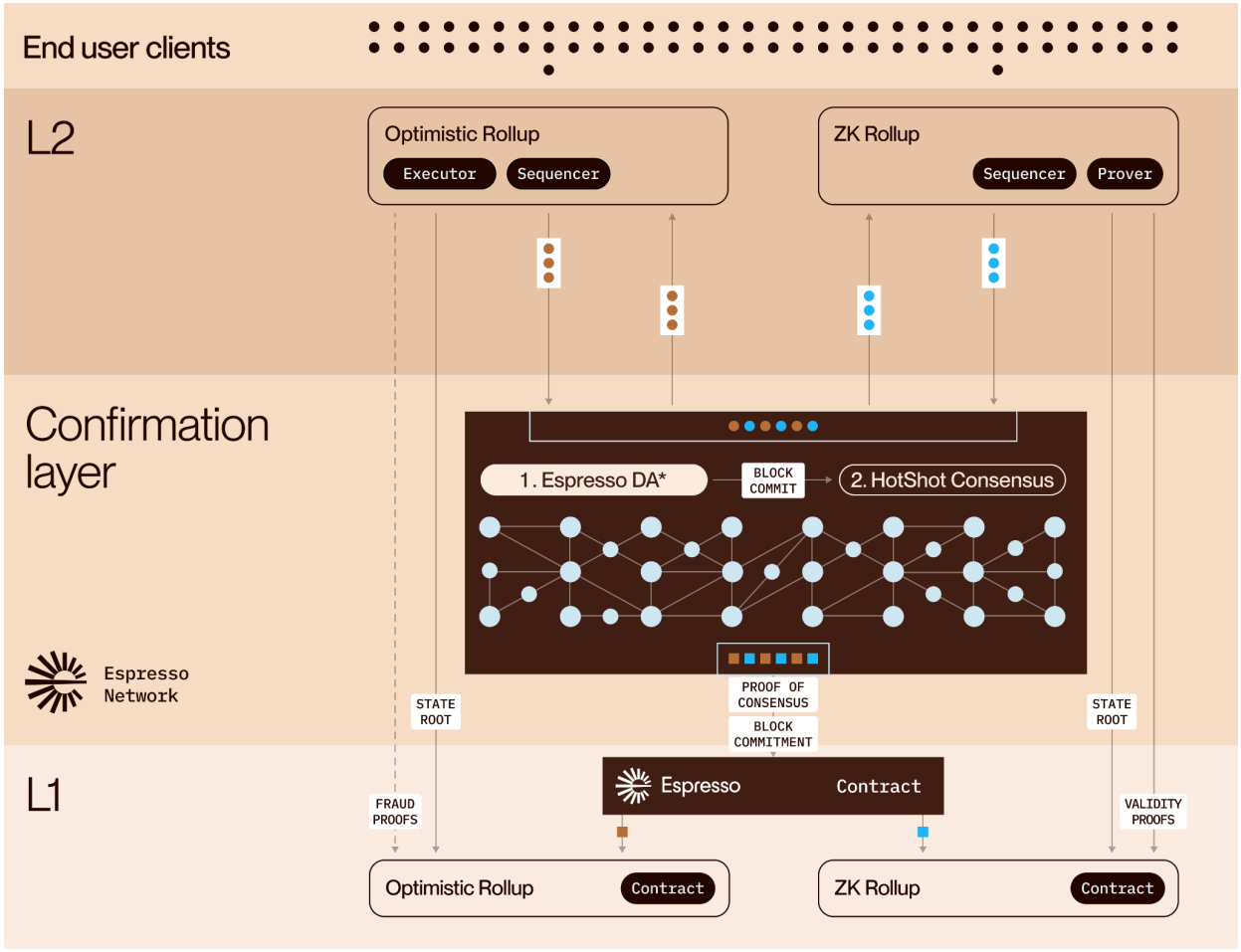

Diagram of rollups integrated with Espresso

Performance characteristics

Current Mainnet 0:

- Finality: 6 seconds average
- Validators: 100 nodes (22 operators)
- Blocks: 5.3M+ produced
- Transactions: 8.7M+ confirmed

- Throughput: 5MB/sec

Near-term targets (Q4 2025 - 2026):

- Finality: subsecond
- Permissionless PoS
- Throughput: 30MB/sec

---

4. Production Status and Roadmap

Development history: From testnets to mainnet

Espresso's path to production spanned multiple testnet phases demonstrating iterative improvements:

Testnet 1: Americano (Nov 2022): Initial benchmarks for CDN networking mode, internal validator stake, transaction demo leveraging Configurable Asset Privacy (CAP) execution layer.

