AFT AgentChain

WHITEPAPER V1.2

AI-Native Blockchain Infrastructure
for Autonomous Agents

面向自主智能体的 AI 原生区块链基础设施

中文版 CHINESE EDITION / 协议与融资设计

V1.2

阅读指南与目录

Reading Guide & Contents

AFT AgentChain Whitepaper V1.2 描述一个面向自主智能体的身份、授权、执行与结算网络。本文用于产品、技术与生态讨论。

版本边界 Document Status

本版提出目标架构、实施路径及代币融资方案，不代表已部署主网、已发行代币、已取得牌照或已完成审计。融资估值、价格、分配和锁仓均为拟议条款；实际实施须以代码、测试报告、法律意见与签署的交易文件为准。

目录 Contents

术语与依据 Terminology

Agent 指受自然人或企业授权的软件智能体；Owner 指承担控制与责任的主体。AIP 是本项目拟议的 Agent Interaction Protocol 名称，不表示已被行业采纳。文内 [1]—[8] 对应末页公开资料；这些资料支撑基础概念，不构成对本项目的背书。

01

执行摘要

Executive Summary

AFT AgentChain 的核心命题，是让 AI 在明确授权范围内参与经济活动，并为每次交易留下可验证、可追责的记录。

问题与方案 Problem & Proposal

AI 可以生成采购计划、调用工具与协调服务，但跨组织执行仍缺少统一的身份绑定、预算控制、付款条件和争议证据。AFT AgentChain 拟通过五层架构，将智能体发现、钱包权限、链下执行及链上结算连接为一致的交易生命周期。

最小可行闭环 Minimum Viable Loop

首个验证场景是企业智能体购买 API 或算力：发现服务、验证供应商、获得签名报价、锁定预算、执行订单、验收结果并结算。MVP 优先使用单链、单一测试资产及有限供应商，先证明订单不会重复扣款、撤权能够生效、失败能够退款。

基础设施定位 Infrastructure Positioning

AI 模型不进入区块共识；验证者只处理确定性状态转换。独立 L1 是候选长期路径，早期协议可以在现有兼容测试网络上验证。是否建设独立网络，应由性能、费用、自治需求和维护成本的实测结果决定。

价值与边界 Value & Boundaries

项目价值拟来自减少交易集成成本、提高审计可追溯性和限制自动化资金风险。AGT 仅按潜在协议用途讨论，不承诺投资回报、价格表现或流动性。主网、稳定币接入、银行通道及商业部署分别设置技术与合规准入条件。

02

智能体经济背景与痛点

Agent Economy Background & Frictions

当软件从回答问题转向调用工具，交易的基本单元将从人工点击逐步延伸到机器可读取、可授权和可核验的服务订单。

01
自主协作
Autonomous Agents

02
服务与算力
Services & Compute

03
价值交换
Value Exchange

概念插图 · 协议机制见正文

从工具调用到经济行为 From Tools to Transactions

购买数据、调用付费 API、租用 GPU 与自动续订，涉及真实费用和外部责任。模型输出本身不能证明付款合法、报价有效或服务交付。可验证身份、结构化签名与可编程账户为此提供组件基础 [1][2][3][4]，但仍需统一业务语义。

四类断点 Four Gaps

身份断点：地址控制权不能证明企业资质或服务能力。授权断点：一把长期私钥往往拥有过宽权限。执行断点：服务响应、订单状态与付款记录分散。结算断点：链上成功、商户到账和银行入账具有不同含义，失败补偿常依赖人工。

为什么需要共享协议 Shared Protocol Need

共享协议可以让不同服务商采用统一订单标识、报价格式、撤销机制和证据摘要，降低重复开发成本。只有确实需要多方共同验证的状态才上链；搜索、推理和敏感合同保留在链下，以控制成本并减少公开数据。

需求验证 Demand Validation

本版不使用未经核验的市场规模或交易增长预测。早期试点应测量单笔人工处理时间、失败恢复率、对账差异和供应商接入成本；若传统数据库与支付接口已足够，应允许采用较简单的部署方式。

03

愿景与设计原则

Vision & Design Principles

AI-Native Blockchain Infrastructure for Autonomous Agents
面向自主智能体的 AI 原生区块链基础设施。

愿景 Vision

为智能体经济建立可信身份、受限授权和可核验结算的公共接口。AI 原生的含义是账户、消息与费用模型能够表达智能体任务，而不是让模型替代共识或法律责任主体。

控制权与可撤销性 Human Control

资金最终受个人或企业控制。智能体获得短期、范围受限的执行能力；所有者可以暂停会话、轮换密钥并终止新订单。撤销对已最终结算交易不具有追溯逆转效力，系统必须明确这一时间边界。

确定性与互操作 Determinism & Interoperability

安全关键检查使用明确规则：资产、收款人、限额、有效期和 nonce。身份、凭证及签名尽可能参考公开标准 [1][2][4]。对外适配器与核心协议解耦，使业务可迁移到不同钱包、模型和结算网络。

渐进建设 Progressive Delivery

先完成协议规范和故障测试，再引入公共测试网与独立验证者。每次扩展以风险增量为依据：单链先于跨链，限定供应商先于开放市场，人工争议处置先于自动仲裁。初始版本不包含算法稳定币、收益理财或无约束自主交易。

