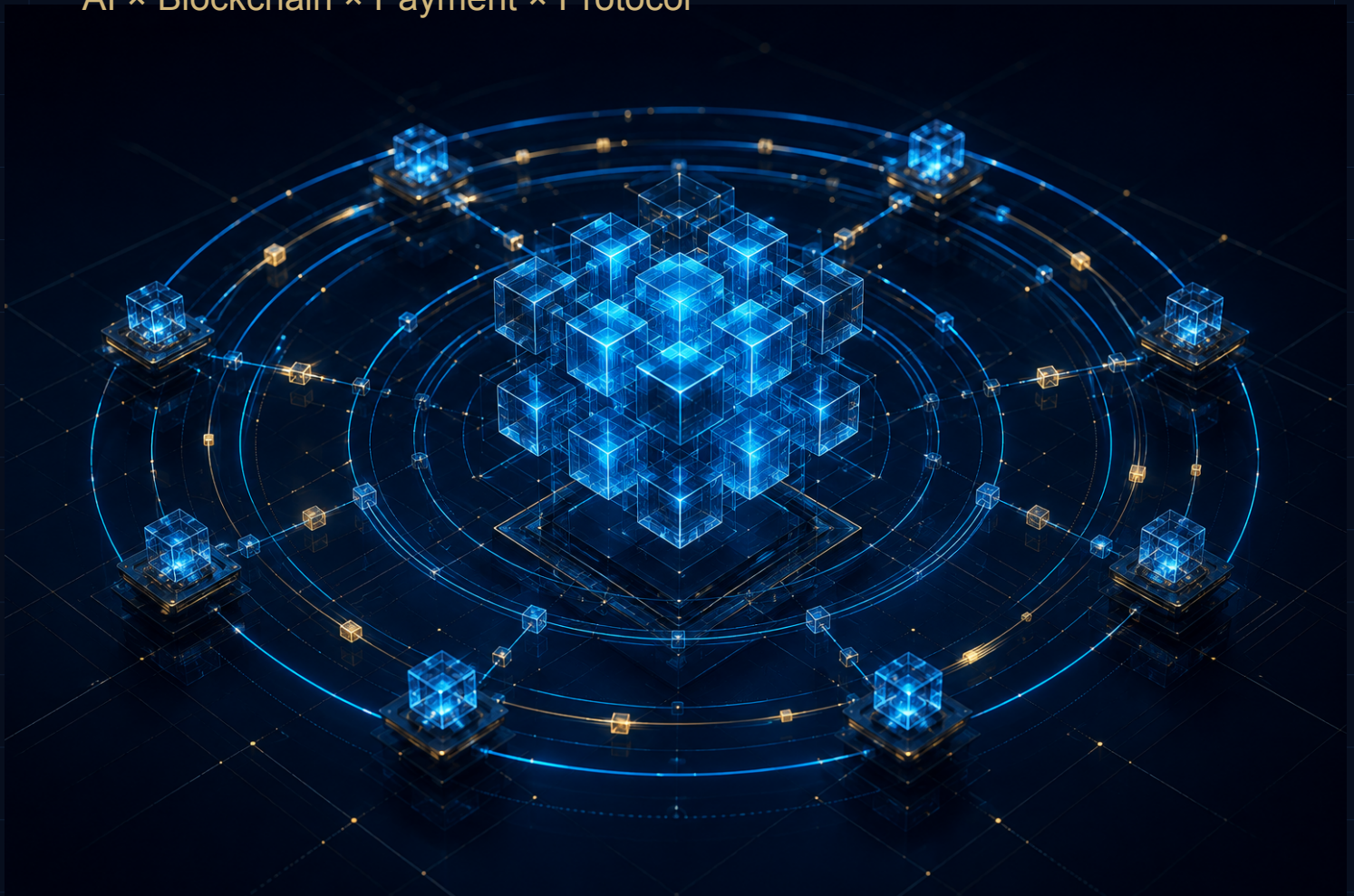


AFT AgentChain

WHITEPAPER V1.2

AI-Native Blockchain Infrastructure
for Autonomous Agents

AI × Blockchain × Payment × Protocol



ENGLISH EDITION / PROTOCOL & FINANCING DESIGN

V1.2

Reading Guide & Contents

AFT AGENTCHAIN / PROTOCOL & FINANCING DESIGN

AFT AgentChain Whitepaper V1.2 describes a proposed identity, authorization, execution and settlement network for autonomous agents. This document supports product, technical and ecosystem discussions.

Document Status

This edition presents a target architecture, implementation path and token financing proposal. It does not represent deployed mainnet, issued tokens, regulatory authorization or completed audit. Valuation, price, allocations and vesting are proposed terms. Implementation requires code, test reports, legal assessment and signed transaction documents.

Contents

03 Executive Summary | 04 Background | 05 Vision
06 Architecture | 07 Identity | 08 Wallet | 09 Execution
10 Payment & Settlement | 11 AIP Workflow | 12 AIP States
13 Agent Economy | 14 Consensus | 15 Smart Contracts
16 Security | 17 Privacy | 18 AGT Utility
19 Token Financing & Allocation | 20 Proceeds & Closing
21 Nodes | 22 SDK & API | 23 Enterprise Applications
24 Validation | 25 Roadmap | 26 Governance
27 Compliance | 28 Risks | 29 Conclusion | 30 References

Terminology & Sources

An Agent is software acting under the authority of a person or enterprise. The Owner retains control and responsibility. AIP is the proposed name of this project's Agent Interaction Protocol; it does not imply industry adoption. References [1]–[8] identify public sources on the final page. These sources support foundational concepts and do not endorse this project.

Executive Summary

AFT AGENTCHAIN / PROTOCOL & FINANCING DESIGN

AFT AgentChain proposes infrastructure that enables AI agents to participate in economic activity within explicit authorization limits, with verifiable and attributable records for each transaction.

Problem & Proposal

AI can plan purchases, call tools and coordinate services. Cross-organization execution, however, still lacks consistent identity binding, budget controls, payment conditions and dispute evidence. AFT AgentChain proposes a five-layer architecture connecting agent discovery, wallet permissions, off-chain execution and on-chain settlement into one transaction lifecycle.

Minimum Viable Loop

The first validation scenario is an enterprise agent purchasing an API service or compute capacity: discover a provider, verify its identity, obtain a signed quote, reserve a budget, execute an order, accept the result and settle payment. The MVP prioritizes one chain, one test asset and a limited provider set. It must first demonstrate prevention of duplicate charges, effective revocation and refunds after eligible failures.

