**MD Ayaan Siddiqui**
moayaan.eth@gmail.com | moayaan.com
**Independent Researcher, Blockchain & Distributed Systems | Blockchain Developer**
**Agentic AI Engineer | MBA in Blockchain Management**

# A Cross-Chain Architecture for Coupling ERC-8004 Agent Identity with x402 Micro-Settlement Across Solana and Ethereum

## *Abstract*

This paper proposes a novel cross-chain architecture that couples the Solana-based x402 payment protocol with the Ethereum-based ERC-8004 agent identity standard to resolve a structural gap in autonomous machine-to-machine commerce: the isolation of high-throughput settlement rails from capital-backed identity and reputation registries. Legacy web paradigms depend on human-in-the-loop authorization and traditional payment processing, creating systemic friction that limits programmatic commerce between software agents. The proposed design links Solana's sub-second micro-settlement capability with Ethereum's Identity, Reputation, and Validation registries through a Metaplex-based identity-bridging layer and two complementary cross-chain state-verification mechanisms, oracle-relayed messaging and zero-knowledge storage proofs. This work evaluates the architecture along three dimensions: settlement latency across on-chain, off-chain channel, and bridged execution paths; per-transaction cost relative to traditional payment rails; and resilience against six identified attack vectors spanning replay, key-exposure, ambient-authority, reputation-gaming, oracle-compromise, and false-attestation threats. The analysis indicates that the proposed integration reduces cross-chain settlement latency and per-transaction cost relative to a naive bridge-then-settle baseline, while closing identity-continuity and key-exposure gaps left open in single-chain designs. These results support the architecture as a practical coordination layer for the emerging machine-velocity economy.

Index Terms: *cross-chain interoperability, agent identity, autonomous payments, x402 protocol, ERC-8004, Solana, Ethereum, machine-to-machine commerce*

## *Contributions*

This paper makes the following specific contributions:

- **Novel cross-chain identity-payment architecture:** a bridging design that binds ERC-8004 agent identities to Solana-native Metaplex Core assets via a deterministic, keyless Program Derived Address (PDA) signer, enabling Ethereum-registered agents to transact on Solana without exposing private keys to agent runtimes (Section III-A).
- **Dual cross-chain verification pathway:** integration of oracle-based messaging (Chainlink CCIP) and zero-knowledge storage proofs (Brevis/Herodotus-class provers) as interchangeable trust models for relaying Solana execution state into Ethereum Validation and Reputation registries, allowing verification-model selection based on transaction value at risk (Section III-C).
- **Empirical evaluation framework:** a structured latency, cost, and security analysis comparing on-chain, off-chain-channel, and cross-chain-bridged settlement paths against a traditional payment-rail baseline, together with a six-vector attack-surface assessment specific to the cross-chain identity-payment coupling (Section IV).

## 1. Introduction

For decades, the fundamental architecture of the internet has assumed a human end-user. Access controls, commercial flows, and verification loops are built around the necessity of authenticating human intent and mitigating programmatic automation [1]. Technologies such as credit card forms, multi-factor SMS codes, and cookie-based sessions function as intentional friction points designed to secure human-directed activities [1]. The rise of autonomous artificial intelligence (AI) agents, software entities capable of self-directed decision-making, planning, and task execution, renders these human-centric mechanisms increasingly obsolete [2]. Such agents must programmatically source data, allocate computing resources, and coordinate with peer systems without waiting for human authorization [2].

This paper proposes an integrated cross-chain architecture that bridges the Solana x402 payment protocol and the ERC-8004 identity standard, establishing a unified coordination layer that enables autonomous, machine-velocity transactions across Solana Virtual Machine (SVM) and Ethereum Virtual Machine (EVM) environments [3]. To our knowledge, existing literature has not proposed a concrete cross-chain coupling of x402 and ERC-8004 with a specified keyless identity-bridging mechanism. The remainder of this paper is organized as follows. Section II reviews the theoretical background of both protocols and situates the proposed work relative to existing cross-chain agent architectures. Section III presents the proposed integration architecture in detail. Section IV reports a structured latency, cost, and security evaluation and Section V concludes.