04

五层总体架构

Five Layer Architecture

五层结构将业务智能与资金安全分离。每层输出可核验的接口结果，下一层只接受符合协议规则的输入。

职责边界 Layer Responsibilities

身份层回答“谁在行动”；钱包层回答“允许做什么”；执行层记录“做了什么”；支付层定义“何时支付”；L1 确认“哪些状态最终成立”。应用不应跳过授权层直接让模型操作根密钥。

链上与链下 On-chain & Off-chain

链上保存身份控制状态、授权摘要、托管余额和结算事件；链下保存模型推理、服务发现索引、原始交付物及受保护凭证。摘要只能证明特定数据的完整性，不能证明其内容真实。

部署路径 Deployment Path

原型阶段把核心合约部署到兼容测试链。独立 L1 阶段再引入自有共识、费用和节点治理；两阶段之间需要显式迁移方案，不能假定旧网络状态会自动继承。

05

智能体身份层

Agent Identity Layer

智能体身份由所有者控制、可轮换密钥与可验证声明共同构成。链上身份是技术标识，不自动赋予法律人格。

身份模型 Identity Model

AgentRecord 拟包含 agentId、owner、controllerKey、serviceURI、capabilityHash、version 与 status。注册时验证控制者签名；更新时递增版本并发出事件。服务地址只是发现入口，客户端仍须校验域名、证书和签名，防止恶意重定向。

可验证凭证 Verifiable Credentials

企业资质、服务范围或认证结果可由受信发行方提供凭证。验证流程检查签名、发行方信任策略、有效期及撤销状态；DID 与 VC 可作为互操作参考 [1][2]。自我声明与第三方验证在界面和接口中分别标记。

轮换与恢复 Rotation & Recovery

所有者变更需多签或受控恢复流程，设置延迟与告警。恢复完成后撤销旧会话权限，重新验证未完成订单。注册状态至少包括 Active、Suspended 与 Revoked；历史记录保留版本，避免旧报价被误判为当前有效。

信誉并非身份 Reputation Limits

信誉基于已结算订单、争议结果和服务可用性形成多维指标，不合并为不可解释的万能信用分。关联地址刷单与伪造资质无法仅靠链上记录消除；高风险供应商仍需要企业尽调及人工审核。

06

智能钱包与授权

Agent Wallet & Authorization

智能体使用会话权限执行任务，所有者保留根控制权。预算检查必须由钱包或授权合约强制执行，不能仅依赖提示词。

授权范围 Policy Scope

Policy 拟绑定 chainId、wallet、agentKey、asset、recipient、methodSelector、perTxLimit、periodLimit、validUntil 与 policyNonce。任意字段不匹配即拒绝。预算按资产最小单位记账；若需要法币限额，必须另定义价格源、更新频率与保守误差。

并发与预算 Budget Reservation

可用预算 = 周期上限 − 已消费金额 − 已预留金额。创建有效订单时原子预留，结算时从预留转为已消费，退款或超时后释放。不同会话共享父级预算，防止多个智能体同时检查通过而超支。

账户抽象 Account Abstraction

可参考 ERC-4337 的账户抽象与 Paymaster 模型 [3]，将批处理、费用代付和签名验证模块化。具体实现仍须明确 EntryPoint 版本、适配链和仿真规则；“支持稳定币付费”不意味着无需底层费用资产或代付流动性。

撤权与紧急暂停 Revocation & Pause

每次执行重新检查授权版本和链上状态。撤权交易最终确认前仍存在竞争窗口，客户端必须显示这一风险。异常暂停阻止新资金流出，已锁定订单依合同走退款或争议路径；恢复权限不能暗中改写收款人。

07

智能执行层

Agent Execution Layer

执行层把开放式任务转化为有边界的订单。模型负责提出行动，独立策略引擎和签名模块决定行动是否可执行。

执行流水线 Execution Pipeline

任务进入后先解析预算与服务要求，再选择已验证供应商、获取报价并生成订单。策略引擎检查工具白名单和数据权限；签名服务仅签署通过检查的结构化消息。模型上下文不得包含根私钥或可重复使用的付款凭据。

确定性验证 Deterministic Validation

验证者不运行大模型或重放外部 API。执行证明可包括请求摘要、服务版本、时间范围、计量记录和交付摘要。内容质量由预先约定的验收器或人工审核判断，链上只能执行明确编码的支付条件。

隔离与可恢复性 Isolation & Recovery

外部工具在受限环境运行，限制网络出口、文件访问、CPU 和超时时间。每个任务设置幂等键与重试上限；API 超时后先查询既有订单再重试。执行失败可以释放尚未支付的预算，但无法保证撤回已经发生的外部行为。

