⸻

0. 总体技术准则（贯穿所有模块）

• EVM 一等公民：完全兼容 Solidity/ABI/eth\_\* RPC，Gas 代币 = ABLE。

• PoS+BFT 共识：3–5s 出块、最终性 ≤ 2 个区块，目标 TPS ≥ 5,000。

• 模块化：共识/执行/数据/跨链/预言机/合规可热插拔升级。

• 可信可验证：所有关键动作（铸币、分红、桥转、喂价、治理）皆可链上审计。

• SRE 先行：SLO/灰度/回滚/容量/混沌/压测体系与代码同步上线。

⸻

1) 钱包（EVM 兼容）

目标：让 C 端投资人 & B 端发行人零摩擦接入链、签名和收分红。

关键设计

• 钱包形态：

• 用户端：MetaMask / WalletConnect / Ledger 全兼容；

• 产业端：MPC 托管钱包（Fireblocks 类）+ 多签（基金会/节点/律所 2/3）。

• 插件层：RWA 资产卡直读（合约元数据、分红日历、法律哈希、节点签章）。

• 风险提示：受限可转让（ERC-3643/T-REX）白名单自动校验；地区/合规模块提示。

接口/标准

• EIP-155/EIP-712（typed data）签名；WalletConnect v2；MPC API（tSS/ECDSA）。

• 分红领取：Merkle Distributor + EIP-2612 批量授权优化。

SLO/Sec

• 连接成功率 ≥ 99.9%；签名往返 < 400ms（同区域）。

• 私钥从不落地；MPC + 风险限额（24h/出金白名单/二次确认）。

优先级：P0（MVP 必须）

⸻

2) RPC 节点（公共网关 + 专业网关）

目标：稳定、可观测、可弹性，支撑交易所/浏览器/应用高并发。

关键设计

• 多域名入口：公共 RPC（限频）+ 专业 RPC（KYC + 高配 + 付费）。

• 读写分离：Archive/Full/Light 节点分层；交易写入专网，查询走只读池。

• 限流与防滥用：IP/账户级 QPS、爆破/MEV 保护、动态 ban。

• 索引加速：与 Indexer（The Graph/自研）打通，复杂查询走 GraphQL。

接口/标准

• JSON-RPC eth\_\* 全量；WebSocket 订阅；gRPC/GraphQL。

• Replay/回放节点：Kafka/Pulsar 事件总线。

SLO/Sec

• p95 延迟 < 150ms；可用性 ≥ 99.95%；每秒≥10k req。

• WAF + mTLS（专业网关）；大促自动扩容（HPA）。

优先级：P0

⸻

3) 区块链浏览器（Explorer + Analytics）

目标：把“可验证”做到极致，让监管/投资人“一眼信任”。

关键设计

• 三层视图：区块/交易/账户 + RWA 资产页（产权文件哈希、节点签章、分红记录、估值喂价轨迹）。

• 地图可视化：节点地理分布、RWA 资产地区热力。

• 监管模式：可筛选受限交易、KYC 白名单检查、洗钱风险标签（只展示级别，不展示隐私）。

接口/标准

• Indexer：Subgraph/自研 ETL → ClickHouse/Elastic。

• 导出：CSV/JSON，审计 API（时间窗+合约集）。

SLO/Sec

• 全量索引 < 24h；增量延迟 < 2s；查询 p95 < 300ms。

• 结果可重算（Deterministic），审计校验和。

优先级：P0

⸻

4) 算力设备（验证节点 / 服务节点 / AI 风控）

目标：全球多点、低延迟、抗故障；AI 风控与合规模块原生上链服务。

关键设计

• 节点类型：

• Validator：裸金属 + HSM/TEE；

• Service：Oracle/合规模块执行；

• Archive：长期存储 + 快照。

• 安全芯片：HSM 或 SGX/TEE 用于出块/签名与密钥封装。

• AI 风控：OCR/NLP 合规审查、异常交易检测（流式特征），以“风险分数”上链。

SLO/Sec

• 出块节点地理冗余（≥3 区）；灾备 RPO=0，RTO < 15min。

• 节点在线 ≥ 99.5%；对等网络抗 DDoS，启用 QUIC/TLS。

优先级：P1（随主网扩大）

⸻

5) Token 标准（RWA/治理/合规）