Testnet 2: Doppio (Jul 2023): Polygon zkEVM stack prototype, optimized benchmarks for CDN networking mode, data availability queries, rollup contract with off-chain DA.

Testnet 3: Cortado (Sep 2023): OP Stack integration prototype, rollup contract verification, early rollup integrations, documentation and endpoints prepared for node onboarding.

Testnet 4: Gibraltar (Jan 2024): Arbitrum stack integration prototype, benchmarking P2P networking mode, randomized committees for DA, first external nodes onboarded.

Testnet 5: Decaf (Sep 2024 - ongoing): Long-running testnet featuring HotShot optimizations and testing, variable stake, randomness beacon, node onboarding, builder integrations. Continues operating alongside mainnet.

Mainnet 0 (October 2024 - present)

Infrastructure

- 22 permissioned node operators including Blockdaemon, Figment, Nethermind, Informal Systems
- 100 geographically distributed nodes

- 5.3M+ blocks produced, 7.2M+ transactions confirmed
- 20+ rollups live or in the integration pipeline
- Ongoing benchmark optimizations

Integrated chains and applications

Bridges:

- Stargate

Interop protocols (coming soon):

- Hyperlane
- MetaLayer
- LayerZero
- AggLayer

Applications:

- Rarible
- Superposition
- Eco

Production rollups:

- RARI Chain (NFTs)
- ApeChain (NFTs, gaming, home of the ApeCoin ecosystem)
- Molten (DeFi)
- LogX (DeFi)
- AppChain (consumer apps)
- T3rn (shared execution platform)
- NodeOps Network (DePIN marketplace)
- Rufus (gaming, metaverse)
- Huddle01 (decentralized video conferencing platform)
- 15+ additional chains in integration pipeline

These span diverse use cases—NFT marketplaces, DeFi, gaming, domain-specific computation—validating Espresso's flexibility.

Mainnet 1.0 (Q4 2025)

Major milestone: Permissionless proof-of-stake

- Upgrade to permissionless proof-of-stake secured by $ESP token
- Any party can operate validator nodes by staking ESP
- Launch of Espresso token ($ESP) with network rewards

- First OP Stack integrations go live with Celo
- Enhanced HotShot optimizations (4 to 3 consensus rounds)
- Improved EspressoDA efficiency
- v1 API release

$ESP token: $4M community sale completed July 2025. Functions: node staking, governance, network rewards. Token generation event coincides with Mainnet 1.0 launch.

Mainnet 2.0 (Q1-Q2 2026)

Focus: Ecosystem expansion and decentralized sequencing

- First bridges and exchanges reading from Espresso confirmations via Caffeinated Nodes
- Decentralized sequencing module production-ready (including collaboration with Offchain Labs and Arbitrum ecosystem)
- Expanded integration support beyond Arbitrum Orbit to multiple frameworks

Mainnet 3.0 (2026)

Focus: SDK and blitzscaling

- Espresso SDK ready to support blitzscaling of rollups/chains migrating to Espresso base layer
- Consensus optimizations targeting 2-second transaction finality
- Streamlined integration process reducing deployment time from weeks to days

Mainnet 4.0 (Q4 2026+)

Focus: Advanced consensus and subsecond finality

- Potential upgrade to Hydrangea or similar consensus protocol to support subsecond transaction finality
- Performance optimizations achieving the 1000x finality improvement target
- Mature ecosystem with comprehensive tooling and integrations

---

5. Team and Backing

Espresso Systems, the original contributor to Espresso, was founded in 2020. The Espresso team comprises a diverse and passionate group of ~40 contributors from around the world.

Espresso Systems raised over $60M from a16z crypto, Greylock Partners, Electric Capital, Sequoia Capital, Polychain Capital, Blockchain Capital, Coinbase Ventures, and Gemini.

Co-founding team

Ben Fisch, CEO & CTO: Professor in Computer Science at Yale. Co-inventor of VDFs (used in Ethereum), proof-of-replication (Filecoin), and state-of-the-art ZKPs Basefold & Blaze (used in Succinct). PhD in Computer Science, Stanford.

Charles Lu, COO: Previously at Binance Labs, Citadel, Meta, and Amazon. BS/MS/PhD (on leave) in Computer Science, Stanford.

Jill Gunter, Chief Strategy Officer: Previously at Slow Ventures (investor in Solana's seed round) and Goldman Sachs. MSc, Oxford; AB, Harvard.

