Radium - The Universe-Scale Ledger Without Limits

Introduction

Radium is a high performance Layer One blockchain that focuses on speed and security, tightly implemented in approximately 121,941 lines of C and C++ code.

Investment

Building a high performance, secure and scalable Layer One blockchain takes many years of research and development from a team of industry experts. With this comes costs from tools, software, hardware, real-world testing expenses, infrastructure, etc. This project is completely self-funded with no Initial Coin Offerings, Grants, Crowdfunding, Community Donations or Venture Capital involvement.

Economics

Issuance

The genesis block mints 6,621,369.408 credits for network and ecosystem bootstrap. Block rewards start at 1 credit. Every 4,536,000 blocks the reward reduces by 1%. 10% of each block reward is deposited into the treasury and the remaining 90% is deposited into the block creators stake account. Credit issuance is finite and the total issuance shall not exceed 460,000,000 credits.

Fees

Native transfer fees are split into three parts and deposited to the block creators stake account, void account and treasury account. Native transfer fees and Token transfer, mint and update fees have a fixed amount of 0.000001 credits and a dynamic amount of 0.0000001 credits per 8 bytes of consumed memory. Token registration fees have a fixed amount of 80 credits.

Stake delegation add, remove and update have zero fees however there is a minimum of 80 locked credits to add a delegation. Atomic swap fees have a fixed amount of 0.000002 credits and a dynamic amount of 0.0000001 credits per 8 bytes of consumed memory which are split between each side of the swap. Atomic swap fees are split into four parts and deposited to the block creators stake account, void account, treasury account and the swap creators fee account. Automated market maker (AMM) network fees are split into three parts and deposited to the block creators stake account, void account and treasury account and are valued as follows:

- Create Pool - 0.000027
- Add Liquidity - 0.000027
- Remove Liquidity - 0.000026
- Swap - 0.000029

When splitting fees if there is a remainder it is deposited into the void account.

Staking

The network operates through a Proof-of-Stake system, it is what drives consensus. Deploying a single-node-per-delegation model promotes network decentralization by requiring stake holders to deploy their own physical hardware. Staked delegates earn a portion of the block reward as well as applicable fees for their participation.

Governance

The network functions as a DAO (Decentralized Autonomous Organization). The treasury is self-funded from 10% of the block reward as well as a portion of network fees. This funding model provides a reliable source of capital for development, marketing, and other project needs without relying on outside investors, sponsors or grants. Staked delegates have direct voting rights on network changes, proposals, and treasury disbursements.

Tokens

Without the use of smart contracts or system programs the network implements native token registrations, mints, transfers and updates.

DeFi and DEX

Native credits and token credits can be traded peer-to-peer with low fees and no KYC.

Swaps

Atomic

The system implements a generic mechanism for swapping native credits and token credits. This system allows swaps to occur off-chain and settled on-chain with great flexibility for 3rd-party developers. Swaps can be fully settled at extremely high speeds, usually in under 700ms. Any staked delegate can order, pair, finalize and submit swaps to a leader for on-chain processing. When a swap is executed the delegate receives a portion of the fees.

Automated Market Maker

The system also implements on-chain automated market maker (AMM) liquidity pools for continuous decentralized trading between native credits and token credits.

Each AMM pool maintains reserves of two assets and issues liquidity provider (LP) shares representing proportional ownership of the pool.

Swaps against AMM pools follow a constant-product pricing model, where the product of the two asset reserves remains approximately constant. Trading fees fixed at 0.3% are collected and distributed to liquidity providers.

Cryptography

Random Number Generator

ChaCha20 is used in deterministic epoch-related schedule generation mechanisms. Mersenne Twister 19937 64-bit is used in various non-deterministic, non-critical sorting mechanisms.

Hashing

Blake3 is the primary hashing algorithm used throughout the system. SHA-256 is used once as part of the Schnorr Tagged Hash domain separation mechanism. SHA-512 is used once as part of the BIP-39 Mnemonic generation algorithm. Lattice16 is used to establish the ledger state hashes as well as the sole system-wide state hash.