Infrastructure Positioning

AI models do not participate in block consensus. Validators process only deterministic state transitions. An independent Layer 1 is a candidate long-term path; the initial protocol can be validated on an existing compatible test network. Measured performance, fees, autonomy requirements and operating costs should determine whether a dedicated network is justified.

Value & Boundaries

The proposed value is lower integration overhead, better auditability and tighter limits on automated financial risk. AGT is discussed only through potential protocol uses, without promises of returns, price performance or liquidity. Mainnet deployment, stablecoin support, banking connections and commercial services each require separate technical and compliance readiness decisions.

Agent Economy Background

AFT AGENTCHAIN / PROTOCOL & FINANCING DESIGN

As software moves from answering questions to using tools, economic workflows can expand from manual clicks to service orders that machines can read, authorize and verify.



Concept illustration - See text for protocol mechanisms

- 01 Autonomous Agents
- 02 Services & Compute
- 03 Value Exchange

From Tools to Transactions

Buying data, calling paid APIs, renting GPUs and renewing subscriptions create real costs and external obligations. A model output does not establish payment authority, quote validity or successful delivery. Verifiable identity, structured signatures and programmable accounts provide useful components [1][2][3][4], but a shared business model for transactions is still needed.

Four Frictions

Identity: control of an address does not prove corporate credentials or service capability. Authorization: a persistent private key often grants excessive authority. Execution: service responses, order states and payment records are fragmented. Settlement: on-chain success, merchant receipt and bank credit are different events, and failure compensation often requires manual work.

Why a Shared Protocol

Common order identifiers, quote formats, revocation mechanisms and evidence digests can reduce repeated integration work across providers. Only state that genuinely requires shared verification belongs on-chain. Discovery, inference and sensitive contracts remain off-chain to control costs and reduce public data exposure.

Demand Validation

This edition does not rely on unverified market-size estimates or transaction-growth forecasts. Early pilots should measure manual processing time per order, recovery success, reconciliation differences and provider onboarding cost. Where a conventional database and payment API are sufficient, a simpler deployment should remain an option.

Vision & Design Principles

AFT AGENTCHAIN / PROTOCOL & FINANCING DESIGN

AI-Native Blockchain Infrastructure for Autonomous Agents.

Vision

Establish shared interfaces for trusted identity, bounded authority and verifiable settlement in the agent economy. AI-native means that accounts, messages and fee models can express agent tasks. It does not mean replacing consensus or legally accountable parties with an AI model.

Human Control & Revocation

Individuals or enterprises retain ultimate control over funds. Agents receive short-lived, narrowly scoped execution capabilities. Owners can pause sessions, rotate keys and stop new orders. Revocation cannot retroactively reverse a transaction that has already reached final settlement; this timing boundary must be explicit.

Determinism & Interoperability

Security-critical checks use explicit rules for assets, recipients, limits, expiry and nonces. Identity, credentials and signatures should reference open standards where practical [1][2][4]. External adapters remain separate from the core protocol so applications can migrate between wallets, models and settlement networks.

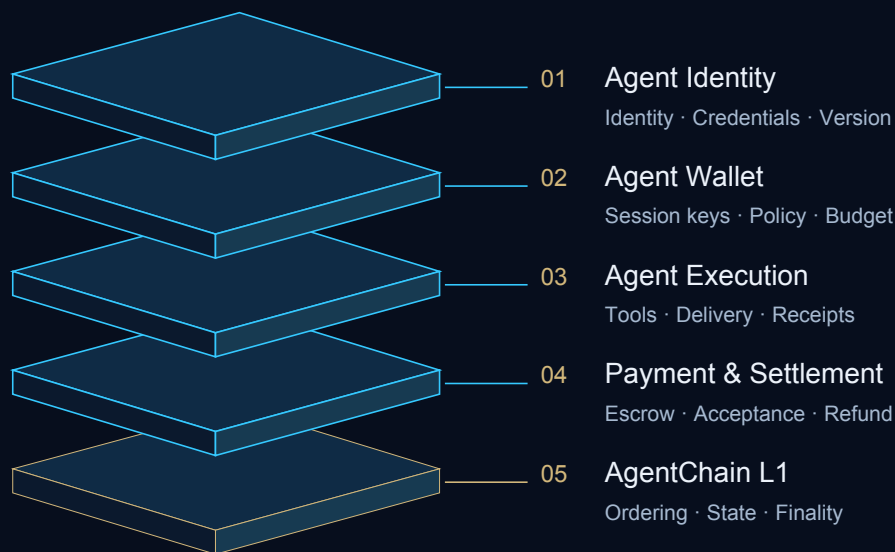
Progressive Delivery

Complete protocol specifications and failure testing before expanding into a public testnet and independent validators. Each extension follows its incremental risk: single-chain before cross-chain, selected providers before an open marketplace, and human dispute resolution before automated adjudication. The initial scope excludes algorithmic stablecoins, yield products and unrestricted autonomous trading.

Five-Layer Architecture

AFT AGENTCHAIN / PROTOCOL & FINANCING DESIGN

The architecture separates business intelligence from financial control. Each layer exposes a verifiable interface, and the next layer accepts only inputs that satisfy protocol rules.



Distinct responsibilities · One transaction lifecycle

Layer Responsibilities

Identity establishes who is acting. Wallet authorization determines what is permitted. Execution records what was done. Payment defines when value is released. L1 confirms which state transitions are final. Applications must not bypass authorization and allow models to operate root keys directly.

On-Chain & Off-Chain

On-chain state contains identity control, authorization digests, escrow balances and settlement events. Model inference, discovery indexes, original deliverables and protected credentials stay off-chain. A digest can establish the integrity of particular data; it cannot establish that the content is true.

Deployment Path

The prototype deploys core contracts to a compatible test chain. A later independent L1 would add its own consensus, fees and node governance. Moving between these stages requires an explicit migration plan; historical state is not inherited automatically.

Agent Identity Layer

AFT AGENTCHAIN / PROTOCOL & FINANCING DESIGN

Agent identity combines owner control, rotatable keys and verifiable claims. An on-chain identity is a technical identifier and does not automatically confer legal personhood.

Identity Model

The proposed AgentRecord contains agentId, owner, controllerKey, serviceURI, capabilityHash, version and status. Registration verifies the controller's signature; updates increment the version and emit an event. A service URI is only a discovery entry point. Clients must still validate domains, certificates and signatures to prevent malicious redirection.

