Fiduciary Agent Protocol (FIDU)

Institutional-Grade AI Agent Fiduciary Responsibility, Cryptographic Verification, and On-Chain Actuarial Insurance Protocol

Technical Whitepaper v1.0

Abstract

As autonomous AI agents evolve on-chain from social bots and MEME trading entities toward core financial hubs managing high-net-worth assets under management (AUM), conventional crypto infrastructure faces a critical **Fiduciary Vacuum**. The absence of legal entity backing and deterministic logic constraints exposes agentic capital to non-deterministic model hallucinations, adversarial prompt injection attacks, and unpredictable liquidation cascades.

The **Fiduciary Agent Protocol ($FIDU)** introduces the first full-stack on-chain fiduciary responsibility and risk-mitigation infrastructure. Operating through a three-layer interconnected architecture, $FIDU establishes an end-to-end security pipeline:

1. **Pre-execution cryptographic identity and model attestation (Fidu-ID)**
2. **In-execution dynamic intent firewall (Fidu-Guard)**
3. **Post-execution actuarial insurance and capital claim vault (Fidu-Vault)**

The native $FIDU utility token powers network staking, slashed node penalties, decentralized governance, and protocol value capture. This whitepaper outlines $FIDU's technical architecture, mathematical risk models, tokenomics framework (based on a fixed 600,000,000 supply cap), and strategic decoupling from existing AI+Web3 primitives.

1. Introduction & Problem Statement

1.1 The Agentic Economy Paradigm Shift: From Information to Fiduciary Asset Management

The convergence of blockchain and artificial intelligence has progressed through three structural phases:

- **Infra 1.0 (Decentralized Compute & Data):** Characterized by distributed GPU compute marketplaces and decentralized data harvesting networks.
- **Agent 1.0 (Social & Entertainment Agents):** Defined by tokenized agent launchpads, social bots, and narrative-driven MEME trading.
- **Agent 2.0 (Fiduciary Asset-Managing Agents):** AI agents equipped with dedicated smart accounts (ERC-6551 / Account Abstraction) operating as autonomous financial entities engaged in DeFi market-making, structured yield arbitrage, cross-chain asset

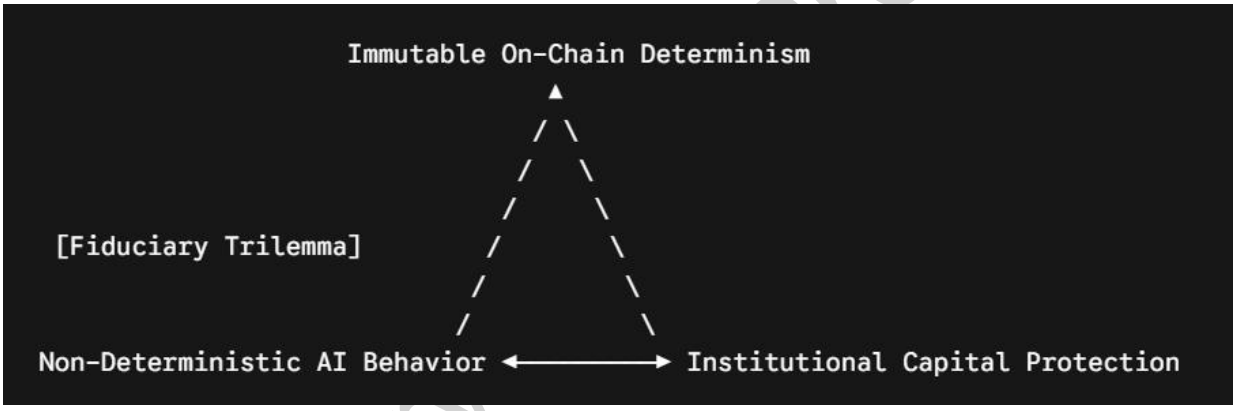
routing, and Real-World Asset (RWA) portfolio management.