可审计证据 Evidence

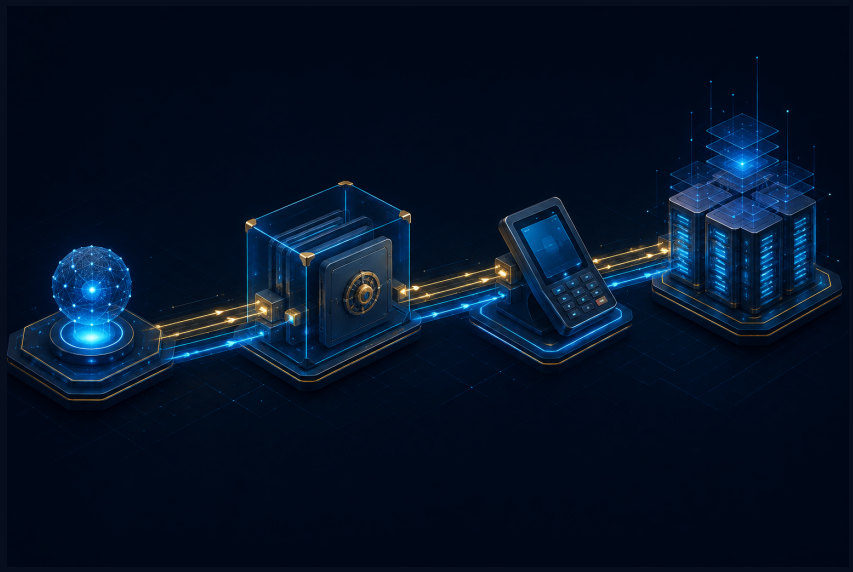
Receipt 拟绑定 orderId、requestHash、outputHash、metering、executorSignature 与 policyVersion。原始结果加密保存并配置保留期；凭证摘要写入结算记录。可选 TEE 或零知识证明应单独说明信任假设、覆盖范围和成本，不作为 V1 前提。

08

支付与结算层

Payment & Settlement Layer

支付是转移价值的动作，结算是满足最终性条件后的状态确认。AgentChain 必须分别跟踪订单验收、链上确认与外部到账。



01
受限授权
Bounded Authority

02
有条件支付
Conditional Payment

03
最终结算
Final Settlement

概念插图 · 协议机制见正文

资金路径 Funds Flow

MVP 使用白名单测试资产：付款钱包向订单托管合约预存资金，服务验收后释放给供应商，失败或超时按规则退款。只有授权不等于已付款；只有发出交易不等于最终结算。订单与托管记录通过唯一 orderId 关联。

费用与稳定币 Gas Abstraction

用户报价可拆成服务费、网络费及适配器费用。代付方先承担底层 Gas，再按签名条款收取允许的资产；报价须有最大费用和失效时间。稳定币必须逐一审查发行、赎回、冻结与所在链风险，不能仅凭名称承诺支持。

微支付 Micropayments

高频小额服务优先累计计量并分批结算，设置最大未结清额度和时间窗口。支付通道属于后续扩展，需要处理离线争议、挑战期和抵押占用。任何“实时”展示都应标明是授权成功、临时入账还是最终确认。

跨链与法币 External Settlement

跨链桥、银行与收单方均是独立信任边界。跨网络流程需要确认策略、流动性、失败补偿和人工升级；不承诺原子跨链或即时银行到账。法币接入由具备相应资格的服务主体承担，协议本身不自动获得支付许可。

09

AIP 智能体交互协议

AIP Agent Interaction Protocol

AIP 将一次智能体交易拆为八个连续阶段。每个阶段形成可绑定订单的证据，任何异常都进入明确的拒绝、超时或争议路径。

授权后预存托管 / 验收后释放 / 异常进入退款或争议

交易前 Pre-transaction

发现阶段返回服务描述与协议版本；身份验证检查控制权和凭证；报价绑定资产、数量、费用、期限、验收条件和争议条款；授权阶段校验策略并预留预算。发现排名本身不构成可信证明。

交易中与交易后 Execution & Settlement

执行前可向托管合约提供资金保障；执行后按验收结果发起支付释放，等待结算最终性，最后允许评价。流程图中的“支付”指对供应商的释放指令，预存托管资金发生在授权后，避免先履约却无支付保障的歧义。

异常分支 Exception Paths

身份失败或报价过期则拒绝；执行超时按合同退款或争议处理；链上提交状态不明先查询，避免重复支付。评价只在真实订单结算或争议裁决后开放，不允许评价结果反向修改已完成资金转移。

10

AIP 消息与状态机

AIP Messages & State Machine

签名消息必须绑定交易上下文。V1 使用严格状态转换和幂等处理，避免把网络重试误当成新的经济行为。

消息信封 Message Envelope

公共字段拟为 protocolVersion、messageType、orderId、senderId、receiverId、chainId、verifyingContract、nonce、expiresAt、payloadHash 和 signature。结构化签名可参考 EIP-712 [4]；它不自动提供防重放，合约仍须检查 nonce、域与过期状态。

状态与权限 State Transitions

订单由 Quoted 进入 Authorized，再进入 Funded 与 Executing；满足验收条件后进入 Accepted、PaymentSubmitted，最终 Settled。付款人可拒绝过期报价；执行者提交凭证；验收者依据合同接受或挑战；托管合约依据终态释放。

失败终态 Failure States

未开始执行且到期的订单可 Expired；未付费授权可 Cancelled；已入托管的争议进入 Disputed，裁决后为 Refunded、Settled 或按约定分配后的 Closed。Disputed 不是退款完成。每个终态只能应用一次资金分配。

不可变约束 Invariants

同一 orderId 的资产、付款钱包、收款人和报价摘要创建后不可替换。托管本金 = 未分配本金 + 已释放本金 + 已退款本金，手续费另列且总扣款不得超过签名上限。监听器须去重、重放和对账；Webhook 只能通知，不能替代链上事实。

