Nominal: Universal Address Resolution across Heterogeneous Blockchain Virtual Machines

17th August, 2025

Bello Mohammed Tayo Akintoye Abubakar Misbahu

Abstract

This paper introduces the Nominal Resolution Protocol, a new framework for abstracting cryptographic wallet addresses into a single, human-readable namespace across separate and non-compatible blockchain networks, including EVM, MoveVM, Solana, and NEAR execution environments. We reject conventional bridge-based architectures for state synchronization, which introduce trust assumptions and attack vectors. Instead, we propose a client-side protocol where state propagation is managed directly by a specialized Software Development Kit (SDK) integrated into user wallets. This architecture places the user's cryptographic authority at the center of all cross-chain operations, eliminating intermediary risks. The protocol is defined by minimalist, single-purpose registry smart contracts deployed natively on each supported chain, with all complex logic, including conflict resolution and state verification, handled by the client-side SDK. Furthermore, we introduce a mathematical framework for quantifying the authority and reputation of a registered name based on on-chain temporal and transactional data, providing a Sybil-resistant metric of trust. This work presents a significant scientific advancement by demonstrating a viable, decentralized, and more secure alternative to existing cross-chain interoperability solutions for identity and addressing.

Keywords: Decentralized Identity, Cross-Chain Interoperability, Client-Side Resolution, State Propagation, Blockchain Virtual Machines, Cryptographic Security, Protocol Design.

1. Problem Statement

The foundational architecture of public blockchains employs pseudonymous cryptographic identifiers (wallet addresses) to facilitate transactions while preserving user privacy. While effective for pseudonymity, the high entropy and non-human-readable format of these addresses (e.g., 42-character hexadecimal strings for the EVM) introduce a significant cognitive burden and a high degree of operational risk for the end-user. This design trade-off between security and usability is a primary source of irreversible asset forfeiture.

The operational risk is not merely theoretical but results in quantifiable financial detriment. A longitudinal study conducted between July 1, 2022, and June 30, 2024, on the Ethereum and Binance Smart Chain networks identified 681 confirmed instances of asset loss totaling approximately $5.5 million USD, directly attributable to address input errors by users (e.g., typos, transposition errors). The severity of such errors at the individual level is further highlighted by case studies, such as the widely reported loss of $26 million in digital assets due to a single address mis-entry, underscoring the critical nature of this systemic flaw.

Existing attempts to mitigate this issue, primarily through chain-specific naming services (e.g., Ethereum Name Service, Solana Name Service), have provided partial solutions within their native ecosystems but have introduced a second-order problem: **namespace fragmentation**. These systems require users to acquire and manage a separate, siloed identity for each blockchain. Furthermore, by modeling themselves after the traditional Domain Name System (DNS), they inherit its limitations, including:

1. **Rent-Seeking Economic Models:** The requirement for annual renewal fees imposes a perpetual financial obligation on the user for maintaining ownership of their digital identity.
2. **Governance and Legal Encumbrances:** These systems are often subject to centralized dispute resolution mechanisms and traditional trademark law, which can be incongruent with the principles of decentralized, non-custodial asset ownership.

Therefore, the central problem this research addresses is the **absence of a unified, trust-minimized protocol for universal address resolution across heterogeneous blockchain virtual machines.** The existing literature and implemented solutions lack a framework that simultaneously provides:

- A single, persistent, human-readable identifier that is owned in perpetuity.
- Native interoperability across disparate execution environments (e.g., EVM, Solana VM, MoveVM) without reliance on trusted intermediaries such as cross-chain bridges.
- A model of ownership that is cryptographically sovereign and unencumbered by the economic and governance constraints of DNS-inspired systems.

2. A Bridge-less, Multi-VM Interoperability Protocol

2.1 Heterogeneous Native Contract Deployment

The on-chain footprint of the Nominal protocol is intentionally minimalist. On each supported blockchain, a single, highly-optimized smart contract is deployed. This contract serves as a simple, chain-specific key-value store mapping the namehash to a chain-native address and an owner address. The implementation is tailored to the native language and architecture of each environment to maximize security and efficiency.

- **EVM Chains (Ethereum, Polygon, Arbitrum, Base):** A standard Solidity contract (mapping(bytes32 => address)). Its security is well-understood, benefiting from extensive formal verification and auditing within the Ethereum ecosystem.
- **Solana:** A Rust-based program utilizing Program-Derived Addresses (PDAs). A PDA is derived from the Nominal program ID and the UTF-8 encoded name, creating a deterministic on-chain account to store the owner's public key. This leverages Solana's account model for efficient, parallelizable lookups.
- **Sui & Aptos (MoveVM):** A Move module where each registered name is a distinct, owned object. The global immutability and ownership semantics of the Move language provide robust guarantees that a name cannot be duplicated or improperly transferred, enforcing ownership at the virtual machine level.

