WHITEPAPER · V2.0 · CHAIN ID 2800

The non-custodial EVM Layer 1 for settlement

AERE is a public EVM Layer 1 (Chain ID 2800) whose economics are immutable *by code*, a sealed 37.5% base-fee burn with no admin, no proxy, and no withdrawal path, paired with an on-chain compliance-and-privacy verification layer: a sanctions-enforcing privacy pool, zero-knowledge KYC attributes, and Travel Rule tooling. Every capability below maps to a contract address you can call. 0.5-second deterministic finality (QBFT). Fixed 2.8B supply, zero insider unlocks. The chain no one can rug.

VERSION 2.0 UPDATED 2026-07-07 CHAIN ID 2800 ~32 MIN READ

BLOCK FINALITY	THROUGHPUT CEILING	MAX SUPPLY	CHAIN ID
0.5s	273k TPS testnet	2.8B AERE	2800
VALIDATORS TODAY	**PER-TX BURN**		
3 → 7 → 21	37.5%		

00 · Overview

Abstract

AERE is a public EVM Layer 1 (Chain ID 2800) whose economics are immutable by code, a sealed 37.5% base-fee burn with no admin, no proxy, and no withdrawal path, paired with an on-chain compliance-and-privacy verification layer: a sanctions-enforcing privacy pool, zero-knowledge KYC attributes, and Travel Rule tooling. Every capability below maps to a contract address you can call. The chain finalises in 0.5 seconds with deterministic QBFT (no probabilistic re-orgs), fixes supply at 2.8B with zero insider unlocks, and ships at full Pectra + Fusaka parity with Ethereum mainnet, the RIP-7951 secp256r1 precompile at `0x100` enabling native account abstraction via WebAuthn + ERC-4337 v0.7 + MultiOwnable recovery + EIP-1271 signature validation.

On throughput: the chain delivers 0.5-second deterministic finality and sub-cent fees today. The 273,000 TPS figure is a QBFT-architecture testnet benchmark, a ceiling the multi-layer roadmap scales toward, not a current mainnet rate (full methodology on /benchmarks). Consensus runs on 3 Foundation validators today, with a public path to 7 and then 21.

AERE supply is fixed at 2,800,000,000 at genesis with no further minting possible. The protocol's economic engine is the **AereFeeBurnVault**: an immutable sealed contract that burns 37.5% of every transaction fee on confirmation, with no admin, no withdraw, no proxy. Combined with the **AereSink** three-bucket router for protocol revenue (BURN / BUYBACK-AND-BURN / STAKER-YIELD, percentages set at deploy and never changeable) and **sAERE** (an ERC-4626 receipt token we structure as a receipt instrument, consistent with the SEC's August 5 2025 staking-receipt guidance, our position, not settled law), AERE compounds toward measurable supply contraction at scale.

Cross-chain rails ship via standard Warp Routes (USDC.e / USDT.e / USDe.e / EURC.e sequence through 2026), ERC-7683 intents, pull-oracle price feeds, and verifiable randomness. Settlement-grade primitives shipping through 2026: **AereProof v0** (verifiable on-chain compliance primitives, OFAC sanctions registry, Travel Rule SDK, Forta detection bots, all read-only, all public), **AERE402** (agentic settlement layer for machine-to-machine payments on Lightning channels), and the 3 → 7 validator

transition. Engineered as the chain no one can rug, immutable, admin-less economics independent of validator count. Funded entirely from the 560M AERE Ecosystem Reserve, no external raise, no insider unlock, no off-chain promise.

---

01 · Chapter

Introduction

1.1 What the chain has to do

Institutional settlement requires three things at the same time: finality that is mathematical (not statistical), execution that is fully Ethereum-compatible (so the existing engineering surface ports without rewrites), and economics that are immutable (so the protocol's monetary policy cannot be changed by a privileged operator with a multisig and a press release).

Most public Layer 1 networks deliver at most two of those three. Probabilistic-consensus chains (Nakamoto-style proof-of-work and most proof-of-stake L1s) trade determinism for openness, every transaction is rewindable until enough blocks have stacked on top to make the rewind economically painful. Permissioned BFT chains deliver determinism but at the cost of EVM compatibility and a static, operator-controlled validator set. Custodial wrappers (centralised settlement layers, tokenised-deposit ledgers) wrap the determinism around a custodian, and a custodian is a single point of permission, capture, and political risk.

> **The settlement gap**
>
> A non-custodial public Layer 1 that runs the same EVM as Ethereum, finalises in 0.5 seconds with deterministic QBFT, and enforces its monetary policy through immutable contracts, no admin, no upgrade proxy, no withdraw. That is the gap AERE fills.

1.2 How AERE solves it

AERE pairs Hyperledger Besu QBFT consensus (deterministic finality, no probabilistic re-orgs, sub-second confirmation) with the full Pectra + Fusaka EVM ruleset (every Ethereum mainnet opcode, every precompile, every account-abstraction primitive). The result is an EVM L1 that institutional teams can adopt without rewriting any contract, while end-users get finality fast enough to feel like a card swipe.

- **0.5-second deterministic finality.** QBFT consensus on Hyperledger Besu. Every confirmed block is final the moment it lands, no probabilistic waiting, no settlement risk windows, no MEV-driven re-orgs by construction. Throughput scales toward a 273k TPS testnet benchmark (methodology on /benchmarks); 3 Foundation validators today, public path to 7 → 21.
- **Full Pectra + Fusaka EVM parity.** RIP-7951 secp256r1 precompile at `0x100`, EIP-7702 EOA delegation, EIP-2537 BLS12-381, EIP-2935 historical block hashes, full Cancun opcode set. Foundry, Hardhat, viem, ethers, every Ethereum tool works day one.
- **Immutable 37.5% per-tx burn.** `AereFeeBurnVault` is a sealed contract, no admin, no withdraw, no upgrade proxy. 37.5% of every transaction fee is burned on confirmation. Monetary policy is enforced by code, not by a multisig with discretion.
- **Passkey-native account abstraction.** ERC-4337 v0.7 + MultiOwnable recovery + EIP-1271 signature validation. WebAuthn keys live in Touch ID, Face ID, Windows Hello, YubiKey, FIPS 186-4 ECDSA on the NIST P-256 curve (secp256r1), the same curve standard used in government/PIV smart cards.
- **Cross-chain Warp Routes.** Bytecode-identical bridged stablecoins (USDC.e, USDT.e, USDe.e, EURC.e) ship through 2026. ERC-7683 intents settle in seconds across 30+ chains. Pull-oracle price feeds; threshold-BLS verifiable

randomness.

