



EB-ENT-006 · ENTERPRISE SERIES

Enterprise Architecture Guide

Reference architectures and integration patterns for institutions adopting Earth Blockchain: deployment models from managed BaaS to self-hosted nodes, ERP and registry integration, identity and key governance, data-residency and evidence patterns, availability and change management, and the compliance-aware controls that make the network procurable.

REFERENCE ARCHITECTURES

BAAS INTEGRATION

KEY GOVERNANCE

CHANGE MANAGEMENT

ESG-READY

Version 1.0 · **Status** Public Release · **Date** July 2026**Canonical source** Earth Blockchain Whitepaper v2.0**Audience** enterprise architects · CIO/CTO teams · system integrators · risk officers

Enterprise Architecture Guide

INTEGRATING EARTH BLOCKCHAIN INTO INSTITUTIONAL SYSTEMS

Purpose and Audience

This guide translates the Earth Blockchain platform into the architecture language of institutions: deployment models with their trust and operational trade-offs, integration patterns for ERP/registry/data estates, identity and key governance, data-residency and evidence design, availability and change management, and control mappings for risk review. It presumes the Whitepaper’s product and platform definitions (§7, §12, §14) and defers protocol internals to EB-SPEC-001 and interface schemas to EB-API-003.

The adoption thesis, restated architecturally. An enterprise never has to choose between “run blockchain infrastructure” and “miss the capability”: the BaaS plane gives production access with zero node operations, and every later step — self-hosted reads, validator participation — is additive, not a migration (Whitepaper §14.2).

Table of Contents

1. Deployment Models and Trust Trade-offs	2
2. Reference Architecture: BaaS-Integrated Enterprise	3
3. Integration Patterns	4
4. Identity, Keys, and Wallet Governance	5
5. Data Architecture: Residency, Evidence, Privacy	6
6. Availability, Performance, and Change Management	7
7. Security and Compliance Controls	8
8. Adoption Roadmap and Operating Model	9
References	10

1. Deployment Models and Trust Trade-offs

CHOOSE OPERATIONAL OWNERSHIP, NOT CAPABILITY

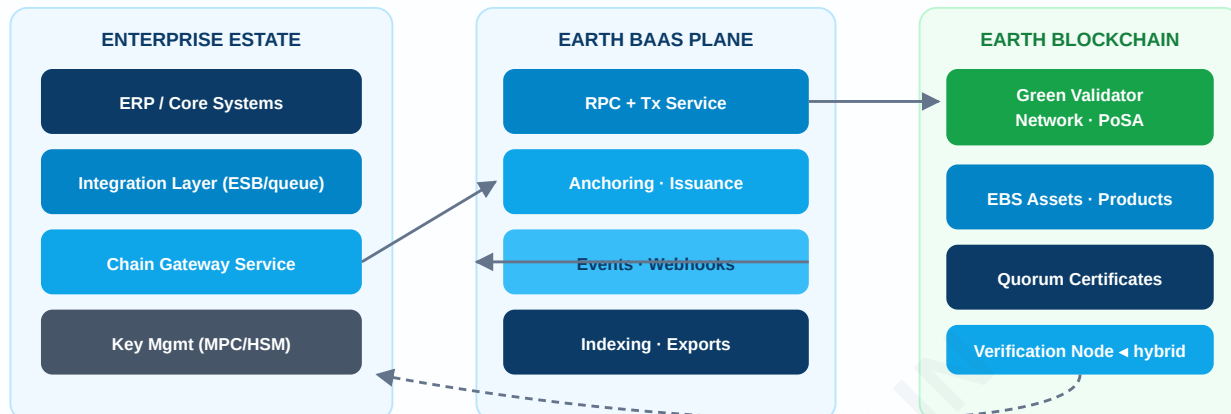
Model	Description	Trust & Ops Profile
Managed BaaS	All access via SLA-backed APIs: RPC, anchoring, issuance, webhooks, indexing (Whitepaper §7.5). EARTH-settled metering available (§7.2).	Fastest; provider-verified data unless you add §1's verification layer. No infra ops.
Hybrid (recommended target)	BaaS for writes and eventing; self-hosted full node for independent reads and certificate verification (EB-API-003 §7).	Provider-independent truth with modest ops; the auditor-friendly posture.
Self-hosted	Own full/archive nodes for all traffic; optional enterprise validator (Whitepaper §5; EB-VAL-004).	Full sovereignty; you become an infrastructure operator — and, as validator, a network stakeholder.
Permissioned subnet (roadmap)	Consortium deployment anchoring state commitments to the public network (Whitepaper §7.5, §16 Phase 3).	Private throughput with public auditability; plan integrations against the anchoring pattern now.