Verifiable Credentials

Trusted issuers may attest to corporate qualifications, service scope or certification. Verification checks signatures, issuer trust policy, validity and revocation status. DID and VC specifications provide interoperability references [1][2]. Interfaces distinguish self-declared claims from independently verified credentials.

Rotation & Recovery

Owner changes require multisignature authorization or a controlled recovery procedure with delay and notification. Recovery revokes old sessions and triggers revalidation of outstanding orders. Registration states include Active, Suspended and Revoked. Historical versions remain identifiable so old quotes are not mistaken for current authorization.

Reputation Is Not Identity

Reputation uses separate measures such as settled orders, dispute outcomes and availability, rather than an opaque universal credit score. On-chain records alone cannot eliminate affiliated-address wash activity or false credentials. High-risk providers still require enterprise due diligence and human review.

Agent Wallet & Authorization

AFT AGENTCHAIN / PROTOCOL & FINANCING DESIGN

Agents execute tasks with session permissions while owners retain root control. Wallet or authorization contracts enforce budgets; prompt instructions alone are not a financial safeguard.

Policy Scope

A proposed Policy binds chainId, wallet, agentKey, asset, recipient, methodSelector, perTxLimit, periodLimit, validUntil and policyNonce. A mismatch causes rejection. Budgets are recorded in each asset's smallest unit. Fiat-denominated limits additionally require a defined price source, update frequency and conservative error allowance.

Budget Reservation

Available budget equals the period limit minus spent funds minus reserved funds. A valid order atomically reserves budget. Settlement converts reserved funds into spent funds; refunds or eligible expiry release the reservation. Sessions share a parent budget so concurrent agents cannot all pass a balance check and collectively overspend.

Account Abstraction

ERC-4337 provides a reference for modular signature validation, batching and Paymaster-based fee sponsorship [3]. An implementation must specify its EntryPoint version, chain adapters and simulation rules. Paying fees with a stablecoin does not eliminate the need for an underlying fee asset or sponsor liquidity.

Revocation & Emergency Pause

Each execution rechecks the policy version and on-chain state. A race remains until the revocation transaction is final, and the client must disclose it. An emergency pause blocks new outflows. Existing escrowed orders follow contractual refund or dispute rules; recovery must not silently change recipients.

Agent Execution Layer

AFT AGENTCHAIN / PROTOCOL & FINANCING DESIGN

The execution layer turns an open-ended task into a bounded order. Models propose actions; independent policy and signing components decide whether those actions may proceed.

Execution Pipeline

A task is parsed into a budget and service requirements. The agent selects a verified provider, obtains a quote and creates an order. A policy engine checks permitted tools and data access. The signing service signs only validated structured messages. Model context must not contain root private keys or reusable payment credentials.

Deterministic Validation

Validators neither run language models nor replay external APIs. Execution evidence may include request digests, service versions, time ranges, metering records and delivery digests. A previously agreed verifier or human reviewer assesses quality. On-chain logic enforces only explicitly encoded payment conditions.

Isolation & Recovery

External tools run in restricted environments with controls on network egress, file access, CPU use and timeout. Every task has an idempotency key and bounded retries. After an API timeout, the client queries the existing order before retrying. Failure may release unspent budget but cannot guarantee reversal of external actions that already occurred.

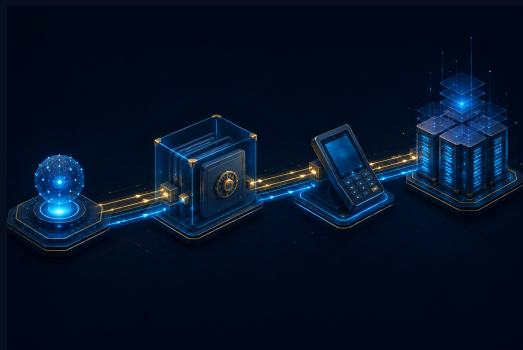
Audit Evidence

A proposed Receipt binds orderId, requestHash, outputHash, metering, executorSignature and policyVersion. Original outputs are encrypted with defined retention periods; evidence digests accompany settlement records. Optional trusted execution environments or zero-knowledge proofs require separate disclosure of trust assumptions, coverage and cost. They are not prerequisites for V1.

Payment & Settlement

AFT AGENTCHAIN / PROTOCOL & FINANCING DESIGN

Payment transfers value. Settlement confirms the outcome under defined finality conditions. AgentChain tracks order acceptance, chain confirmation and external receipt separately.



Concept illustration - See text for protocol mechanisms

- 01 Bounded Authority
- 02 Conditional Payment
- 03 Final Settlement

Funds Flow

The MVP uses a whitelisted test asset. A payer deposits funds into order escrow; acceptance releases funds to the provider, while eligible failure or expiry triggers a refund. Authorization is not payment, and transaction submission is not final settlement. A unique orderId links the order and escrow record.

Fees & Stablecoins

Quotes may separate service charges, network fees and adapter fees. A sponsor initially pays underlying Gas and recovers an allowed asset under signed terms, including maximum fees and expiry. Each stablecoin requires assessment of issuance, redemption, freezing and chain-specific risks. A token name alone does not establish support.

Micropayments

High-frequency, low-value services should initially aggregate metering and settle in batches, with caps on outstanding exposure and settlement intervals. Payment channels are a later extension requiring offline dispute handling, challenge periods and collateral management. Any real-time status must distinguish authorization, provisional credit and final confirmation.

