

Whitepaper: nome.social (English)

Title: nome.social: A Sovereign Identity Protocol for Brazil on the ENSv2 Stack

Version: 1.0 | September 26, 2025

Abstract

nome.social is an open-source protocol designed to establish a sovereign, Sybil-resistant identity layer for Brazil, built on Ethereum. The protocol leverages two key infrastructures: Brazil's PIX instant payment system for a unique Proof of Humanity (PoH) mechanism, and the emerging ENSv2 stack (NameHash Labs) for decentralized, on-chain naming and identity. The core output for a verified user is a Hybrid Citizenship Kit: a non-transferable on-chain attestation (via EAS) certifying their uniqueness, and an associated ENS subdomain (user.nomes.eth). The protocol aims to provide a foundational public good for the Brazilian Web3 ecosystem.

1. Thesis: Integration over Extraction

The central thesis of nome.social is that a scalable identity system for Brazil should not rely on the extraction of sensitive biometric data. Instead, it should integrate with existing, trusted national infrastructure. We leverage the PIX system, used by over 160 million Brazilians, to validate identity. A state-changing R\$ 0.01 micro-transaction allows the protocol to verify a user's unique fiscal ID (CPF) in a private, low-cost, and sovereign manner.

2. Core Architecture: An Application on Shared Infrastructure

nome.social is designed as a best-in-class application, not as a new, low-level infrastructure. We build upon the professional, open-source ENSv2 stack to de-risk execution and focus on our core innovation.

- **On-Chain Identity:** User verification is registered as an on-chain attestation using the **Ethereum Attestation Service (EAS)**. This ensures interoperability and adherence to open standards, rather than creating a proprietary SBT.
- **Decentralized Naming:** Subdomains under .nomes.eth are managed via smart contracts built with **NameKit** and interacted with via the **ENS.node** API. This aligns the protocol with the future of ENS scalability (Namechain).
- **User Security:** The registration flow will integrate **NameGuard** to protect users from malicious or confusing names.
- **User Onboarding:** The user-facing application will utilize an open-source Account Abstraction stack, such as **Openfort**, to provide a seamless, gasless experience for users new to Web3.

3. Protocol Mechanics

The protocol operates a "freemium" model designed to maximize adoption while ensuring sustainability.

- **Verification:** Any Brazilian citizen can undergo the PIX verification to receive their on-chain attestation.
- **Subdomain Issuance:** A verified identity is eligible to register one 5+ character .nomes.eth subdomain, free for the first year.
- **Sustainability Model:** The protocol's treasury, governed by the future BrazilDAO, is funded by:
 1. The sale of premium subdomains (fewer than 5 characters).
 2. The sale of any additional subdomains to verified users.
 3. Annual renewal fees for all subdomains.

4. Roadmap

The development is phased to prioritize security and validation.

- **Phase 1 (MVP):** A functional prototype on the Base testnet, demonstrating the full PIX-to-EAS-attestation and ENS subdomain registration flow. This will be presented at the ETHLatam Hackathon (Nov 2025).
- **Phase 2 (Security & Launch):** A full, independent security audit of all custom smart contracts and backend logic, followed by a mainnet launch (Namechain).
- **Phase 3 (Decentralization):** Establishment of the BrazilDAO to assume governance and control over the protocol's treasury and key contracts.

Whitepaper: nome.social (Português)

Título: nome.social: Um Protocolo de Identidade Soberana para o Brasil no Stack ENSv2

Versão: 1.0 | 26 de Setembro de 2025

Resumo (Abstract)

O nome.social é um protocolo de código aberto projetado para estabelecer uma camada de identidade soberana e resistente a ataques Sybil para o Brasil, construído sobre a Ethereum. O protocolo alavanca duas infraestruturas chave: o sistema de pagamentos instantâneos do Brasil, o PIX, para um mecanismo único de Prova de Humanidade (PoH), e o emergente stack ENSv2 (NameHash Labs) para nomes e identidade on-chain descentralizada. O resultado principal para um usuário verificado é um Kit de Cidadania Híbrida: uma atestação on-chain intransferível (via EAS) certificando sua unicidade, e um subdomínio ENS associado (usuario.nomes.eth). O protocolo visa fornecer um bem público fundamental para o ecossistema Web3 brasileiro.

1. Tese: Integração em Vez de Extração

A tese central do nome.social é que um sistema de identidade escalável para o Brasil não deve depender da extração de dados biométricos sensíveis. Em vez disso, deve se integrar com a infraestrutura nacional, existente e confiável. Alavancamos o sistema PIX, usado por mais de 160 milhões de brasileiros, para validar a identidade. Uma microtransação de R\$ 0,01 que altera o estado permite ao protocolo verificar a identidade fiscal única de um usuário (CPF) de forma privada, de baixo custo e soberana.

2. Arquitetura Central: Uma Aplicação sobre Infraestrutura Compartilhada

O nome.social é projetado como uma aplicação de ponta, não como uma nova infraestrutura de baixo nível. Construímos sobre o stack profissional e de código aberto da ENSv2 para mitigar riscos de execução e focar em nossa inovação principal.

- **Identidade On-Chain:** A verificação do usuário é registrada como uma atestação on-chain usando o **Ethereum Attestation Service (EAS)**. Isso garante interoperabilidade e aderência a padrões abertos, em vez de criar um SBT proprietário.
- **Nomes Descentralizados:** Os subdomínios sob .nomes.eth são gerenciados via smart contracts construídos com o **NameKit** e interagimos com eles através da API do **ENS.node**. Isso alinha o protocolo com o futuro da escalabilidade da ENS (Namechain).
- **Segurança do Usuário:** O fluxo de registro integrará o **NameGuard** para proteger os usuários de nomes maliciosos ou confusos.
- **Onboarding do Usuário:** A aplicação voltada para o usuário utilizará uma stack de Abstração de Conta de código aberto, como o **Openfort**, para fornecer uma experiência fluida e sem gas para usuários novos na Web3.

3. Mecânicas do Protocolo

O protocolo opera um modelo "freemium" projetado para maximizar a adoção e garantir a sustentabilidade.

- **Verificação:** Qualquer cidadão brasileiro pode passar pela verificação via PIX para receber sua atestação on-chain.
- **Emissão de Subdomínio:** Uma identidade verificada é elegível para registrar um subdomínio .nomes.eth de 5+ caracteres, gratuito pelo primeiro ano.
- **Modelo de Sustentabilidade:** O tesouro do protocolo, governado pela futura BrazilDAO, é financiado por:
 1. Venda de subdomínios premium (menos de 5 caracteres).
 2. Venda de quaisquer subdomínios adicionais a usuários verificados.
 3. Taxas de renovação anuais para todos os subdomínios.

4. Roadmap

O desenvolvimento é faseado para priorizar segurança e validação.

- **Fase 1 (MVP):** Um protótipo funcional na testnet da Base, demonstrando o fluxo completo de verificação PIX para atestação EAS e registro de subdomínio ENS. Será apresentado no Hackathon ETHLatam (Nov 2025).
- **Fase 2 (Segurança e Lançamento):** Uma auditoria de segurança completa e independente de todos os contratos e lógicas de backend, seguida pelo lançamento em mainnet (Namechain).
- **Fase 3 (Descentralização):** Estabelecimento da BrazilDAO para assumir a governança e o controle do tesouro e dos contratos chave do protocolo.