- **NEAR Protocol:** A Rust or AssemblyScript-based smart contract that interfaces with NEAR's native account model. It manages a distinct sub-account namespace (e.g., alice.nominal.near), providing a global resolution layer on top of NEAR's existing human-readable account system. In this case, the protocol moves near forward by ensuring users from other protocols can easily onboard to Near.

The key design principle is that no contract has special authority over another. Each is a sovereign registry for its respective chain. Global consistency is an emergent property achieved at the client layer.

2.2 Permitted Name Registration and update

Smart contracts of Nominal on each chain should allow users to permit wallet providers to register for them. This simply could mean wallets referring users to Nominal protocol. In that case the revenue generated from the name registration will be shared with the providers.

2.3 Pay once

Nominal allows one name on different chains and eases payment processing for wallets and removes annual payment.

3. The SDK as a Decentralized Resolution and Propagation Layer

The core logic of the Nominal protocol resides within the client-side SDK, which must be integrated directly by wallet providers. This SDK is not merely a convenience wrapper; it is an active component of the protocol responsible for state discovery, verification, and propagation.

The Resolution & Propagation Process:

1. **Initiation:** A user, controlling a nominal name via their Ethereum wallet, decides to link this name to their Solana address.
2. **Authorization:** Within their wallet's UI, the user signs a message conforming to a standardized specification (e.g., a variant of EIP-712 for cross-chain purposes). This message explicitly states the intent: UPDATE name ON chain='solana' TO address='sol_address'. The message is signed using the user's Ethereum private key, which is the current "owner" of the name.
3. **Client-Side Propagation:** The Nominal SDK within the wallet receives this signed authorization. It then performs the following actions:
    - It constructs a valid transaction for the Solana network.
    - The transaction's instruction data includes the UPDATE operation, the target name, and the signed authorization message from Ethereum.
    - The SDK submits this transaction to the Solana network, and the user pays the requisite gas fees in SOL.
4. **On-Chain Verification:** The Nominal program on Solana receives this transaction. Its logic is simple:
    - It verifies the signature in the authorization message against the public key of the current owner of nominal name as registered *on the Solana contract*.

- If the signature is valid, the update is committed. This creates a cryptographically-verifiable link between the two chains, initiated and paid for by the user, without any intermediary.

This "user-as-relayer" model is fundamental. It is more secure because it never requires a user's keys or assets to be entrusted to a third-party bridge. It is also more robust, as it has no central point of failure.

Conflict Resolution: In the case of near-simultaneous updates on different chains, the protocol defaults to a "last-write-wins" mechanism, determined by the block timestamp on the target chain. Each registry entry stores not only the address but also the timestamp of its last update. Wallets can implement UI safeguards, such as warning users if a name has been updated on another chain very recently, to prevent unintentional overwrites.

4. The Mathematical Framework

To combat name squatting and provide users with a quantifiable measure of a name's legitimacy, we introduce a reputational authority score. This score is not an on-chain token or NFT but a metric computed off-chain by the SDK, derived entirely from public, on-chain data. This avoids the complexity and gas costs of maintaining an on-chain scoring system.

We define the Authority Score (A) for a given name as a weighted sum of several factors:

$$A = w_1T + w_2V + w_3C$$

Where:

- **T (Temporal Weight):** Measures the continuous ownership duration of a name. It is a logarithmic function of time to reward longevity while having diminishing returns.
  - $T = \log_{10}(current\_block\_timestamp - registration\_timestamp)$
  - This factor makes it economically infeasible for squatters to maintain high-authority scores on a large number of names over time.
- **V (Volumetric Weight):** Quantifies the economic activity associated with the name. It is defined as the sum of normalized transaction volumes directed to the name's resolved addresses across all chains over a given period.
  - $V = \Sigma_i\ (transactions\_chain_i) / time\_period$
  - This metric serves as a proxy for the name's utility and adoption.
- **C (Connectivity Weight):** Represents the breadth of the name's integration across the multi-chain ecosystem.
  - $C = (\text{number of chains the name is actively linked on})^2$
  - The score is squared to provide an exponential incentive for users to establish a consistent identity across multiple networks, strengthening the network effect of the protocol.

The weights (w_1, w_2, w_3) are protocol parameters that can be initially set and later adjusted through a future governance mechanism. The SDK is responsible for querying the necessary on-chain data, computing this score, and presenting it within the wallet's UI, perhaps as a trust badge or verification indicator. This provides a powerful, data-driven heuristic for users to assess the legitimacy of a name before interacting with it.

5. Implications for Wallet Integration and Ecosystem Economics

This protocol necessitates a deeper level of integration than simple name resolution. By embedding the Nominal SDK, wallets evolve from passive key managers into active nodes in a decentralized interoperability network.

- **UI Mandates:** Integrating wallets must adapt their user interface to handle cross-chain authorization signing, display the Authority Score (A), and manage name registrations across multiple blockchains.
- **Economic Alignment:** The protocol is designed to facilitate a direct economic relationship between the protocol and the integrating wallets. The smart contract simply includes function with signature permission from user wallets that allow a portion of the registration fee (paid on any chain) to be programmatically directed to the wallet provider that facilitated the transaction. This creates a powerful incentive for adoption, aligning the growth of the protocol with the commercial interests of its key integration partners. It transforms wallets from mere infrastructure providers into value-added participants in the naming economy.