02 · Chapter

Technical architecture

2.1 Key equations

The AERE architecture rests on a handful of explicit relations. They are stated here so a technical reader can check the claims rather than take them on faith.

Transaction throughput (single-chain QBFT)

```
TP = B / Tblock
```

TP = transactions per second; B = effective transactions per block (gas-limit / avg-tx-gas); Tblock = block time (0.5s on AERE). AERE executes on a single QBFT chain, there is no sharding. Higher throughput surfaces are delivered via L2 rollups (§2.4), not base-layer shards.

Gas calculation

```
Gtotal = Gbase + Gdata × Size + Gexec
```

Gtotal = total gas; Gbase = base gas (21,000 for a standard transfer); Gdata = gas per data byte; Size = data size in bytes; Gexec = contract-execution gas. Gas costs match the Pectra + Fusaka schedules.

Staking reward (fee-share, no emission)

```
Rstaker = (S / Stotal) × Tf × β
```

Rstaker = staker reward over the epoch; S = individual stake; Stotal = total stake in the sAERE pool; Tf = fees routed through AereSink during the epoch; β = STAKER-YIELD bucket share of Tf (set immutably at AereSink deploy time). AERE has no block subsidy, staking yield is paid entirely from fee flow.

Network security threshold

```
Tsecurity = ⌊(n − 1) / 3⌋
```

Tsecurity = maximum Byzantine validators the network tolerates; n = total validators. With n = 3 today, tolerance is 0 faulty nodes; the transition to 7 validators raises it to 2.

2.2 Consensus mechanism

AERE runs **Hyperledger Besu QBFT** (Quorum Byzantine Fault Tolerance), a BFT consensus with immediate finality and 0.5-second block production. QBFT is chosen for its predictable latency and deterministic finality (no probabilistic confirmations), the property that makes it suited to settlement, where a transaction must not be rewindable once confirmed. AERE runs 3 Foundation-operated validators today, with a public path to 7 and then 21 (§6). The network is not yet decentralised; this is stated plainly, not implied away.

- **0.5s deterministic finality:** transactions reach immediate, deterministic finality in 0.5 seconds, no probabilistic confirmations, no reorgs. Suited to settlement and real-time payments.
- **Energy profile vs proof-of-work:** QBFT consumes orders of magnitude less energy than proof-of-work chains. Throughput scales toward a 273k TPS testnet benchmark, the architectural ceiling, not the current mainnet rate; sustained mainnet throughput under real load is publicly observable via the live indexer. See /benchmarks for methodology.
- **Byzantine fault tolerance (f < n/3):** QBFT tolerates up to ⌊(n−1)/3⌋ Byzantine validators. With 3 validators today, the network tolerates 0 faulty nodes; the transition to 7 validators raises tolerance to 2.
- **Validator set and economics:** 3 Foundation-operated validators today, public path to 7 and then 21. The network is Foundation-operated at consensus level and not yet decentralised, the immutable economics (§3.3) are what make it rug-proof today, independent of validator count. Validators are compensated from coinbase rewards routed through the AereCoinbaseSplitter (62.5% validator / 37.5% AereFeeBurnVault). There is no block emission; rewards are purely fee-based.

2.3 Single-chain QBFT execution

AERE is a **single-chain QBFT network**, there is no base-layer sharding, no beacon chain, no parallel shard execution. All transactions execute on one canonical chain with deterministic 0.5-second finality. Higher aggregate throughput targets are addressed via Layer-2 anchors (§2.4 / §6.3), not by partitioning the base layer. This is intentional: shared single-chain state composes natively with EVM tooling, removes cross-shard atomicity edge cases, and matches the settlement use case AERE targets.

2.4 Multi-layer scaling architecture (forward-looking targets)

AERE's scaling roadmap stacks Layer-2 systems above the QBFT base chain. The list below is a **forward-looking target stack** with explicit per-line dates; current deployments are tracked in §6. See /benchmarks for methodology behind the up-to-273,000 TPS aggregate test result.

- **Base Layer (QBFT, live):** single-chain execution, 0.5-second deterministic finality, throughput bounded by per-block gas limit.
- **Optimistic Rollups (target Phase 3, Q2, Q4 2027):** chainIds 28001-28008 with AereRollupVerifier + ZK finality gates per rollup.
- **ZK-Rollups (target Q4 2027):** scale-out to 15 operators with Groth16 validity proofs; one production AereZKRollup8 anchor live today.
- **State Channels (target Q4 2027):** scale to 7,500 active channels; AereLightningChannels primitive live today.
- **Plasma Chains (target Phase 3, Q2, Q4 2027):** AerePlasmaRootV2, sparse Merkle UTXO tree (depth 16, 65,536 UTXOs).

2.5 EVM compatibility

AERE ships full Pectra + Fusaka EVM parity. Solidity, Vyper, and any EVM-compatible language compile and execute identically to Ethereum mainnet, with no source modifications required for existing contracts. Compatible with Foundry, Hardhat, Remix; full integration with web3.js, ethers.js, viem, and all Ethereum client libraries; native support for MetaMask, Ledger, Trezor, WalletConnect, and every major Ethereum wallet.

> **Current EVM ruleset: Pectra + Fusaka (both activated 2026-05-31)**

> Chain 2800 runs the Pectra + Fusaka hardfork rulesets, functional parity with Ethereum mainnet's current EVM specification, both activated the same day via coordinated rolling validator restart on Hyperledger Besu v26.4.0. Zero downtime, no rollback.