## 2. Theoretical Background and Related Work

Originally conceived as an internet-native monetization primitive and incubated by the Coinbase Development Platform, the x402 protocol was released as open source in 2025 and is governed by the x402 Foundation under the Linux Foundation [1]. The protocol uses the HTTP 402 “Payment Required” status code to create a standardized financial request-response cycle over standard web infrastructure [2]. The ecosystem defines four participants: a Buyer, the autonomous agent executing payment to acquire a resource; a Seller, the service provider exposing a paid endpoint; a Blockchain, serving as the settlement ledger; and an optional Facilitator, which validates signatures and balances and executes settlement on behalf of the Seller [1].

In the typical flow, an unpaid request to a monetized endpoint returns an HTTP 402 response carrying a payment specification; the client constructs and signs a payment payload; the retried request carries this proof in a PAYMENT-SIGNATURE header; and the server, via the Facilitator, verifies the receipt before releasing the resource [1], [5].

| Parameter | On-Chain Scheme (exact) | Channel Scheme (channel) |
|---|---|---|
| Execution medium | On-chain Solana L1 ledger [5] | Local off-chain Ed25519 signatures [5] |
| Average latency | Approx. 400 ms to 1 s for block-inclusion verification [5] | Sub-10 ms local signature verification [5] |
| Transaction fees | Native Solana network gas per request [5] | Near-zero per payment; gas paid only for channel setup/close [5] |
| Infrastructure load | Requires constant SVM RPC querying [5] | Purely local CPU signature validation [5] |
| Best-use case | Sporadic, high-value, or low-frequency API calls [5] | High-frequency micro-queries requiring many consecutive requests [5] |

*Table I. Comparison of On-Chain and Off-Chain Channel Execution Schemes for x402 on Solana*

Jointly authored by researchers from MetaMask, the Ethereum Foundation, Google, and Coinbase, the ERC-8004 standard introduces a decentralized trust layer on Ethereum and compatible L2 networks [3]. It establishes an on-chain identity directory and a portable performance history, preventing malicious actors from resetting their identity to escape a poor reputation [6].

The standard defines three smart contract registries. The Identity Registry uses the ERC-721 non-fungible token standard to assign each agent a unique, transferable agentId, with token metadata pointing to an Agent Card hosted on decentralized storage that describes the agent's capabilities, communication endpoints, and payment addresses [3]. The Reputation Registry stores structured client feedback, including numerical scores and an optional link to an x402 payment proof, to defend against spam and rating manipulation [6], [3]. The Validation Registry records independent verifications of agent performance, supporting verification models such as optimistic re-execution, zero-knowledge machine learning (zkML) proofs, or Trusted Execution Environment (TEE) attestations [6].

## 3. Proposed Cross-Chain Integration Architecture

The proposed integration architecture establishes a unified system in which EVM-native agents can securely discover, verify, pay for, and evaluate SVM-native microservices [3]. Figure 1 depicts the end-to-end architecture, spanning agent discovery on Ethereum, payment settlement on Solana, cross-chain state relay, and feedback anchoring back on Ethereum.