Signatures

Schnorr is the primary and only signing and signature verification mechanism.

Encryption

The system does not use encryption of any kind.

Network and Consensus

An IPv6-only network backbone powers the consensus algorithms, combining a purpose-built, high-throughput UDP transport with a multicast-based dissemination model to efficiently propagate messages across the network. This foundation supports a simple, fast, and secure Byzantine fault tolerant single-phase, two-chain design, with consensus rounds paced by verifiable slot timing that collapses traditional multi-step coordination into a unified voting cycle and enables deterministic sub-second finality.

IPv6

By operating exclusively over IPv6, the network benefits from simplified packet processing and source-controlled fragmentation via Path MTU Discovery, eliminating in-network fragmentation and middle-box interference. The absence of Network Address Translation restores true end-to-end connectivity between nodes, reducing congestion and latency while enabling efficient multicast-based data distribution. IPv6's vast address space allows globally unique node identities, and its native support for IPsec provides a foundation for secure, authenticated communication at the network layer.

Byzantine Fault Tolerance

At the consensus layer a single-phase, vote-to-all Byzantine Fault Tolerant design built around a two-chain pipeline. Each round has a designated leader to propose a block, but voting is never centralized: every delegate broadcasts its vote to the entire committee, allowing all nodes to independently observe quorum formation and aggregate proofs locally. This removes the need for multi-step leader coordination and eliminates entire classes of attacks, including silent leader withholding and tail forking, since no single node controls progress or proof assembly. Proposals can flow continuously while commitment trails safely behind in a bounded pipeline, enabling fast, deterministic finality even under the presence of adversarial network conditions.

Slots

Governed by a difficulty-based verifiable delay that requires the leader to demonstrably wait before assembling a block, with the minimum difficulty calibrated to the time needed on modern single-core processors to verify thousands of Schnorr transaction signatures. Each proposal therefore carries a slot, a proof showing that the leader yielded to the transaction queue, operated within realistic performance bounds, and allowed the tail-chain head to commit across the network before advancing consensus. In this way, the delay functions as a proof of performance rather than proof of work: it does not reward speed or parallelism, but attests that the leader can sustain real-time validation, respect network pacing, and advance the chain in an orderly, verifiable manner.

Transport and Routing

The transport layer is built directly on UDP, giving the protocol explicit control over packetization, timing, and delivery behavior without the constraints of connection-oriented transports. Messages are propagated using a deterministic multicast-based routing model, where proposals are distributed through scheduled layers, reducing redundant traffic, and ensuring rapid, predictable dissemination. By decoupling transport mechanics from consensus logic, the system sustains high throughput and low latency while preserving clear, protocol-level guarantees on message handling and progression.

Together, these elements create a robust foundation for high-throughput applications, where low latency and irrevocable transactions are critical for real-world adoption.

Transaction Processing

The system deploys a parallel transaction processing unit where as transactions arrive from the network their signatures are verified in parallel across a pool of CPU cores. Each transaction is validated and checked against system state on parallel pipelines. The system is able to ingest up to 64,000 transactions per second before a block is to be assembled.

Data Storage

The system stores data as key value pairs or using key value separation to store binary large objects (BLOBS) directly to disk with pointers stored in LSM trees. By storing blocks and other large objects directly to disk we bypass database synchronization and achieve high IO/s. The system uses approximately many independent databases allowing block commits to be parallelized to a high degree.

Acknowledgements

We thank the anonymous reviewers and testers for their participation and input. Kevin Lewi, Wonho Kim, Ilya Maykov, and Stephen Weis for their ideas on homomorphic hashing and rolling state. HandSolo for their ideas on Proof-of-Performance and verifiable slots timing. The late Claus P. Schnorr for his work on creating Schnorr groups.