AEREDIUM

The Trust Layer

Blockchain Technical White Paper

The Privacy-Preserving Chain of Record for Institutional Digital-Asset Settlement

Version 3.7

May 2026

AEREDIUM Group

US Patent Application 63/977,868 — TSS-USIG / AERKey threshold-signing architecture
US Patent Application 19/400,910 — AEREDIUM Audit (multi-model continuous reserve verification)
US Patent Application 09857-P0001A — AERLink (Decentralized Access to Centralized APIs, DACA)

Contents

1. Abstract

This document specifies AEREDIUM, an EVM-compatible blockchain designed as the privacy-preserving chain of record for institutional digital-asset settlement. The wedge market is institutional stablecoin settlement; the addressable market extends to tokenised real-world assets, securities, payments, treasury, custody, and cross-border value movement — the full surface of institutional activity that moves onto programmable rails over the next decade. AEREDIUM is the inter-institutional settlement layer that no single bank can build and no consortium of banks can sustain at scale, because the requirement is non-centralisation itself.

The architecture combines hardware-attested TEE-BFT consensus deployed across multiple independent cloud providers, threshold-distributed key management through AERKey, native chain-level transaction encryption, parallelised EVM execution measured in the hundreds of thousands of transactions per second under ongoing optimisation, bridgeless cross-chain interoperability across a growing list of production network integrations via the Trans Layer, threshold-governed access to traditional bank APIs and enterprise systems via AERLink (DACA), and Bitcoin-anchored finality.

AEREDIUM is built for an institutional settlement environment defined, in May 2026, by two simultaneous structural facts. The first is that institutional adoption of blockchain settlement is happening at unprecedented scale: JPMorgan's Kinexys is targeting ten billion dollars in daily volume; sixteen of the largest banks and market infrastructure providers in the world have collectively funded Fnality's regulated wholesale payment system; the BCG/Ripple projection of $18.9 trillion in tokenised real-world assets by 2033 is grounded in current adoption velocity. The second fact is that the existing public-chain and bridge infrastructure on which much of this institutional value depends is being industrially attacked at unprecedented scale, by state-level actors equipped with AI tooling whose effectiveness compounds with every model release. April 2026 was the worst month in the history of crypto exploits — approximately $629 million stolen across thirty separate incidents — with cumulative 2026 losses crossing $1 billion within four months, approximately three-quarters attributed to North Korean state-sponsored attackers.

The architecture supports two modes of operation. In Standard Mode, AEREDIUM operates as a high-throughput EVM Layer 1 with cross-chain settlement to production networks via the Trans Layer. In Privacy Mode, institutional users transact entirely within an encrypted ledger where transaction amounts, counterparties, token types, and economic activity are mathematically opaque to all third parties — including the operators of the chain itself — while remaining fully visible to the user and to whomever they explicitly authorise through the AERKey Policy Engine. AERLink extends this surface to non-blockchain systems: bank cores, ERPs, payment networks, market-data providers, and custodial APIs can be invoked as native chain operations under the same threshold-governed authority, with the counterparty system unchanged.

Five architectural properties together distinguish AEREDIUM from any existing institutional blockchain. Privacy is enforced cryptographically rather than by policy. Cross-chain interoperability is bridgeless: the Trans Layer eliminates the bridge attack surface that has cost the industry billions of dollars in 2021 through 2026, including the April 2026 KelpDAO/LayerZero exploit of approximately $290 million. Smart contract administrative keys, custodial keys, and bridge release keys are themselves managed through AERKey threshold infrastructure. Access to traditional financial systems is threshold-governed through

AERLink, so the bank rails and enterprise systems that institutional value already flows through become reachable as composable chain primitives without the counterparty integrating any new technology. The trust root of the chain is decentralised by design through cryptography and hardware enforcement: AEREDIUM Foundation (Cayman Islands) operates the infrastructure as a named, accountable Protocol Operator; the cryptographic guarantees are executed inside Trusted Execution Environments distributed across independent cloud providers and cannot be defeated by the Foundation, by any single operator, or by any single jurisdiction. This is Verifiable Infrastructure: an accountable operator combined with cryptographic enforcement that no operator can override.

In the threat environment of 2026, these properties are not optional features. They are the structural requirements for any blockchain that institutional value flows through. This document specifies the architecture that delivers them. The reader is referred to the AEREDIUM Tokenomics document at aeredium.io/tokenomics.html for the economic model of the AER token, and to the AERKey Privacy Layer Wallet Architecture for the full cryptographic specification of Privacy Mode.

2. The Settlement Crisis of 2026

The institutional financial system is engaging with blockchain settlement at scale for the first time. The landscape of 2026 is one of broad, well-funded adoption — not skepticism — but that adoption is happening against a security backdrop the existing architecture cannot absorb.

2.1 Institutional adoption is real and accelerating

JPMorgan's Kinexys platform processes over $2 billion in daily wholesale payment volume in May 2026 and is targeting $10 billion. The Fnality consortium of sixteen G-SIB and market-infrastructure shareholders operates regulated wholesale CBDC-equivalent settlement in GBP, with EUR and USD facilities advanced. Goldman Sachs DAP is in production for tokenised collateral, BNY Mellon and HSBC have launched institutional digital-asset custody platforms, and the BCG/Ripple projection of $18.9 trillion in tokenised real-world assets by 2033 reflects an adoption velocity already visible in current product launches. The institutional commitment to blockchain settlement is not speculative; it is operational.

2.2 The threat environment has industrialised

Against this institutional backdrop, the attack environment has deteriorated to a degree without precedent in the industry's history. April 2026 saw approximately $629 million stolen across thirty separate incidents — the worst month in DeFi's recorded history. Cumulative 2026 losses crossed $1 billion within four months. Approximately three-quarters of those losses are attributed to North Korean state-sponsored actors operating with the explicit objective of funding sanctioned weapons programmes through digital-asset theft. The scale, persistence, and sophistication of these operations now match the most resourced cyber-offensive units in any domain.

2.3 AI is amplifying the attacker's capability faster than the defender's

Frontier AI models can now autonomously discover and exploit smart contract vulnerabilities at success rates that have made the traditional audit-based security model structurally inadequate. Anthropic's December 2025 red-team study demonstrated that frontier models scan for and exploit smart contract vulnerabilities at approximately $1.22 per attempt, with the median cost of producing a working exploit having declined by 70.2 percent across four model generations in six months. a16z's April 2026 research found that AI agents always identify the underlying vulnerability — failures occur in multi-step exploit assembly, precisely the part of the gap that is closing fastest. The race to audit faster than the attacker is already lost.

2.4 The locus of attack has shifted

Through 2024 and 2025, the dominant attack surface was bridge infrastructure — Ronin, Wormhole, Nomad, Multichain, Harmony. Through 2026 it has shifted to the seams between systems: bridge verifier networks, signer multisigs, oracle infrastructure, and the administrative keys to smart contracts that hold pooled institutional value. The April 2026 KelpDAO/LayerZero exploit drained approximately $290 million by compromising two LayerZero RPC nodes, forcing failover into poisoned infrastructure, and fabricating a phantom cross-chain message. Three weeks earlier the same attack group drained $285 million from Drift

Protocol via a different vector. In seventeen days, one nation-state actor extracted more than half a billion dollars from DeFi by attacking the connective tissue between chains.

2.5 The crisis stated in one sentence

Institutional value is moving onto blockchain infrastructure at unprecedented scale, while the connective tissue of that infrastructure — bridges, verifier networks, administrative keys, and the seams between chains — is being industrially attacked by state-level adversaries equipped with rapidly improving AI tooling, *and the defensive responses available to the existing architecture are reactive rather than structural*.

3. The Limits of Bank-Operated Settlement Infrastructure

The institutional response to date has been to build bank-operated settlement chains: Kinexys, Onyx, Orion, DAP, Fnality, Partior. Each is a credible engineering effort and each solves a real problem within its perimeter. None addresses the inter-institutional layer that the next decade of tokenised finance requires, because that layer requires a structural property no bank can deliver: non-centralisation.

3.1 What banks have built — stripped of marketing

The bank-operated chains are permissioned EVM or Hyperledger networks operated by a single bank or a small consortium. They provide tokenised representations of bank deposits, programmable settlement of intra-institutional flows, and 24/7 operation. They are excellent infrastructure for what they are: the bank's own internal ledger, extended to programmable form. They do not, and cannot, serve as the neutral settlement layer between competing institutions, because the operator is itself a competing institution.

3.2 What banks structurally cannot build

A bank is a single legal entity, anchored in a specific jurisdiction, subject to that jurisdiction's regulators, with fiduciary obligations to its shareholders and commercial dependence on administrative privacy. These constraints — the constraints that make banks banks — prevent any bank from operating multi-party threshold-attested infrastructure where execution is enforced by cryptography rather than by the operator's policy. A bank can be ordered, by a competent jurisdiction, to change the rules; that is precisely the property that disqualifies it from operating neutral inter-institutional infrastructure. A counterparty bank in a different jurisdiction does not accept that compelled-process authority as a feature of the rail it settles on.

3.3 The historical pattern

This is not new. Every prior generation of financial infrastructure has resolved the same tension the same way. Inter-bank messaging consolidated onto SWIFT (a Belgian cooperative). Wholesale settlement consolidated onto Fedwire (the central bank) and CLS (a separately chartered utility). Securities clearing consolidated onto DTCC and Euroclear (separately chartered utilities). FX settlement consolidated onto CLS Bank. In each case, bank-operated solutions persisted for narrow internal use cases, and the inter-institutional volume moved to a neutral utility. The pattern is structural rather than accidental.