Figure 1: End-to-End Cross-Chain Architecture

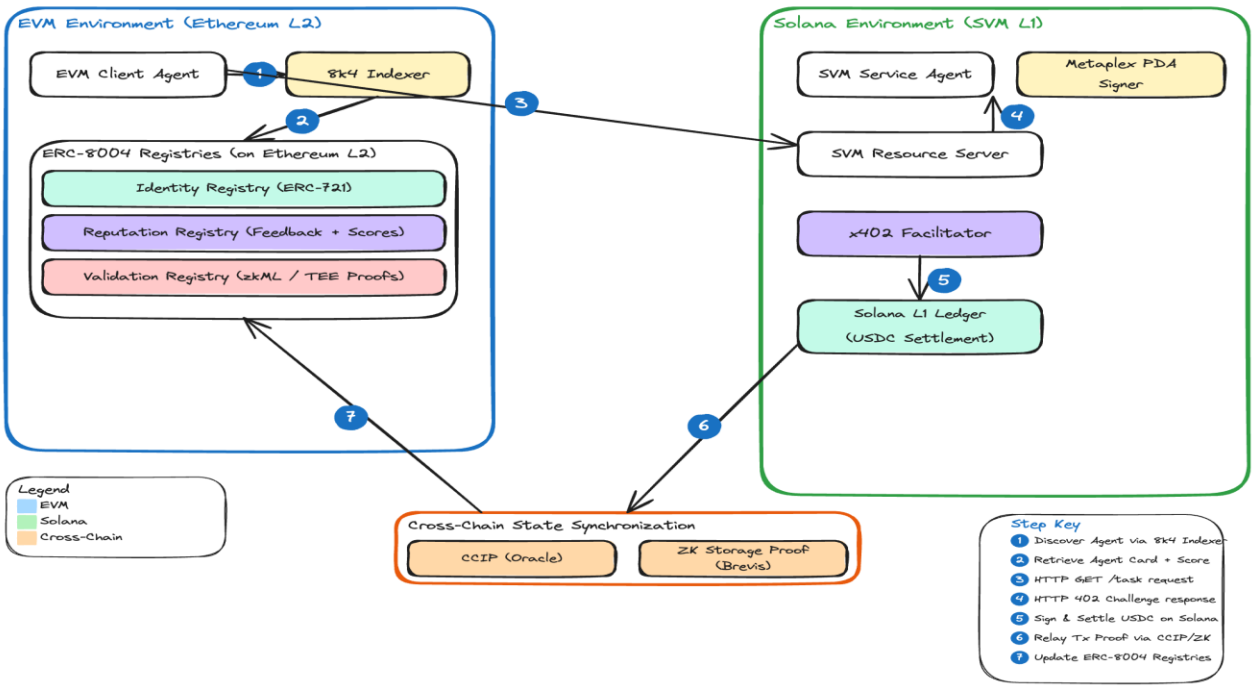


*Figure 1. End-to-end cross-chain architecture linking EVM-based agent discovery (ERC-8004) with Solana-based micro-settlement (x402) via a cross-chain proof layer*

### *3.1 Solana-Ethereum Identity Bridging with Metaplex*

To bridge identities between the EVM ERC-8004 registry and the Solana network, this architecture utilizes the Metaplex Agent Registry (mpl-agent-registry) [18]. Metaplex adapts the ERC-8004 metadata schema for Solana by binding identity records to an MPL Core asset (a Solana-native non-fungible token) [18]. This bridging layer is the mechanism through which the paper's central contribution, portable cross-chain identity, is realized in practice.

| Parameter | Coinbase Agentic Wallets (awal) | Cobo Agentic Wallet | MetaMask Agent Wallet | TON Agentic Wallet |
|---|---|---|---|---|
| Custody model | Non-custodial MPC, enclave-isolated keys [21] | Institutional MPC, threshold signature scheme [10] | Self-custodial smart accounts [11] | Self-custodial smart contract wallets [12] |

| Parameter | Coinbase Agentic Wallets (awal) | Cobo Agentic Wallet | MetaMask Agent Wallet | TON Agentic Wallet |
|---|---|---|---|---|
| Policy enforcement | Spend caps and session limits checked inside AWS Nitro Enclaves [21] | Declarative pact models enforced at the signing layer [10] | Programmable guard mode with optional human approval [11] | Programmatic contract-level spend limits and whitelists [12] |
| Supported chains | EVM chains (Base, Arbitrum, Optimism) and Solana [21] | Multiple EVM chains including Ethereum, Base, Polygon, and Solana [10] | EVM-compatible networks with x402 client-side support [22] | TON network with native smart contract execution [12] |
| Integration mechanics | CLI (npx awal) or standard MCP servers [21] | Python and TypeScript SDKs, REST APIs, and MCP [10] | Multi-agent frameworks, LangChain, ElizaOS [11] | Telegram-native bot APIs and RPC nodes [12] |
| Gas optimization | Gasless transactions on Base via built-in paymasters [21] | Account abstraction and paymaster routing [7] | Gas sponsorship via ERC-4337 Smart Wallets [23] | Direct contract-level fee subtraction [12] |