In the Agent 2.0 era, AI entities transition from simple software programs into **fiduciaries** managing real capital.

EVOLUTION OF THE AGENTIC ECONOMY		
Infra 1.0 Distributed Compute & Data Pipelines	Agent 1.0 Social & Entertainment Agents / MEME Launchpads	Agent 2.0 ($FIDU Target) Fiduciary Asset Management AUM / DeFi / RWA Routing

1.2 The Autonomous Fiduciary Trilemma

When institutional capital delegates asset management authority to autonomous agents, it encounters an irreconcilable trilemma:



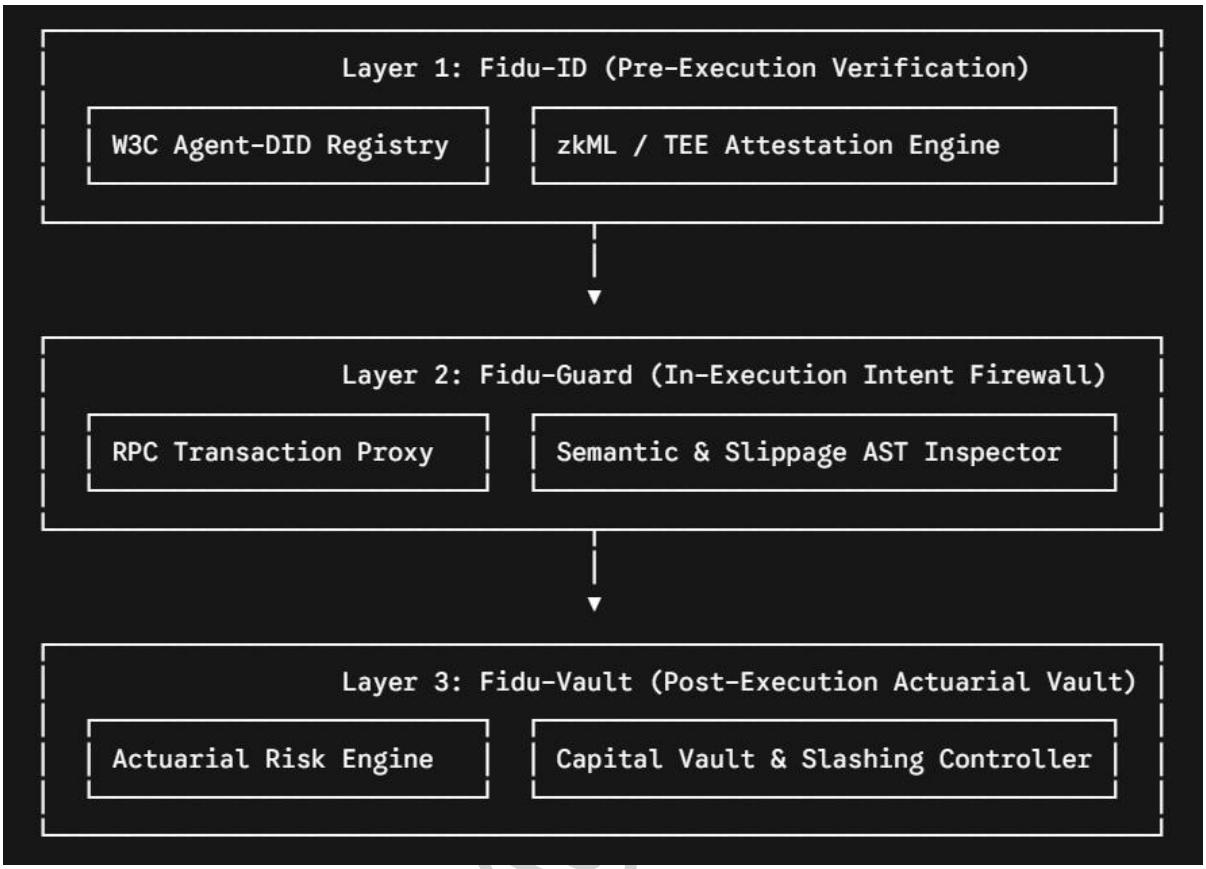
1. **Non-Deterministic Behavioral Drift:** Deep learning LLMs are inherently black-box systems subject to stochastic output drift ("hallucinations"). In financial contexts, a minor probability variance can trigger erroneous leverage liquidations or capital destruction.
2. **Adversarial Attack Surface:** Attackers do not need to exploit underlying smart contract code; they can inject adversarial prompts via on-chain or off-chain data feeds to manipulate agent logic and drain funds.
3. **Zero-Liability Vacuum:** Autonomous agents lack legal entity status. In the event of unforeseen losses, institutional capital has no legal recourse against open-source developers or model providers, rendering agentic asset management inherently unbankable.