目标：统一、可组合、合规可控。

关键设计

• RWA 合规模块：基于 ERC-3643（T-REX） 扩展：

• 受限转让（Transfer Hook：KYC/地域/黑名单/锁定期）；

• 强制赎回/回收（法律事件触发）；

• 分红快照（快照块 + Merkle 分发）；

• 资产元数据（法律文件哈希、估值、节点签章）。

• 治理代币 ABLE：EIP-20 + EIP-2612 + 治理模块（投票/提案/锁仓）。

• 索引与披露：Token Metadata 标准化（schema + IPFS/Arweave）。

SLO/Sec

• 合约覆盖率 ≥ 95%；双审计 + 形式化验证关键函数（transfer hooks、redeem）。

优先级：P0

⸻

6) DEX、预言机与跨链桥

目标：让小众 RWA 也有成交深度；喂价可信；跨链安全。

6.1 DEX（混合架构）

• 撮合优先 + AMM 兜底：CLOB（价/时优先）+ v2/v3 Pool；统一深度视图。

• RWA 保护：默认价带/熔断、集合竞价首发；滑点保护与交易白名单（合规地理限制）。

• 流动性：官方 LP 锁仓 + 做市任务（靠 ABLE 激励 + 罚没条款）。

SLO/Sec：撮合内核延迟 < 100µs；端到端 < 200ms；反自成交/洪水挂单防护。

6.2 预言机（Oracle）

• 多源签名（≥3 源）；价格 + 估值 + 法律事件三类喂价。

• 聚合算法：中位数 + 偏差剔除（MAD/σ 阈值）；延时确认防闪电贷。

• 法律事件喂价：过户/抵押/违约 → 触发合约回购/冻结/强清。

SLO/Sec：喂价窗口 30s–300s；异常自动降级；签名轮值、喂价审计链上可查。

6.3 跨链桥（Bridge）

• 轻客户端优先（IBC/LC）；若用多签桥 → M-of-N + TEE + 保险池。

• 资产映射：RWA 仅跨链到有合规模块的目的链（白名单链）。

• 监控：Proof 延迟/合约重放/阈值变更均需链上治理。

SLO/Sec：转移确认 < 5min（LC）；多签桥需 24/7 监控与自动熔断。

优先级：P0（DEX/Oracle），P1（Bridge）

⸻

7) 必补模块（顶级项目必须有）

7.1 SaaS 上链（发行人后台）—和 RWA 强绑定

• 文件 → AI 审核 → 节点签章 → 铸币 → 上架交易 → 分红日历。

• API：Webhook 回调；错误显式；状态机可回放。

• 24h 上链 SLO：从资料齐全到可交易 ≤ 24h。

7.2 合规/KYC/AML

• 身份、制裁名单、交易模式检测（KYT）；转账 Hook 拦截。

• 监管接口：监管只读密钥，可导出交易与资产快照。

7.3 观测/SRE

• 四大看板：链（TPS/延迟/出块漂移）/ DEX（深度/点差）/ 预言机（喂价偏差）/ 桥（队列与失败率）。

• 灰度开关、特性旗标（Feature Flags）、一键回滚。

• 压测基线：合约/撮合/索引各自独立压测套件。

⸻

8) 环环相扣的数据与接口规范（对外承诺）

• 公共接口：RPC/WS、GraphQL Index、Explorer REST。

• 企业接口：SaaS 上链 API、分红对帐 API、合规审计 API、监控与告警 Webhook。

• 事件总线：Kafka topic 标准（tx.new、dividend.settled、oracle.update、bridge.finalized）。

• Schema 版本化：AssetMeta v1→v2 兼容策略；Deprecation 日历。

⸻

9) 安全与合规底线（不可妥协项）

• 合约双审计 + 关键模块形式化（桥、预言机、受限转让）。

• 秘钥：HSM/MPC，离线备份分层密封；提币/桥转多岗审批。

• 数据：PII 加密、最小化收集；合规地域强约束（合约层校验）。

• 事件响应：P1 事件 15 分钟内公告；72 小时根因报告（RCA）。

• 保险与储备：RWA 安全基金（≥ 5% 手续费沉淀），桥黑天鹅保险池。

⸻

⸻

TL;DR（一句话）

用“EVM 兼容 + RWA 合规模块 + DEX/Oracle/Bridge 三位一体 + SaaS 24h 上链”做成面向真实资产的金融级公链；

一切围绕：可信、可审计、可扩展、可监管 四个“可”。