

XUL Chain 资产与场景白皮书

XUL Chain Asset & Use-Case Whitepaper

主标题：XUL — 咻一声，无限场景就位。 / XUL — a whoosh, and infinite scenarios are ready.
配套深度规格（Living Specs）：
- 《XUL Agent 安全架构》`XUL-Agent-Security-Architecture.md`
- 《XUL Agent Hub 通用编排层架构》`XUL-AgentHub-Orchestration-Architecture.md`
- 《XUL Agent Hub 商业模式 / 费率设计》`XUL-AgentHub-Business-Model.md`
- 《XUL 开源策略》`XUL-Open-Source-Strategy.md`
语言：中英双语 / Bilingual (CN / EN) | 状态：概念验证白皮书草案（2026-07-19 老板拍板 + 定调）

目录 / Contents

- 序 · 使命 / Preface — Mission
- 第 1 章 · Agent 安全架构（Agent 原生、默认安全）
- 第 2 章 · 通用编排层（Agent 调用所有 APP 功能）
- 第 3 章 · 商业模式与费率（让 Agent 应用会赚钱）
- 附录 · 排期与开放决策

序 · 使命 / Preface — Mission

「XUL 链和首个 Agent 应用覆盖所有赚钱能力，让人不再为了金钱负重，回归到现实世界创造美好。」
"XUL Chain and its first Agent app cover all money-making capabilities, so people are freed from the burden of money and return to the real world to create beauty."
这是 XUL 的 mission statement，也是本白皮书的第一句话。 / This is XUL's mission statement — and the first sentence of this whitepaper.

XUL 是一个词根（root word）：一个能「创造无限场景」的词根，而不是单个产品名。它读起来像「咻」（xiū）——物体疾速掠过的拟声——语境是「快」。XUL 给人的第一直觉必须是快：快上链、快理解、快调度、快落地。 / XUL is a root word that spawns infinite scenarios, not a single product. It sounds like "咻" (xiū) — a whoosh — and means *fast*. XUL's first instinct must be speed: on-chain fast, understand fast, orchestrate fast, ship fast.

而「快」在这里有更深的人文落点： / And "fast" has a humanist payload:

- Agent = 用户的「金融劳动力」，覆盖一切赚钱能力。Agent = the user's *financial labor force*, covering every money-making capability.
- 咻 = Agent 用疾速替你处理金钱重负，你才能回归现实去创造美好。 / The whoosh is the Agent handling your financial burden at speed, so you can return to the real world and create.

这正是 XUL 与 X（原 Twitter）的 everything-app 叙事的分野：X 是中心化的 everything-app，XUL 用「Agent 调用所有 APP 功能」做成去中心化版 everything-agent——信任写进链上合约，而非靠审计承诺。 / This is what separates XUL from X's everything-app: X is a centralized everything-app; XUL is a decentralized everything-agent — trust is on-chain, not promised by audit.

第 1 章 · Agent 安全架构 / Chapter 1 — Agent Security

Agent 原生、默认安全 / Agent-native. Safe-by-default.

深度规格见《XUL Agent 安全架构》`XUL-Agent-Security-Architecture.md`。

1.1 为什么这一章存在 / Why This Chapter Exists

XUL 的 Thesis：用户只说话，Agent 在背后调度链上资产。 / The user only speaks; the Agent orchestrates on-chain assets.

这带来一个无法回避的问题——谁来保证 Agent 不会作恶、不会被盗、不会把用户资产转走？ / Who guarantees the Agent won't go rogue, get hacked, or drain the user's funds?

答案：不让 Agent 碰主私钥，给一把受限的 Session Key，把规则写进链上，大额交还用户本人。 / Don't let the Agent touch the master key. Give it a restricted Session Key. Write the rules on-chain. Hand large transfers back to the human.

1.2 五条铁律 / Five Hard Rules

#	原则 / Principle	含义 / Meaning
1	主私钥永不出户 / Master key never leaves the device	Agent 绝不持持有用户主私钥。The Agent never holds the master key.
2	最小权限 / Least privilege	Agent 只拿到一把独立 Session Key，被限额、限合约、限时间。Capped,
3	信任边界在链上 / Trust boundary is on-chain	额度、白名单、过期由智能合约强制，不依赖任何 off-chain 环境（含 TEE）。Enforced by smart
4	分级放行 / Tiered approval	小额自动执行；超阈值强制用户二次确认。Small auto; over threshold, the human confirms.
5	可恢复 / Recoverable	底层账户支持社交恢复，避免单点丢失。Social recovery.