Benedikt Bünz, Chief Scientist: Professor in Computer Science at NYU. Co-inventor of Bulletproofs (Monero), VDFs (Ethereum), HyperPlonk, Zether, and Provisions (proofs of solvency). MS/PhD in Computer Science, Stanford.

Strategic partnerships

Arbitrum/Offchain Labs: Joint development of Decentralized Timeboost specification for Orbit chains using Espresso infrastructure.

Polygon Labs: Collaboration on AggLayer integration for cross-rollup interoperability, leveraging Espresso's fast finality.

Caldera: Collaborative deployment of rollups using Espresso including ApeChain and RARI Chain.

AltLayer: Collaborative deployment of rollups using Espresso including Flint/LogX.

Framework integrations: Arbitrum Orbit and Cartesi production support. OP Stack integration (Q4 2025 with Celo), Polygon CDK (2024).

---

6. Research Contributions

Beyond production infrastructure, Espresso has contributed significant R&D to the blockchain scaling and privacy space. Projects using research from Espresso team members include Ethereum, Solana, Monero, Filecoin, and others.

Selected research publications from Espresso team members

Zether: Towards Privacy in a Smart Contract World	B. Bünz; D. Boneh;	2020	Research paper	Foundation for private smart contracts.	https://link.springer.com/chapter/10.1007/978-3-030-51280-4_23
Verifiable delay functions	B. Bünz; B. Fisch	2018	Research paper	Introduction of VDFs. Used in Solana's consensus protocol.	https://eprint.iacr.org/2018/601.pdf
Bulletproofs: Short proofs for confidential transactions and more	B. Bünz; D. Boneh; G. Maxwell; P. Wuille	2018	Research paper	Privacy without trusted setup. Used in Monero.	https://ieeexplore.ieee.org/abstract/document/8418611/
PoReps: Proofs of Space on Useful Data	B. Fisch	2018	Research paper	Data availability and storage. Used by Filecoin	https://eprint.iacr.org/2018/678.pdf

Espresso systems related research

CIRC: Coordinated Inter-Rollup Communication

CIRC is Espresso's stack-agnostic protocol for coordinated message-passing between chains, enabling both asynchronous and synchronous composability. The protocol addresses liquidity

fragmentation by allowing chains to communicate directly without relying on third-party liquidity providers.

Decentralized Timeboost

In collaboration with Offchain labs we have designed a decentralized version of the Timeboost sequencing protocol. This allows rollups to maintain fair transaction ordering in a decentralized setting.

Research into the Espresso Network's design

1. The Espresso Sequencing Network (2024/1189): https://eprint.iacr.org/2024/1189.pdf
2. The Espresso Sequencer: https://hackmd.io/@EspressoSystems/EspressoSequencer
3. HotShot and EspressoDA: https://hackmd.io/@EspressoSystems/HotShot-and-Tiramisu
4. Market Design for Sequencing Auctions: https://hackmd.io/@EspressoSystems/market-design
5. Based Espresso: https://hackmd.io/@EspressoSystems/BasedEspresso
6. Bridging research: https://hackmd.io/@EspressoSystems/bridging
7. Decentralized Timeboost: https://github.com/OffchainLabs/decentralized-timeboost-spec
8. BFT & Preconfirmations: https://hackmd.io/@EspressoSystems/bft-and-proposer-promised-preconfirmations
9. Derivation Pipeline: https://hackmd.io/@EspressoSystems/the-derivation-pipeline

These contributions demonstrate thought leadership and technical depth, even where concepts aren't yet in production.

---

7. Conclusion

The blockchain industry faces an inflection point. As applications become independent chains, the critical bottleneck is finality speed—the foundational requirement for composability in an asynchronous multi-chain world.

Ethereum provides exceptional security and serves as the natural settlement layer. But Ethereum was designed as a monolithic smart contract platform, not for coordinating thousands of L2s. Its 12-15 minute finality creates an architectural constraint for the multi-chain ecosystem.

Espresso fills this gap as a base layer purpose-built for fast finality. Through HotShot consensus and EspressoDA, Espresso achieves ~1000x faster finality—not through marginal optimization but through architectural design optimized specifically for this use case. The result is infrastructure enabling money and digital assets to move across platforms as easily as information moves across the web.

With Mainnet 0 operational since November 2024, 20+ chains integrating, strategic partnerships with Arbitrum, Polygon, and major bridge protocols, and $60M+ in funding from tier-1 investors, Espresso has moved from research to production infrastructure. The phased approach to decentralization prioritizes stability while maintaining a clear path to trustlessness.