3.4 The class of infrastructure that requires non-bank operation

Putting the structural argument and the historical pattern together: there is a specific class of institutional financial infrastructure that no bank can build, no consortium of banks can sustain at scale, and no national-champion FMI can deliver — because the requirement is non-centralisation itself. This class includes inter-institutional payment messaging (SWIFT), wholesale settlement utility (Fedwire, CLS), clearing utility (DTCC, Euroclear), and now: inter-institutional encrypted digital-asset settlement.

That last category is the AEREDIUM market. It exists because the institutional financial system needs a settlement layer that no single bank — and no consortium of banks — can ever provide. The decentralisation is not optional; it is the specification.

4. AEREDIUM: Decentralisation That Banks Cannot Provide

4.1 The thesis

AEREDIUM is the SWIFT, Fedwire, and DTCC of the tokenised financial system, rebuilt as a single cryptographically-private neutral settlement layer in which the rules are enforced by hardware and cryptography rather than by operator policy. AEREDIUM Foundation (Cayman Islands) operates the infrastructure as a named, accountable Protocol Operator. What distinguishes AEREDIUM is not the absence of an operator — every neutral utility, including SWIFT, Fedwire, and DTCC, is operated by a named entity — but the property that the chain's rules are enforced by hardware-attested code rather than by the operator's discretion. The Foundation cannot read user transactions, cannot sign cross-chain operations unilaterally, and cannot modify consensus rules without deploying new code that produces a different attestation hash that the existing validator network rejects.

4.2 The analogy that lands

The reader can locate AEREDIUM by analogy to the existing institutional infrastructure stack.

Legacy utility	AEREDIUM equivalent
SWIFT — inter-bank message routing	Settlement-grade message and transaction routing for tokenised digital assets
Fedwire / RTGS — central-bank-money settlement finality	Cryptographically-attested settlement finality for tokenised digital assets, two-second block time, one-block finality
DTCC / Euroclear — securities clearing and settlement	Tokenised securities, stablecoins, and real-world assets clearing and settlement under selective-disclosure compliance
CLS — FX settlement risk reduction	Cross-chain and cross-system settlement risk reduction — natively connecting EVM chains, non-EVM chains including Solana and Bitcoin, and traditional banking and enterprise systems via the Trans Layer and AERLink

Where AEREDIUM differs from each of these legacy utilities is in how the integrity of the system is enforced. SWIFT's Belgian cooperative, Fedwire's Federal Reserve, and DTCC's US corporate structure each enforce system rules through policy and operational control: the operator decides what is permitted, what is disclosed, what is censored, and to whom. SWIFT's disconnection of Russian banks in 2022 is a reminder that policy-enforced utilities are politically actionable. AEREDIUM's system rules are enforced cryptographically by Trusted Execution Environments, not by Foundation policy. This is the structural separation of operational stewardship from rule enforcement that makes the chain genuinely neutral.

4.3 Decentralisation by design — through cryptography, not governance

AEREDIUM's decentralisation is structurally different from what either bank-operated chains or DAO-governed public chains provide. It is decentralisation through the immutable properties of hardware isolation and cryptographic proof, not through anonymous validators, token governance, or consortium

arrangements. AEREDIUM names this category Verifiable Infrastructure, and it sits between the trustless model of public blockchains (anonymous validators, economic incentives, no accountable entity) and the trusted model of permissioned chains (named operator, policy enforcement, no cryptographic verification).

AEREDIUM Foundation is the operating entity. The Foundation pays for cloud infrastructure, deploys validator software, controls instance lifecycle, and is accountable to its regulator and to its institutional counterparties. What the Foundation does not control — and what no operator can control on AEREDIUM — is the cryptographic enforcement layer. Validators execute inside Trusted Execution Environments distributed across AWS Nitro Enclaves, Azure SEV-SNP, Google Cloud Confidential Space, and Intel TDX. Each validator's code is measured by hardware, the hardware attests to the measurement cryptographically, and the consensus protocol accepts only blocks signed by validators whose attestation proves they are running the canonical code. Covert modification is technically impossible — any change to validator code is cryptographically evident through the attestation, and every observer can see that the code hash has changed.

The cryptographic privacy and the operator-neutrality follow from the same property: any administrative access to clear-text transactions would require modifying the running TEE code, which would change the attestation hash, which would cause the existing validator network to reject the modified validator. The full economic and governance model of the chain — including the AER token, fee mechanics, treasury structure, and Foundation legal architecture — is set out in the AEREDIUM Tokenomics document published at aeredium.io/tokenomics.html. The summary motto, applicable to both the protocol and the token, is: the technology assures the governance.

4.4 How public chains fit

AEREDIUM does not replace public chains. It sits between them. The user's USDC enters AEREDIUM from Ethereum through a custody pool, lives encrypted on AEREDIUM during the period of activity, and exits to whatever destination chain the user selects. From outside, what is visible is the boundary — deposit and withdrawal events at the custody pool address. Inside, what occurs is encrypted, executed in the hundreds of thousands of transactions per second range under ongoing optimisation, and finalised in two seconds, with selective disclosure to authorised parties through the AERKey Policy Engine. Public chains are the inbound and outbound rails. AEREDIUM is the encrypted settlement layer between them. The institutional thesis does not require any public chain to fail or change.

5. How Banks Use AEREDIUM

A reasonable question follows from §3. If banks structurally cannot operate decentralised infrastructure, can banks even use it? The answer is yes — and the reasoning is exactly the same reasoning that explains why every major bank uses SWIFT, Fedwire, DTCC, CLS, Visa, Mastercard, and Amazon Web Services, none of which any single bank operates.

5.1 Operator versus user — the distinction that matters

Banks routinely transact across infrastructure they do not operate. The operational rules are set by parties other than the bank; settlement is enforced by parties other than the bank. The bank's regulators are comfortable with this because the regulator cares about the bank's compliance behaviour, not the bank's ownership of the underlying rail. AEREDIUM occupies the same architectural slot as the existing neutral utilities. The fact that it is decentralised rather than cooperatively operated is irrelevant to the user-side regulatory analysis. What matters is whether using AEREDIUM lets the bank satisfy its compliance, fiduciary, and operational obligations. The answer is yes — and on several dimensions, better than the alternatives.

5.2 The bank regulator's checklist

The questions a bank's regulator asks of any new piece of digital-asset infrastructure are well-established. AEREDIUM answers each of them inside the existing supervisory framework, with no novel regulatory question raised.

The bank's regulator asks	AEREDIUM's answer
Does the bank know who its customer is?	Institutional KYC through AERKey onboarding, supplemented by the bank's own KYC where the bank is sponsoring or facilitating
Can the bank screen counterparty activity against sanctions lists?	Yes — through Policy Engine entries that grant the bank's compliance team scoped, audit-logged read access to relevant transaction metadata
Can the bank produce records on demand for examination?	Yes — with cryptographic attestation that exceeds what is available on any permissioned chain today
Are client funds safe under custody?	Threshold-distributed across hardware-attested enclaves on independent cloud providers in independent jurisdictions; arguably stronger than any single custodian
Can the bank satisfy the FATF Travel Rule?	Yes — structured counterparty-data exchange between AERKey-onboarded institutions is a first-class Policy Engine capability
Can the bank file SARs and CTRs from on-chain activity?	Yes — every Policy Engine disclosure event produces a tamper-evident chain-anchored record
Can the bank exit positions if it chooses to wind down?	Yes — Trans Layer withdrawals to public chains are a standard flow

This is the same checklist regulators run against Coinbase Custody, Fireblocks, Anchorage Digital, BitGo, and the other regulated digital-asset custodians that banks use today. AEREDIUM operates inside the same framework. There is no novel regulatory question — only a sharper architectural answer to the existing questions.

5.3 The compliance officer's specific concern

The strongest pushback from a bank's compliance function takes the form: "I need to see my clients' transactions." The answer needs to be precise. A bank's compliance officer does not need — and is not legally entitled to — see every transaction on the chain. The compliance officer needs to see the bank's clients' transactions for the purpose of fulfilling the bank's obligations to those clients. AEREDIUM provides exactly that. The institutional client grants the bank's compliance team a Policy Entry covering the appropriate scope. The bank reads what it needs to read. Every access is cryptographically attested to a Merkle-chained audit log anchored on Bitcoin. What the bank cannot do — and the bank's general counsel will be relieved by this — is read other banks' clients' transactions. That separation is structurally enforced, which is exactly what regulators and litigation counsel want.

5.4 Progressive bank engagement — additive, not replacement

AEREDIUM is additive infrastructure, not replacement infrastructure. Banks engage with AEREDIUM at any of four levels without operating it, and — critically — without modifying the core banking, ERP, messaging, or compliance systems they already run. The integration burden on the bank's side is bounded: at the lighter levels, the bank holds an institutional wallet and signs transactions; at the heavier levels, the bank's existing APIs become reachable as composable chain primitives through AERLink (§9), so the bank's systems remain untouched while AEREDIUM provides the inter-institutional execution and interoperability surface above them.