Verification is cheap — buy it. Whatever the model, one library call verifies a quorum certificate against the validator set (EB-API-003 §7). Institutions that verify never have to trust an endpoint, including ours.

2. Reference Architecture: BaaS-Integrated Enterprise

THE PATTERN BEHIND MOST PRODUCTION DEPLOYMENTS

Fig. 1 — Enterprise Integration Reference Architecture



Solid: request path (gateway → BaaS → chain) and finalized event path (webhooks → integration layer). Dashed: independent certificate verification (hybrid model).

Fig. 1. The gateway pattern: one internal service owns chain semantics; core systems speak queues and webhooks, never RPC.

- **Chain Gateway Service.** The single internal owner of nonces, retries, idempotency, and finality gating (EB-DEV-002 §5). Core systems submit intents; the gateway returns settled facts.
- **Eventing inward.** BaaS webhooks (finalized-only, HMAC-signed — EB-API-003 §5.3) land in the integration layer as ordinary messages; ERP teams never learn blockchain vocabulary.
- **Evidence outward.** Documents, ESG data, and supply-chain payloads stay in the estate; only hashes anchor on-chain (§5).

3. Integration Patterns

FOUR PATTERNS COVER NEARLY EVERY USE CASE

Pattern	Shape	Typical Products
Anchor & Verify	Hash internal artifacts via Anchoring API; counterparties verify statelessly. No asset issuance at all.	EarthDoc, EarthESG evidence, EarthSCM telemetry.
Issue & Administer	Deploy EBS assets from registry templates; administer roles via governed keys; lifecycle events flow back as webhooks.	Earth RWA instruments, EarthESG credits, passports.
Consume & Reconcile	Read finalized streams into the data warehouse as the reconciliation source of truth.	Treasury, audit, Scope 3 aggregation.
Delegate to Agents	Mandated EarthAI agents transact within policy; the estate reviews trails, not transactions.	Procurement, machine payments (Whitepaper §12.5).

Patterns compose: a supplier-finance program is Issue & Administer (invoice assets, EBS-3525) + Anchor & Verify (documents) + Consume & Reconcile (positions) on one ledger — the compounding effect described in Whitepaper §12.

4. Identity, Keys, and Wallet Governance

CUSTODY AS AN ORG CHART, NOT A FILE

- **Wallet classes.** Treasury (cold/MPC, board policy), Operations (MPC with transaction policies and approval workflows — Earth Wallets custodial tier, Whitepaper §7.4), Service (gateway hot keys, minimal balances, sponsored-gas where possible), Agent (EBS-6551 accounts under mandates, EB-SCC-005 §7.2).
- **Policy enforcement on-chain.** Spending limits, counterparty classes, and role separation live in smart-account policies and EBS role systems — controls auditors can read, not just screenshots of an admin console.
- **Claims-based counterparties.** Eligibility (KYC status, jurisdiction) is consumed as registry claims (EBS-3643 pattern), so counterparty risk logic is deterministic and revocation is immediate.
- **Joiner–mover–leaver.** Key custody maps to HR events: MPC shares and roles are rotated on movers/leavers with on-chain events as the audit record.

EARTH BLOCKCHAIN

5. Data Architecture: Residency, Evidence, Privacy

HASHES TRAVEL, DATA STAYS

The suite-wide rule (Whitepaper §12): content remains in enterprise custody and jurisdiction; the chain carries commitments, issuer identity, validity, and revocation. Consequences for architects:

- **Residency.** No personal or commercial content crosses borders via the ledger; anchoring is compatible with strict residency regimes because only digests are public.
- **Erasure requests.** Deleting the off-chain content renders the on-chain hash meaningless to third parties; design keying so hashes are not linkable identifiers across records (salted commitments per document).
- **Selective disclosure.** Prove properties (“degree $\geq$ year X”, “emissions verified by V”) without revealing documents, per the EarthDoc schema model (Whitepaper §12.1).
- **Retention.** The certificate chain is permanent evidence; pair it with WORM storage of the underlying artifacts for end-to-end audit trails.

