HMN Whitepaper

hmn.is

January 4, 2025

Abstract

HMN contracts provide a decentralised, human-verified on-chain financial system where each participant can be trusted to be a unique human. The HMN token contracts serve as an immutable, trustless cross-chain token that encourages anonymous humanity verification with World ID, resist Sybil attacks, and support account recovery. The non-upgradeable HMN token is supported by management contracts that serve as a delayed-upgradeable human verification registry, achieving a balance between long-term trustlessness and adaptivity.

1 Introduction

The HMN contracts form a foundational layer for a decentralised financial system where each participant can stay anonymous, but still be trusted as a unique, verified human. The HMN contracts and token are part of the hmn.is verification and certificate service. The token initially serves as a reward token for social media account verification. Its main purpose, however, is to serve as the first step towards a Mutually Exclusive and Collectively Exhaustive (MECE) financial system that will eventually cover all asset, agent, and resource classes, including externalities. In this first step, the goal is to ensure that each human has exactly one set of verified accounts, thereby eliminating multi-account exploitations with bots and fake accounts, and enabling trust and enforcement of fairness.

The hmn.is ecosystem builds on the World ID system that combines iris and facial recognition with zero-knowledge proofs to anonymously verify the humanness of participants. The HMN contracts provide an on-chain cross-chain registry of verified human accounts. This unique-human mapping unlocks a range of possibilities, from recovery of lost accounts, and Sybil-resistant reward systems, all the way to universal income funded eg. by bot transfer taxation.

The contracts are divided into two parts: the immutable HMN token contracts are designed for trustlessness and operate largely independently of the manager registry, ensuring guaranteed market functionality and safety with minimal attack surfaces. The delay-upgradeable manager contracts, on the other hand, are designed for minimised trust while still being flexible and future-proof, allowing new verification schemes and extension to other blockchains.

2 HMN Token Contracts

The HMN ERC-20 token is digital currency designed to encourage and enforce ownership by unique, verified humans, while operating trustlessly across multiple blockchains.

2.1 Token Distribution

The HMN token has a fixed total supply of 8,200,000,000 tokens – one for every human. The distribution is designed to support network growth and provide fair and wide holder distribution to early adopters:

- **Rewards - 50%:** Half of the tokens are allocated for verification reward programs, including up to 20% for an initial 2025 rewards program.
- **Initial Supply - 30%:** Approximately a third of all tokens will be included in initial supply, with 24% distributed through a fair, 'bonding curve' inspired pricing. Liquidity provider tokens are time-locked into a safe contract, allowing fee collection but preventing sudden liquidity removal.
- **Community Growth - 10%:** Allocated for ecosystem development, including up to 5% airdrop to active OP Superchain addresses shortly after launch.
- **Team Incentives - 10%:** Reserved for future team incentive programs with 4-year vesting periods, secured in time-locked contracts until program initiation.

The 'bonding curve' distribution mechanism aims to create a fair and wide token allocation among early participants. The substantial 30% initial supply ensures adequate market liquidity at launch to avoid spikes and volatility. It also serves as a hefty counterweight for limiting the dilution of the initial 2025 rewards program.

In effect, the token distribution creates a system that finances network growth with controlled, manageable dilution via reward programs carefully designed for significant and relevant user and follower growth.

2.2 Token Features

Its core features include:

- **ERC-20 compliance:** Compatibility across the Ethereum ecosystem and beyond.
- **Non-upgradeable design:** The HMN token has a fixed supply of 8,200,000,000 tokens and limits owner abilities to one-way feature enabling operations.
- **Limited attack surface:** Minimal token-side functionality and re-entry guards for critical features make the HMN token contract secure with minimal attack surface.
- **Cross-chain bridging:** Built-in mechanisms support bridging HMN tokens to OP Superchain and Arbitrum, maintaining consistent functionality and trust models across L2s (and beyond).
- **Derived standards:** ERC-1363 (transfer-and-call) and ERC-20 Permit (gasless approvals) extensions enhance user experience with latest capabilities.
- **Opt-in account recovery:** Users may enable recovery features, allowing a designated key or human verification proof to regain control if keys are lost. Recovery is optional and trustlessly behind explicit user request.
- **Future proofed for human verification:** While disabled at launch, the token has built-in functionality for imposing bot-transfer fees and/or blocking unverified or bot-labeled addresses. Verified human accounts remain unaffected.