Pectra-activated EIPs (block 2,075,363):

- **EIP-7702**, EOA delegation to smart-contract code (native account abstraction; complements ERC-4337).
- **EIP-2537**, BLS12-381 curve precompiles at 0x0b, 0x11 for cheap on-chain BLS signature verification (~70× cheaper than Solidity).
- **EIP-2935**, historical block hashes (up to 8,192 blocks back) via system contract; enables trustless cross-chain state proofs.
- **EIP-1153**, transient storage opcodes (TSTORE/TLOAD); gas-efficient reentrancy guards and callbacks.
- **EIP-5656**, MCOPY opcode for efficient memory operations.
- **EIP-6780**, scoped SELFDESTRUCT semantics.
- **EIP-7516**, BLOBBASEFEE opcode (returns 0 on AERE; no consensus-layer blob market).

Fusaka-activated additions:

- **RIP-7951**, secp256r1 / P-256 signature-verification precompile at address `0x100`. Verifies signatures from Apple Face ID / Touch ID, Apple Secure Enclave, Windows Hello, Android biometric APIs, YubiKey, TPM 2.0, EMV cards, and the EU Digital Identity Wallet at ~3,500 gas, versus ~250,000 gas required to verify the same signature via Solidity. Foundational primitive for passkey-based wallet UX on AERE.

QBFT-specific notes: EIP-4788 parent_beacon_block_root is set to zero on every block (AERE has no separate consensus-layer beacon chain). EIP-4844 blob header fields are present but no blob transactions are produced or accepted. Fusaka EIPs that are consensus-layer-only or rollup-only (PeerDAS, FOCIL, EOF) are no-ops on QBFT.

---

03 · Chapter

Tokenomics & burn engine

3.1 AERE token overview

AERE is the native token of chain 2800 and the only token on the chain, there is no wrapped stablecoin, no governance token, no liquidity-mining token. AERE pays gas, secures stake, and earns variable staking yield from protocol fee flow. AERE has no mining, no proof-of-work, and no block subsidy on QBFT. Total supply is fixed at 2.8 billion at genesis; no further minting can occur. Distribution is fully transparent on-chain, every AERE sits at one of six genesis-allocated reserve addresses, queryable via `eth_getBalance`.

- **Maximum supply:** 2.8 billion AERE (fixed at genesis, no further minting possible).
- **Token standard:** native chain-2800 token; ERC-20 wrapper (WAERE) available for DEX integration.
- **Block subsidy:** none. QBFT validators earn transaction fees only. No PoW emission, no inflation.

3.2 Token distribution

The 2.8 billion supply was allocated at genesis-v2 (2026-05-07) to six reserve addresses, all visible on-chain and queryable in real time on the public RPC.

- **Reserve (scheduled distribution) · 1.4B AERE (50%)**, released exclusively through the `AereMiningSubscription` contract (its on-chain name; the mechanism is not proof-of-work mining, there is no block subsidy on QBFT). A transparent, scheduled, contract-mediated distribution from an existing reserve. Reserve `0x038f…fFB8`.
- **Ecosystem Reserve · 560M AERE (20%)**, developer grants, ecosystem partnerships, liquidity provisioning on AERE-native DEX venues, cross-chain-registry integration incentives. Reserve `0xB6a3…1C75`.
- **Team Reserve · 420M AERE (15%)**, contributing team and advisors, subject to multi-year linear vesting. Reserve `0x7968…CCdf`.
- **Foundation Treasury · 180M AERE (6.43%)**, validator hosting, infrastructure, contract deployments, paymaster funding for onboarding, ongoing development. Available from day 1. Address `0x0243…f3C3`.
- **Airdrop Reserve · 140M AERE (5%)**, community distribution events, ambassador programs, retroactive contributor rewards, milestone-triggered airdrops. Reserve `0x2619…28B1`.
- **Strategic Allocation · 100M AERE (3.57%)**, distributed off-chain to strategic backers who funded early development; fully unlocked at genesis as part of the 280M initial circulation. Address `0xaee2…1311`.

Verification: *all six reserve addresses are listed on [docs.aere.network] and balances can be queried via* `eth_getBalance` *on* `rpc.aere.network` *at any block. The supply math is verifiable to the wei: total of all six reserves + burns + circulating EOAs = exactly 2,800,000,000 AERE.*

3.3 Burn engine + sAERE flywheel

AERE's monetary policy is enforced by immutable on-chain contracts, not by a multisig with discretion. Every transaction fee that lands in the protocol passes through these contracts on confirmation; the percentages are set at deploy and cannot be changed by any operator, validator, or Foundation address. The Foundation cannot pause them, withdraw from them, or upgrade them, they have no admin role, no upgrade proxy, and no rescue function.

- `AereFeeBurnVault`**, 37.5% per-transaction burn.** A sealed contract that receives 37.5% of every transaction fee at block confirmation and burns it by transferring to `0x000…dEaD`. No admin, no withdraw, no upgrade. Verifiable on the explorer at every block: `burnVault.balance` increases monotonically with network activity. Deployed `0x696a…B2c6`.
- `AereSink`**, three-bucket immutable router.** A second immutable router that routes protocol-level revenue (sAERE staking flow, DEX swap fees, lending interest, agentic settlement) into three fixed buckets, BURN / BUYBACK-AND-BURN / STAKER-YIELD, split 15 / 40 / 45. Percentages are set at deploy and never changeable. No admin, no upgrade. Deployed `0x6958…1676`.
- `sAERE`**, ERC-4626 receipt token.** Stakers deposit AERE and receive sAERE, a non-rebasing ERC-4626 receipt token. We structure sAERE as a receipt instrument, consistent with the SEC's August 5 2025 staking-receipt guidance (the analysis applied to stETH). This is our position, not settled law. sAERE accrues protocol revenue via AereSink's STAKER-YIELD bucket. No insider unlock, no privileged emission, no governance discretion. Deployed `0xA212…50b0`.
- **Reserve release schedule (not a PoW halving).** The AereMiningSubscription contract distributes from the 1.4B scheduled-distribution reserve on a step-down schedule. This is a transparent, scheduled, contract-mediated distribution from an existing reserve, not a proof-of-work emission. There is no QBFT block subsidy and no new minting, total supply remains 2.8B fixed.