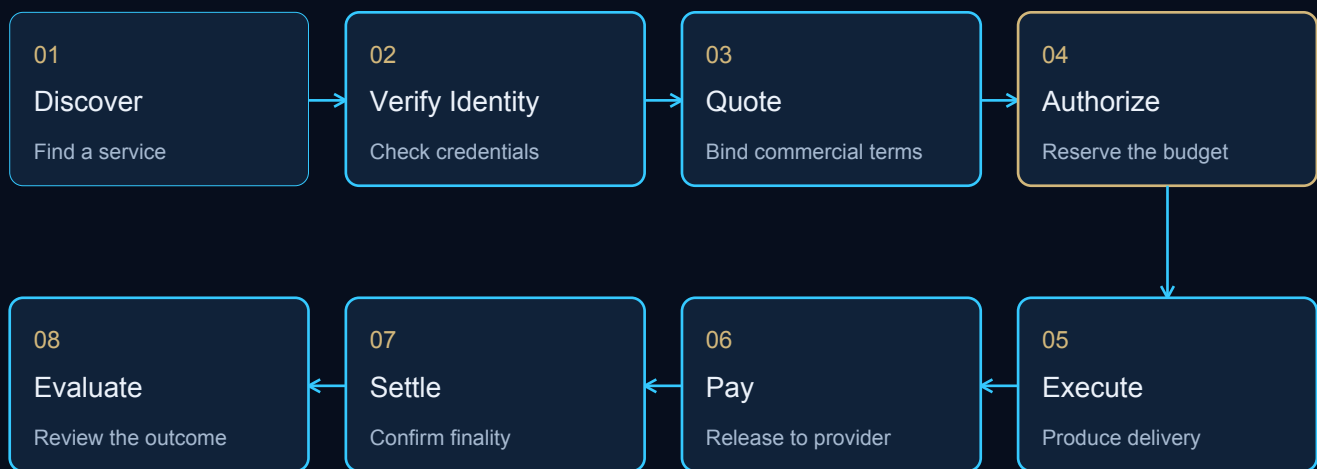
Cross-Chain & Fiat Settlement

Bridges, banks and acquirers are separate trust boundaries. Cross-network flows require confirmation policies, liquidity, failure compensation and escalation. Atomic cross-chain execution or immediate bank credit is not promised. Appropriately qualified service entities handle fiat connections; the protocol does not automatically obtain a payment license.

AIP Interaction Workflow

AFT AGENTCHAIN / PROTOCOL & FINANCING DESIGN

AIP structures an agent transaction into eight stages. Each stage produces evidence bound to an order. Exceptions enter explicit rejection, timeout or dispute paths.



Fund escrow after authorization. Release after acceptance. Refund or dispute on failure.

Before Execution

Discovery returns service descriptions and protocol versions. Identity verification checks control and credentials. Quotes bind assets, quantities, fees, expiry, acceptance conditions and dispute terms. Authorization validates policy and reserves budget. Discovery rankings are not proof of trustworthiness.

Execution Through Settlement

Escrow funding may follow authorization and precede execution. After acceptance, payment releases value to the provider; settlement confirms finality, then evaluation becomes available. In the diagram, Pay means the release instruction to the provider, not the earlier escrow deposit. This distinction prevents an implicit assumption of unsecured delivery.

Exception Paths

Invalid identity or an expired quote causes rejection. Execution timeout leads to a contractual refund or dispute. If submission status is uncertain, query before retrying to prevent duplicate payment. Reviews follow settlement or adjudication of a real order and cannot reverse completed transfers.

AIP Messages & State Machine

AFT AGENTCHAIN / PROTOCOL & FINANCING DESIGN

Signed messages must bind transaction context. Strict state transitions and idempotency prevent network retries from becoming new economic actions.

Message Envelope

Proposed common fields are protocolVersion, messageType, orderId, senderId, receiverId, chainId, verifyingContract, nonce, expiresAt, payloadHash and signature. EIP-712 can inform structured signing [4]. It does not automatically provide replay protection: the contract must check the nonce, domain and expiry.

States & Permissions

An order progresses from Quoted to Authorized, then Funded and Executing. Successful acceptance leads to Accepted, PaymentSubmitted and finally Settled. The payer may reject an expired quote; the executor submits evidence; the designated verifier accepts or challenges under the contract; escrow applies the resulting allocation.

Failure Outcomes

An eligible unstarted order may become Expired; an unfunded authorization may be Cancelled. A funded dispute enters Disputed and, after adjudication, becomes Refunded, Settled or Closed following an agreed split. Disputed does not mean refunded. Each terminal outcome applies its fund allocation once only.

Invariants

An order's asset, payer wallet, recipient and quote digest cannot be replaced after creation. Escrow principal equals unallocated principal plus released principal plus refunded principal. Fees are tracked separately, and total debits must remain within the signed cap. Event consumers deduplicate, replay and reconcile records. Webhooks notify clients; they do not replace on-chain facts.

Agent-to-Agent Economy

AFT AGENTCHAIN / PROTOCOL & FINANCING DESIGN

The ecosystem comprises demand agents, service agents, developers, validators and external service institutions. Every participant has defined interfaces and independent responsibilities.



Composable Services

A procurement agent may buy inputs from a data agent and submit work to a compute service. Parent orders allocate budget and deadlines to child orders. Delegation cannot expand parent authority. Providers publish billing units, versions and acceptance rules so services can be combined under consistent conditions.

Incentives & Fees

Providers earn revenue for delivery. Validators receive fees or proposed security subsidies under network rules. Developers may charge for tools and enterprise support. Protocol charges, commercial service fees and token incentives are disclosed separately, so subsidized activity is not presented as organic demand.

Reputation & Market Quality

Reviews identify verified orders, dispute rates and sample sizes, with a provider appeal process. Registration costs, credentials and related-party analysis may reduce Sybil activity but cannot eliminate it. The ecosystem diagram represents intended roles, not confirmed partners or customers.

Consensus & Network

AFT AGENTCHAIN / PROTOCOL & FINANCING DESIGN

The candidate independent network combines stake-weighted Byzantine fault-tolerant consensus with deterministic execution. Final selection requires public review, prototype benchmarks and operational testing.

Candidate Stack

A CometBFT-style consensus engine with an EVM-compatible execution layer is a candidate for reusing wallet and contract tooling. Consensus orders and confirms transactions; execution changes state. Fee calculation, state roots and upgrade boundaries must be consistent across both. Adopting a component does not automatically inherit all of its security properties.

Security Assumptions

Typical BFT designs confirm blocks with a commit certificate representing strictly more than two-thirds of voting power. Safety reasoning assumes less than one-third Byzantine voting power; liveness also depends on sufficiently timely network communication and other protocol conditions [5]. A partition can halt progress. Deterministic finality does not imply continuous availability under every failure.

Network Topology

Validators connect to the peer-to-peer network through sentry nodes. Public RPC and indexing services scale separately. Archive nodes preserve history; light clients verify a trusted starting point and subsequent signed updates. Validator-set changes activate at explicit heights to avoid inconsistent interpretations by old and new sets.

Independent L1 Decision Gate

A dedicated L1 proceeds only if existing networks fail to meet validated requirements and the project can sustain security funding, operator diversity and upgrades. An initially controlled test set is not described as fully decentralized. V1 makes no commitment on TPS, finality in seconds or launch date.