- **Shared secondary chain and specialized Mainnet functionality:**
  - `HmnBase` implements shared, chain-agnostic transfer verification logic.
  - `HmnMain` implements the master Ethereum Mainnet token, providing account recovery and token bridging configuration.
- **Trustlessness and independence:** HMN token contracts cooperate with the `HmnManager`, but retain independence by
  - ensuring guaranteed tradability with permanent whitelists,
  - enforcing a maximum unverified account / bot transfer fee of 1%, and by
  - providing a future possibility for totally opting out from the manager's verification services by opting to pay the fee.

Transfer verification logic is tested at launch and disabled shortly after, allowing HMN to function like a standard ERC-20 token, while learning and expanding its network of trusted contracts. Over time, upon community-driven decisions, transfer taxes or controls can be activated and tuned to enforce the human verification guarantee and disincentivise bot usage.

3 HMN Manager Contracts

The `HmnManager`, `HmnManagerImplBase` and `HmnManagerImplMainLogicV1` contracts orchestrate on-chain human verification, registry management, trusted contract whitelists, and adjustable transfer taxation and restrictions. The upgradeability functionality is delayed by `OwnerUpgradeableImplWithDelay`, giving users time to respond to proposed changes. The upgrade delay is initially set to 7 days, and will be increased to 30 days after the contracts are deemed stable, providing users ample time to respond to proposed changes.

3.1 Features and Capabilities

Key aspects include:

- **Delayed upgradability:** A standard (UUPS, ERC-1967) proxy upgrade pattern with a mandatory delay allows users to exit if malicious upgrades are attempted by compromised governance.
- **Cross-chain verification registry:** The managers maintain a universal registry of verified human account addresses that are synced across a growing number of bridged chains.
- **Support for diverse chain formats:** With a datamodel supporting multiple chains and longer address formats, the manager can accommodate future blockchains with differing address lengths.
- **On-chain World ID orb verification:** World ID's secure and anonymous zero-knowledge proofs prevent Sybil attacks and ensures each human can hold only one verified account (or, in the future, a linked set of accounts).
- **Off-chain device verification:** As an onboarding feature, device-based verification (which is not supported on-chain by World ID) may be signed by a trusted server, enabling user acquisition without World ID Orb verification.

- **Account recovery:** If explicitly configured by the user via the immutable token contract, the manager authenticates secure account recovery after a safety period.

- **Account migration:** Users can migrate their account and HMN funds to a new wallet address.

- **Transfer tax and control modes:** While initially off, transfer tax or restrictions can be activated by the governing community to favor humans and encourage participation by imposing up to 1% tax on unverified transfers, or by limiting transactions completely to verified humans and trusted contracts.

- **Network expansion with trusted pioneers:** A pioneering mode empowers a core set of trusted pioneer users to dynamically grow the network's registry of trusted contracts, while the manager tracks their work and allows for error correction.

- **Shared secondary chain and specialized Mainnet functionality:**

  - `HmnManagerImplBase` implements generic, chain-agnostic registry and transfer verification logic.
  - `HmnManagerImplMainLogicV1` provides human verification, registry management, account migration & recovery, and verification state broadcasting to other chains.

3.2 Cross-Chain Bridging and Future Prospects

HMN's bridging contracts propagate registry updates and trust lists to L2s and other chains. As users verify their humanness on Ethereum Mainnet, their verified status propagates globally, ensuring a consistent trust model throughout multiple ecosystems. This approach allows HMN tokens and human verification capabilities to extend outside Ethereum, and provide human verification capabilities to chains not directly supported by World ID.

Over time, the HMN ecosystem can expand to cover all chains and asset classes, reinforcing guarantees that each participant is a singular, verified human, and advancing the MECE vision of a fair and inclusive global economic system.

4 Conclusion

The HMN token and its manager contracts establish a blueprint for a decentralised financial system grounded in strong identity guarantees. By combining standard ERC-20 functionality, on-chain verification via World ID, bridging to L2s and beyond, and experimenting with fee/tax models for unverified participants, HMN builds towards a fairer financial system of trusted participants.

The system's architecture, featuring non-upgradeable token contracts coupled with delayed-upgradeable managers, strikes a balance between trustless robustness and flexibility. As adoption grows, HMN's approach to verification-based trust and resource management has the potential to reduce fraud, improve fairness, and eventually provide a foundation for a more equitable global economic system.