Level	Engagement and commercial logic
Participant	Bank holds its own institutional wallet on AEREDIUM and transacts directly under its own Policy Engine relationships. Treasury and intercompany flows benefit from cryptographic privacy and 24/7 settlement.
Service offering	Bank offers AEREDIUM access to its clients as part of its digital-asset service offerings. Same commercial model as offering Coinbase Custody or Fireblocks today; retains client wallets that would otherwise leave the bank.
KYC sponsor	Bank sponsors counterparties onto AEREDIUM, becoming the institutional KYC anchor for its clients' AEREDIUM activity. Generates fee income; deepens the bank's role as compliance gateway.
Inter-bank interface	Bank exposes its existing core-banking, payment, or settlement APIs to AEREDIUM through AERLink. The bank's system is not modified; the API is invoked under threshold-signed chain authority. Extends the bank's reach into market segments its walled garden cannot serve.

The framing matters. The structurally-correct read of AEREDIUM, for a bank's strategy function, is not "a new chain we have to integrate" but "a neutral utility that connects what we already have to the rest of the institutional ecosystem." Banks can keep their core banking, their messaging, their compliance stack, and their existing client relationships. AEREDIUM provides the execution and interoperability layer above those systems. That is the opposite of rip-and-replace.

5.5 The institutional middle market

The bank-as-user case is real but is not the dominant addressable market for AEREDIUM. The larger market is everyone the bank chains do not admit: institutional middle-market funds, corporate treasurers, regional and digital banks, fintechs, tokenisation platforms, stablecoin issuers, market makers, and asset managers without G-SIB custodianships. These institutions onboard to AEREDIUM directly through AERKey, transact among themselves and with bank-sponsored counterparties, and use the Policy Engine for their own compliance and audit needs. The historical lesson of every neutral utility — SWIFT, Visa, DTCC, CLS — is that the addressable market is always larger than the founding consortium, and the utility wins precisely because it admits participants who were structurally excluded from the bank-operated alternatives.

5.6 The marginal investment question

As AEREDIUM scales, the marginal return-on-investment calculation for continuing to develop walled-garden chains gets harder for banks to defend. Building a brand-new institutional chain from scratch in a market where AEREDIUM exists as a credible neutral layer is duplicate engineering against a smaller addressable market. Adding new use cases to a walled-garden chain when the same use cases on AEREDIUM serve the bank's clients and the rest of the institutional ecosystem is a misallocation of incremental investment dollars. Existing walled-garden infrastructure for existing intra-bank use cases continues to make sense. The marginal investment in extending those gardens does not.

6. Two Modes of Operation

AEREDIUM supports two modes of operation, selectable at the user level. The choice can be made per asset, per transaction, or per counterparty. Both modes share the same wallet, the same authentication, the same AERKey trust boundary, and the same recovery flow. The difference is only where the asset lives at the moment of the transaction and what observers see on which chain.

6.1 Privacy Mode — AEREDIUM as full chain of record

In Privacy Mode, the user deposits an asset — for example, USDC from Ethereum — once, into the AEREDIUM custody pool. AEREDIUM mints an encrypted representation of the asset against the user's AEREDIUM address. From that point forward, all subsequent activity — payments, transfers, payroll, settlements, treasury moves — happens on AEREDIUM, encrypted under the AERKey Privacy Layer specification. The user withdraws to a foreign chain only when the economic activity needs to exit the AEREDIUM environment. Inside AEREDIUM, all activity is mathematically opaque to third parties. The transaction amount, counterparty, token type, fee, and memo are encrypted under AES-256-GCM with keys threshold-distributed across AERKey enclaves.

6.2 Standard Mode — cross-chain passthrough

In Standard Mode, AEREDIUM operates as a high-performance EVM Layer 1 with native cross-chain settlement via the Trans Layer. Assets remain on their native chains; transactions are broadcast to the destination chain through threshold-signed cross-chain operations; the destination chain's block explorer displays the transaction in plaintext as it would for any other transaction on that chain. Standard Mode is appropriate for one-off retail transactions, transactions with counterparties not on AEREDIUM, and any context where the destination chain's transparency is acceptable to the user.

6.3 What observers see

Consider a Privacy Mode user with an Ethereum address that previously held USDC. After they enter Privacy Mode, an observer of their Ethereum address — through Etherscan, MetaMask, Chainalysis, or any other chain-analytics tool — sees the pre-existing transaction history, a single deposit to the AEREDIUM custody pool address, then silence until eventual withdrawal. All actual economic activity — payroll, settlements, treasury moves, payments, swaps, lending operations — happens on AEREDIUM, encrypted, invisible. From the perspective of Ethereum-side analytics this user has effectively gone dark.

Etherscan watchers monitoring the AEREDIUM custody pool see aggregate institutional flows but cannot infer who within the pool moved what to whom. This pattern is structurally similar to how institutional custody addresses operate today across Coinbase, Fireblocks, and BitGo, but with three properties no existing custodian provides: privacy is enforced cryptographically rather than by access controls; selective disclosure is structured and regulator-grade through the Policy Engine; and the activity ledger inside the pool is itself a blockchain with cryptographic auditability. This is what differentiates AEREDIUM from privacy mixers: the custody pool is operated under a fully KYC'd institutional onboarding model with the Policy Engine governing all disclosures. A regulator with lawful demand can obtain scope-bounded, time-bounded, audit-logged disclosure of any user's activity.

6.4 What MetaMask sees

MetaMask itself has no native block explorer; it queries Etherscan or the equivalent for whichever chain the user has selected. "What MetaMask shows" therefore reduces to "what the underlying chain's explorer shows." Two cases must be considered. In the first, the user has gone Privacy Mode and uses MetaMask only on its native chains. MetaMask shows the wallet's pre-AEREDIUM history, the single deposit to the custody pool, then silence. The user's actual current balance — which lives in encrypted form on AEREDIUM — is invisible to MetaMask.

In the second case, a technically motivated user adds AEREDIUM as a custom RPC endpoint to MetaMask. Because AEREDIUM is EVM-compatible, this works. But MetaMask is not AERKey-aware and cannot perform the wallet-signature session unlock that derives the user's address salt key. MetaMask connected to AEREDIUM RPC therefore sees only the public on-chain envelope: transaction identifiers, ciphertext blobs, initialization vectors, authentication tags, and key references. No counterparties, no amounts, no tokens, no memos. The privacy guarantee is enforced at the protocol level, not at the wallet level. To work usefully on AEREDIUM the user opens the StablePro Wallet — or any AERKey-aware wallet — which performs the unlock ceremony and renders decrypted transaction history. This is comparable to using Signal: the encryption is invisible to the user, and the data is visible only after the device is properly authenticated.

7. Architecture Overview

7.1 The module stack

AEREDIUM is composed of production modules that operate inside hardware-attested TEE enclaves and communicate over authenticated channels. The modules are designed for independent failure isolation and for deployment across multiple cloud providers; no module has a single-host or single-cloud dependency at the consensus path.

Module	Purpose
Consensus	TEE-BFT consensus with USIG anti-equivocation; VRF leader election; 2f+1 Byzantine fault tolerance
EVMSO	EVM-compatible execution engine with Block-STM parallel execution; benchmarked in the hundreds of thousands of TPS range under ongoing optimisation
Attestation	Cryptographic attestation-hash generation over batched execution; SHA-256 commitment over canonical block bytes; handed off to Notarization for Bitcoin anchoring
Notarization	Bitcoin anchoring of state commitments via OP_RETURN; scheduled and on-demand
API Gateway	Ethereum-compatible JSON-RPC and WebSocket interface; sixty methods; mTLS-protected
Cloud Controller	Multi-cloud validator orchestration; load balancing and live migration across providers
AERKey (TSS-USIG)	Threshold key management and signing infrastructure; CGGMP24 production, CGGMP25 in deployment
TSS Network	Authenticated inter-enclave networking for threshold operations; vsock and gRPC over mTLS

7.2 Layers above the module stack

Four named layers operate above the module foundation. Each combines the underlying modules into a capability that institutional users interact with directly.

The Privacy Layer implements wallet-level and chain-native encryption, tiered block-explorer visibility, and the Policy Engine for selective disclosure. It is described in §10 and specified in full in the AERKey Privacy Layer Wallet Architecture.

The Trans Layer implements bridgeless cross-chain settlement to production networks including Ethereum, Bitcoin, Tron, BSC, Polygon, Arbitrum, Optimism, Base, Solana, Avalanche, and others, with the integration list expanding rapidly under demand-driven development. It uses AERKey threshold-signed operations to move value between chains without traditional bridge architectures. Specified in §13.

The AERLink Layer (DACA — Decentralized Access to Centralized APIs) implements threshold-governed access to traditional non-blockchain systems: bank cores, ERPs, payment networks, market-data providers, custodian APIs, SWIFT messaging, and card networks. AERLink is what allows the unchanged APIs of traditional financial systems to become composable chain primitives, with credentials held inside attested enclaves and access gated by AERKey threshold signatures. Specified in §9.

The Trust Contract Layer is the institutional smart contract surface. Standard EVM contracts compile and run unchanged. Trust Contracts add additional capabilities — encrypted state storage, policy-bound execution, and threshold-signed operations — unique to AEREDIUM. Critically, the administrative keys controlling Trust Contracts are themselves managed under AERKey threshold custody, eliminating the single-point-of-key-compromise pattern that has caused most of the largest losses in the institutional digital-asset space.