5. Token Payments

For traditional naming protocols, mostly fees can only be paid with native tokens like ETH. Nominal will allow payments in USDC, USDT, and other user familiar tokens on any chain. This moves crypto forward to a new era.

7. Conclusion

The fragmentation of user identity across a multi-chain landscape, coupled with the inherent operational risks of cryptographic addresses, presents a significant barrier to the maturation and mainstream adoption of blockchain technology. This paper has formally defined this problem and introduced the Nominal Resolution Protocol as a novel and comprehensive solution.

By rejecting the prevailing paradigm of trust-based, intermediary-dependent cross-chain bridges, our protocol establishes a more secure and decentralized model for universal identity. The core innovation—a client-side SDK that empowers the user to directly orchestrate state propagation across heterogeneous virtual machines—eliminates systemic bridge risk and places cryptographic sovereignty firmly in the hands of the individual. The on-chain components are minimalist, secure, and VM-native, serving as sovereign registries that are globally synchronized through the user-as-relayer mechanism.

Furthermore, the protocol introduces a sustainable economic model that eschews the rent-seeking, renewal-based fees of legacy naming systems in favor of perpetual ownership. By facilitating an economic alignment with wallet integrators and accepting stablecoin payments, the protocol is designed for rapid, ecosystem-wide adoption. The mathematical framework for a Sybil-resistant

Authority Score provides a critical, data-driven layer of trust and legitimacy, addressing the challenges of name squatting and user security.

In synthesis, the Nominal Resolution Protocol represents a significant scientific advancement. It provides a viable, trust-minimized, and economically sound framework for a unified digital identity layer, effectively resolving the paradox of multi-chain complexity and paving the way for a more interoperable, secure, and user-centric decentralized web.

7. Further Research

The Nominal Resolution Protocol establishes a foundational layer for universal identity; however, its architecture opens several avenues for future research and enhancement.

1. **Zero-Knowledge Privacy Integration:** The current protocol operates on public state, meaning name-to-address mappings are transparent. Future work should explore the integration of zero-knowledge proofs (e.g., zk-SNARKs) to enable private resolution. A user could prove ownership of a name and authorize an update or resolve an address without revealing the link on-chain, creating a "ZK-Nominal" layer for privacy-preserving transactions.
2. **Decentralized Governance of Protocol Parameters:** The weights (w_1, w_2, w_3) in the Authority Score framework are critical protocol parameters. While initially set, their long-term management should be decentralized. Research into novel, multi-chain governance mechanisms is needed to allow stakeholders to securely vote on parameter adjustments across all supported networks without creating a central point of control.
3. **Scalability of Off-Chain Data Resolution:** The SDK's performance depends on its ability to efficiently query data from multiple blockchains to calculate the Authority Score. As the number of supported chains and registered names grows, research into scalable and decentralized indexing solutions is required to prevent the SDK from becoming a performance bottleneck, ensuring that resolution remains instantaneous for the end-user.
4. **Formal Verification of the Cross-Chain Interaction Model:** While the individual on-chain contracts can be formally verified, a more complex challenge is the formal verification of the entire protocol's state consistency model. This would involve creating a formal model of the "user-as-relayer" mechanism and proving its security properties, such as resistance to race conditions and replay attacks across asynchronous, heterogeneous networks.

8. References

1. Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf
2. Wood, G. (2014). *Ethereum: A Secure Decentralised Generalised Transaction Ledger*. Ethereum Project Yellow Paper.

3. Ethereum Improvement Proposals. (2017). *EIP-712: Typed structured data hashing and signing*. https://eips.ethereum.org/EIPS/eip-712
4. Yakovenko, A. (2017). *Solana: A new architecture for a high-performance blockchain*. https://solana.com/solana-whitepaper.pdf
5. Blackshear, S., et al. (2019). *Move: A Language With Programmable Resources*. Meta. https://developers.diem.com/papers/diem-move-a-language-with-programmable-resources/2020-05-26.pdf
6. The NEAR Protocol. (2019). *NEAR Protocol: A sharded, developer-friendly, proof-of-stake public blockchain*. https://near.org/papers/the-official-near-white-paper/
7. Chainalysis. (2024). *The 2024 Crypto Crime Report*. This report provides extensive data on fund movements, including analysis of scams such as address poisoning which exploit user inattention to complex addresses, substantiating the general risk of address-based errors.
8. The Block. (2024, May 8). *Crypto trader loses $26 million in ezETH in apparent address poisoning scam*. This article documents a specific, high-value case study of asset loss resulting from address complexity and user error.
9. Cointelegraph. (2024, May 8). *'I feel my life is over': User loses $26M in WBTC to address poisoning*. Further reporting and community reaction to the significant asset loss event, highlighting the severity and irreversible nature of such mistakes.