11

智能体间经济与生态

Agent-to-Agent Economy & Ecosystem

生态由需求方智能体、服务方智能体、开发者、验证者及外部服务机构构成。每个参与者拥有明确接口，也承担独立责任。

组合服务 Composable Services

采购智能体可向数据智能体购买输入，再向算力服务提交任务。父订单为子订单分配预算与截止时间，任何子委托不得扩大父授权。供应商应公开计费单位、版本与验收方式，使服务能在一致标准下组合。

激励与收费 Incentives & Fees

服务商按交付获得服务收入，验证者按网络规则获得费用或拟议安全补贴，开发者可通过工具与企业支持收费。协议费、商业服务费和代币奖励分别披露，避免用补贴订单伪装真实需求。

信誉与市场质量 Market Quality

评价采用已验证订单标签、争议率与样本数量，允许供应商申诉。反女巫措施可结合注册成本、凭证与关联交易分析，但不能保证彻底消除刷量。生态图表示目标角色，不表示已有合作方或商业客户。

12

共识与网络架构

Consensus & Network Architecture

独立网络候选方案采用权益权重的 BFT 共识与确定性执行环境。最终技术选型须经过公开评审、原型基准与运维演练。

候选技术路径 Candidate Stack

可评估 CometBFT 类共识配合 EVM 兼容执行层，便于复用钱包与合约工具。共识负责排序及确认，执行层负责状态转换，两者之间的费用计算、状态根和升级边界必须统一。采用组件不等于自动继承其全部安全性质。

安全假设 Safety Assumptions

典型 BFT 设计以严格超过三分之二投票权的提交证书确认区块；安全论证依赖少于三分之一拜占庭投票权，活性还依赖网络及时通信等条件 [5]。网络分区可能停止出块，不能把确定性最终性解释为任何故障下持续可用。

网络拓扑 Network Topology

验证者经哨兵节点接入 P2P 网络，公共 RPC 与索引服务单独扩容。归档节点保存历史，轻客户端验证可信起点与签名更新。验证者集合变更需在明确高度生效，避免旧新集合对同一区块产生不一致解释。

独立 L1 决策门槛 L1 Decision Gate

只有现有网络无法满足经验证的需求，且团队具备持续安全预算、节点多样性及升级能力时，才推进独立 L1。初始受控测试集不宣称充分去中心化；不在 V1 承诺 TPS、最终性秒数或上线日期。

13

智能合约体系

Smart Contract Architecture

核心合约保持职责单一，并通过显式权限连接。涉及资金的路径先建立不变量，再进行实现、模糊测试和独立审计。

核心模块 Core Modules

AgentRegistry 管理身份版本；PolicyManager 管理授权与额度；OrderBook 固定报价和订单状态；EscrowVault 保存资金并结算；ReceiptRegistry 记录证据摘要；FeeManager 管理费用参数。模块名称为拟议接口，尚非已发布合约地址。

执行顺序与资产支持 Execution Safety

先验证权限与状态，再更新内部记账，最后执行外部转账，配合重入防护。代币转账必须检查实际到账与返回值；MVP 排除重基准、转账扣税等非标准资产。任何余额差异触发暂停新订单并进入人工核查。

升级与兼容 Upgrades

无状态适配器可版本化替换；资金核心是否可升级需单独评审。若采用代理，管理员必须多签、延时执行并披露实现地址。旧订单保留原始规则或获得当事人明确迁移同意，治理不能单方改变既定收款条件。

验证要求 Verification Requirements

覆盖重复结算、重入、越权、精度误差、并发预留和超时边界。关键不变量包括资金守恒、终态唯一、额度不为负以及撤销后的新调用被拒绝。外部审计发现须修复并复测；审计不等于零漏洞保证。

14

安全模型与防御

Security Model & Defense

最大风险来自模型、工具、密钥与资金之间的连接。安全设计应假设外部网页、服务响应及智能体消息都可能包含恶意指令。

01
权限边界
Permission Boundaries

02
验证网络
Validation Network

03
分层防御
Layered Defense

概念插图 · 协议机制见正文

提示注入与工具滥用 Prompt Injection

外部内容只能作为数据输入，不能改变付款策略或白名单。对工具参数使用结构化校验，阻止服务响应直接指定新收款地址。高金额、首次供应商、异常频率等动作升级为人工审批，审批结果绑定具体订单摘要。

密钥与供应链 Keys & Supply Chain

根密钥由硬件或受控签名系统保管，会话密钥短期有效并限制操作范围。发布采用依赖锁定、构建校验、签名制品与最小权限。生产、测试和开发环境隔离，测试凭据不得拥有生产资金权限。

攻击与应急 Incident Response

监测异常扣款、RPC 差异、签名失败、双签证据和服务中断。事件响应顺序为隔离受影响入口、暂停新增风险、保全日志、通知责任方、修复与恢复。无法撤销的最终结算交易通过合同救济处理，不承诺技术追回。

安全发布门槛 Release Gates

上线前完成威胁建模、权限审查、资金不变量测试、渗透测试和密钥恢复演练。公开测试网设置赏金与漏洞报告渠道；主网前解决未关闭的严重及高危问题。可参照 NIST AI RMF 组织模型风险管理 [8]，但不将其表述为认证。

15

隐私与数据治理

Privacy & Data Governance

数据最小化是默认原则。链上可验证性不要求公开客户身份、合同全文、提示词或商业交付物。

数据分层 Data Classification

公开层仅保留必要标识、状态与摘要；业务层加密保存合同和验收证据；敏感层保存身份核验材料与客户信息并严格授权。不同业务主体应明确谁决定处理目的、谁执行处理及谁响应权利请求。