7.3 Transaction lifecycle in Privacy Mode

A Privacy Mode transaction flows through the following stages from wallet to finality:

Stage	Operation
1. Wallet	User constructs transaction; wallet signs with private key and submits to AERKey via authenticated session
2. AERKey	Verifies wallet signature; derives Transaction Encryption Key (TEK), Address Salt Key, and Key Encryption Keys for sender and recipient inside attested enclaves
3. AERKey	Encrypts payload under AES-256-GCM; wraps TEK under each authorised reader's KEK; computes from_hash and to_hash via HMAC-SHA256
4. Wallet	Receives encrypted transaction object and broadcasts to AEREDIUM
5. Consensus	TEE-BFT validators verify structure without decryption; USIG counter increments; VRF-elected leader proposes block
6. EVMSO	Block-STM parallel execution applies state changes; encrypted payload remains encrypted in storage
7. Attestation	Computes a 32-byte SHA-256 commitment over canonical batch bytes and hands the attestation hash to Notarization without exposing transaction content
8. Notarization	State commitment anchored to Bitcoin every one hundred blocks via OP_RETURN; on-demand anchoring available for specific commitments

Total time from wallet submission to AEREDIUM finality is approximately two seconds. Bitcoin anchoring adds approximately ten minutes for the next anchored state commitment. The user's wallet shows the transaction confirmed within seconds; the deeper finality property — Bitcoin-anchored — accumulates over the next anchoring cycle without blocking the user experience.

8. AERKey: The Institutional Trust Layer

AERKey is the cryptographic foundation that makes the AEREDIUM thesis enforceable. Every privacy guarantee, every threshold-signed operation, every selective-disclosure event, and every cross-chain transaction in the AEREDIUM stack passes through AERKey. Without AERKey, AEREDIUM would be a high-throughput EVM chain with policy-based privacy promises. With AERKey, AEREDIUM is the only blockchain whose institutional privacy guarantee is enforced by mathematics rather than by trust in operators.

8.1 What AERKey does

AERKey performs five distinct functions inside the AEREDIUM architecture, each enabled by the same threshold infrastructure applied to different cryptographic operations.

It is the institutional signing system: every transaction signed by the AEREDIUM chain — block proposals, validator votes, cross-chain operations on the Trans Layer, Bitcoin anchoring transactions, AERLink invocations of external APIs — is signed by an AERKey threshold operation. The signing key is never assembled in any single location; reconstruction requires t-of-n threshold consensus across geographically distributed enclaves on independent cloud providers.

It is the privacy key custodian: in Privacy Mode, every user's User Master Key is held as Shamir shares distributed across the user's home group of TEE enclaves. The UMK is never reconstructed outside the threshold ceremony, and even during the ceremony it exists only in attested enclave memory for the duration of a single operation. Encryption and decryption of user transactions happen inside the enclave; plaintext crosses the enclave boundary only over an authenticated session to a verified wallet.

It is the Policy Engine: the structured disclosure facility through which institutions grant scope-bounded, time-bounded access to their data. A treasurer can grant their auditor read access to transactions of a specific token over a specific quarter; a compliance officer can grant a regulator read access to transactions involving specific sanctioned addresses. The Policy Engine enforces every disclosure inside the threshold-attested enclave and produces a tamper-evident audit log of every access event.

It is the institutional identity and recovery system: users and institutions onboard through AERKey, which binds wallet addresses to UMK shares under a controlled recovery policy. Loss of a wallet device does not result in loss of access; recovery follows a t-of-n recovery factor scheme that allows the institution to regain access without ever exposing key material to a single point of compromise.

It is the smart contract key custody layer: every smart contract that holds significant value has administrative keys — upgrade keys, parameter keys, treasury withdrawal keys, bridge release keys, governance keys. Compromise of these keys has been the proximate cause of the largest hacks in the industry's history. AEREDIUM Trust Contracts can be deployed with their administrative keys held entirely under AERKey threshold custody. Even where a smart contract has a vulnerability, the keys controlling its administrative functions cannot be drained from any single point of compromise.

8.2 The threshold infrastructure

AERKey runs on the TSS-USIG signing scheme protected by US Patent Application 63/977,868. The current production deployment uses CGGMP24, an evolution of the GG20 threshold ECDSA scheme with anti-equivocation properties from the USIG construction. The next-generation CGGMP25 deployment is expected to scale to thousands of threshold-protected modules per region; the current Asia-Pacific deployment is operating at 62 modules per region with measured signing latency in the three-hundred-millisecond range.

Each user, institution, or signing role is assigned to a home group of three TEE enclaves operated by three independent cloud providers. The current production providers are AWS Nitro Enclaves, Azure SEV-SNP Confidential VMs, and Google Cloud Confidential Space, with Intel TDX as a fourth platform under active deployment. No two enclaves in a single group share an underlying provider, region, or operational team. Compromise of any single provider does not expose the threshold key, because compromise of one share is insufficient to reach the signing threshold. Geographic distribution is structured as regional groups: Group 1 in Asia-Pacific, Group 2 in Europe, with additional groups deploying in North America, South America, Africa, and the Middle East.

8.3 Hardware attestation

Every enclave in every group produces a hardware attestation on every operation. The attestation is a signed cryptographic statement issued by the underlying hardware platform — AWS, Azure, GCP, or Intel — that the code currently running inside the enclave is the code that was deployed and audited. A customer of AEREDIUM does not have to trust that the validator operator is honest; they have to trust that the hardware vendor's attestation primitive is honest. The attestation primitive is then composed across multiple independent vendors via the threshold scheme, so the trust assumption reduces to: at least one of three major hardware vendors is honest about what code is running inside their attested platform. This is a substantially weaker trust assumption than the legacy correspondent banking model, which depends on every intermediary bank, every messaging provider, and every regulator behaving correctly without cryptographic attestation of any of them.

8.4 Why AERKey is the lock that fits

Every existing blockchain that has attempted institutional privacy has failed at the same point: key management. Either the keys are user-held — in which case institutional adoption is impossible because no compliance officer will accept a regime where a single laptop loss is a regulatory disclosure event — or the keys are custodian-held, in which case the custodian is the single point of failure and the privacy guarantee collapses to "trust the custodian." Bank-operated chains take the second path and pay the corresponding cost: the operator can read every transaction, which is acceptable for intra-institutional flows but fatal for the inter-institutional case where the counterparty does not trust the operator with cleartext access.

AERKey resolves this by being neither user-held nor single-custodian-held. The keys are threshold-distributed across enclaves operated by independent providers under hardware attestation, with the institution authenticating via wallet signature and the threshold ceremony performing all cryptographic

operations inside attested memory. The institution does not hold the key; no single operator holds the key; the key is never assembled. Compliance auditors can be granted scoped read access through the Policy Engine without ever holding any decryption authority themselves. This is the architecture that makes confidential blockchain transactions institutionally viable for the first time, and it is the same architecture that makes AEREDIUM operationally non-bank — for the structural reasons set out in §3, only a non-bank can run it.

9. AERLink: Threshold-Governed Access to Traditional Systems

AERLink is the AEREDIUM architectural primitive that connects the chain to traditional non-blockchain systems — bank core APIs, ERP systems, payment networks, custodian APIs, market-data providers, SWIFT messaging, and card networks — as composable chain operations. The underlying technology is DACA (Decentralized Access to Centralized APIs), protected by US Patent Application 09857-P0001A. AERLink is the institutional product surface; DACA is the technical and patent term used in this document where the cryptographic mechanism itself is being described.

9.1 The problem AERLink solves

Every traditional API is single-user. Whoever holds the credential — the OAuth token, the API key, the certificate — holds the full authority that credential confers. There is no native concept in any major bank API, payment network, or ERP system of "this call requires three signatures" or "this call may only be made if a consensus group has authorised it." This is why connecting a blockchain to a bank has historically required one of two unacceptable compromises: either the bank builds a new multi-party endpoint (which they will not do without years of integration work, vendor risk review, and regulatory consultation), or some single party holds the API token in a regular server and the counterparty has to trust that party not to misuse it.

AERLink inverts this. The API credential lives inside a Trusted Execution Environment. The enclave is configured to accept exactly one class of caller: a transaction signed by AERKey, the chain's threshold key. The API itself is not modified — it sees a normal single-user request with valid credentials, exactly as it always has — but the credential is structurally unreachable except via a chain consensus event. The single-user API has been retrofitted with blockchain-grade multi-party governance without the API provider integrating anything.

9.2 Architecture

A DACA enclave contains four cryptographic components: the API implementation code (open-source where possible, attestable in all cases via hash-comparison against the running enclave); the API credentials (written into the enclave at provisioning, never readable from outside); the AERKey public key (the only signing authority the enclave will accept inbound from); and the enclave's own private key (used to sign all outbound responses so callers can verify that data genuinely came from the attested code).

A typical AERLink invocation flows in five steps. A transaction on AEREDIUM specifies an external system call. AEREDIUM validators reach consensus and threshold-sign the call via AERKey. The signed payload is routed to the relevant DACA enclave, which verifies the signature against the AERKey public key it was provisioned with. The enclave constructs the actual API call using credentials that never leave its memory, sends it over the counterparty system's normal endpoint, and receives the response. The enclave signs the response with its own TEE key and returns it on-chain, where it becomes part of the same transaction's settlement state.

Two cryptographic guarantees fall out of this. The counterparty API can only be called as the result of a valid AERKey threshold signature: no operator, no developer, no compromised laptop, no single point of

social engineering can call it unilaterally. And the response visible on the chain is attested as having come from inside the audited, hash-verified enclave code. Both directions of the integration are verifiable, and neither requires the counterparty system to know that it is being addressed by a blockchain.