The blockchain industry's trajectory points toward dozens or hundreds of specialized execution layers. This future requires multiple base layers, each optimized for different functions. Espresso positions itself as base layer infrastructure for fast finality and cross-chain coordination, working alongside settlement layers like Ethereum to support the multi-chain ecosystem.

The internet of value requires many chains, not one. Espresso is building base layer infrastructure to make those many chains work together seamlessly.

---

8. References

Technical Papers and Specifications

1. Bearer, J., et al. (2024). "The Espresso Sequencing Network: HotShot Consensus, Tiramisu Data-Availability, and Builder-Exchange." *Cryptology ePrint Archive*, Paper 2024/1189. https://eprint.iacr.org/2024/1189.pdf

2. Espresso Systems (2024). "The Espresso Sequencer." *HackMD*. https://hackmd.io/@EspressoSystems/EspressoSequencer

3. Espresso Systems (2024). "Combining HotShot Consensus with Espresso's Data Availability." *HackMD*. https://hackmd.io/@EspressoSystems/HotShot-and-Tiramisu

4. Fisch, B. (2024). "Based Espresso: ad-hoc shared sequencing for all L2s, from based rollups to validiums." *HackMD*. https://hackmd.io/@EspressoSystems/BasedEspresso

5. Espresso Systems (2024). "Market Design: Shared Sequencing Auctions." *HackMD*. https://hackmd.io/@EspressoSystems/market-design

6. Espresso Systems (2024). "The Derivation Pipeline." *HackMD*. https://hackmd.io/@EspressoSystems/the-derivation-pipeline

7. Espresso Systems (2024). "Bridging fast and safe with Espresso." *HackMD*. https://hackmd.io/@EspressoSystems/bridging

8. Espresso Systems (2024). "Analyzing BFT & Proposer-Promised Preconfirmations." *HackMD*.

https://hackmd.io/@EspressoSystems/bft-and-proposer-promised-preconfirmations

9. Offchain Labs & Espresso Systems (2024). "Decentralized Timeboost Specification." *GitHub*. https://github.com/OffchainLabs/decentralized-timeboost-spec

Official Documentation

13. Espresso Systems Official Documentation: https://docs.espressosys.com/

14. Espresso Systems Blog: https://medium.com/@espressosys

15. Espresso Systems Technical Writing: https://hackmd.io/@EspressoSystems

16. Espresso Foundation Blog: https://mirror.xyz/espressofndn.eth

---

9. Glossary

Base Layer (L1): The foundational blockchain layer providing core services like consensus, data availability, and security. Ethereum and Espresso are both base layers with different specializations.

BFT (Byzantine Fault Tolerant): A property of consensus protocols that remain correct even when up to 1/3 of participants act maliciously or fail arbitrarily.

Confirmation Layer: Infrastructure that provides cryptographic confirmations of transaction ordering and inclusion, enabling chains to trust each other's state without waiting for final settlement.

DA (Data Availability): The guarantee that transaction data is publicly accessible and retrievable, enabling anyone to reconstruct blockchain state.

EspressoDA: Espresso's three-layer data availability system combining Verifiable Information Dispersal, DA committee, and CDN for optimal security-performance tradeoffs.

Finality: The point at which a transaction is guaranteed to be permanent and cannot be reverted.

HotShot: Espresso's Byzantine Fault Tolerant consensus protocol achieving linear communication complexity and optimistic responsiveness.

L2 (Layer 2): Execution layer built on top of a base layer, processing transactions off-chain while posting commitments for security and data availability.

Light Client: Software that verifies blockchain state by checking headers and cryptographic proofs without downloading full blocks.

Optimistic Responsiveness: Consensus property where blocks finalize as fast as actual network conditions allow rather than waiting for predetermined conservative timeouts.

Preconfirmation: Promise that a transaction will be included in the canonical chain, provided before final consensus finality.

QC (Quorum Certificate): Aggregated signature from 2/3+ validators proving a block has been validated by consensus supermajority.

Rollup: Layer-2 scaling solution that executes transactions off-chain, batches them, and posts compressed data/commitments to a base layer for security.

VID (Verifiable Information Dispersal): Cryptographic technique that erasure-codes data and distributes chunks across validators, enabling reconstruction from any sufficient subset.

This whitepaper presents the technical architecture and high-level status of Espresso Network as of October 2025.

For the most current information:

- *Technical Documentation: https://docs.espressosys.com/*
- *GitHub Repository: https://github.com/EspressoSystems*

Document Version 1.0 – October 2025