EARTH BLOCKCHAIN

6. Availability, Performance, and Change Management

DESIGNING TO THE NETWORK'S ACTUAL GUARANTEES

- **Latency budget.** Settlement is deterministic at $\approx 3\text{--}6$ s (inclusion + certificate; Whitepaper §6.4). Design SLOs around *finality latency*, not block time; batch where business processes allow.
- **Throughput.** Size against your own measured testnet throughput for your transaction mix; the platform publishes no synthetic TPS claims, and neither should your architecture documents.
- **Degradation modes.** BaaS outage → gateway queues intents (chain unaffected). Finality stall (network incident) → gateway holds irreversible actions; webhooks resume with backfill (at-least-once, idempotent consumers — EB-API-003 §5.3).
- **Change management.** Protocol changes reach mainnet only through the 48 h EarthDAO Timelock (EB-SPEC-001 §9). Subscribe the CMDB to the Timelock queue: every network change arrives as a scheduled change record, testable on testnet first (parameters identical, EB-SPEC-001 §13).

EARTH BLOCKCHAIN

7. Security and Compliance Controls

CONTROL OBJECTIVES – PLATFORM MECHANISMS

Control Objective	Mechanism on Earth Blockchain
Integrity of records	Quorum-certified finality; independent verification via light-client checks (EB-API-003 §7).
Authorization & segregation of duties	On-chain roles, smart-account policies, controller mandates (EB-SCC-005 §4–§7); every privileged action is an event.
Non-repudiation & audit trail	Signed transactions + certificates + append-only evidence logs (EB-SPEC-001 §8.2–§8.3); exportable via Indexing API.
Data protection	Hash-only anchoring, salted commitments, selective disclosure (§5).
Change control	Timelocked governance with public queue; testnet parity (§6).
Third-party risk	Hybrid verification removes endpoint trust; bridge exposure bounded by rate limits (EB-SPEC-001 §10.2).
Sustainability disclosure	Network energy posture is itself reported through EarthESG with validator green attestations (Whitepaper §13) — usable in your Scope 3 narrative.

Framework mappings (structural, not certifications): the mechanisms above align naturally with common ISMS and IT-general-control expectations; formal attestations are a program decision for each deployment, not a property this document can claim.

8. Adoption Roadmap and Operating Model

PILOT → INTEGRATION → PRODUCTION, INSTITUTIONALLY

1. **Pilot (weeks).** One bounded flow via BaaS (typically Anchor & Verify); success metrics in business language — fraud reduction, audit hours, settlement time (Whitepaper §14.2).
2. **Integration (months).** Stand up the Chain Gateway, wallet governance (§4), webhook consumers, and the hybrid verification node; wire monitoring and the Timelock feed into existing NOC/CMDB.
3. **Production (quarters).** Volume issuance, multi-department rollout, and — where strategic — enterprise validator participation, converting the institution from consumer to stakeholder in network security and governance (Whitepaper §14.2; EB-VAL-004).

Operating model. A small platform team owns the gateway, keys, and vendor relationship; product teams consume queues and APIs. Budget lines: BaaS metering (optionally EARTH-settled), key-management tooling, and — in the validator stage — infrastructure plus bonded stake, with rewards and slashing mechanics per EB-VAL-004 §9.

EARTH BLOCKCHAIN

References

SUITE CROSS-REFERENCES

- [1] Earth Blockchain Whitepaper v2.0 — platform (§7), products (§12), sustainability (§13), adoption (§14).
- [2] EB-SPEC-001 — finality, governance timelock, bridge enforcement, parameter registry.
- [3] EB-API-003 — BaaS schemas, webhook security, light-client verification.
- [4] EB-SCC-005 — role systems, policy accounts, controller mandates.
- [5] EB-VAL-004 — enterprise validator operations and economics.

EB-ENT-006 v1.0 (July 2026). Architectural guidance is advisory and deployment-specific; regulatory and certification decisions rest with each adopting institution. This document does not constitute financial, investment, tax, or legal advice. © 2026 Earth Blockchain Corp. (Wyoming, USA) · Alpha Blockchain Private Limited (India). All rights reserved.

EARTH BLOCKCHAIN