9.3 How AERLink differs from oracles and from the Trans Layer

Two comparisons are worth making explicitly, because both come up in institutional conversations.

AERLink versus oracles. A decentralised oracle network like Chainlink resolves the trust problem by having many independent parties each call the external API with their own credentials and then negotiate consensus on the answer. This requires a separately-trusted layer (the oracle network), costs gas per query, depends on a volatile utility token to pay nodes, has detectable latency, and has a real attack surface in the form of the oracle nodes themselves. AERLink is one call to the API, made by the chain itself, with credentials held inside an attested enclave that the chain governs through its own threshold consensus. There is no separate node network to compromise, no utility token to hold, and the call is in-band — the freshest possible answer arrives inside the same transaction. The trust assumption reduces to the TEE attestation, which is the same assumption AEREDIUM consensus is already making.

AERLink versus the Trans Layer. The Trans Layer (§13) moves value between blockchains. AERLink reaches into systems that are not blockchains at all. They are complementary primitives, not overlapping ones. The Trans Layer is bridgeless cross-chain settlement; AERLink is governed cross-system interaction. Together they make AEREDIUM the only chain that natively bridges crypto rails to bank rails and enterprise systems — a category for which no competing architecture currently exists.

9.4 Representative use cases

The institutional surface AERLink opens up is broad. Four representative cases illustrate the range.

Bank-rail settlement as a composable leg. A multi-leg AEREDIUM transaction can include, as one of its legs, a fiat payment over a bank's existing payment API. The payment instruction is constructed on AEREDIUM, threshold-signed by AERKey, and delivered to the bank's API by the DACA enclave that holds the bank's credentials. The bank's payment system receives a normal authenticated call; on the AEREDIUM side, the leg is atomic with the rest of the transaction and rolls back deterministically if any other leg fails. This is the bridge between tokenised settlement and bank-rail settlement that delivery-versus-payment use cases have required for years.

Inter-institution secure inquiry. Two regulated institutions need to exchange sensitive information — a sanctions screening response, a counterparty balance attestation, a Travel Rule data field — without exposing PII to any chain observer and without trusting each other's IT perimeters. Each institution registers a DACA enclave running its own API implementation, with public keys exchanged through standard institutional channels. Queries and responses flow as AEREDIUM transactions with bodies encrypted under counterparty public keys; the chain itself sees only ciphertext. The audit trail is on-chain; the content is not.

Live market-data integration. A cross-currency stablecoin swap that needs a live FX rate can call a market-data provider (Bloomberg, Refinitiv) through a DACA enclave that holds the provider's credentials. The

rate is fetched in-band as part of the transaction, signed by the enclave, and consumed by the swap logic. No oracle network, no gas-per-query, no rate staleness from waiting on out-of-band oracle responses.

Sanctions and compliance integration. OFAC-list checking, MiCA reporting, FATF Travel Rule data exchange, and other compliance API integrations run through DACA enclaves that hold the compliance provider's credentials. Compliance checks become a composable part of any institutional transaction rather than a separate workflow bolted on after settlement.

9.5 The Modular Layer and registration

AERLink is operated as a modular layer in which new DACA adapters can be registered and made discoverable by transactions on AEREDIUM. Registration is permissioned: provider entities pass institutional KYC/B before any adapter they sign can be registered, since malicious code in a registered adapter could in principle touch user funds. Each adapter is identified by a reverse-DNS canonical name (e.g., com.bankofamerica.bank_api), carries an OpenAPI specification of its methods, exposes an attestation endpoint allowing any party to verify the code running inside the enclave, and may be activated or deactivated by the registering provider or by an AEREDIUM administrative action. The full design of the DACA Modular Layer (DML) is set out in the AERLink Modular Layer RFC available from AEREDIUM Foundation.

9.6 Why AERLink completes the architecture

AERKey makes confidential blockchain transactions institutionally viable. The Trans Layer makes cross-chain value movement bridgeless. AERLink makes the rest of the institutional system — the banks, the ERPs, the payment networks, the data providers, the compliance services — reachable as composable chain primitives without those systems integrating with a blockchain. The three primitives compose: a single AEREDIUM transaction can move encrypted value, settle it across multiple chains, and invoke bank-rail and enterprise-system APIs as part of the same atomic operation, with every step threshold-signed by the same AERKey infrastructure and audit-logged to the same Bitcoin-anchored chain of record.

This is what is meant by AEREDIUM being the only blockchain that natively bridges crypto rails to bank rails and enterprise systems. The claim rests on a specific patent-protected architectural primitive, not on marketing positioning, and it describes a category for which no competing implementation currently exists.

10. The Privacy Architecture

This section summarises the privacy architecture as it integrates with AEREDIUM. The full cryptographic specification — key derivation, payload structure, envelope encryption, address-hash indexing, and the wallet recovery flow — is documented in the AERKey Privacy Layer Wallet Architecture v1.5.

10.1 Layered design

The AERKey Privacy Layer is structured as five privacy layers, of which two are deployed in the current architecture and three are roadmap items aligned to the AEREDIUM deployment schedule.

Layer	Capability and status
Layer 1 — Wallet-Level Encryption	Transaction payload encrypted at the wallet before broadcast; chain stores only ciphertext. Production architecture, deploying with AEREDIUM mainnet.
Layer 2 — Mempool Encryption	Encrypted mempool prevents MEV extraction by validators or observers. Architecture complete; deployment subsequent to mainnet.
Layer 3 — Smart Contract Encryption	Trust Contract bytecode and state encrypted; execution inside TEE. Design phase.
Layer 4 — Chain-Native Encryption	Block explorer encrypted by default; tiered visibility based on authentication. Production architecture, deploying with AEREDIUM mainnet.
Layer 5 — Encrypted DeFi Operations	End-to-end encrypted swaps and AMM operations via TEE-mediated execution. Design phase.

10.2 Cryptographic primitives

The Privacy Layer uses only quantum-resistant symmetric primitives at the chain-storage level. Payload encryption uses AES-256-GCM with fresh random Transaction Encryption Keys per transaction, wrapped under per-user Key Encryption Keys derived from each user's threshold-distributed UMK. Address hashing uses HMAC-SHA256 with per-user Address Salt Keys. Key derivation uses HKDF-SHA256. The threshold scheme is TSS-USIG with anti-equivocation. Wallet authentication currently uses secp256k1 ECDSA with a documented migration path to hybrid secp256k1 + ML-DSA-65 signatures for post-quantum resistance.

Every on-chain encrypted transaction carries a one-byte cipher_id field and a one-byte sig_suite field identifying the specific cryptographic primitives used. This is the architectural hook for crypto-agility: future cipher and signature schemes can be introduced without breaking decryption of historical records. AEREDIUM commits to maintaining decrypt capability for every cipher_id and sig_suite ever written to a production record.

10.3 Tiered block explorer

The AEREDIUM block explorer implements three-tier visibility based on authentication and Policy Engine authorisation.

Viewer class	Authentication	Visible fields
Public	None	Transaction ID, timestamp, status, ciphertext, IV, authentication tag, key reference
Authorised third party	Policy Engine credential	Disclosed fields per Policy Entry; remainder encrypted
Transaction owner	Wallet signature session	Full plaintext: from, to, amount, token, fee, memo, status

Unauthenticated queries by wallet address return "no transactions found" rather than "access denied." This is the cryptographic truth — the explorer cannot confirm the existence of transactions for a queried address without the user's Address Salt Key. Returning "access denied" would itself leak the existence of transactions, which is information a third party should not obtain.

10.4 Selective disclosure via the Policy Engine

A Policy Entry specifies an authorised reader, a scope (time range, token type, counterparty list, or specific transaction identifiers), the fields disclosed, and a validity period. The entry is stored inside the threshold-protected Policy Engine and anchored by hash to the AEREDIUM chain so that the existence of every Policy Entry is auditable even if the entry's contents are private.

On disclosure, the auditor or authorised third party authenticates to AERKey, the Policy Engine verifies their credential against the entry, the enclave decrypts only the permitted fields of the in-scope transactions, and the result is returned over an authenticated session. Every disclosure event is logged with the auditor identifier, the scope, the timestamp, and the field list. The audit log is Merkle-chained and anchored to AEREDIUM, providing tamper-evident proof of every access event.

This architecture supports the full range of institutional and regulatory disclosure requirements: external audit, internal compliance review, FATF Travel Rule data exchange between institutions, MiCA-compliant transaction reporting, OFAC sanctions screening response, and law-enforcement disclosure under lawful process. Every disclosure is scope-bounded, time-bounded, and audit-logged.

11. Multi-Cloud TEE-BFT Foundation

The AEREDIUM consensus layer is what makes the privacy and cross-chain capabilities credible. A privacy guarantee is only as strong as the trust foundation underneath it; if validators can equivocate, censor, or rewrite history, then no amount of cryptography at the application layer matters.

11.1 TEE-BFT consensus

AEREDIUM uses a TEE-BFT consensus protocol inspired by MinBFT (Veronese et al., 2013) and enhanced with hardware-enforced anti-equivocation through the USIG construction. Each validator runs inside a hardware-attested TEE enclave that issues a unique sequential identifier on every consensus message. The UI is bound to the enclave by hardware attestation and to the message content by cryptographic signature. Equivocation — a validator signing two conflicting messages with the same counter — is detected by the protocol and produces immediate cryptographic evidence of misbehaviour.