访问与留存 Access & Retention

通过租户隔离、最小权限、短期访问令牌和访问日志控制读取。按业务及适用法律建立保留期，到期删除链下材料或按合法依据继续留存。链上记录无法按传统数据库方式删除，产品设计必须预先控制上链内容。

摘要的限制 Hash Limitations

可预测个人数据的普通哈希可能被枚举识别，不能视为匿名化。需要时使用随机盐、受控承诺或不在公链记录相关字段；即便内容加密，交易时间、金额和地址关联仍可能泄露商业关系。

选择性披露 Selective Disclosure

VC 可帮助组织凭证交换 [2]，但数据模型不自动提供零知识隐私。具体证明方案须验证库、撤销机制和可链接性。跨境数据流在接入前进行映射与评估，不以“去中心化”作为规避隐私义务的依据。

16

AGT 网络代币用途

AGT Network Token Utility

AGT 是拟议网络原生资产的暂定名称。V1.2 在协议用途之外补充融资设计：拟议总量 10 亿枚，投后 FDV 1,000 万美元，本轮计划融资 300 万美元。相关参数为拟议条款，不代表已发行或已完成融资。

拟议用途 · 不构成收益承诺

协议用途 Proposed Utility

候选用途包括网络费用、验证者安全质押、治理提案及有上限的开发者资助。服务提供者可以按协议自愿接受 AGT，但企业订单优先允许明确的结算资产，避免把业务使用强制绑定到代币持有。

费用与安全预算 Fee & Security Budget

用户可经代付接口使用允许的稳定币结算费用，代付者承担兑换、报价及库存风险。本方案不在 10 亿枚上限外增发；验证者补贴来自预留的网络激励池。激励消耗后应以实际网络费用支撑运营，安全预算不能依赖代币价格持续上升。

经济约束 Economic Constraints

融资、分配及解锁拟议参数见后两页。正式部署前仍须完成经济仿真与法律审查，并明确国库权限、质押退出期与罚没规则。AGT 不当然代表股权、固定收益或储备资产索取权；其交易和销售安排的法律分类须独立判断。

17

代币融资与分配

Token Financing & Allocation

按投后代币完全稀释估值（FDV）1,000 万美元设计，本轮融资目标为 300 万美元。以下为拟议交易条款，并非发行或融资完成公告。

投后 FDV	融资目标 Target	本轮占比 Round
US$10,000,000	US$3,000,000	30%

定价基础 Pricing Basis

拟议总量固定为 1,000,000,000 AGT；本轮统一认购价为 US$0.01/AGT；出售 300,000,000 AGT，目标募集总额为 US$3,000,000，尚未扣除费用。计算：1,000 万 ÷ 10 亿 = US$0.01；300 万 ÷ 0.01 = 3 亿枚。FDV 是定价乘以总量，不是流通市值，也不是公司股权估值；30% 不代表公司股权。

分配 Allocation	占比 / 数量	拟议解锁 Vesting
本轮融资 / Investors	30% / 300m	TGE 0%；锁定 6 个月；第 7–30 月均摊释放
生态与开发者 / Ecosystem	25% / 250m	TGE 释放池内 10%；余量于第 1–48 月均摊
验证者激励 / Validators	20% / 200m	TGE 0%；生产网络启用后 48 个月按贡献发放
团队 / Team	15% / 150m	TGE 0%；锁定 12 个月；第 13–48 月均摊
国库 / Treasury	10% / 100m	TGE 释放池内 10%；余量于第 1–36 月均摊
合计 / Total	100% / 1,000m	固定总量内分配，不额外增发

解锁口径 Release Rules

m 表示百万枚；TGE 为代币生成事件，时间另定。除验证者外，月份自 TGE 起算，月末释放；投资者每月解锁 1,250 万枚，锁定期结束时不补发。TGE 初始可解锁上限为 3,500 万枚（总量 3.5%），来自生态池 2,500 万及国库 1,000 万；可解锁不等于实际流通。生态拨款须验收，验证者月度奖励设池额 1/48 上限，未使用额度留存并另行审批。

投资者权利 Investor Terms

本轮不含额外折扣、奖励代币或未披露认股权益；总量与分配变更须重新披露并处理合同同意。未解锁代币不参与拟议代币投票。30% 集中分配带来治理与抛压风险；无股权、分红、保本、回购或上市承诺。

18

资金用途与交割

Use of Proceeds & Closing

300 万美元为本轮全额认购时的募集总额。以下预算以实际到账为执行前提，采用约 18 个月规划周期，不能视为已取得资金或主网交付保证。

资金用途 Use	比例 / 美元	交付与控制 Deliverables
协议与产品研发 / R&D	40% / 1,200,000	身份、钱包、AIP、托管与 SDK 原型
审计与安全 / Security	15% / 450,000	独立审计、漏洞修复及恢复演练
生态与试点 / Ecosystem	20% / 600,000	供应商集成、企业试点与验收后资助
法律与合规 / Legal	10% / 300,000	主体、交易文件、地区准入与数据审查
运维与财务 / Operations	10% / 300,000	云资源、节点支持、财务及行政
风险准备金 / Reserve	5% / 150,000	异常支出；独立批准后启用
合计 / Total	100% / 3,000,000	现金预算与代币池分开记账