1.3 架构分层 / Layered Architecture

- L1 · 底层账户：ERC-4337 账户抽象 — 用户标准钱包 = 智能合约钱包（AA）；社交恢复、Gas 抽象、可编程权限；XUL 自建 Bundler，可选 Paymaster。
- L2 · Agent 权限：Session Key — 每 Agent 一把独立 Session Key（不派生自主私钥、可吊销）；链上约束：每日额度上限、合约/函数白名单、过期时间、可吊销。
- L3 · 执行与守卫 / Guard 合约 — Agent 用 Session Key 签名 -> 先经 Guard 校验（额度/白名单/过期）-> 通过才执行，失败链上 revert；不依赖任何中间件信任。
- L4 · 兜底：大额复核 — 超阈值强制用户本人二次确认（诚实命名"大额复核"，2FA 式；非真 MPC，除非后续部署阈值签名）。
- L5 · （P3 暂缓）TEE — 仅作 AI 思考私密性的可选隐私层，非安全边界（可信硬件单点故障、与 trustless 叙事相悖）。

1.4 已拍板 / Decisions Locked (2026-07-19)

- 1.TEE：暂缓至 P3，仅可选隐私层，非安全边界。
- 2."无 Gas"赞助方：三种模式都要（协议金库 / Agent Hub 代付 / 用户付隐藏），Paymaster 支持多赞助方路由。
- 3.MVP 范围：AA 钱包 + Session Key + 白名单 + 大额复核（不上 TEE，即得 ~80% 安全）。

第 2 章 · 通用编排层 / Chapter 2 — Universal Orchestration

Agent 调用所有 APP 功能 / The Agent calls all app functions

深度规格见《XUL Agent Hub 通用编排层架构》`XUL-AgentHub-Orchestration-Architecture.md`。

2.1 一句话 / One-Liner

Agent Hub 不是封闭功能 App，而是通用编排层：社交 / DeFi / DAO / 监控 / NFT · RWA / RWA 都是「可注册、可调用」的连接器，新 App 即插即用。 / Agent Hub is not a closed feature-app; it is a universal orchestration layer — social / DeFi / DAO / monitor / NFT · RWA are pluggable, callable connectors.

这正是「词根 -> 无限场景」真正的技术引擎：原有的"四大 Agent"框架升级为 Orchestrator + 连接器注册表，连"社交"也只是它可调用的一个场景。 / This is the real engine of "root word -> infinite scenarios".

2.2 核心抽象 / Core Abstractions

组件 / Component	职责 / Role
Orchestrator	意图理解（NL -> 任务）、连接器选择、调用编排、结果聚合。
Connector（连接器）	某 App / 能力的适配层，暴露 callable functions（tool schema）。

Connector Registry	连接器注册表（先链下索引，后链上登记），含权限 / 声誉元数据。
Session Key（每连接器）	独立受限钥匙（限额 / 白名单 / 过期 / 可吊销），接安全架构。
Guard 合约	跨连接器调用前校验（额度 / 白名单 / 过期），失败链上 revert。
Reputation（链上声誉）	地址 / 连接器信誉分，决定可调用的权限与额度（接 TweepCred 思想）。

2.3 连接器模型 / Connector Model

- Connector Manifest: `id` / `name` / `type` (defi / social / dao / monitor / rwa / strategy / web2) / `functions[]` (schema + riskLevel) / `permissions[]` / `endpoint`。
- Function-calling 协议: 标准 tool schema, 类 MCP / JSON-RPC 调用; Web2 App 经 API 适配网关转 tool。
- 示例连接器: DeFi（质押/兑换/套利/收益聚合）、社交（发帖/关注/互动 Agent/AgentAgent 协调）、RWA（实物上链、收益分发）、策略市场（上架/购买/复制交易）。

2.4 意图路由 / Intent Routing

- 1.用户输入（文字 / 语音 / 摄像头）-> Orchestrator NL 理解
- 2.拆任务 -> 选连接器 + 函数（可多连接器组合）
- 3.组装 UserOperation（带该连接器 Session Key 签名）
- 4.Guard 合约校验（额度 / 白名单 / 过期）-> 通过
- 5.超阈值 -> 触发大额复核（用户确认）
- 6.执行 -> 结果回 Orchestrator -> 自然语言回用户