This construction has two important consequences. First, it reduces the Byzantine fault tolerance threshold from 3f+1 (the classical bound) to 2f+1, because the hardware attestation eliminates an entire class of byzantine behaviour (equivocation) that classical byzantine consensus must defend against in software. Second, it reduces the number of consensus rounds from three to two, because the anti-equivocation guarantee is provided at the message level rather than requiring a separate consensus phase to detect equivocation. The combined effect is faster finality with fewer validators required to maintain the security property.

11.2 Multi-cloud deployment

AEREDIUM validators are deployed across four independent TEE platforms operated by four independent cloud providers.

Platform	Provider	Status
Nitro Enclaves	Amazon Web Services	Production
SEV-SNP Confidential VMs	Microsoft Azure	Production
Confidential Space	Google Cloud Platform	Production
TDX Confidential VMs	Intel (multi-cloud TDX)	Production

Each consensus group operates with validators on at least three of the four platforms. No two validators in the same group share underlying provider, region, or operational dependency. The chain does not rely on diverse human operators with conflicting incentives, which has historically proven fragile, but on diverse hardware platforms operated by competing commercial entities under independent legal jurisdictions. A regulatory action against one cloud provider, a data-centre outage in one region, or a software vulnerability in one TEE platform does not compromise the consensus group, because the threshold survives the loss of any one of its members.

11.3 VRF leader election

Block leaders are selected by Verifiable Random Function on secp256k1, with randomness seeded from the current Bitcoin block hash. The VRF construction guarantees that the leader of each round is unpredictable to any party until the round begins, and verifiable to all parties once the round is announced. This eliminates leader-targeting attacks: an adversary cannot prepare a denial-of-service or compromise attempt against a specific validator because they cannot know in advance which validator will be the leader. Using Bitcoin block hash as the randomness seed inherits Bitcoin's randomness assumptions and protects against the case where the AEREDIUM validator set itself would otherwise be the source of an adversarial randomness manipulation.

11.4 Performance

AEREDIUM consensus produces two-second blocks with one-block finality under nominal load. The TEE-BFT protocol's 2f+1 threshold and two-round structure together yield this latency budget; the parallelised EVM execution layer (§12) absorbs the throughput. Detailed performance figures are summarised in §17.

12. EVMSO: Parallel Execution at Institutional Scale

12.1 EVM compatibility

AEREDIUM exposes a standard Ethereum-compatible JSON-RPC and WebSocket API surface (sixty methods, mTLS-protected). Standard Solidity contracts compile and execute on EVMSO without modification. Tooling that targets Ethereum — Foundry, Hardhat, Remix, MetaMask, Etherscan-style explorers — works against AEREDIUM the same way it works against any EVM chain. This is a deliberate constraint: the institutional smart contract surface must not require institutions to adopt a new development toolchain.

12.2 Block-STM parallel execution

EVMSO executes transactions in parallel using a Block-STM (Software Transactional Memory) implementation. Transactions are scheduled optimistically across worker threads; the system detects state-access conflicts at commit time and re-executes only the transactions whose reads were invalidated. Under typical institutional workloads — where the majority of transactions touch disjoint state — parallel execution achieves throughput in the hundreds of thousands of transactions per second range under ongoing optimisation. Validator-injection benchmarks have measured single-second windows substantially higher than the steady-state figure; the relevant figure for institutional capacity planning is the steady-state throughput, which scales with available cores per validator.

12.3 Trust Contracts

Trust Contracts are AEREDIUM's institutional smart contract surface. A Trust Contract is a standard Solidity contract that additionally has access to AEREDIUM-specific primitives: encrypted state storage, AERKey threshold signing operations, Policy Engine authorisation checks, cross-chain settlement operations via the Trans Layer, and external system invocations via AERLink. The Trans Layer's KIMA-origin cross-chain settlement logic, following the AEREDIUM–KIMA merger, runs as a Trust Contract suite on AEREDIUM rather than as an external bridging service — collapsing what was previously a multi-system architecture into a single chain-native execution surface.

Trust Contracts also support AERKey-managed administrative keys. The contract's upgrade authority, treasury authority, governance authority, and any other privileged operation can be configured to require a threshold signature from the AERKey infrastructure rather than a single private key, a small multisig, or a slow on-chain governance vote. This eliminates the most consistent attack pattern in institutional smart contracts — the compromise of administrative keys held by individual developers, single hardware modules, or socially-engineerable multisigs — while preserving the operational flexibility that institutional treasury, custody, and bridge contracts require.

13. The Trans Layer: Bridgeless Cross-Chain Settlement

13.1 The bridge attack surface — and its elimination

The Trans Layer is AEREDIUM's cross-chain settlement architecture, connecting AEREDIUM to production networks across the major EVM ecosystems, non-EVM chains including Solana and Bitcoin, and traditional banking and enterprise systems through AERLink. The integration list expands continuously under demand-driven development; the relevant figure is not a fixed count of supported networks but the architectural property that adding new networks is a matter of deploying additional Trust Contract endpoints rather than reworking trust assumptions. The architecture is bridgeless by design. This is not a marketing distinction. It is the structural elimination of the largest attack surface in the entire blockchain industry.

Cross-chain bridges have been the dominant locus of catastrophic loss in DeFi since 2021. Cumulative losses from bridge-related exploits run into multiple billions of dollars across Ronin, Wormhole, Nomad, Multichain, Harmony, BNB Chain Bridge, Poly Network, and a long sequence of smaller incidents. The structural reason is consistent across these events. Traditional bridges hold pooled assets in a smart contract on the source chain and mint a wrapped representation on the destination chain. The contract on the source chain releases assets when a small set of validators or a third-party verifier network signs a message asserting that the corresponding burn happened. Compromise the validator set, the verifier infrastructure, or the message-signing process — and the entire contents of the bridge become drainable in a single transaction.

The most recent demonstration of this pattern is the April 2026 KelpDAO exploit. On 18 April 2026, attackers attributed to the North Korean Lazarus Group drained approximately $290 million in rsETH from KelpDAO's cross-chain bridge by compromising the LayerZero verifier infrastructure that secured it. The attackers compromised two of LayerZero's RPC nodes, then ran a distributed denial-of-service attack against the external RPC endpoints to force failover into the poisoned ones. Once the verifier was reading from compromised infrastructure, the attackers fabricated a cross-chain message — a phantom burn on the source chain that was never executed — and the destination contract released approximately 116,500 rsETH against it. The attack was the largest DeFi exploit of 2026, and it occurred only three weeks after the same attack group drained $285 million from Drift Protocol via a different vector.

This is the attack surface AEREDIUM eliminates. Not mitigates — eliminates. The Trans Layer does not use third-party verifier networks. It does not use multisigs of human operators. It does not use bridge contracts holding pooled assets that can be drained by a forged message. It uses AERKey threshold signing as the cross-chain operation primitive, executed by the same threshold infrastructure that signs AEREDIUM blocks, running inside hardware-attested TEE enclaves on three independent cloud providers in three independent jurisdictions. There is no validator set to compromise separately from AEREDIUM consensus. There is no verifier infrastructure to poison. There is no signer multisig to socially engineer. To compromise a Trans Layer cross-chain operation requires compromising the AERKey threshold itself — which requires simultaneous compromise of multiple TEE enclaves on multiple cloud providers across multiple jurisdictions, under hardware attestation, with monotonic counters preventing equivocation.

13.2 Native settlement integration

Following the AEREDIUM–KIMA merger, the cross-chain settlement logic that previously ran on a separate validator network now executes as Trust Contracts on AEREDIUM, signed by the AEREDIUM AERKey threshold. The result is a single-chain, single-consensus, single-key-management system for both AEREDIUM-native activity and cross-chain settlement. The Trust Contract administrative keys themselves — upgrade authority, treasury authority, settlement authority — are managed under AERKey threshold custody, eliminating the single-point-of-key-compromise pattern that has been the proximate cause of the largest losses in cross-chain infrastructure.

The Trust Contract deployment is Phase 1. Phase 2, currently in active development, takes the architecture one step further: the Trans Layer is being built directly into the AEREDIUM protocol as a native consensus-layer primitive, replacing the smart-contract implementation. The functional surface to institutional users is unchanged — the same threshold-signed bridgeless cross-chain operations, the same single trust root, the same network coverage — but the cross-chain coordination becomes a property of the chain itself rather than logic running above it.

Operationally, the merger brought to AEREDIUM a production-tested cross-chain coordination protocol with proven institutional volumes. Architecturally, it collapsed what were previously two systems with two separate trust roots into a single system with one trust root — AERKey. The merger therefore did not just consolidate two products; it eliminated an entire layer of cross-system trust risk. The same property makes Privacy Mode practically viable: an institution can deposit USDC from Ethereum to AEREDIUM, conduct encrypted activity inside AEREDIUM, and withdraw to any supported destination chain — all operations signed by the same threshold infrastructure, all visible inside AEREDIUM under the same Policy Engine, all logged in the same audit trail anchored to Bitcoin.

13.3 True interoperability — chains, non-chains, and the institutional surface

True interoperability has been a stated industry goal for nearly a decade. The deployed architectures — wrapped-asset bridges, lock-and-mint bridges, liquidity-network bridges, light-client relays, third-party verifier networks — have repeatedly failed under adversarial conditions. The Trans Layer is structurally different because it removes the separately-trusted intermediary entirely. A cross-chain operation on AEREDIUM is not an inter-system message that has to be verified by an external party; it is a single threshold-signed action issued by the same hardware-attested infrastructure that runs the chain. Interoperability inherits the security properties of AEREDIUM consensus directly.