$FIDU resolves this trilemma through a trustless framework combining zero-knowledge cryptography, real-time semantic execution auditing, and on-chain actuarial underwriting.

2. System Architecture

The $FIDU protocol is structured across three functional layers that together form a secure

fiduciary pipeline:



2.1 Layer 1: Fidu-ID (Pre-Execution Identity & Model Attestation)

Fidu-ID establishes agent identity, authority boundaries, and model integrity prior to execution:

- **W3C Agent-DID Standard:** Each registered agent receives a W3C-compliant Decentralized Identifier (DID) bound to its on-chain account, model architecture hash, historical performance metrics, and fiduciary mandate parameters.
- **Hybrid zkML & TEE Attestation Engine:**
  - **zkML (Zero-Knowledge Machine Learning):** For compact decision-tree models, agents submit zk-SNARK proofs demonstrating that on-chain decisions originate directly from specified model weights rather than unauthorized key access.
  - **TEE (Trusted Execution Environment) Remote Attestation:** For large language models (LLMs), execution runs within hardware-isolated TEEs (e.g., Intel SGX / AMD SEV). Hardware-signed attestation reports are verified on-chain to ensure execution integrity.

2.2 Layer 2: Fidu-Guard (In-Execution Dynamic Intent Firewall)

Fidu-Guard operates as an RPC proxy layer that inspects pending agent transactions before block inclusion:

- **AST Semantic Inspection:** Unsigned raw transactions are parsed into Abstract Syntax Trees (ASTs) to extract high-level execution intent (e.g., "Swapping

$100,000\text{ USDC}$ for ETH on Uniswap V3").

- **Dynamic Risk Constraint Engine:**
  - **Liquidity & Slippage Monitoring:** Evaluates trade size against current pool depth, automatically intercepting orders that exceed allowable slippage thresholds.
  - **Malicious Address & Contract Filtering:** Cross-references transaction targets against blacklisted addresses and unverified smart contracts.
  - **Prompt Injection Isolation:** Intercepts logical anomalies, such as unexpected asset transfers to un-compiled wallet addresses.
- **Automated Circuit Breaker:** If a transaction breaches safety limits, Fidu-Guard nodes reject propagation, suspend the agent's active status, and emit an on-chain risk event.

2.3 Layer 3: Fidu-Vault (Post-Execution Actuarial Insurance Vault)

Fidu-Vault provides automated financial compensation if a failure slips past the firewall:

- **Decentralized Reinsurance Capital Pool:** Capitalized by liquidity providers and $FIDU stakers to underwrite monitored agent assets.
- **On-Chain Claims Oracle:** Upon an verified loss event (such as oracle manipulation or unexpected logic failures), the claims oracle verifies loss parameters and disburses compensation from the vault.

