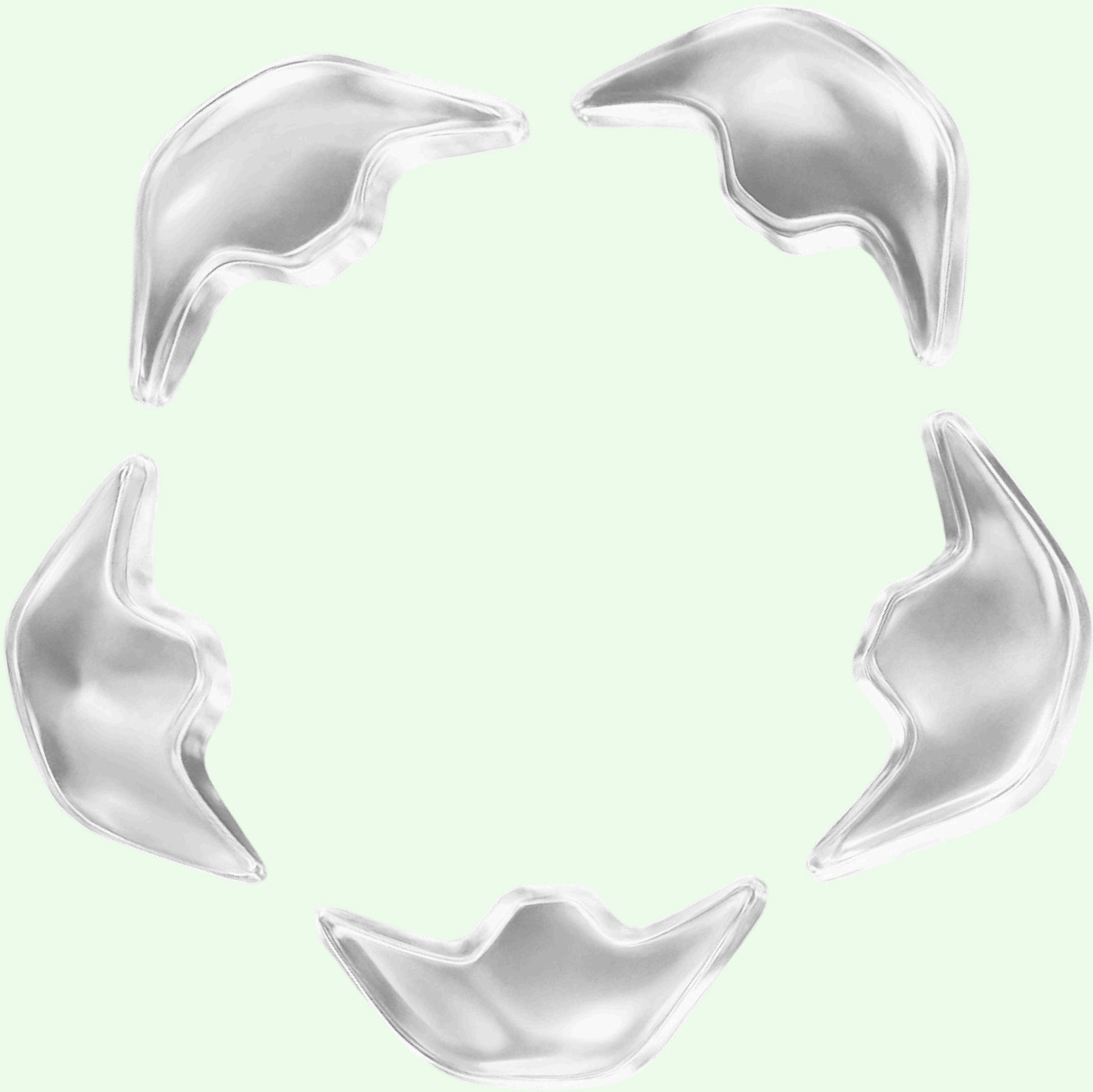
humanity



2026

What is Humanity?

The internet was originally designed as a global network that let computers exchange information.