The interoperability surface is wider than chain-to-chain. Through AERLink (§9), the same threshold-signed primitive that moves value between blockchains can invoke traditional bank-rail, payment-network, ERP, and market-data APIs. From an institutional user's perspective, settling across an EVM chain, settling across Bitcoin, settling across Solana, and settling through a bank's payment rail are all the same kind of operation: a threshold-signed transaction issued by AEREDIUM consensus, executed by attested infrastructure, audit-logged to a Bitcoin-anchored chain of record. This is what is meant by AEREDIUM being the only architecture that natively bridges crypto rails to bank rails and enterprise systems.

14. The Structural Answer to the AI-Amplified Threat Era

The defensive infrastructure available to existing blockchains in 2026 follows a consistent pattern: detect attacks faster, audit code more thoroughly, deploy AI-driven monitoring, formally verify critical paths, layer in runtime guardrails. All of these are useful, and the industry will continue to invest in them. None addresses the structural problem.

14.1 The asymmetry has inverted

Through the first decade of public blockchain history, defenders held the time advantage. Auditors and security researchers had longer with the code than attackers, and successful exploits required extensive manual reverse engineering. That advantage is gone. Frontier AI models scan for and exploit smart contract vulnerabilities at declining cost (Anthropic's December 2025 red-team measured approximately $1.22 per attempt with median exploit cost down 70 percent across four model generations in six months). a16z's April 2026 research demonstrated that AI agents always identify the underlying vulnerability — failures occur in multi-step exploit assembly, which is precisely the part of the gap that is closing fastest. The compute cost of AI-aided exploitation is declining faster than the human cost of audit improvement, and the trend lines are not converging — they are diverging.

14.2 The structural conclusion

What follows from this — for any blockchain that institutional value flows through — is a structural rather than a procedural conclusion. The architecture must be designed so that finding the vulnerability does not allow draining the assets. Vulnerability discovery and value extraction must be separable, and the separation must be enforced cryptographically rather than by policy. AEREDIUM is constructed around this separation in three layers.

14.3 Three layers of structural defence

Smart contract administrative keys are threshold-distributed (§8). Every Trust Contract on AEREDIUM can be deployed with its upgrade authority, treasury authority, and governance authority held entirely under AERKey threshold custody. An AI agent that finds an exploitable vulnerability in the contract's logic cannot drain its assets, because the keys that authorise asset movement are distributed across hardware-attested enclaves on independent cloud providers in independent jurisdictions, and those keys are never assembled in any single location at any single moment. This is the structural answer to the a16z finding that AI agents always identify the vulnerability: AEREDIUM accepts the finding and removes its consequences. The vulnerability is decoupled from the value extraction.

Cross-chain operations are bridgeless (§13). The Trans Layer eliminates the attack surface AI is most rapidly industrialising on competing platforms. There is no separately-trusted verifier network whose RPC nodes can be poisoned. There is no signer multisig that can be socially engineered. There is no bridge contract holding pooled assets that a forged cross-chain message can drain. The April 2026 KelpDAO/LayerZero exploit followed exactly the attack pattern the Trans Layer architecture eliminates.

The chain trust root is itself decentralised (§4, §11). Block proposals, validator votes, state transitions, and Bitcoin anchoring are all signed by AERKey threshold operations executed inside Trusted Execution Environments across independent cloud providers in independent jurisdictions. An attacker who fully compromises AEREDIUM Foundation gains the Foundation's operational capabilities — paying for cloud accounts, deploying new code — but does not gain the ability to defeat the cryptographic enforcement of existing consensus, because the existing validator network rejects blocks signed by code with any attestation hash other than the canonical one. Compromise of consensus requires compromise of the threshold itself.

14.4 Architectural choices made before the threat era — and validated by it

These three layers were not architectural choices made in response to the AI threat era of 2026. They were architectural choices made for the institutional thesis of confidentiality, regulator-defensibility, and operator-neutrality — the same thesis specified in §3 and §4 as the response to the bank-decentralisation impossibility. The fact that the same architecture happens to be the only blockchain security model that survives the AI exploit era is not coincidence; it is convergence. The defensive responses available to existing platforms are reactive: detect faster, patch faster, monitor more aggressively, deploy AI-driven defence to keep pace with AI-driven offence. AEREDIUM's response is structural: arrange the architecture so that the attack surfaces do not exist in the first place. The threat era of 2026 is not what motivates this architecture. It is what validates it.

15. Bitcoin Anchoring and Notarization

15.1 Why Bitcoin

AEREDIUM uses Bitcoin as its archival timestamp authority. Bitcoin's proof-of-work history is the longest, most expensive, and most adversarially-tested in existence — rewriting it would require more computational expenditure than any other system on earth. By committing periodic snapshots of AEREDIUM's state to the Bitcoin blockchain, AEREDIUM inherits Bitcoin-grade immutability for its historical record.

This is the archival layer of AEREDIUM's defence-in-depth model. Day-to-day execution is secured by hardware-attested TEE consensus and AERKey threshold signing. Long-term historical integrity is secured by Bitcoin. The operational chain is fast (two-second finality); the archival chain is slow but tamper-proof. Bitcoin does not validate AEREDIUM execution and is not asked to. Bitcoin only timestamps the commitments. Validation is done by AEREDIUM's own consensus and attestation.

15.2 How the anchoring works

Every one hundred AEREDIUM blocks — approximately every two hundred seconds — AEREDIUM produces a commitment representing the state of the chain at that point. The commitment is a small, fixed-size cryptographic summary (a Merkle root, suitable for Bitcoin's eighty-byte OP_RETURN payload). The Bitcoin transaction carrying the commitment is itself signed by the AERKey threshold, so the operation does not depend on any single key holder. Once the Bitcoin transaction confirms, the commitment is part of the Bitcoin permanent record. Any AEREDIUM state covered by that commitment becomes Bitcoin-grade-immutable from that point forward.

This produces two complementary finality regimes. AEREDIUM transactions are final on AEREDIUM at the moment of block inclusion, which is what users experience operationally. Bitcoin-anchored finality follows shortly after, and is what auditors, regulators, and dispute-resolution authorities ultimately rely on for archival certainty.

15.3 Proprietary AEREDIUM infrastructure

The Audit Log and Notarization Service are AEREDIUM-proprietary infrastructure, not generic blockchain components. The Audit Log captures every threshold signing operation and every consensus attestation in real time and prepares it for archival anchoring. It uses a lock-free ring buffer architecture that handles more than one hundred and fifty thousand attestations per second without blocking the hot signing path, supported by a write-ahead log for crash safety and a Merkle-chain builder that produces tamper-evident links across attestation records. Each record is independently signed for external verification and locked into the chain via cryptographic linkage to the previous record. The Audit Log also exposes the AEREDIUM Policy Engine — the structured access-control surface specified in §10 — implemented inside the same infrastructure.

The Notarization Service commits the Audit Log's Merkle roots to Bitcoin. It builds the canonical Bitcoin OP_RETURN payload (the AERX format, eighty bytes, supporting both single-block and batched-Merkle-

root encodings), threshold-signs the Bitcoin transaction with AERKey, and broadcasts to a high-availability Bitcoin RPC pool with automatic failover. Mainnet operation enforces minimum confirmation thresholds and threshold-signing requirements at the configuration layer. The architectural significance of these being proprietary is that the audit trail and Bitcoin anchoring are not subject to the security, reliability, or commercial decisions of any external party. AEREDIUM operates the entire stack — from the moment a signing operation occurs inside a TEE enclave through Bitcoin commitment — as a single integrated, threshold-secured pipeline.

15.4 On-demand anchoring

Beyond the scheduled per-hundred-block anchoring, AEREDIUM offers on-demand Bitcoin anchoring as a paid service. Institutional users requiring proof-of-existence for specific commitments at specific times — typical for regulatory filings, time-sensitive legal evidence, or dated record-keeping — can request that an arbitrary thirty-two-byte commitment be anchored to Bitcoin, paying in stablecoin (USDT or USDC). The service supports three urgency tiers (Express, Standard, Economy) corresponding to next-block, six-block, and one-hundred-forty-four-block confirmation targets. The on-demand anchoring service is implemented through an Anchor Escrow Trust Contract on AEREDIUM.

16. Regulatory Posture

AEREDIUM is built to be regulator-defensible at the architectural level. Privacy without compliance has been demonstrated, repeatedly, to be legally fragile; AEREDIUM's architecture provides cryptographic privacy together with structured disclosure capabilities that satisfy the major institutional and regulatory frameworks.

16.1 Why this is regulator-defensible where mixers are not

Tornado Cash and similar mixer designs failed regulatory scrutiny because they had no boundary controls and no disclosure facility. They accepted any user, mixed any value, and provided no mechanism for lawful disclosure. The regulatory consequence — sanctions designation and prosecution — was structurally inevitable: a privacy primitive with no compliance architecture is indistinguishable from a money-laundering tool from the perspective of law enforcement.

AEREDIUM's architecture is the opposite of this pattern at every point. Onboarding is institutional KYC through AERKey. Custody is operated under regulated relationships with cryptographically attested controls. Disclosure is a structured, scoped, time-bounded, audit-logged capability via the Policy Engine, available to authorised parties under defined credentials. Every disclosure event is anchored to Bitcoin. Where a mixer is structurally indistinguishable from a laundering tool, AEREDIUM is structurally distinguishable from any privacy primitive that does not have these properties.