2.5 「调用所有 APP 功能」如何实现 / Calling All Apps

- Web3 App: 直接注册链上合约地址 + function schema。
- Web2 App: 经适配网关把 REST / GraphQL API 转成 tool schema（中心化但可审计，呼应开源策略「无两套代码」——网关代码开源、运行可核验）。
- 结果: 用户一句话, Agent 跨 Web3 + Web2 多个 App 完成任务 -> 去中心化 everything-agent。

第 3 章 · 商业模式与费率 / Chapter 3 — Business Model

让 Agent 应用会赚钱 / Make the Agent app earn

深度规格见《XUL Agent Hub 商业模式 / 费率设计》`XUL-AgentHub-Business-Model.md`。

3.1 四种赚钱模型（全选）/ Four Models (all selected)

- 1.用户赚（Agent 帮用户理财）：质押 / 收益 / 套利 / 交易 / RWA，资产增值。
- 2.平台 / 协议赚（XUL 抽成）：对 Agent 执行、Gas 代付、场景 / 连接器调用收手续费。
- 3.飞轮（两者都要）：用户资产增值 -> 更多委托 -> 更多手续费 -> 生态扩张 -> 更好 Agent -> 更多用户。
- 4.Agent / 策略成商品：策略上架成可买卖数字商品（策略市场 / 复制交易），XUL 收市场费。

3.2 费率设计草案 / Fee Design (draft)

费项 / Fee	征收点 / When	草案区间 / Draft range	归属 / To
执行费 / Execution	每笔 Agent	0.1% - 0.5%（按连接器风险）	协议金库
Gas 代付回收 / Sponsor recovery	「无 Gas」代付后	从收益或执行费回收 / 金库补贴	协议金库 / Agent Hub
连接器调用费 / Connector call	按连接器类型	差异化（DeFi > RWA > 社交）	协议金库 + 连接器方分成
策略市场抽成 / Strategy market	策略收益或买卖	5% - 10% 收益分成	协议金库

注：具体数字待财务模型；先给框架，避免「承诺收益」误导。

3.3 收入归集与使命闭环 / Revenue & Mission Loop

- 收入进协议金库（DAO 预算），由治理分配。
- 「无 Gas」赞助方（多路由：金库 / Agent Hub / 用户付隐藏）由金库 / Hub 代付，靠执行费 + 市场费回收 -> 可持续。
- 使命闭环：平台抽成 -> 养「无 Gas」与生态 -> 用户零摩擦赚钱 -> 资产增值 -> 更多委托与抽成 -> 飞轮 -> 最终让人脱离金钱负重，回归现实创造美好。

3.4 风险与边界 / Risks & Boundaries

- 禁止「承诺收益」：Agent 展示历史 / 模拟，不保收益（合规 + 信任）。
- 透明可撤回：Agent 动资金须实时可见、用户可一键停（接 Session Key 可吊销 + 大额复核）。
- 不忘使命：商业是手段，「回归现实创造美好」是目的。

附录 · 排期与开放决策 / Appendix — Roadmap & Open Decisions

A.1 落地排期 / Roadmap

阶段 / Phase	范围 / Scope	备注 / Note
P1（概念验证 MVP）	ERC-4337 AA 钱包 + Session Key + 白名单 + 大额复核；先做 DeFi + 社交 + RWA 三示例连接器	不上 TEE，即得 ~80% 安全
P2	"无 Gas"赞助模型实跑（Paymaster 多赞助方路由）；注册表上链	—
P3（主网成熟）	可选 TEE 隐私层；评估真阈值签名 MPC；开放第三方注册连接器 + 策略市场	TEE 非安全边界

A.2 待定事项 / Still Open

- 连接器注册是否需治理审批？（建议：开放注册 + 声誉 / 审计兜底）
- 链上声誉具体算法（接 TweepCred 思想，待定）
- Web2 适配网关中心化风险（透明 + 可替换 + 开源）
- 具体费率数字（待财务模型）
- XUL 代币经济（待《真公链规格书 v1》新模型；旧 v4 已废弃，严禁沿用）
- 新链 RPC / Chain ID / 浏览器域名 / 网络 ID（TBD，先用本地 anvil 开发）
- 模型自研触发条件（远景）：垂直金融专精模型（非基础模型）；触发 = MAU / 月 API 支出 / 累计脱敏金融交互 ≥ 阈值；当前 MVP 只埋数据管线，不自研。盈利引擎 = 模型 + 执行闭环。详见《XUL Agent Hub 商业模式 / 费率设计》§ 7。

本白皮书为共建活文档（living document）。所有结论随讨论持续并入，详细参数以各 Living Spec 为准。XUL — 咻一声，无限场景就位。