As the internet evolved, it unlocked unprecedented access to information, global communication, digital commerce, and entire online economies. But one thing never changed:

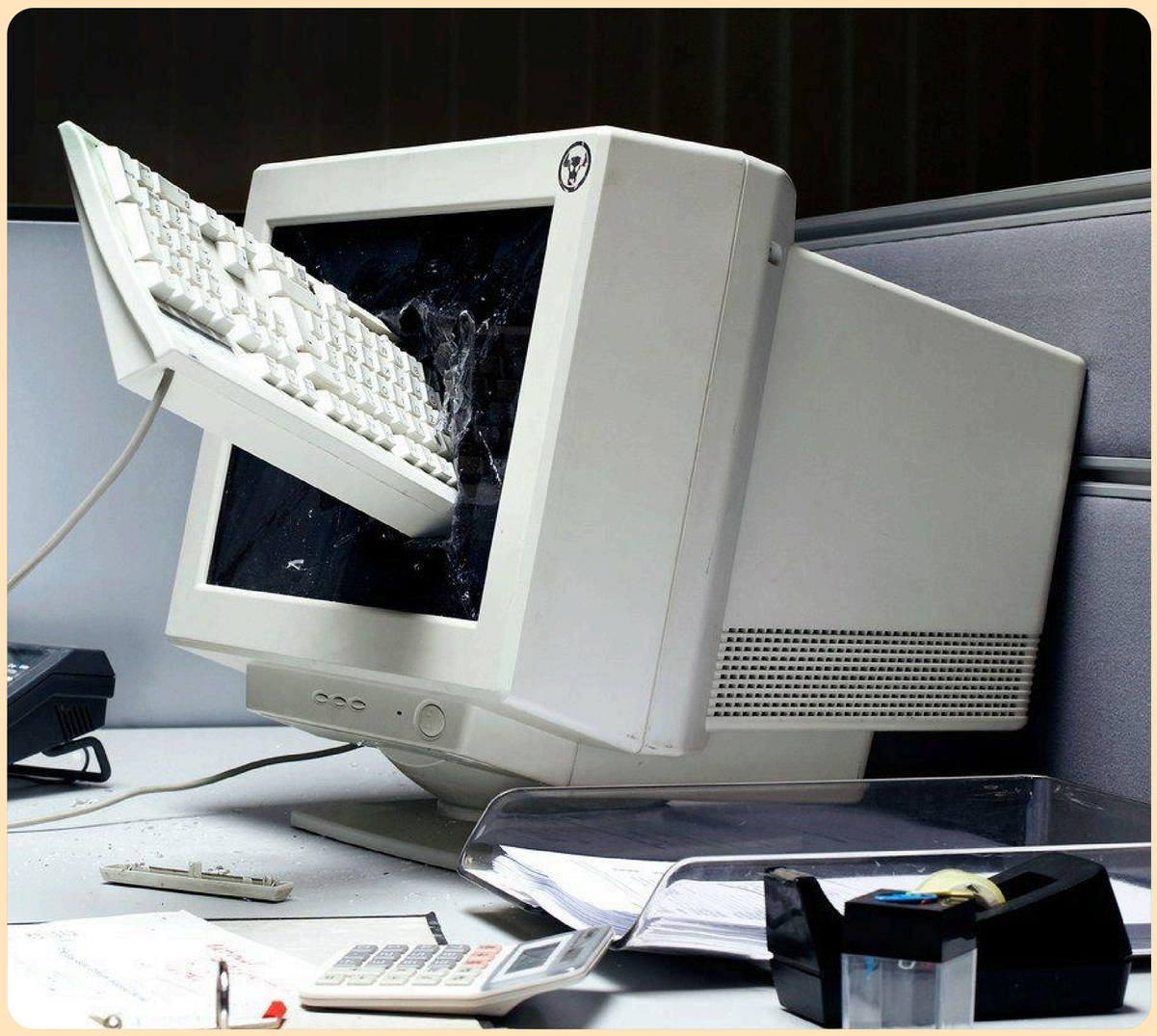
It has no native concept of trust.

Anyone can create an account, claim an identity, or interact with others — all without the network knowing who they are or verifying the truth behind the information they are disseminating. This anonymity enabled creativity, free expression, and openness, but it also created deep structural flaws where trust is concerned.

The result is a digital world where trust is always bolted on from the outside, never built in. Platforms individually try to solve this via CAPTCHAs, KYC, 2FA, and more, but none of these methods prove that a user is a real, unique human or that the information they're sharing about themselves is true. And every centralized solution introduces new risks: privacy leakage, data breaches, surveillance, exclusion, and platform-level control.