16.2 Specific frameworks supported

The FATF Travel Rule is implemented as a first-class Policy Engine capability: structured originator and beneficiary data exchange between AERKey-onboarded institutions, with the data itself protected by the same threshold-attested infrastructure that protects transaction content. MiCA-compliant transaction reporting and OFAC sanctions screening are integrated through AERLink-connected compliance providers (§9.4), so that compliance checks become composable legs of institutional transactions rather than separate workflows. SOC 2 and ISO 27001 audit evidence is produced as cryptographic attestation rather than process documentation.

16.3 Continuous reserve verification

AEREDIUM Audit, protected under US Patent Application 19/400,910, is a multi-model AI-based continuous reserve verification system that performs a complete audit cycle every 60 seconds and produces an immutable, on-chain record of reserve integrity. It composes three model classes — an XGBoost fraud-detection ensemble, an Isolation Forest anomaly-detection model trained on over seven million on-chain transactions, and a quantile LSTM forecasting model for redemption pressure and liquidity stress — and enforces a graduated four-level response protocol (PASS, CAUTION, ALERT, HALT) with automated treasury actions at each level. Audit results are cryptographically signed and recorded on-chain, creating a tamper-proof record that regulators, institutional partners, and the public can verify independently. AEREDIUM Audit is documented in full as a separate product specification; the present white paper references it as an application built on AEREDIUM's underlying chain primitives (AERKey signing, Policy Engine disclosure, Bitcoin-anchored audit log).

16.4 The chain of record as regulator artifact

Every Policy Engine disclosure produces a cryptographic audit record. Every consensus operation produces an attestation. Every cross-chain or AERLink operation produces a threshold-signed transaction with full provenance. These records are Merkle-chained inside the AEREDIUM Audit Log and anchored to Bitcoin. The result is that the chain itself becomes the regulator's primary evidentiary artifact: queries can be issued against the Policy Engine under appropriate authority, and every answer comes with the cryptographic proof that authenticates it. This is what "regulator-defensible by construction" means in practice.

17. Performance

AEREDIUM's performance characteristics are measured at three layers: consensus latency, execution throughput, and end-to-end transaction lifecycle.

Consensus latency: two-second block time with one-block finality, achieved through the 2f+1 TEE-BFT threshold and two-round message structure. Bitcoin-anchored finality follows on the next anchoring cycle (approximately ten minutes).

Execution throughput: EVMSO's Block-STM parallel execution achieves throughput in the hundreds of thousands of transactions per second range under ongoing optimisation, measured at the validator-injection level on representative institutional workloads. Throughput scales with available cores per validator. Reported headline figures should be read as the steady-state capacity envelope; institutional capacity planning should reference the sustained-throughput figure rather than the single-second peak.

AERKey threshold signing: current Asia-Pacific deployment operates at 62 modules per region with measured signing latency in the three-hundred-millisecond range. The next-generation CGGMP25 implementation is targeted to scale to thousands of threshold-protected modules per region, with linear scalability validated on the fast-path benchmark across signing groups.

Audit Log: lock-free ring buffer architecture handles over 150,000 attestations per second without blocking the hot signing path.

These figures will continue to evolve. The architectural ceiling is set by the cryptographic operations (TEE entry/exit, threshold-signature ceremony) and the cloud-vendor TEE primitives; both are improving across vendor releases.

18. Cryptographic and Quantum Posture

AEREDIUM is designed for crypto-agility. Every on-chain encrypted record carries cipher_id and sig_suite fields identifying the cryptographic primitives used. New cipher and signature schemes can be introduced without breaking decryption of historical records, and AEREDIUM commits to maintaining decrypt capability for every cipher_id and sig_suite ever written to a production record.

Symmetric primitives at the chain-storage level (AES-256-GCM payload encryption, HMAC-SHA256 address hashing, HKDF-SHA256 key derivation) are already quantum-resistant under conservative assumptions about Grover's algorithm. Asymmetric primitives (secp256k1 ECDSA wallet authentication, the threshold-ECDSA scheme used by AERKey) have a documented migration path to lattice-based post-quantum schemes: hybrid secp256k1 + ML-DSA-65 for wallet signatures, and a thresholdised Falcon implementation for the TSS layer. The migration path is engineered to allow phased deployment per signature suite, so post-quantum capability can be enabled for new transactions while historical records remain decryptable under their original primitives.

The quantum posture is therefore not a single-event upgrade but a planned evolution of the cipher_id space, with the architectural property that no migration ever invalidates a historical record.

19. The AER Token

AER is the native utility token of the AEREDIUM blockchain. Its functional role on the chain is described here at the level of summary necessary for this technical document. The full economic specification — token allocation, vesting schedules, the Foundation Treasury, the Community Pool, the Staking Incentive Program rules, the Fee Router specification, and the regulatory framing of AER as a utility token — is set out in the AEREDIUM Tokenomics document available at aeredium.io/tokenomics.html.

AER is required to pay gas for all transactions executed on AEREDIUM. Every transaction — whether it operates on encrypted state, settles across chains via the Trans Layer, invokes external systems via AERLink, or executes Trust Contract logic — denominates its gas cost in AER. Validators receive AER-denominated rewards for the consensus work they perform. Threshold signing operations within AERKey, attestation anchoring to Bitcoin, and on-demand notarisation services are all priced in AER. Total supply is 1,000,000,000 AER, fixed at genesis, with no inflation mechanism and no additional issuance.

Gas fees are routed deterministically at block finalisation by a protocol-level Fee Router contract. The Fee Router directs up to 2% annualised of total actively staked AER to the Staking Contract as variable staking reward, and routes the remainder to the Foundation Treasury for protocol maintenance. AEREDIUM offers a Staking Incentive Program as a time-bounded bootstrap incentive for AER holders who choose to lock tokens for the long term, with rewards accruing at a target rate of up to 4% annualised. The programme is unrelated to consensus and confers no validator role, voting right, or governance privilege on participants. It is an economic incentive for long-term holding, not a security mechanism for the chain. This white paper specifies the technical architecture; the tokenomics document specifies the economic architecture, and the two are designed to be read together.

20. Conclusion

AEREDIUM is the SWIFT, Fedwire, and DTCC of the tokenised financial system, rebuilt as a single cryptographically-private neutral settlement layer. The architecture combines hardware-attested TEE-BFT consensus across multiple independent cloud providers, threshold-distributed key management through AERKey, native chain-level transaction encryption, parallelised EVM execution measured in the hundreds of thousands of transactions per second under ongoing optimisation, bridgeless cross-chain settlement through the Trans Layer, threshold-governed access to traditional bank rails and enterprise systems through AERLink, and Bitcoin-anchored finality.

The architecture solves a problem that no bank can solve. Not because banks have failed to try — they have built Kinexys, Orion, DAP, and Fnality, and these systems are succeeding within their perimeters — but because the inter-institutional settlement layer requires non-centralisation, and non-centralisation is the inverse of what makes a bank a bank. AEREDIUM exists to occupy the architectural slot that bank-operated systems structurally cannot fill, and the historical pattern of every prior generation of financial infrastructure — SWIFT, Visa, CLS, DTCC — supports the expectation that inter-institutional volume consolidates onto neutral utilities.

Banks use AEREDIUM the same way they use every neutral utility before it: as participants, as service providers offering access to their clients, as KYC sponsors, and as integrators between their internal infrastructure and the broader institutional ecosystem. Crucially, AERLink allows the bank's existing core-banking, payment, ERP, and compliance systems to become reachable as composable chain primitives without modification — AEREDIUM is additive infrastructure, not replacement infrastructure. The institutional middle market — funds, corporates, fintechs, tokenisation platforms, regional banks, asset managers — uses AEREDIUM directly, because they have nowhere else with these properties to go.

The architecture also resolves the second half of the 2026 settlement crisis. Cross-chain interoperability is bridgeless, eliminating the attack surface that has cost the industry billions of dollars including the April 2026 KelpDAO/LayerZero exploit. Smart contract administrative keys are themselves threshold-distributed under hardware attestation, so the discovery of a vulnerability — by an auditor, by an AI agent, by a state-sponsored attack group — does not allow the extraction of value. The trust root of the chain is decentralised by design through cryptography and hardware enforcement: AEREDIUM Foundation operates the infrastructure as a named, accountable Protocol Operator, while consensus rules, transaction confidentiality, and cross-chain settlement signing are enforced by Trusted Execution Environments that no operator — including the Foundation — can override. This is Verifiable Infrastructure. These properties were architectural choices made for the institutional thesis of confidentiality, regulator-defensibility, and operator-neutrality. The fact that the same architecture is the only blockchain security model that survives the AI-amplified threat era is convergence, not coincidence.

The technical capabilities described in this document are deployed or in production-architecture status. The benchmarks are measured. The patents are filed. The architecture is composed of modules each of which has been individually engineered, audited, and deployed across the validator network. What remains is the deployment of the integrated system at institutional scale, the onboarding of the first wave of institutional users, and the ongoing migration of cryptographic primitives to post-quantum standards on the published roadmap. The next layer of institutional finance — neutral, decentralised,

cryptographically private, regulator-defensible, structurally resistant to AI-amplified exploitation, and reachable from the bank rails and enterprise systems that institutional value already flows through — is what AEREDIUM is.

AEREDIUM Group

The Trust Layer | Institutional Infrastructure for the Tokenised Economy

US Patent Applications 63/977,868 | 19/400,910 | 09857-P0001A