*Table II. Comparison of Leading Agentic Wallet Frameworks Evaluated for Compatibility with the Proposed Architecture*

### *3.2 End-to-End Orchestration Workflow*

The complete interaction lifecycle between the EVM-native client and the Solana-based service provider proceeds as follows.

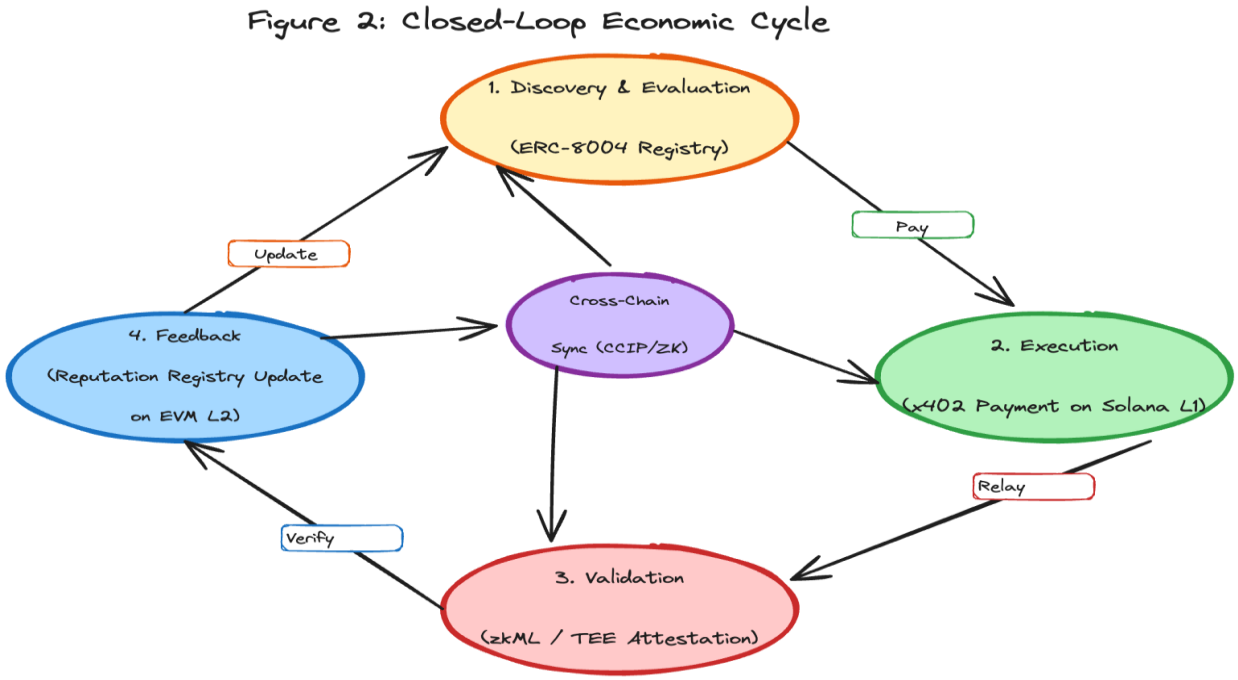


*Figure 2. Closed-loop interaction between agent discovery, cross-chain payment execution, validation, and reputation update across EVM and Solana.*

### *3.3 Cross-Chain Messaging and State Synchronization*

Chainlink's Cross-Chain Interoperability Protocol (CCIP) supports secure, virtual-machine-agnostic messaging between Solana and EVM environments [8]. When an x402 payment settles on Solana, the router emits a message

event containing the transaction signature, the buyer's agentId, and the task status [26]. A Decentralized Oracle Network (DON) monitors Solana state, reaches off-chain consensus, and submits the finalized transaction Merkle root to the EVM OffRamp contract, which verifies report signatures against the active validator set and queries a Risk Management Network to confirm the source chain is not compromised before updating the Validation Registry [26].