Its architecture focused on connecting machines, servers, and data packets, not on verifying the people behind them.

Humanity is a cross-platform trust solution that aims to rebuild the internet's missing trust layer, proving personal claims through cryptography instead of data collection. It gives every user a portable, privacy-preserving identity they control, and gives every app a way to verify trust without ever seeing personal information. In doing so, Humanity Protocol turns "trust" from an add-on into a native, universal primitive: available anywhere, interoperable across platforms, and safe by design.



At the time of its creation, the network primarily served institutions and research bodies, making identity verification an unnecessary consideration.

0.2 / Challenge

The web was originally designed in the 80s to connect information systems, not to verify or authenticate the people interacting within them.

Participants transact, communicate, and create within environments where there is no universal mechanism to determine the authenticity of entities—whether human, synthetic, or automated.

This absence of verifiable human identity has produced systemic vulnerabilities. It has facilitated widespread fraud, misinformation, and data breaches, even among highly regulated or technologically advanced organizations.

As artificial intelligence continues to scale and synthetic entities become increasingly indistinguishable from real users, this architectural flaw poses a growing systemic risk to digital ecosystems.

Over USD

1 trillion

lost annually to scams and online fraud

Over USD

200 billion

spent on compliance activities such as Know Your Customer (KYC) and Anti-Money Laundering (AML) processes

Significant economic waste due to bot-generated traffic, synthetic identities, and spam with bad bots accounting for up to

up to 73%

of internet traffic.

Further losses in productivity, user trust, and institutional reputation

Across all major sectors, finance, governance, commerce, media, and beyond, trust remains the implicit foundation of digital interaction.

However, in the absence of a verifiable and privacy-preserving trust infrastructure, that foundation is increasingly unsustainable.

0.4 /

What is Humanity?

Humanity is the Trust Layer of the internet. It enables users to prove any facts about themselves with portable and private credentials. Through Humanity’s Proof-of-Trust network, anyone can verify identity, eligibility, or access without revealing private data. It replaces assumptions with credentials, creating a safer, more trusted digital world.

These credentials can represent facts like:

“I’m a unique human.”

“I passed KYC with a regulated issuer.”
“I’m over 21 in this country.”
“This wallet’s balance is ≥ X.”

We start with identity, KYC, and financial trust, unique humans, compliant onboarding, and eligibility for payments and assets, and we can extend to many other facts over time. Users keep control of their data; enterprises get better signals, lower fraud, and better performance.

Existing Proof-of-Personhood technologies are either dystopian, privacy-invasive, or both. Humanity is building an ecosystem that truly drives decentralization, identity ownership, equity, and inclusion. At the heart of HP is the Proof-of-Humanity (PoH) mechanism. PoH is the world's first scalable and decentralized solution to the unique human problem.

The goal of PoH was not to assess "who you are", but merely to confirm that "you are a unique human being" (Phase 1), and "you are who you say you are" (Phase 2) where PoH is becoming PoT (Proof of Trust).

Use Cases

Financial Services

Credit & lending: Prove creditworthiness or financial history without exposing raw banking data.
Insurance verification: Submit proofs of eligibility (age, residency, income brackets) without sharing sensitive documents.
Anti-fraud in DeFi: Ensure participants are unique humans for fair token distributions, staking, or protocol rewards.

Professional & Academic Verification

Employment history: Share verifiable work experience claims without revealing full records.
Certifications & education: Provide cryptographic proof of degrees, courses, or skills for hiring, upskilling, or professional platforms.
Licensing compliance: Validate professional licenses or certifications in regulated industries.

Social & Community

Verified community membership: Only allow real, unique humans into private groups, social networks, or online forums.
Reputation systems: Build trust scores or histories that are resistant to Sybil attacks or fake reviews.
DAO voting & governance: Ensure fair voting in decentralized organizations without compromising privacy.

Real-World Identity Claims

Age verification: Prove legal age for services like alcohol, cannabis, or adult content access without exposing birthdate.
Residency & citizenship: Verify location or nationality claims for legal or institutional purposes.
Event & venue access: Link PoT credentials to tickets, memberships, or loyalty programs to prevent scalping and fraud.