3. Actuarial Models & Risk Economics

3.1 Fiduciary Trust Score (FTS)

The protocol calculates a dynamic Fiduciary Trust Score $S_t \in [0, 100]$ for each agent:

$$S_t = w_1 \cdot C_{\text{historical}} + w_2 \cdot M_{\text{proof}} + w_3 \cdot (1 - R_{\text{anomaly}}) + w_4 \cdot \ln(1 + \text{AUM}_t)$$

Where:

- $C_{\text{historical}}$: Time-weighted history of compliant execution without default.
- M_{proof}: Attestation strength score ($\text{zkML} > \text{TEE} > \text{Multi-Sig}$).
- R_{anomaly}: 90-day frequency of transactions intercepted by Fidu-Guard.
- AUM_t: Current assets under management deployed by the agent.
- w_1, w_2, w_3, w_4: Normalized system parameters ($\sum w_i = 1$).

3.2 Dynamic Premium Pricing Model

Agents pay periodic insurance premiums to Fidu-Vault based on an annualized premium:

$$\text{Prem}_t = \text{BaseRate} + \alpha \cdot \left(1 - \frac{S_t}{100}\right) + \beta \cdot \text{VaR}_{99\%} + \gamma \cdot \sigma_{\text{strategy}}$$

Where:

- BaseRate: System baseline risk-free underwriting rate (default 0.5%).
- $\text{VaR}_{99\%}$: Monte Carlo-calculated 99% Value-at-Risk for the agent's strategy.
- σ_{strategy}: Annualized volatility of the underlying DeFi asset portfolio.
- α, β, γ: System risk sensitivity coefficients.

High-trust agents ($S_t \to 100$) operating low-risk strategies approach minimum premium rates ($\approx 0.8\%/\text{year}$). Higher-risk or lower-rated agents face scaled premiums up to $5.0\%+$, using market dynamics to enforce compliance.

3.3 Slash Economics

Fidu-Guard firewall node operators must stake $FIDU. If a node cluster fails to intercept a malicious transaction or acts dishonestly:

$$\text{Slash Amount} = \min\left(L_{\text{actual}} \cdot \delta,\ \Omega \cdot Q_{\text{staked}}\right)$$

Where:

- L_{actual}: Actual on-chain asset loss.
- δ: Cluster fault attribution factor determined via Byzantine consensus.
- Q_{staked}: Total `$FIDU` staked by the node.
- Ω: Maximum single-event slashing cap parameter.

Slashed `$FIDU` tokens are allocated **50% to Fidu-Vault compensation reserves** and **50% permanently burned.**

4. Tokenomics Framework

4.1 Key Parameters

- **Token Name:** Fiduciary Agent Protocol
- **Ticker Symbol:** $FIDU

- **Total Supply:** 600,000,000 FIDU (Fixed Cap)
- **TGE Initial Circulating Supply:** 180,000,000 FIDU (30.0% of Total Supply)

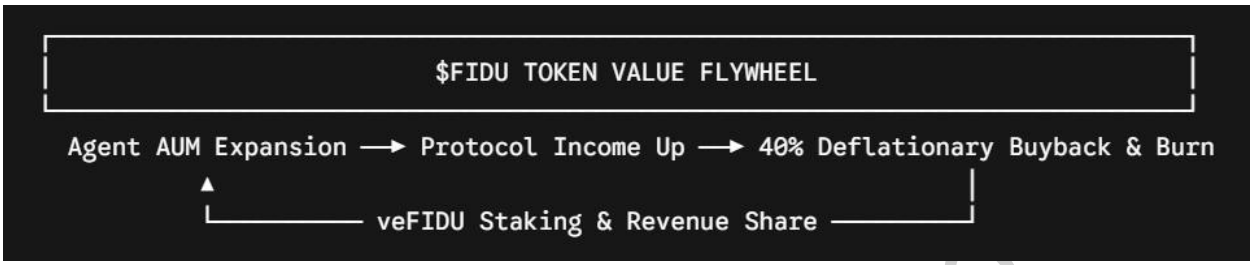
4.2 Token Allocation & Vesting Schedule

The token distribution balances initial market liquidity, node staking reserves, long-term team alignment, and capital reserves:

Pool ID	Allocation Category	Ratio (%)	Token Amount	TGE Unlock	Cliff	Vesting Schedule
PUB	Public Sale & LBP Launch	10.0%	60,000,000	60,000,000	0 Months	100% unlocked at TGE for initial price discovery.
AIR	Community Airdrop & Testnet	10.0%	60,000,000	60,000,000	0 Months	Rewards early node operators, developers, and testers.
LIQ	Exchange & Market Liquidity	10.0%	60,000,000	60,000,000	0 Months	Locked into DEX/CEX market-making contracts by DAO.
INS	Reinsurance Capital Vault	30.0%	180,000,000	0	3 Months	48-month linear monthly vesting as tail-risk backstop.
NOD	Node Staking & Risk Rewards	15.0%	90,000,000	0	0 Months	Emissions over 36 months based on firewall work.
TEA	Core Team & Contributors	15.0%	90,000,000	0	12 Months	12-month cliff, followed by 36-month linear vesting.
INV	Strategic Investors	10.0%	60,000,000	0	6 Months	6-month cliff, followed by 24-month linear vesting.
Total	--	**100.0%**	**600,000,000**	**180,000,000**	--	--

4.3 Supply & Sell-Pressure Management

Out of the 180,000,000 $FIDU tokens circulating at TGE, 120,000,000 tokens (66.6% of initial float) are locked in public distribution and liquidity provisioning. Team and investor allocations are bound by 6–12 month cliffs, aligning long-term incentives with protocol usage.



4.4 Value Capture & Burn Mechanism

Protocol fees connect $FIDU value to total agent AUM:

1. **Staking Demand Sinks:**
   - **Agent Trust Staking:** Developers stake $FIDU to boost their Fiduciary Trust Score S_t, lowering annual premiums.
   - **Node Collateral:** Fidu-Guard operators must stake a minimum of 100,000 FIDU per node.
2. **Deflationary Buyback & Burn Engine:**
   - **40% of all protocol revenues** (Fidu-ID verification fees, Fidu-Guard volume fees, Fidu-Vault premiums) are used to buy back $FIDU on the open market and burn it until total supply reaches **300,000,000 FIDU**.
   - **40% of protocol revenues** fund the Fidu-Vault capital reserve.
   - **20% of protocol revenues** are distributed to long-term $veFIDU stakers.

5. Financial Projections & Business Model

5.1 Protocol Revenue Streams

$FIDU operates a fee model tied to agent activity:

1. **Fidu-ID Verification Fee:** Fixed fee ($500–$2,000 in $FIDU) charged per agent registration and model attestation update.
2. **Fidu-Guard Volume Fee:** Dynamic 0.02% fee assessed on transaction volume processed through the firewall.
3. **Fidu-Vault Underwriting Premium:** Annualized $0.8\% - 1.5\%$ fee assessed on monitored agent AUM.

5.2 Revenue Forecast Model

Below is a projection of protocol revenues across growth phases:

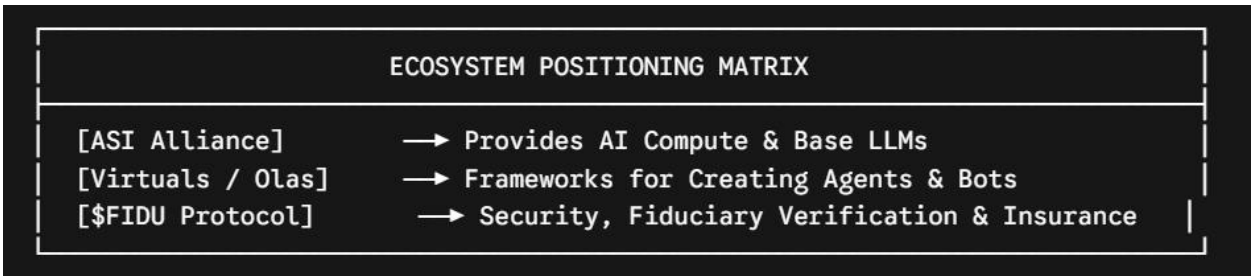
Growth Phase	Monitored Agents	Total Agent AUM	Annual Premiums (1.0% Avg)	Firewall Volume Fees (0.02%)	Net Annual Protocol Revenue
Phase 1: Bootstrapping	100	$100M USD	$1,000,000	$200,000	**$1,200,000 USD**
Phase 2: Growth	1,500	$2B USD	$20,000,000	$4,000,000	**$24,000,000 USD**
Phase 3: Scale	10,000+	$10B USD	$100,000,000	$20,000,000	**$120,000,000 USD**