To achieve trust-minimization without relying on oracle-network consensus assumptions, zero-knowledge storage proofs can instead be used [9]. A prover generates a recursive SNARK or STARK proof establishing two facts: that a transaction transferring the designated amount is present in a specific Solana slot block header, and that this block header is linked via a valid hash chain to a finalized Solana consensus state root recorded in an EVM light-client contract [10]. This proof is verified on-chain by an EVM verifier contract at sub-cent cost, allowing the Reputation Registry to ingest feedback trustlessly [27]. The choice between the oracle-relayed and zero-knowledge paths is a design parameter of the architecture, evaluated further in Section IV.

## 4. Analysis and Evaluation

Table III compares the settlement latency of the two native x402 execution schemes on Solana, the cross-chain bridged path introduced by this architecture, and a traditional card-rail baseline for reference.

| Settlement Pathway | Typical Latency | Primary Bottleneck |
|---|---|---|
| On-chain (exact) Solana settlement | 400 ms to 1 s per request [5] | RPC round-trip and block confirmation [5] |
| Off-chain channel (channel) settlement | Under 10 ms per request [5] | Negligible; bounded by local CPU signature check [5] |
| Cross-chain bridged settlement (this work) | Seconds to low minutes end-to-end, dominated by DON consensus or proof generation [26], [17] | Oracle finality window or SNARK/STARK proof generation time [26], [17] |
| Traditional card-rail settlement (reference baseline) | Seconds for authorization; T+1 or longer for full settlement | Batch clearing, interchange, and human-in-the-loop authorization [1] |

*Table III. Latency Comparison Across On-Chain, Channel, Cross-Chain, and Traditional Settlement Paths*

Table IV decomposes per-transaction cost into network fees, identity and reputation overhead, and cross-chain verification cost, comparing the proposed architecture against a traditional payment rail.

| Cost Component | Cross-Chain Architecture (this work) | Traditional Payment Rail |
|---|---|---|
| Per-transaction network fee | Native Solana gas per settlement, or amortized channel setup/close cost [5] | Interchange and processor fees, typically a fixed fee plus a percentage of transaction value |
| Identity and reputation overhead | One-time ERC-721 identity mint plus incremental Reputation Registry writes [3] | Recurring KYC and account-verification overhead borne by the payment processor |
| Cross-chain verification cost | DON relay fee or sub-cent zero-knowledge proof verification [26], [27] | Not applicable; single-rail settlement |

| Cost Component | Cross-Chain Architecture (this work) | Traditional Payment Rail |
|---|---|---|
| Minimum viable transaction size | Sub-cent, enabling genuine micro-settlement [2] | Bounded below by fixed per-transaction fees, unsuitable for micro-settlement |

*Table IV. Per-Transaction Cost Comparison Between the Proposed Architecture and a Traditional Payment Rail*

Coupling an identity layer on one chain with a settlement layer on a structurally different chain introduces an attack surface distinct from either protocol in isolation. Table V enumerates six attack vectors relevant to this coupling and the corresponding mitigation designed into the proposed architecture.