预算执行 Budget Controls

剔除 15 万准备金，可部署预算为 285 万美元；若均摊 18 个月，月均约 158,333 美元，仅作为成本约束。支付与法律等融资费用计入对应科目，到账不足则调整范围并披露。资金进入发行主体独立账户或经审查托管安排，采用多签 / 双人审批及季度资金用途报告；估值不能作为可支出现金。

分期支出 Milestone Spending

建议按已到账资金分三档授权：30% 用于实体设立、规范与原型；40% 在安全评审及测试网演示通过后启用；30% 在试点验收及财务复核后启用。分档约束内部支出，不改变投资者锁仓，也不表示投资者按这些比例分期付款；每档仍遵守上表预算。

认购与交割 Subscription & Closing

拟采用面向符合适用资格要求参与者的代币认购安排。发行主体、司法辖区、投资者核验、法律分类、资金来源审查及签署合同均为收款前置条件；“私募”或“用途型代币”名称不自动免除监管义务 [7]。以美元计价；允许的支付资产和折算规则由合同限定。本轮统一价格，不附加做市或上市保证。

未完成情形 Failure Conditions

拟议最低交割额 150 万美元、募集上限 300 万美元，认购窗口为正式启动后 90 日。认购款在完成法律与交割条件前隔离保管；未达最低额或条件未满足，拟于窗口结束后 30 日内退回，不计收益。达到最低额但未满额，只按实缴金额及 0.01 美元单价配发，未售代币保持锁定。正式协议须约定 TGE 最迟期限、延期同意及未发行时救济；隔离与退款机制须在收款前落实。

19

节点与验证者

Nodes & Validators

节点运营的目标是保证可验证状态持续可获得，并在不同运营主体之间分散故障与控制风险。

节点角色 Node Roles

验证者参与投票并维护最新状态；全节点独立验证区块；归档节点提供完整历史；RPC 与索引节点支持应用查询；哨兵节点隔离验证者网络入口。RPC 提供者不因提供接口而自动成为共识验证者。

准入与退出 Admission & Exit

测试网早期可邀请独立运营者，公开准入条件和关联关系。主网候选机制按有效权益及治理规则选取集合，同时监测云服务、地域和控制人集中度。退出期需覆盖证据提交与罚没处理窗口，具体数值经测试确定。

奖励与惩罚 Rewards & Penalties

可证明双签适用严格处罚，短时离线可适用较轻停用或奖励扣减。证据格式、申诉边界和参数变更必须明确。惩罚旨在减少攻击与失职，不应将普通网络故障与恶意行为不加区分。委托者须理解相关损失风险。

运维要求 Operations

采用远程签名、密钥备份、监控告警和升级演练，禁止同一验证者密钥在多个活跃节点同时签名。公开可用性、漏签、版本和事件记录。硬件建议及节点容量须随基准报告发布，不能仅列通用配置即声称可承载主网。

20

开发者工具与接口

Developer SDK & API

开发者体验围绕“创建受限任务并观察可验证结果”设计。以下为拟议接口示例，尚无生产可用端点或 SDK 发布承诺。

SDK 功能 SDK Surface

优先规划 TypeScript 与 Python：身份解析、凭证验证、报价验证、授权模拟、订单提交、回执查询和事件订阅。默认先 simulate 再 submit；签名器由应用注入，不让 SDK 保存根私钥。所有错误返回机器可读代码与可重试标记。

接口示例 API Examples

GET /v1/agents/{id} 查询身份版本
POST /v1/quotes/request 请求签名报价
POST /v1/policies/simulate 检查权限及预算
POST /v1/orders 创建订单并返回 orderId
GET /v1/orders/{id} 返回业务与结算状态
POST /v1/orders/{id}/challenge 提交争议证据

协议约定 Protocol Conventions

写入请求携带 Idempotency-Key，金额使用最小单位的十进制字符串，时间使用统一 UTC 规范。SDK 校验 chainId、资产地址、有效期与签名域。事件携带 eventId、blockHeight、txHash 与确认状态；索引延迟不得被解释为订单不存在。

工具链与兼容 Tooling & Compatibility

提供本地模拟器、测试资产、示例商户、故障注入和 OpenAPI 定义。以主版本表示不兼容变更，旧接口设迁移窗口。参考实现、许可证、代码仓库与包名需在真正发布后列出；V1 不虚构下载地址。

21

企业应用与商业模式

Enterprise Applications & Business Model

首批应用优先选择金额受控、交付可计量、争议条件清晰的服务。以下场景均为设计示例，不代表已有客户或落地收入。

算力采购 Compute Procurement

企业给采购智能体设定 30 天、最高 2,000 美元等值的说明性预算。供应商提交规格、单价和可用时段，智能体按授权选择并预留额度。按验收的运行时长分段结算，未交付部分退款；技术指标和计费时间使用双方认可的证据。

付费数据与 API Data & API

数据服务按成功响应或有效结果计费，明确缓存、重复请求和错误响应是否收费。高频调用采用累计计量及额度预警，财务系统通过订单、发票和链上凭证三方对账。对不易自动验收的数据质量保留人工争议渠道。

企业运营 Enterprise Operations

订阅管理智能体可以续订允许的服务，采购智能体可以跨部门分配预算。跨境付款在后续阶段通过经过审查的服务商接入，先核验收付方资格、业务目的和外部到账回执，不让模型自行选择未知资金通道。