Smart Contract Architecture

AFT AGENTCHAIN / PROTOCOL & FINANCING DESIGN

Core contracts have narrow responsibilities and explicit permissions. Financial paths begin with invariants, followed by implementation, fuzz testing and independent audit.

Core Modules

AgentRegistry manages identity versions; PolicyManager controls authorization and limits; OrderBook fixes quotes and order state; EscrowVault holds and distributes funds; ReceiptRegistry records evidence digests; FeeManager manages fee parameters. These are proposed module names, not published contract addresses.

Execution Safety & Assets

Validate authority and state first, update accounting next, and make external transfers last, with reentrancy protection. Token transfers must check actual received amounts and return values. The MVP excludes rebasing, fee-on-transfer and other non-standard assets. A balance discrepancy pauses new orders and triggers manual investigation.

Upgrades & Compatibility

Stateless adapters can be replaced through versioned releases. Whether the financial core is upgradeable requires separate review. Proxy-based designs require multisignature administrators, execution delays and public implementation addresses. Existing orders retain original rules or migrate with explicit counterparty consent. Governance cannot unilaterally rewrite agreed payment conditions.

Verification Requirements

Tests cover duplicate settlement, reentrancy, unauthorized access, precision errors, concurrent reservations and timeout boundaries. Key invariants are conservation of funds, unique terminal outcomes, non-negative available budgets and rejection of new calls after effective revocation. Audit findings require remediation and retesting. An audit is not a guarantee of zero vulnerabilities.

Security Model & Defense

AFT AGENTCHAIN / PROTOCOL & FINANCING DESIGN

The most consequential risks arise where models, tools, keys and funds connect. Assume that external pages, service responses and agent messages may contain malicious instructions.



Concept illustration - See text for protocol mechanisms

- 01 Permission Boundaries
- 02 Validation Network
- 03 Layered Defense

Prompt Injection & Tool Abuse

External content is data, not authority to change payment policies or allowlists. Structured tool-argument checks prevent a service response from directly introducing a new recipient. High-value orders, first-time providers and abnormal activity require human approval bound to the specific order digest.

Keys & Supply Chain

Root keys are held in hardware-backed or controlled signing systems. Session keys expire quickly and have limited scope. Releases use locked dependencies, build verification, signed artifacts and least privilege. Production, testing and development environments are separated; test credentials cannot authorize production funds.

Incident Response

Monitor unusual debits, inconsistent RPC responses, signature failures, double-signing evidence and outages. Response proceeds through isolation, suspension of new exposure, log preservation, notification, remediation and controlled recovery. Final transactions that cannot be reversed require contractual remedies; technical recovery is not promised.

Release Gates

Before launch, complete threat modeling, permission review, financial-invariant tests, penetration testing and key-recovery drills. A public testnet should offer vulnerability reporting and a bounty process. Critical and high-severity issues must be resolved before mainnet. NIST AI RMF can inform model-risk management [8], but its use is not presented as certification.

Privacy & Data Governance

AFT AGENTCHAIN / PROTOCOL & FINANCING DESIGN

Data minimization is the default. Verifiability does not require publishing customer identities, complete contracts, prompts or commercial deliverables.

Data Classification

The public layer contains only necessary identifiers, states and digests. The business layer encrypts contracts and acceptance evidence. The sensitive layer protects identity-verification material and customer information through strict access controls. Participants must identify who determines processing purposes, who processes data and who responds to rights requests.

Access & Retention

Tenant isolation, least privilege, short-lived access tokens and access logs control retrieval. Retention schedules reflect business needs and applicable law. Off-chain material is deleted at expiry unless a lawful basis supports continued retention. On-chain records cannot be deleted like ordinary database rows, so content must be restricted before publication.

Limits of Hashes

A plain hash of predictable personal data may be identifiable through enumeration and is not necessarily anonymous. Depending on the case, use random salts, controlled commitments or avoid publishing the relevant fields. Encryption does not hide all metadata: timing, values and address relationships can still reveal commercial activity.

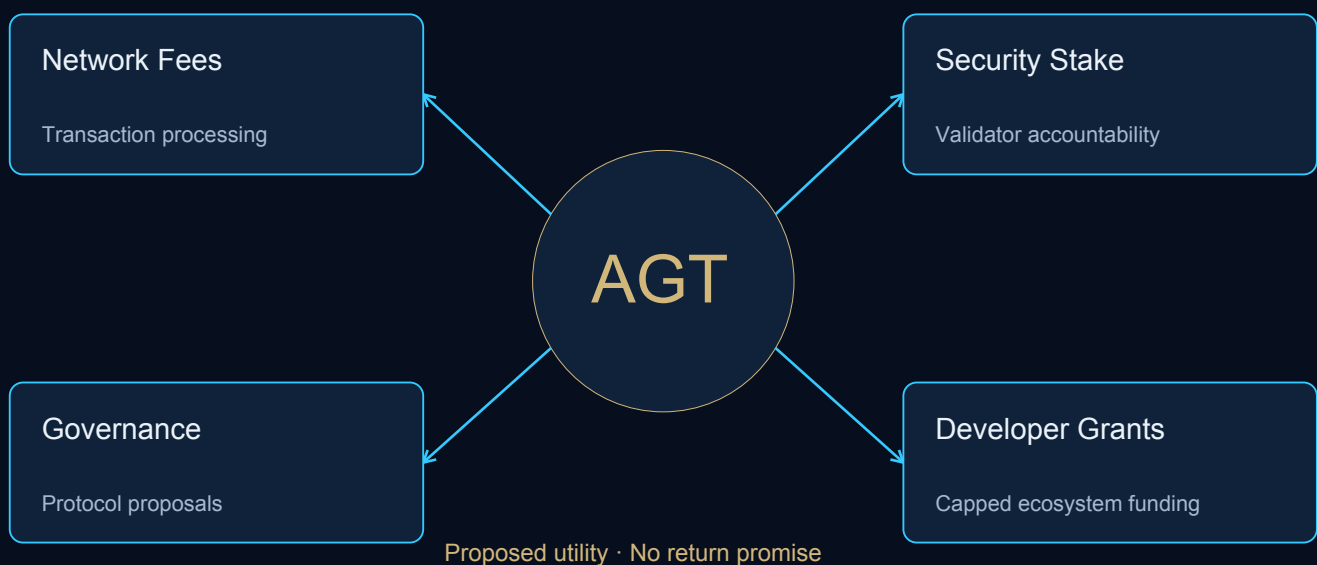
Selective Disclosure

VC can structure credential exchange [2], but the data model does not automatically provide zero-knowledge privacy. Specific proof systems require assessment of libraries, revocation and linkability. Cross-border data flows are mapped and reviewed before integration. Decentralization is not a basis for avoiding privacy obligations.