04 · Chapter

DAO governance

4.1 Governance model

AERE's target governance design is a token-weighted DAO framework that lets AERE holders propose, vote on, and execute protocol-level changes. Decisions are bound by on-chain timelocks and supermajority thresholds rather than off-chain coordination. Votes are weighted by sAERE balance at snapshot block; holders may delegate voting power to a representative address, revocable per-block. Approved proposals are executed by the governance contract automatically after the 48-hour timelock expires, with no manual operator step. Security rests on NIST-grade cryptographic primitives (FIPS 186-4 ECDSA P-256, FIPS 180-4 SHA-256) plus mandatory timelock delays.

> **Honest status: on-chain governance is not yet operational**
>
> Token-weighted on-chain governance is not yet live. The network runs on 3 Foundation-operated validators, and protocol parameters plus Foundation-held reserves are administered by the Foundation today. Like the consensus set (3 validators, not yet decentralised, §2.2), governance is on the decentralisation path, not a claim it is already operational. The staking and delegation contracts are deployed, but binding token-weighted proposal execution is a roadmap item, not a shipped capability. The parameters below describe the target design.

4.2 Governance parameters (target design)

- **Proposal threshold:** 100,000 AERE to submit an on-chain proposal.
- **Voting window:** 7 days.
- **Execution delay:** 48-hour timelock before an approved proposal deploys.
- **Quorum:** 10% of staked tokens must participate.
- **Approval threshold:** 66% supermajority for protocol changes.

Note: the governance surface is scoped to protocol parameters. It cannot alter the immutable burn/router economics (§3.3), those contracts have no admin path, by design.

05 · Chapter

sAERE · AereProof · AERE402

5.1 sAERE flywheel, non-custodial staking receipt

`sAERE` is the canonical staking receipt for AERE. Stakers deposit AERE and receive sAERE at deposit time; the conversion ratio drifts upward as protocol revenue accrues through AereSink. sAERE follows ERC-4626, the standard for tokenised vault shares. We structure it as a receipt instrument, consistent with the SEC's August 5 2025 staking-receipt guidance (the analysis applied to stETH); this is our position, not settled law. It is the one approved exception to the AERE-only-token rule.

> **Why a receipt token, not a new asset**
>
> Our position is that a non-rebasing ERC-4626 share is best characterised as a deposit receipt rather than a new asset, it is not a wrapped stablecoin or a governance token. It represents the depositor's underlying claim on the staking position

> and accrues real protocol revenue via the immutable AereSink, not via emission or inflation. This is a characterisation, not a legal determination; the regulatory status of staking receipts is unsettled and jurisdiction-dependent.

5.2 AereProof v0, verifiable on-chain compliance

`AereProof v0` is a stack of verifiable on-chain compliance primitives, positioned as a public good and operated by the Foundation as a read-only service. The goal is to make institutional compliance integration verifiable from the chain itself, without requiring a centralised attestor or custodian intermediary.

- `AereSanctionsRegistry` **PRODUCTION**, a read-only registry of OFAC SDN-listed addresses, updated by Foundation-operated cron pulling the official SDN list. Any contract or front-end can read it to check whether a counterparty is sanctioned. Public, auditable, no fee. Deployed `0xb7d2…Cacf`.
- **Chainalysis oracle wrapper** **PRODUCTION**, wraps Chainalysis's free sanctions oracle for on-chain reads. Deployed `0x1B7B…f85c`.
- **Notabene Travel Rule SDK** **PRODUCTION**, FATF Travel Rule message exchange for institutional transfers above threshold, plus an on-chain Travel-Rule hash registry (`0xcF0E…4c84`).
- **Forta detection bots** **PRODUCTION**, real-time detection bots monitor for suspicious-flow patterns and emit on-chain alerts. Open-source; the alert stream is read-only and public.
- `AereZKScreen`**, zero-knowledge compliance screening** **PRODUCTION**, a privacy-preserving screening anchor on the SP1 zkVM. A user proves, in zero knowledge, that they belong to a Foundation-authorised allow-list (KYC, accredited-investor, or eligible-jurisdiction set) *without* revealing their identity or which entry is theirs, no personal data ever touches the chain. The proof is verified on-chain by the SP1 v6.1.0 Groth16 verifier, and the program binds a Foundation-set authorised root, so a proof only counts against the official list. dApps gate access with `isCleared(user, program, minTimestamp)`. Proven end-to-end on 2026-07-07: a real SP1 Groth16 proof cleared an address on chain 2800 (`0x3A09…C2f1`) with no PII revealed. Designed as necessary-not-sufficient, consuming applications combine it with a live sanctions check and a freshness window.
- `AereCompliancePool`**, compliant privacy pool** **PRODUCTION**, a Privacy-Pools construction (Buterin et al.) with a Travel-Rule hook. Fixed-denomination deposits; withdrawals require an association-set proof so an OFAC-sanctioned address cannot exit. This is a sanctions-*enforcing* privacy primitive, the opposite of an evasion mixer, deployed on chain 2800 (`0x7973…D41d`) with a real SP1 circuit verification key. It gives users lawful financial discretion while keeping the compliance guarantees regulators require.
- `AereAIProof`**, AI model-output attestation** **PRODUCTION**, an EIP-712 attestation log for AI model outputs. A registered model's signer attests `(modelId, inputHash, outputHash, requesterHash)` so an output's provenance is tamper-evident without revealing prompts or completions. Deployed `0xFf92…97e6`.
- **Zero-knowledge attribute family** **EXPERIMENTAL**, beyond allow-list membership, AereZKScreen defines distinct SP1 attribute programs, each a separate verification key bound to a Foundation-authorised issuer root: **over-18** (proves an issuer-attested birth year means age ≥ 18 without revealing the date of birth), **EU-jurisdiction** (proves the attested jurisdiction is one of the 27 EU member states without revealing the country), and **accredited-investor** (proves attested net worth ≥ $1,000,000 under the US Reg D test without revealing the amount). The over-18 program has a real Groth16 proof generated end-to-end and is pending a single Foundation authorising signature on-chain; the EU-jurisdiction and accredited-investor programs are specified against the same circuit pattern and not yet proven on-chain.
- **Recursive proof aggregation** **RESEARCH · DEMO-SCALE**, a single 356-byte Groth16 proof cryptographically attests that several inner SP1 proofs were verified inside the zkVM (`verify_sp1_proof`), one proof attesting a user passed both the KYC allow-list screen and the over-18 attribute. Built at demo scale and accepted by the live SP1 gateway on chain 2800, a demonstration of the compression primitive, not yet a production-scale aggregation service.