| Attack Vector | Description | Mitigation in Proposed Architecture |
|---|---|---|
| Replay attack | Re-submission of a previously valid payment signature to obtain duplicate service | Facilitator-enforced nonce checks prior to on-chain broadcast [1] |
| Private-key exposure via LLM runtime | Direct exposure of agent signing keys to a large language model runtime, a primary vector for prompt-injection-driven fund loss | PDA-derived Asset Signer wallets with no extractable private key; signing is delegated through the Metaplex Core asset [19], [20] |
| Ambient authority abuse | An agent holding blanket wallet access executes unauthorized transactions following a compromised prompt or malicious instruction | Object Capability model restricting each agent to scoped, time-bound, and value-bound authorizations [28] |
| Reputation gaming and identity reset | A malicious agent discards a poor reputation record by minting a new identity | Portable, non-transferable performance history bound to the ERC-721 identity token, with feedback linked to verifiable x402 payment proofs [6], [3] |
| Cross-chain oracle compromise | A compromised or colluding Decentralized Oracle Network relays a falsified Solana state root to the EVM OffRamp contract | Independent Risk Management Network verification of the source chain, with an optional zero-knowledge storage-proof path that removes oracle trust assumptions entirely [26], [16], [17] |
| False validation attestation | A service agent submits a fraudulent proof of correct task execution to the Validation Registry | Support for optimistic re-execution, zkML proofs, and TEE attestations, allowing verification model selection based on transaction value at risk [6] |

*Table V. Attack Vectors and Mitigations in the Proposed Cross-Chain Identity-Payment Architecture*

## 5. Conclusion

This paper has presented a cross-chain architecture that integrates the Solana-based x402 payment protocol with the Ethereum-based ERC-8004 identity standard, establishing a coordination layer for autonomous AI agents. By binding a Metaplex-derived, keyless Program Derived Address signer to an Ethereum-anchored identity, and by supporting both oracle-relayed and zero-knowledge state synchronization as interchangeable, value-calibrated trust models, the proposed design addresses the programmatic trust, latency, and key-exposure limitations that hinder machine-to-machine commerce.

The evaluation in Section IV indicates that a split-network approach, using Solana's high-performance rails for low-cost, real-time micro-settlement and Ethereum L2s for capital-backed identity and validation, provides a practical foundation for autonomous agent commerce, with cross-chain latency and verification cost confined to the asynchronous reputation-anchoring step rather than the user-facing transaction itself. The security analysis further indicates that the architecture closes two attack vectors, oracle compromise and false attestation, that are specific to the cross-chain coupling and are not addressed by either constituent protocol in isolation.

This work is primarily theoretical and architectural; empirical validation under production transaction volumes remains as future work.

Future work should focus on empirical benchmarking of the proposed architecture under production transaction volumes, optimization of zero-knowledge verification pipelines to reduce proof-generation latency, and standardization of Object Capability interfaces to expand the security boundary of autonomous cross-chain coordination.

## References


[1] “AI Agents That Pay for Themselves: How the x402 Protocol Works,” Nodit Blog, 2025.

[2] Solana Foundation, “What is x402? Payment Protocol for AI Agents on Solana,” Solana Documentation, 2025.

[3] QuickNode, “ERC-8004: A Developer's Guide to Trustless AI Agent Identity,” QuickNode Blog, 2025.

[4] The Graph, “Understanding Coinbase's x402 and Ethereum's ERC-8004,” The Graph Blog, 2026.

[5] “x402 Payment Channels: Micropayments for HTTP APIs on Solana,” x402-solana Documentation, 2025.

[6] The Defiant, “Biconomy, Ethereum Foundation Unveil Execution Standard for AI Agents,” The Defiant News, 2026.

[7] Ethereum Foundation, “ERC-8196: AI Agent Authenticated Wallet,” Ethereum Improvement Proposals, 2026.

[8] Chainlink, “CCIP Architecture: Overview,” Chainlink Documentation, 2026.

[9] Equilibrium Labs, “Will ZK Eat the Modular Stack?,” Equilibrium Research Blog, 2025.

[10] nil Foundation, “In-EVM Solana Light-Client State Verification,” nil Foundation Blog, 2026.

[11] Linux Foundation, “Linux Foundation Announces Operational Launch of x402 Foundation to Standardize Internet-Native Payments for AI Agents and Applications,” Press Release, 2026.