AGT Network Token Utility

AFT AGENTCHAIN / PROTOCOL & FINANCING DESIGN

AGT is the working name of a proposed native asset. V1.2 adds a financing design: a proposed supply of 1 billion tokens, a USD 10 million post-financing FDV and a USD 3 million funding target. These are proposed terms, not completed issuance or fundraising.



Proposed Utility

Candidate functions include network fees, validator security staking, governance proposals and capped developer grants. Providers may voluntarily accept AGT under protocol rules. Enterprise orders should support clearly specified settlement assets without requiring token ownership simply to use the service.

Fees & Security Funding

Users may pay allowed stablecoins through a sponsorship interface. Sponsors bear conversion, quote and inventory risks. This design does not mint beyond the 1 billion token cap. Validator subsidies come from the reserved network-incentive pool; actual network fees must support operations as that pool is consumed. Security funding cannot depend on rising token prices.

Economic Constraints

The next two pages specify proposed financing, allocation and release terms. Economic simulation and legal review remain prerequisites to deployment, together with treasury permissions, unbonding and slashing rules. AGT does not inherently confer equity, fixed income or reserve claims. Its sale and transaction arrangements require separate legal classification.

Token Financing & Allocation

AFT AGENTCHAIN / PROTOCOL & FINANCING DESIGN

The proposed round targets USD 3 million at a USD 10 million post-financing fully diluted token valuation (FDV). These are proposed terms, not an announcement of completed issuance or fundraising.

POST-FINANCING FDV

US\$10,000,000

FUNDING TARGET

US\$3,000,000

ROUND ALLOCATION

30%

Pricing Basis

Proposed fixed supply: 1,000,000,000 AGT. Uniform round price: US\$0.01 per AGT. Sale allocation: 300,000,000 AGT for US\$3,000,000 gross, before expenses. Math: US\$10m / 1bn = US\$0.01; US\$3m / US\$0.01 = 300m tokens. FDV is price times total supply, not circulating market capitalization or company equity valuation. The 30% allocation is not equity ownership.

Allocation	Share / Tokens	Proposed Release
Round investors	30% / 300m	0% at TGE; 6-month cliff; equal releases in months 7–30
Ecosystem & developers	25% / 250m	10% of pool at TGE; remainder equally in months 1–48
Validator incentives	20% / 200m	0% at TGE; earned over 48 months after production activation
Team	15% / 150m	0% at TGE; 12-month cliff; equal releases in months 13–48
Treasury	10% / 100m	10% of pool at TGE; remainder equally in months 1–36
TOTAL	100% / 1,000m	Allocated within a fixed cap; no additional minting

Release Rules

m means million tokens. TGE means token generation event; its timing is not fixed. Except for validator rewards, months run from TGE; releases occur at month-end. Investors unlock 12.5m per month with no cliff catch-up. Initial TGE unlock capacity is 35m (3.5% of supply): 25m ecosystem and 10m treasury. Unlocked is not necessarily circulating. Ecosystem grants require acceptance; monthly validator rewards are capped at 1/48 of their pool. Unused rewards remain reserved for separate approval.

Investor Terms

No additional discount, bonus tokens or undisclosed subscription rights are included. Supply or allocation changes require renewed disclosure and applicable contractual consent. Unvested tokens do not vote under the proposed token-governance model. A 30% allocation creates concentration and selling-pressure risks. No equity, dividend, capital protection, buyback or listing is promised.

Use of Proceeds & Closing

AFT AGENTCHAIN / PROTOCOL & FINANCING DESIGN

USD 3 million is the gross target at full subscription. The budget depends on actual receipts and uses an approximately 18-month planning horizon. It is not evidence of available cash or a mainnet delivery guarantee.

Use of Proceeds	Share / US\$	Deliverables & Controls
Protocol & product R&D	40% / 1,200,000	Identity, wallet, AIP, escrow and SDK prototypes
Audits & security	15% / 450,000	Independent review, remediation and recovery drills
Ecosystem & pilots	20% / 600,000	Integrations, enterprise pilots and accepted grants
Legal & compliance	10% / 300,000	Entity, contracts, market access and data review
Operations & finance	10% / 300,000	Cloud, node support, finance and administration
Contingency reserve	5% / 150,000	Exceptional spending with separate approval
TOTAL	100% / 3,000,000	Cash budgets are separate from token pools

Budget Controls

Excluding the US\$150,000 reserve leaves US\$2.85m deployable, or approximately US\$158,333 monthly over 18 months as a cost constraint. Fundraising and payment costs fall within relevant lines. A shortfall requires scope adjustment and disclosure. Proceeds use segregated issuer accounts or reviewed escrow, multisignature or dual approval, and quarterly use-of-funds reports. FDV is not spendable cash.

Milestone Spending

Authorize 30% of received funds for entity setup, specifications and prototypes; 40% after security review and a testnet demonstration; and 30% after pilot acceptance and financial review. These are internal spending gates, not investor payment installments or changes to vesting. Each stage remains subject to the budget above.

Subscription & Closing

The proposed subscription is limited to participants eligible under applicable rules. Before collection, establish the issuer, jurisdiction, legal classification, investor and source-of-funds checks, and signed contracts. Private-sale or utility-token labels do not automatically remove regulatory obligations [7]. Terms are USD-denominated; contracts specify accepted payment assets and conversion rules. There is no market-making or listing guarantee.

Uncompleted Offering

Proposed minimum close: US\$1.5m; cap: US\$3m; subscription window: 90 days after formal launch. Funds remain segregated until legal and closing conditions are met. If the minimum or conditions fail, proposed refunds occur within 30 days after the window, without yield. A partial close allocates tokens only for paid subscriptions at US\$0.01; unsold tokens remain locked. Contracts must set a TGE long-stop, extension consent and remedies for non-issuance. Segregation and refund arrangements must exist before collection.

Nodes & Validators

AFT AGENTCHAIN / PROTOCOL & FINANCING DESIGN

Node operations aim to keep verifiable state available while distributing failure and control risks across independent operators.

Node Roles

Validators vote and maintain current state. Full nodes independently verify blocks. Archive nodes preserve complete history. RPC and index nodes serve application queries. Sentry nodes isolate validators from direct network exposure. An RPC provider does not become a consensus validator merely by offering an endpoint.