Cryptography research tracks (honest status)

zkML RESEARCH, a real neural-network forward pass (a 4→8→3 MLP, integer arithmetic) runs inside the SP1 zkVM and proves its classification without revealing the input; the committed `modelHash` binds the proof to the exact weights, and the Groth16 proof is accepted by the live gateway on chain 2800. This is a working demonstration of the primitive behind private scoring/eligibility, a small model, not a production one. Production-scale private credit scoring or medical triage would require a materially larger model and a dedicated build.

Post-quantum (hash-based) PRODUCTION, `AerePQCVerifier` (`0x1cE2…6F82`) verifies a WOTS+ (Winternitz) hash-based signature natively in Solidity. Its security rests on keccak pre-image resistance, which quantum computers do not break. Live-verified on chain 2800: valid signatures pass, forgeries are rejected. This is the XMSS/SPHINCS+ building block; lattice schemes and PQC consensus signing are separate, harder tracks.

Lattice core (Falcon/Dilithium family) N=64 DEMO, `AereLatticeVerifier` (`0x60c0…dfD9`) performs negacyclic polynomial arithmetic in the ring Z_q[x]/(x^n+1) with q=12289 (the Falcon modulus) and checks the short-vector bound, the mathematical heart of lattice signature verification. Live-verified at n=64: a valid short signature passes, a forgery is rejected. This is a reduced-parameter demonstration, not production Falcon-512, which additionally needs SHAKE HashToPoint, compressed-signature decoding, and NTT-accelerated arithmetic at n=512/1024.

DePIN compute market EXPERIMENTAL, `AereComputeMarket` (`0xf0c8…F350`) is the on-chain settlement + trust rail for a decentralized compute marketplace: providers stake native AERE, requesters escrow payment, compute happens off-chain, results confirm (or auto-confirm after a window) and pay out; disputes go to Foundation arbitration with stake slashing. The software rail is live; a real GPU network is only as deep as the hardware providers who join.

5.3 AERE402, agentic settlement layer

`AERE402` extends HTTP 402 (Payment Required) into a production settlement primitive for machine-to-machine economic interactions. Where REST APIs today rely on out-of-band API keys and centralised billing, AERE402 lets any HTTP-402 client or autonomous agent pay per call directly on-chain, with sub-second confirmation and the same execution guarantees as settlement, a standard payment interface, not a partnership with any specific model provider. The companion `AereAgent` runtime provides a Lightning-channel-style payment-channel layer for sub-cent settlement of high-frequency agent interactions. Off-chain ticks net to on-chain settlement at channel close, preserving full atomicity and dispute resolution. Deployed: `AERE402Facilitator` (`0xbA6e…4E56`), `AereAgent` (`0xE963…3536`).

---

06 · Chapter

Development roadmap

6.1 Phase 1: Foundation, completed (May, Jul 2026)

- Mainnet on QBFT consensus, Chain ID 2800, 0.5-second blocks (transitioned from 1s at block 2,138,451).
- Pectra EVM ruleset activated (2026-05-31): EIP-7702, EIP-2537, EIP-2935, full Cancun opcode set, functional parity with Ethereum mainnet.
- Fusaka EVM ruleset activated (2026-05-31): RIP-7951 secp256r1 / P-256 precompile at `0x100`.
- Multi-Paymaster stack live: EntryPoint plus OnboardingPaymaster, TokenPaymaster, StakeQuotaPaymaster, and a permissionless AppPaymasterFactory.

- Cross-chain messaging layer live: AereMessenger (Mailbox-compatible bus) + AereIGP (Interchain Gas Paymaster).
- Intent-based cross-chain UX live: AereSpokePool (ERC-7683-compatible) + AereERC7683 (IOriginSettler).
- IPyth-interface pull oracle live: AerePyth + AereOracleAdapter.
- Verifiable randomness beacon live: AereRandomnessBeacon + AereDrandConsumer (threshold-BLS-12-381).
- Deflationary fee-burn flow live: AereCoinbaseSplitter routes 37.5% of every validator coinbase sweep to AereFeeBurnVault (permanently destroyed), 62.5% back to the validator. `burnVault.balance` publicly readable.
- MEV-resistant batch-auction DEX live: AereSettlement (CoW-style batch settlement), AereVaultRelayer, AereSolverRegistry.
- Developer fee monetization live: AereFeeMonetization, registered contracts earn a share of the gas fees users pay to them.
- Sub-second block time activated (2026-05-31): QBFT block period dropped 1s → 0.5s at block 2,138,451.
- Universal Login deployed (2026-06-01): AerePasskeyAccountFactoryV2 (`0x5FFa…34fdA`) + AereEntryPointV2 (`0x8D6f…aF770`). Multi-owner accounts, real ERC-4337 validateUserOp + EIP-1271, recovery via owner-self-add.
- Passkey wallets via Touch ID / Face ID (2026-06-01): AerePasskeyAccountFactory (`0xfB0e…30739`). secp256r1 ECDSA verified on-chain in ~6,900 gas via RIP-7951.
- Native zk-proof verification (2026-05-31): SP1 v6.1.0 + RISC Zero zkVM verifier contracts deployed via the upstream gateway/router pattern. First real application-level proof followed 2026-07-07: AereZKScreen cleared an address through a genuine privacy-preserving compliance screen.
- zkML mechanism demo **RESEARCH** (2026-07-07): a 4→8→3 MLP forward pass runs inside SP1 and proves its classification without revealing the input; the Groth16 proof is accepted by the live gateway. A working demonstration of the primitive, not a production model.
- Post-quantum hash-based signature verification **PRODUCTION** (2026-07-07): AerePQCVerifier verifies WOTS+ signatures natively in Solidity.
- Lattice verification core **N=64 DEMO** (2026-07-07): AereLatticeVerifier does negacyclic ring arithmetic and short-vector checks at n=64, a reduced-parameter demonstration, not production Falcon-512.
- DePIN compute coordination layer **EXPERIMENTAL** (2026-07-07): AereComputeMarket, on-chain settlement + trust rail; a real GPU network is only as deep as the providers who join.
- Live block explorer at explorer.aere.network; public RPC at rpc.aere.network (TLS) and WebSocket at wss.aere.network.