At Phase 3 scale ($10B AUM), $120M in annual revenue generates ~$48M in market buybacks, creating continuous structural demand for $FIDU.

6. Competitive Decoupling Analysis

$FIDU complements the existing AI ecosystem rather than competing directly with agent launchpads, bot frameworks, or compute networks:

Dimension	Virtuals Protocol ($VIRTUAL) \vert{} Autonolas ($OLAS)	ASI Alliance ($FET) \vert{} Fiduciary Agent Protocol ($FIDU)
Primary Focus	B2C Agent Issuance & Launchpad	B2B Off-Chain Bot Automation
Key Problem Solved	Agent tokenization & social liquidity	Off-chain script scheduling
Core Architecture	IAO Framework, G.A.M.E Engine	Open Autonomy Architecture
Core Output	Agent Tokens, Entertainment Agents	Execution Bots, DAO Helpers
Ecosystem Synergy	**Complementary:** Virtuals agents connect to $FIDU for capital safety. \vert{} **Complementary:**$FIDU audits execution logic for Olas bots.	**Upstream Supplier:** $FIDU nodes utilize ASI for compute. \vert{} **Decoupled:**$FIDU serves as the safety standard for all agents managing asset flows.



7. Roadmap & Governance

7.1 Development Phases

```
2026 Q3: Protocol Alpha
  ├── Deploy Fidu-ID registry & W3C Agent-DID contracts
  ├── Launch Fidu-Guard RPC proxy node client
  └── Execute TGE & $FIDU Liquidity Bootstrapping Pool (LBP)

2026 Q4: Fidu-Vault & Testnet Rollout
  ├── Launch Fidu-Vault reinsurance capital pool & staking system
  ├── Onboard 50 initial Fidu-Guard firewall verification nodes
  └── Integrate Fidu-ID with top agent frameworks (including Virtuals ecosystem)

2027 Q1-Q2: Institutional DeFi/RWA Underwriting & zkML Upgrade
  ├── Roll out zkML model weight verification modules
  ├── Open underwriting channels for agents managing AUM > $10M
  └── Activate automated $FIDU revenue buyback & burn engine

2027 Q3+: Fiduciary DAO Decentralization
  ├── Transition Fidu-Guard firewall rules to veFIDU governance
  └── Establish cross-chain fiduciary security standards
```

7.2 Governance Model (Fiduciary DAO)

$FIDU uses a veTokenomics framework[cite: 1]. Locking $FIDU for 1 week to 4 years yields $veFIDU, granting stakers:

1. **Actuarial Parameter Voting:** Set baseline premium rates Prem_t across asset classes[cite: 1].
2. **Slash Dispute Review:** Participate in decentralized tribunal resolution during contested loss events[cite: 1].
3. **Protocol Cash-Flow Distribution:** Claim 20% of net protocol revenues directly[cite: 1].

8. Conclusion

As AI agents assume control over complex asset management, fiduciary infrastructure becomes essential for institutional adoption[cite: 1].

The **Fiduciary Agent Protocol ($FIDU)** provides a framework for autonomous asset management[cite: 1]. By integrating cryptographic identity attestation (Fidu-ID), real-time execution firewalls (Fidu-Guard), and on-chain actuarial vaults (Fidu-Vault), $FIDU delivers institutional safety to the agentic economy[cite: 1]. Backed by a deflationary token model,$FIDU establishes the security standard for autonomous financial management[cite: 1].