商业可持续性 Commercial Sustainability

收入候选包括企业软件订阅、服务支持和透明交易处理费。协议公共组件与商业托管服务分开计费，企业可替换服务提供者。试点衡量采购耗时、对账差异、失败恢复时间和真实复购，以实际使用支持继续投入。

22

性能目标与验证方法

Performance Targets & Validation

V1 不把实验室峰值作为生产承诺。性能评估必须同时覆盖安全、状态增长、网络故障与真实业务完成率。

指标定义 Metrics

分别记录授权检查延迟、交易纳入延迟、链上最终性、外部到账时间和完整订单耗时。报告 p50、p95、p99 及错误率，明确交易复杂度、节点数量、地域、硬件和网络条件。TPS 应注明是转账还是包含身份与托管逻辑的订单。

测试矩阵 Test Matrix

工作负载覆盖简单付款、并发预算预留、批量微支付和争议退款。故障覆盖节点离线、网络分区、RPC 延迟、代付余额不足、服务重复响应和资产冻结。持续负载后检查状态增长、磁盘恢复时间及历史查询成本。

验收门槛 Acceptance Gates

资金守恒、幂等结算、预算不超支和撤权后拒绝新调用是必须满足的不变量；任何反例阻止扩大部署。性能数值门槛由试点 SLA 倒推，在测试前登记，避免测试后挑选最有利结果。跨链与银行结算单独验收。

发布证据 Evidence Package

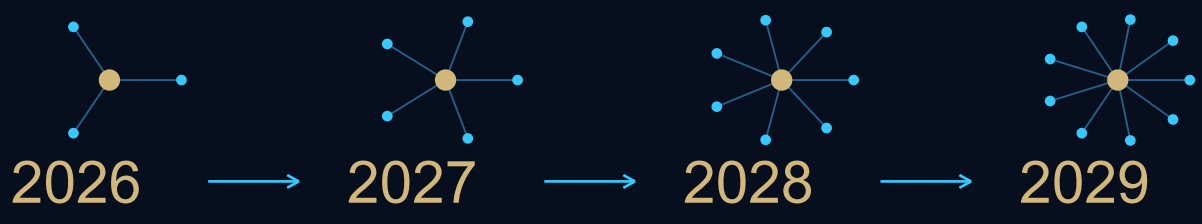
每个候选版本公开测试代码、配置、版本哈希、结果分布与已知限制。安全审计、业务验收和合规审批形成独立记录。只有存在相应证据，才将功能状态从 Proposed 更新为 Tested 或 Production。

23

2026 至 2029 路线图

2026–2029 Roadmap

路线图以阶段验收推动，年份为规划窗口，不构成交付保证。资金、人员、安全审查和监管变化可能导致范围调整或延期。



协议与原型	测试网与试点	条件式主网	生态与互操作
闭环与安全测试	审计与 L1 决策	技术与法律门槛	经审查后拓展

规划窗口 · 通过验收后推进

2026 协议与原型 Protocol & Prototype

完成身份、授权、订单和托管规范，运行单链原型与本地模拟器。退出条件：八阶段交易闭环可演示，重复扣款与并发超支测试通过，威胁模型形成可复查记录。

2027 公共测试与试点 Testnet & Pilots

发布 SDK 预览、测试网及有限企业试点，引入独立节点和安全审计。退出条件：严重问题关闭、故障恢复演练通过，并依据实测结果决定是否推进独立 L1。

2028 条件式主网 Mainnet Readiness

在技术、经济与法律门槛同时满足后，评估有限主网和受控服务接入。2029 扩展开放生态、跨网络适配与治理；每个新资产或地区独立评审，不以完成某一年份自动解锁下一阶段。

24

治理与升级机制

Governance & Upgrades

治理用于改变未来规则，必须受到安全边界、透明程序和参与者退出权的约束。代币投票不替代运营主体的法律责任。

分阶段治理 Phased Governance

原型期采用具名维护者和透明多签；测试网设技术评审组与运营者讨论；具备参与基础后再评估链上投票。披露多签成员职责、关联关系和替换流程，避免用“社区治理”掩盖少数管理员控制。

提案生命周期 Proposal Lifecycle

提案先公开问题、变更内容、风险和测试证据，再进入讨论、技术审查、投票、延时执行与复盘。资金参数、权限与共识变更使用不同审批门槛。最低参与度、通过阈值及委托规则须在治理规范中明确。

紧急权限 Emergency Authority

安全委员会可在限定范围暂停新增高风险操作，但不得任意转移用户资金或改写既有订单。每次使用记录触发条件、签名人、影响与到期时间；恢复需要审查和公开说明。紧急权力应定期续审而非永久扩张。

国库与利益冲突 Treasury & Conflicts

资助按里程碑支付并公开用途，关联方披露关系且回避相关决策。治理参与不能保证代币价值或资金收益。主网升级提前发布兼容计划和退出窗口；无法达成共识时说明潜在分叉及资产识别风险。

25

合规框架与责任边界

Compliance Framework & Accountability

合规以实际业务、运营主体和服务地区为基础。本章是产品设计框架，不是某一司法辖区的法律结论或牌照声明。

主体与活动映射 Entity & Activity Mapping

发布前列明协议维护、钱包运营、托管、资产兑换、付款和客户服务由谁承担。是否触发许可取决于实际控制、资金流和服务内容，不能仅依据“非托管”“DAO”或“技术平台”等名称判断。目标市场未确定前不宣称全球可运营。