6.2 Phase 2: Expansion (Jun 2026, Q1 2027), in progress

- Cross-chain bridge contract deployed (federated 2-of-N, ready for counterparties).
- Staking live: stake AERE for sAERE (ERC-4626 receipt) earning variable STAKER-YIELD from protocol fee flow. AERE is QBFT, so there is no mining, no hashpower, and no promised or fixed return.
- DeFi suite: yield farms, oracle feeds, payment channels, NFT marketplace, faucet.
- Lending engine live and proven end-to-end (2026-07-07) using existing sAERE/WAERE, no new token. Note: AereUSD/AereUSDC was retired per the AERE-only-token rule; stablecoin settlement is via USDC.e Warp Route (§6.4).
- Vote delegation + locked staking tiers (30/90/180/365-day) live.
- Validator set expansion to 7 nodes (tolerates 2 Byzantine per ⌊(n-1)/3⌋), pending capacity.

6.3 Phase 3: Innovation (Q2, Q4 2027), base-layer anchors live, scaling out

This tier distinguishes **shipped contract** from **planned network**. Live today: the base-layer anchor contracts, one production ZK-rollup anchor, one reference ZK system, and the Lightning / state-channel primitives. The multi-instance networks (8

optimistic rollups, 6 plasma chains, a full Lightning routing mesh, 15-operator ZK scale-out) are **not yet built**; they are §2.4 forward-looking targets with per-line dates, not a claim they run at target scale in production today.

- **Live · Layer-2 anchor contracts deployed:** AereRollupVerifier, AerePlasmaRootV2, AereShardCoordinator, base-layer primitives that L2 systems anchor to.
- **Live · one production ZK-rollup anchor:** AereZKRollup8 (depth-3 Poseidon Merkle state, Groth16 transfer proofs). One reference ZK system: circom 2 Poseidon preimage circuit + Groth16 on BN254 (/zk.html), browser-generated, verified on-chain.
- **Live · Lightning / payment-channel primitives:** AereHTLC, AereChannelRegistry, AereLightningChannels reference contracts with in-channel HTLCs and a 1-day dispute challenge window. These are building-block primitives, not a production-scale routing mesh.
- **Planned / not yet built (target Q2, Q4 2027):** 8 optimistic rollups (chainIds 28001-28008), each with sequencer + L1↔L2 bridge and a ZK finality gate.
- **Planned / not yet built (target Q2, Q4 2027):** 6 plasma child chains, each with its own AerePlasmaRootV2 and a sparse Merkle UTXO tree (depth 16, capacity 65,536 UTXOs).
- **Planned / not yet built (target per §2.4):** scale-out to 15 ZK-rollup operators + 7,500 state channels, and multi-shard committees on AereShardCoordinator.

6.4 2026 ship list (zero-cash plan)

Funded entirely from the 560M AERE Ecosystem Reserve; no external raise, no insider unlock.

- **sAERE flywheel:** ERC-4626 receipt token + AereSink 3-bucket immutable router (BURN / BUYBACK-AND-BURN / STAKER-YIELD).
- **USDC.e cross-chain Warp Route:** EU/UK BaaS rail, institutional default settlement currency.
- **AereProof v0:** verifiable on-chain compliance primitives, sanctions registry + Chainalysis wrapper + Notabene Travel Rule SDK + Forta detection bots.
- **AereSettlementHub:** institutional rails for tokenized assets (BUIDL, USDY, OUSG, LBTC, SolvBTC, pumpBTC).
- **AereBugBountyVault:** bug bounty paid in AERE; Code4rena / Cantina / Sherlock contest outreach.

6.5 Q4 2026, agentic + cross-chain

- **AERE402 + AereAgent:** agentic settlement layer (HTTP 402) + Lightning-channel-style payment-channel runtime.
- **USDT.e / USDe.e / EURC.e Warp Routes:** emerging-markets, synthetic-dollar, and EUR settlement rails.
- **AereDelegate7702:** EIP-7702 batched session keys for advanced wallet UX.
- **Threshold-encrypted mempool + Timeboost auction:** anti-MEV ordering at the protocol layer.
- **Collateral Wave 1 bridged:** BUIDL, USDY, OUSG, LBTC, SolvBTC, pumpBTC live on AereSettlementHub.

6.6 Q1 2027, scale + decentralisation

- **3 → 7 validator transition (public path to 21):** expansion to community-operated verification nodes; the network is Foundation-operated at consensus level today and this is the decentralisation path, not a claim it is already decentralised.
- **Native perp DEX:** native order-book + AMM hybrid execution venue.
- **ML-DSA precompile (FIPS 204):** post-quantum signature track.

- **CCRI Climate Rating certification:** verified ~99% less energy than proof-of-work.
- **External audit contests:** Code4rena, Cantina, Sherlock, paid in AERE.
- **AereProof v1 production:** hardened compliance primitives, third-party-audited.

---

07 · Closing

Conclusion

AERE is an EVM Layer 1 with 0.5-second deterministic QBFT finality, full Pectra + Fusaka parity, passkey-native account abstraction via the RIP-7951 secp256r1 precompile, and an immutable 37.5% per-transaction burn enforced at the protocol layer. Total supply is fixed at 2,800,000,000 AERE at genesis with no further minting possible. Distribution flows transparently through the scheduled, contract-mediated release of the reserves, ecosystem grants from the 560M AERE Ecosystem Reserve, team vesting, and airdrops, every reserve address is on-chain and queryable via the public explorer.