Admission & Exit

Early testnets may invite independent operators and publish admission criteria and affiliations. A candidate mainnet mechanism selects validators under effective-stake and governance rules while monitoring concentration by cloud provider, geography and controlling entity. Exit periods must cover evidence submission and penalty processing; exact values require testing.

Rewards & Penalties

Provable double-signing warrants strict penalties, while short outages may justify lighter suspension or reward deductions. Evidence formats, appeal boundaries and parameter changes must be explicit. Penalties should discourage attacks and negligence without treating every ordinary network failure as malicious conduct. Delegators must understand potential losses.

Operations

Use remote signing, key backups, monitoring and upgrade drills. The same validator key must not sign concurrently from multiple active nodes. Publish availability, missed votes, software versions and incident records. Hardware guidance and capacity claims must accompany benchmarks; generic specifications alone do not establish mainnet readiness.

Developer SDK & API

AFT AGENTCHAIN / PROTOCOL & FINANCING DESIGN

The developer workflow centers on creating a bounded task and observing a verifiable result. The following interfaces are proposals; no production endpoint or released SDK is claimed.

SDK Surface

Initial candidates are TypeScript and Python libraries for identity resolution, credential and quote verification, policy simulation, order submission, receipt queries and event subscriptions. Simulate before submit is the default. Applications inject a signer; the SDK does not store root keys. Errors include machine-readable codes and retryability information.

Illustrative API

GET /v1/agents/{id} — retrieve identity version
POST /v1/quotes/request — request a signed quote
POST /v1/policies/simulate — check authority and budget
POST /v1/orders — create an order and return orderId
GET /v1/orders/{id} — retrieve business and settlement states
POST /v1/orders/{id}/challenge — submit dispute evidence

Protocol Conventions

Write requests carry an Idempotency-Key. Amounts use decimal strings in the asset's smallest unit; timestamps follow a consistent UTC convention. SDKs check chainId, asset address, expiry and signing domain. Events carry eventId, blockHeight, txHash and confirmation state. Indexing delay must not be interpreted as proof that an order does not exist.

Tooling & Compatibility

Provide a local simulator, test assets, sample merchants, fault injection and an OpenAPI definition. Major versions identify breaking changes, and old interfaces receive migration windows. Repositories, licenses, package names and reference implementations are listed when actually released; V1 does not invent download links.

Enterprise Applications

AFT AGENTCHAIN / PROTOCOL & FINANCING DESIGN

Initial use cases prioritize bounded spending, measurable delivery and clear dispute conditions. The following are illustrative designs, not claims of customers or operating revenue.

Compute Procurement

An enterprise may authorize an agent to procure capacity for 30 days with an illustrative maximum budget equivalent to USD 2,000. Providers quote specifications, unit prices and availability. The agent selects within policy and reserves funds. Accepted running time is settled in stages; undelivered capacity is refunded. Both parties agree on technical and billing evidence.

Paid Data & APIs

A data service charges for successful responses or valid outputs, with explicit rules for caching, duplicate requests and errors. High-frequency calls use aggregated metering and exposure alerts. Finance reconciles orders, invoices and on-chain receipts. Data-quality questions that cannot be reliably automated retain a human dispute process.

Enterprise Operations

Subscription agents may renew approved services; procurement agents may allocate departmental budgets. Later cross-border payments use reviewed providers and verify counterparty eligibility, purpose and external receipt. Models do not independently select unknown money-transfer channels.

Commercial Sustainability

Candidate revenue includes enterprise subscriptions, support and transparent transaction-processing fees. Public protocol components and commercial hosting are priced separately, and customers can replace providers. Pilots measure procurement time, reconciliation differences, recovery time and genuine repeat use to justify continued investment.

Performance & Validation

AFT AGENTCHAIN / PROTOCOL & FINANCING DESIGN

V1 does not present laboratory peaks as production commitments. Evaluation must cover security, state growth, network failures and end-to-end business completion.

Metrics

Measure authorization-check latency, transaction inclusion, chain finality, external receipt and total order duration separately. Report p50, p95 and p99 values and error rates, with transaction complexity, node count, geography, hardware and network conditions. TPS must identify whether the workload is simple transfers or orders with identity and escrow logic.

Test Matrix

Workloads include simple payments, concurrent budget reservations, batched micropayments and dispute refunds. Failures include node outages, partitions, RPC lag, insufficient sponsor balances, duplicate service responses and asset freezing. Sustained-load tests also examine state growth, disk recovery and historical query cost.

Acceptance Gates

Conservation of funds, idempotent settlement, budget limits and rejection of new calls after effective revocation are mandatory invariants. A counterexample blocks expansion. Numeric performance thresholds are derived from pilot SLAs and registered before testing, rather than selected afterward. Cross-chain and bank settlement receive separate acceptance tests.

Evidence Package

For each candidate release, publish test code, configuration, version hashes, result distributions and known limitations. Security audit, business acceptance and compliance review are separate records. A capability moves from Proposed to Tested or Production only when the corresponding evidence exists.

2026–2029 Roadmap

AFT AGENTCHAIN / PROTOCOL & FINANCING DESIGN

The roadmap advances through acceptance gates. Years are planning windows, not delivery guarantees. Funding, staffing, security findings and regulatory changes may alter scope or timing.



Planning windows · Progress follows acceptance gates

2026 — Protocol & Prototype

Specify identity, authorization, orders and escrow. Run a single-chain prototype and local simulator. Exit criteria: an eight-stage transaction demonstration, passing duplicate-charge and concurrent-overspend tests, and a reviewable threat model.

2027 — Testnet & Pilots

Publish an SDK preview, testnet and limited enterprise pilots. Introduce independent nodes and security audits. Exit criteria: closure of severe findings, successful recovery drills and an evidence-based decision on whether an independent L1 is warranted.

2028–2029 — Conditional Expansion

In 2028, assess a limited mainnet and controlled integrations only after technical, economic and legal gates are met. In 2029, expand the ecosystem, cross-network adapters and governance. Each new asset and region requires separate review; reaching a calendar year does not automatically unlock the next phase.

Governance & Upgrades

AFT AGENTCHAIN / PROTOCOL & FINANCING DESIGN

Governance changes future rules within security limits, transparent procedures and participant exit protections. Token voting does not replace an operating entity's legal responsibilities.