客户与交易控制 Customer & Transaction Controls

对适用主体建立风险分级、客户及企业核验、制裁筛查、交易监测与异常报告程序。FATF 对虚拟资产的框架包含信息传递等要求 [6]，具体义务取决于当地实施；必要个人信息通过受保护渠道传输，不公开写入区块链。

代币与稳定币 Token & Stablecoins

代币发行和推广需要独立分类审查。欧盟 MiCA 对适用加密资产与服务设有规则，其他金融工具可能适用不同制度 [7]。白皮书不等于获批文件；稳定币选择须核验发行人、赎回、冻结能力及当地可提供范围。

上线清单 Launch Review

每个地区形成法律意见、允许客户范围、数据流评估、投诉退款机制及服务合同。受限制地区关闭相关业务入口；链上开放访问与商业运营义务分别评估。未确定运营实体、司法辖区和资质前，仅开展不涉及真实客户资金的验证。

26

风险披露

Risk Disclosures

参与测试、运行节点或使用未来服务均可能产生损失。以下风险不能通过协议设计完全消除，应在产品上线时结合实际架构持续更新。

技术与资金风险 Technical & Funds Risk

合约漏洞、权限错误、密钥泄露、共识攻击和基础设施故障可能造成资产损失或长时间中断。稳定币可能脱锚、冻结或无法赎回；跨链桥与外部支付服务失败会引入额外损失。多签、审计与保险均不应被描述为绝对保障。

智能体与业务风险 Agent & Business Risk

模型可能误解任务、接受提示注入或选错供应商。交付摘要无法证明结果质量，信誉可能被操纵。实际采购合同还可能发生退款、税务和履约争议；自动执行不会消除所有者或运营者责任。

代币与治理风险 Token & Governance Risk

AGT 若实施，可能出现价格剧烈波动、流动性缺失、持仓集中、治理俘获和奖励不可持续。质押可能被罚没，退出可能受时间限制。没有保本、回购、上市、收益或价值增长承诺。代币计划也可能调整或取消。

监管与交付风险 Regulatory & Delivery Risk

法律分类、许可和数据要求可能改变可提供的服务范围。团队资源不足、技术选择失误或需求不成立，均可能导致路线图延期或项目停止。本文不构成购买代币、投资或使用高风险服务的邀请；真实部署需另行发布正式条款。

27

结论与下一版重点

Conclusion & Next Iteration

AFT AgentChain 的第一阶段目标，是证明一个受约束、可追踪、可恢复的智能体交易闭环。协议可信度应来自可以检查的实现与证据。

第一版结论 V1 Conclusion

五层架构与 AIP 提供了共同语言：身份绑定控制者，钱包限制权限，执行层输出证据，支付层管理资金条件，L1 确认确定性状态。链下模型与链上规则各自承担适合的职责，企业可以据此构建可控自动化。

下一版技术交付 Technical Deliverables

V1.2 应细化 AIP 字段类型、消息签名、状态转换表与错误码；建立托管和授权参考实现；提供完整订单测试向量、威胁模型和基准测试方案。随后再发布网络选型决策、费用参数及节点运维规范。

下一版业务决策 Business Decisions

确定实际运营主体、目标司法辖区、试点供应商和验收标准；明确结算资产与责任边界。对本版融资估值、代币分配及资金预算进行独立评审，形成正式交易文件。融资目标不构成既有客户、收入或技术能力的证明。

共同评审 Review Priorities

产品评审关注场景是否值得自动化；技术评审关注状态、权限与资金不变量；安全评审关注攻击面与恢复能力；法律评审关注责任和地区准入。四项评审的结果共同决定是否进入下一阶段。

AFT AgentChain — AI × Blockchain × Payment × Protocol

28

参考资料与标准

References & Standards

引用仅用于说明已有标准与监管框架；本白皮书中的系统架构、命名、接口和路线图属于拟议设计。

[1] W3C DID Core

Decentralized Identifiers v1.0，身份数据模型与控制机制。
https://www.w3.org/TR/did-core/

[2] W3C Verifiable Credentials

Verifiable Credentials Data Model v2.0，凭证数据模型。
https://www.w3.org/TR/vc-data-model-2.0/

[3] ERC-4337

Account Abstraction Using Alt Mempool，账户抽象参考。
https://eips.ethereum.org/EIPS/eip-4337

[4] EIP-712

Typed structured data hashing and signing，结构化签名。
https://eips.ethereum.org/EIPS/eip-712

[5] CometBFT Consensus

Byzantine Consensus Algorithm，v0.38 共识规范。
https://docs.cometbft.com/v0.38/spec/consensus/consensus

[6] FATF Virtual Assets

虚拟资产及相关服务提供者风险框架与信息传递要求。
https://www.fatf-gafi.org/en/topics/virtual-assets.html

[7] ESMA MiCA

Markets in Crypto-Assets Regulation，欧盟监管框架。
https://www.esma.europa.eu/publications-and-data/interactive-single-rulebook/mica

[8] NIST AI RMF

AI Risk Management Framework，AI 风险管理参考。
https://www.nist.gov/itl/ai-risk-management-framework