Through 2026 and into 2027, AERE ships the settlement-grade primitives that turn a fast EVM L1 into a public settlement layer with verifiable on-chain compliance: sAERE (an ERC-4626 receipt token we structure as a receipt instrument, consistent with the SEC's August 5 2025 staking-receipt guidance, our position, not settled law), AereSink (the immutable three-bucket revenue router), AereProof v0 (verifiable on-chain compliance primitives operated as a public good), cross-chain Warp Routes for USDC.e / USDT.e / USDe.e / EURC.e, and AERE402 (the agentic settlement layer for machine-to-machine payments).

Faster than thought. Final as math. Open as air.
The chain no one can rug.

---

08 · Disclosures

Risk factors & forward-looking statements

This whitepaper and all marketing communications referencing AERE Network contain forward-looking statements regarding the network's architecture, performance targets, validator decentralisation, custody model, ecosystem partners, and product roadmap. These statements reflect current expectations as of the date of publication and are subject to risks, uncertainties, and assumptions. Actual outcomes may differ materially. AERE Foundation undertakes no obligation to update forward-looking statements except as required by applicable law.

8.1 Current network state

- As of publication, the QBFT consensus validator set comprises 3 Foundation-operated nodes. Expansion to 7 and then 21 is a forward-looking item per §6.
- Performance figures (up to 273,000 TPS) reflect QBFT-architecture testnet benchmarks under specified conditions; sustained mainnet throughput under real load varies and is publicly observable via the live indexer.
- Layer 2 systems referenced in §6 (rollups, plasma chains, ZK rollups, Lightning channels, ERC-4337 stack) are either deployed, in development, or in design at varying stages. The canonical list of deployed contracts is at docs.aere.network#contracts.

8.2 Custody model

AERE Network itself is a non-custodial settlement layer. The chain does not custody user assets; AERE balances and contract state are controlled exclusively by private-key holders. Applications built on AERE may offer additional services, including custodial fiat services such as IBAN accounts, through licensed third-party partners (e.g. EMI-licensed BaaS providers). Where applicable, custodial services are subject to the partner's own authorisations and disclosures. Bank28 (a non-custodial neobank application built on AERE) is independently branded and operates under its own terms.

8.3 Regulatory status

AERE Network is a permissionless EVM Layer 1 blockchain. The AERE token is the network's native utility and gas token. Nothing in this whitepaper constitutes investment advice, an offer to sell, or the solicitation of an offer to buy any security or financial instrument. Token holders should independently verify the legal status of AERE in their jurisdiction before acquiring, holding, or transacting. For European users, AERE is communicated in accordance with Regulation (EU) 2023/1114 (MiCA); for UK users, communications follow the FCA's Cryptoasset Financial Promotions regime. AERE Foundation does not solicit users in jurisdictions where the offering or promotion of AERE would be prohibited.

8.4 Technology risks

- **Smart-contract risk:** deployed contracts have passed internal review, and a published Slither static-analysis report (Trail of Bits' analyzer, 14 core contracts, solc 0.8.23) found zero genuine high-severity issues (see /slither-audit). That is automated analysis, not a named third-party human audit; no named human audit (Code4rena, Cantina, Sherlock, or a firm engagement) is published yet. It is a roadmap item (§6.6); the live adversarial mechanism today is the bug bounty.
- **Validator-set risk:** a permissioned QBFT consensus with a small validator count concentrates trust in the Foundation; the expansion roadmap is described in §6.
- **Oracle risk:** AereOracle is a multi-reporter median oracle; in single-reporter periods, AERE- and FX-denominated quotes are subject to single-reporter risk.
- **Bridge risk:** cross-chain settlement is migrating from the legacy federated AereBridge to standard cross-chain Warp Routes (USDC.e Q3 2026, others following). Warp Routes use configurable Interchain Security Modules (ISMs); the trust assumption is the chosen ISM committee.
- **Upgrade risk:** hardfork rulesets (Pectra, Fusaka) are activated via coordinated validator restart. Past upgrades have been zero-downtime; future upgrades carry standard chain-upgrade risk.

8.5 Updates & contact

Material updates to this whitepaper, the contract registry, the validator set, and the custody model are published at aere.network/legal. Inquiries regarding regulatory status, audit reports, or partnership disclosures may be directed to the AERE Foundation at partnerships@aere.network.

Appendix

Deployed contract addresses (chain 2800)

Canonical mainnet addresses. All Ownable contracts are owned by the Foundation `0x0243A4f47D44b40b65D33f20329dE20D00c6f3C3`. The immutable economic contracts (AereFeeBurnVault, AereSink) have no admin role, no upgrade proxy, and no withdrawal path by construction. Source of truth: docs.aere.network. Every address below is queryable on `rpc.aere.network` and `explorer.aere.network`.

Genesis reserves

ALLOCATION	ADDRESS	AMOUNT
Strategic Investor	0xaee2f3989f0AB23296Fa3b92247fe67587141311	100M · off-chain
Foundation	0x0243A4f47D44b40b65D33f20329dE20D00c6f3C3	180M · chain admin / contract owner
Reserve (scheduled distribution)	0x038f59A40ceeCd599A4588E4B0ff4642a0fbfFB8	1.4B
Ecosystem Reserve	0xB6a364F47d21DC2CbEB803565c111c1026e11C75	560M
Team Reserve	0x7968C438204a78B4e032fcFFd9A56Edb15fdCCdf	420M
Airdrop Reserve	0x261913fA73D6F109382F1aE98Ff6822ff03628B1	140M

Core & immutable economics

CONTRACT	ADDRESS	NOTE
WAERE	0x7e84d7d66d5da4cfE46Da67CDEeB05B323e1f5e8	ERC-20 wrapper for DEX integration
AereFeeBurnVault	0x696afDF4f814e6Fd6aa45CE14C498ed9375fB2c6	37.5% per-tx burn; stateless, no admin
AereCoinbaseSplitter	0xb4b0eCe9011613A5b84248a9B42a0f309E6F01Ec	37.5% → burn vault, 62.5% → validator
AereSink	0x69581B86A48161b067Ff4E0154478062 5B231676	Immutable 3-bucket router 15/40/45
sAERE	0xA2125bE9C6fd4196D9F94757Df18B3a2A5e650b0	ERC-4626 receipt, 7-day drip
AereLockedStaking	0x21108c28A849b05aE6b7a3a5bc435C9Bc897E7Ad	Fixed-term staking (30/90/180/365d), holder yield, not delegation, not validation
AereLockedStaking	0x21108c28A849b05aE6b7a3a5bc435C9Bc897E7Ad	30d/90d/180d/365d locks
AereGovernanceStaked	0x8D77C888e439C4fADb2e23F1567a0A1965F80bCb	Stake-weighted governance
AereMiningSubscription	0xDad25d2163187DF8AAEcf9EA31b6355315Bb69f1	On-chain name; scheduled reserve distribution, not PoW mining; 4 tiers, 30-day periods