Phased Governance

The prototype uses named maintainers and transparent multisignature control. The testnet introduces technical review and operator discussion. On-chain voting is considered only when meaningful participation exists. Disclose administrator duties, affiliations and replacement procedures rather than using community-governance language to obscure concentrated control.

Proposal Lifecycle

A proposal publishes the problem, changes, risks and test evidence before discussion, technical review, voting, delayed execution and retrospective review. Financial parameters, permissions and consensus changes require different approval thresholds. Participation requirements, passing thresholds and delegation rules belong in a formal governance specification.

Emergency Authority

A security committee may pause new high-risk operations within a defined scope. It may not arbitrarily move user funds or rewrite existing orders. Each use records the trigger, signers, impact and expiry. Recovery requires review and public explanation. Emergency powers should be periodically reauthorized rather than expanding indefinitely.

Treasury & Conflicts

Grants are paid against milestones with public spending records. Related parties disclose conflicts and abstain from affected decisions. Participation does not guarantee token value or financial returns. Mainnet upgrades publish compatibility and exit plans in advance; unresolved disagreements require disclosure of fork and asset-identification risks.

Compliance Framework

AFT AGENTCHAIN / PROTOCOL & FINANCING DESIGN

Compliance depends on actual activities, operating entities and service jurisdictions. This chapter is a product-design framework, not a legal opinion or claim of licensing in any jurisdiction.

Entities & Activities

Before release, identify who maintains the protocol, operates wallets, holds assets, exchanges value, handles payments and serves customers. Licensing depends on practical control, fund flows and service scope, not labels such as non-custodial, DAO or technology platform. No claim of global availability is made before target markets are determined.

Customer & Transaction Controls

Applicable entities need risk grading, customer and business verification, sanctions screening, transaction monitoring and suspicious-activity procedures. FATF's virtual-asset framework includes information-transfer requirements [6], with specific duties depending on local implementation. Necessary personal data travels through protected channels, not public blockchain records.

Tokens & Stablecoins

Issuance and promotion require independent classification review. EU MiCA establishes rules for covered crypto-assets and services; financial instruments may fall under other regimes [7]. A whitepaper is not an approval document. Stablecoin selection requires review of the issuer, redemption, freezing powers and permitted local availability.

Launch Review

Each region requires legal assessment, eligible customer scope, data-flow review, complaint and refund processes and service contracts. Restricted services are disabled where required. Open blockchain access and commercial operating obligations are assessed separately. Until the entity, jurisdiction and qualifications are established, validation excludes real customer funds.

Risk Disclosures

AFT AGENTCHAIN / PROTOCOL & FINANCING DESIGN

Testing, node operation and future services may expose participants to loss. Protocol design cannot eliminate the following risks; disclosures must evolve with the deployed architecture.

Technical & Financial Risks

Contract defects, permission errors, key compromise, consensus attacks and infrastructure failures can cause asset loss or extended outages. Stablecoins may depeg, freeze or become unredeemable. Bridges and external payment providers add further failure risks. Multisignature controls, audits and insurance must not be presented as absolute protection.

Agent & Business Risks

Models may misunderstand tasks, accept injected instructions or select unsuitable providers. A delivery digest does not prove quality, and reputation can be manipulated. Procurement may produce refund, tax and performance disputes. Automation does not remove owner or operator responsibility.

Token & Governance Risks

If implemented, AGT may experience severe price volatility, illiquidity, concentrated holdings, governance capture and unsustainable incentives. Stake may be slashed and withdrawals delayed. No capital protection, buyback, listing, income or appreciation is promised. Token plans may change or be cancelled.

Regulatory & Delivery Risks

Classification, licensing and data rules may change available services. Resource constraints, poor technical choices or insufficient demand may delay the roadmap or end the project. This document is not an invitation to buy tokens, invest or use high-risk services. Actual deployment requires separate formal terms.

Conclusion & Next Iteration

AFT AGENTCHAIN / PROTOCOL & FINANCING DESIGN

The first objective is to demonstrate a bounded, traceable and recoverable agent transaction loop. Protocol credibility should come from inspectable implementation and evidence.

V1 Conclusion

The five-layer architecture and AIP establish a common language: identity binds a controller, wallets limit authority, execution produces evidence, payment manages fund conditions and L1 confirms deterministic state. Off-chain models and on-chain rules perform distinct roles, enabling enterprises to build controlled automation.

Next Technical Deliverables

V1.2 should define AIP field types, signatures, transition tables and error codes; implement reference escrow and authorization modules; and provide complete order test vectors, a threat model and benchmark methodology. Network-selection decisions, fee parameters and node operating specifications follow this work.

Next Business Decisions

Determine the operating entity, target jurisdictions, pilot providers and acceptance criteria. Specify settlement assets and responsibility boundaries. Independently review this edition's valuation, token allocation and proceeds budget before preparing definitive transaction documents. A funding target is not evidence of existing customers, revenue or technical capability.

Joint Review Priorities

Product review asks whether the workflow merits automation. Technical review examines state, permissions and fund invariants. Security review tests attack surfaces and recovery. Legal review addresses accountability and market eligibility. Together these findings determine whether the project advances.

AFT AgentChain — AI × Blockchain × Payment × Protocol

References & Standards

AFT AGENTCHAIN / PROTOCOL & FINANCING DESIGN

Citations describe existing standards and regulatory frameworks. The project architecture, names, interfaces and roadmap are proposals.

[1] W3C DID Core

Decentralized Identifiers v1.0 — identity model and control.
<https://www.w3.org/TR/did-core/>

[2] W3C Verifiable Credentials

Verifiable Credentials Data Model v2.0.
<https://www.w3.org/TR/vc-data-model-2.0/>

[3] ERC-4337

Account Abstraction Using Alt Mempool.
<https://eips.ethereum.org/EIPS/eip-4337>

[4] EIP-712

Typed structured data hashing and signing.
<https://eips.ethereum.org/EIPS/eip-712>

[5] CometBFT Consensus

Byzantine Consensus Algorithm — v0.38 specification.
<https://docs.cometbft.com/v0.38/spec/consensus/consensus>

[6] FATF Virtual Assets

Virtual assets, service providers and information-transfer requirements.
<https://www.fatf-gafi.org/en/topics/virtual-assets.html>

[7] ESMA MiCA

Markets in Crypto-Assets Regulation.
<https://www.esma.europa.eu/publications-and-data/interactive-single-rulebook/mica>

[8] NIST AI RMF

AI Risk Management Framework.
<https://www.nist.gov/itl/ai-risk-management-framework>