Compliance & privacy (AereProof v0)

CONTRACT	ADDRESS	STATUS
AereSanctionsRegistry	0xb7d235718D99560F6EA4Fc5eAea2F8a306A3Cacf	Production
ChainalysisOracleWrapper	0x1B7Be82C80f368f75Cb3807B1bc05E86A498f85c	Production
AereTravelRuleHashRegistry	0xcF0E2e010E6e4506672019b1e570874AEeBC4c84	Production
AereZKScreen (v3)	0x3A097A459FD26aC79573aCB5adB51430e473C2f1	Production · zk allow-list + attributes
AereCompliancePool	0x79735c31F289F7A4d6Be3E02aaB70B544796D41d	Production · sanctions-enforcing privacy pool
AereCompliancePoolSP1Verifier	0xE2D3fa91b680E835c971761ba75Fde0204AEF95E	SP1 circuit vkey
AereAIProof	0xFf92c669AbF4C1DAE31eBFCC017764036d9D97e6	Production · EIP-712 model attestation
AereForensicEventRegistry	0x4a7526A068e5DDE9788f6571E4A99095b14C6fff	Production

Cryptography research tracks

CONTRACT	ADDRESS	STATUS
AerePQCVerifier	0x1cE2949e8cE3f1A77b178aF767a4455c08ec6F82	Production · WOTS+ hash-based PQC
AereLatticeVerifier	0x60c06E6A3CC201B46A16650be096C6E45424dfD9	Research · n=64 lattice demo
AereComputeMarket	0xf0c8178a5d9feb0f70C5f184e79edeEDaddcF350	Experimental · DePIN settlement rail

zk-verifier stack (multi-prover)

CONTRACT	ADDRESS	NOTE
SP1VerifierGateway	0x9ca479C8c52C0EbB4599319a36a5a017BCC70628	Stable route target (SP1)
SP1VerifierGroth16_v6_1_0	0xb5456d48bFdA70635c13b6CBE1Ad0310Dc0171aD	Current production Groth16
RiscZeroVerifierRouter	0x3f7015BC3290e63F7EC68ecF769b00aB296a249C	Stable route target (RISC Zero)
AereProofRegistry	0x0A9b09677DbE995ACfC0A28F0033e68F068517Ee	Multi-prover attestation log

Account abstraction & paymasters

CONTRACT	ADDRESS	NOTE
AereEntryPointV2	0x8D6f40598d552fF0Cb358b6012cF4227B86aF770	ERC-4337-shaped EntryPoint
AerePasskeyAccountFactoryV2	0x5FFa9a6487DA4641a1A1e7900ff2bD4525D34fdA	Multi-owner passkey accounts
AereOnboardingPaymaster	0x4058E406475Dbed7056Aee0c808f293F05fEa879	Foundation-funded, hard-capped
AereTokenPaymaster	0xEb6e2Eb24e597C85392DdCD68a1F9b654FffdcB2	Pay gas in whitelisted ERC-20
AereStakeQuotaPaymaster	0xD16C86D792444c2667A26dB62f01b90FC0DaB87b	Stake → daily free-tx quota
AereAppPaymasterFactory	0xEC22603E8712cBc5c31E53370D10f1a80CcB4DF0	Permissionless per-dApp paymaster

Cross-chain, oracle & randomness

CONTRACT	ADDRESS	NOTE
AereMessenger	0xe54c2329f0786CFE3420c566B646148D25477325	Mailbox-compatible message bus
AereIGP	0x61B48615F490A23945988c92835eF35fdD86E837	Interchain Gas Paymaster
AereSpokePool	0xCAB1DBA5f6F06198000C20a974d675f1B3181AbD	ERC-7683 / Across-v3 compatible
AereERC7683	0x67Fb9830e3a2BC06cEb641cfF3beD87b273ccb29	IOriginSettler
AerePyth	0xb7F3354C1E0C5ef89D8b1072a3CEa7FFEf2FfE3F	IPyth-compatible pull oracle
AereRandomnessBeacon	0x25b6317efD8C7d425210F56Ee1E204852CD8213C	Threshold-BLS drand consumer

DeFi, settlement & agentic

CONTRACT	ADDRESS	NOTE
AereSwapFactory	0xf0a8df7BDc25721892475B21271e52D77B0e84DC	V2 AMM factory
AereSwapRouter	0x7526B2E5526EfA84018378b60F2844Dad77523D8	V2-style periphery
AereSettlement	0x9C2957b1622567B4802E4AFd4c42FB2ec70dE875	CoW-style batch settlement
AereSettlementHub	0x2a02fD80c16293D2B5D8a295F31D1a6E6a582c02	Tokenized-asset rails
AereLendingMarket (sAERE/WAERE)	0x2C2d39dB711C0A33De04Dc74b1E22f4760FD4bb0	Engine proof market (no new token)
AereLendingOracle	0xc0f18A567067F1B84BDf75eDEbFaDdCBb70A4C49	Multi-source lending oracle
AERE402Facilitator	0xbA6e6700D629a5E3C885778a42885a944CA84E56	HTTP-402 machine payments
AereAgent	0xE96396B4b596B3A74e4195Be12aADd5257863536	Agent runtime / payment channels
AereFeeMonetization	0x6b62DC6cC974F779354c953F41b64a7aB994dd98	Developer fee-share NFTs
AereInsuranceFund	0x5Ab95C549c2A2b07913Df7edD4a16fd108B7CAAC	7-day cooldown, bad-debt coverage

← Interactive whitepaper · Open explorer · LLM reference (llms-full.txt)