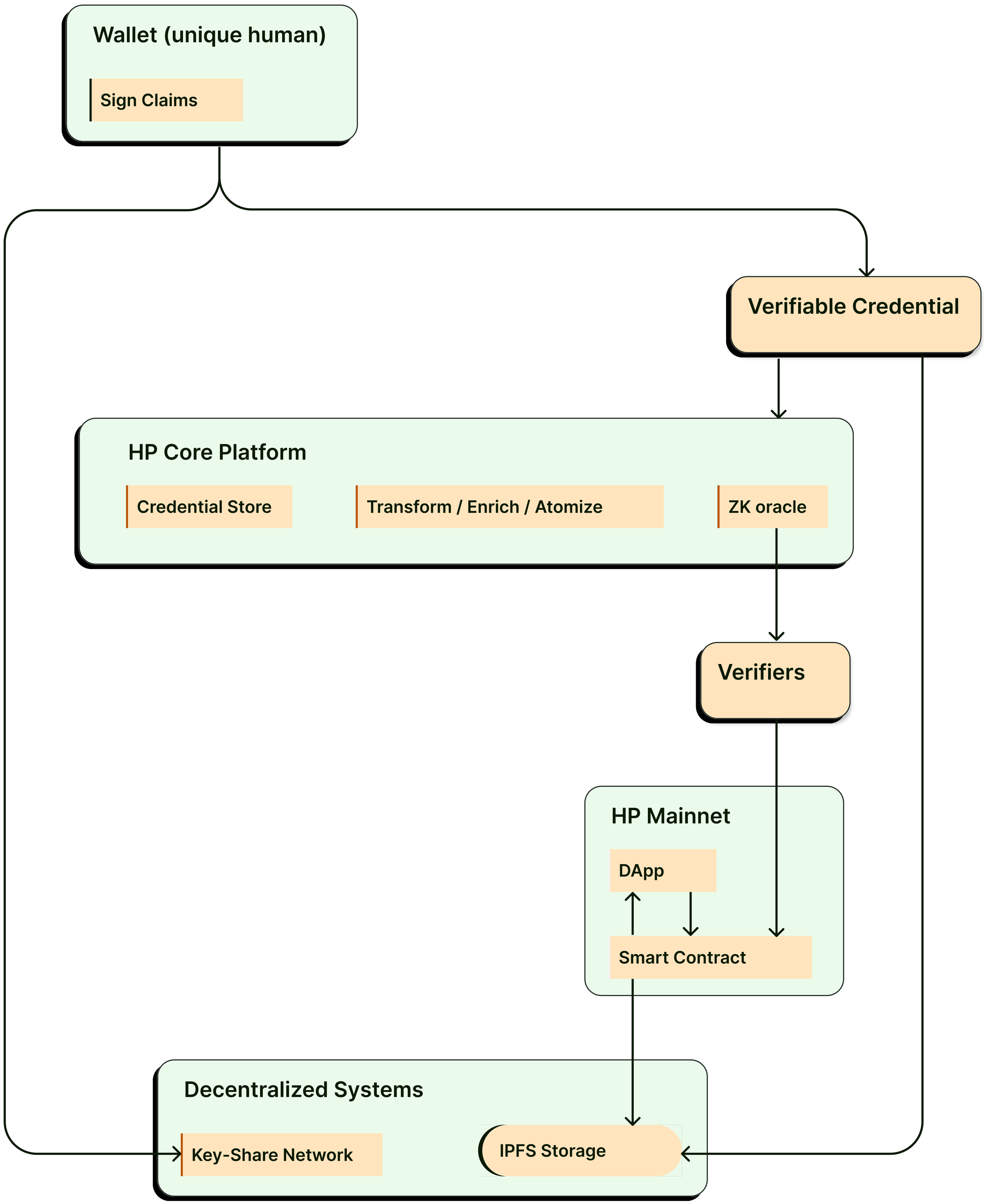
Digital & Physical Asset Trust

NFT & digital asset ownership verification: Prove a human owns or controls an asset before enabling trading, voting, or access to perks.
Payment and subscription validation: Associate identity with payment methods for recurring services without storing sensitive payment info.
IoT device authentication: Ensure devices are operated by verified humans in sensitive or private networks.

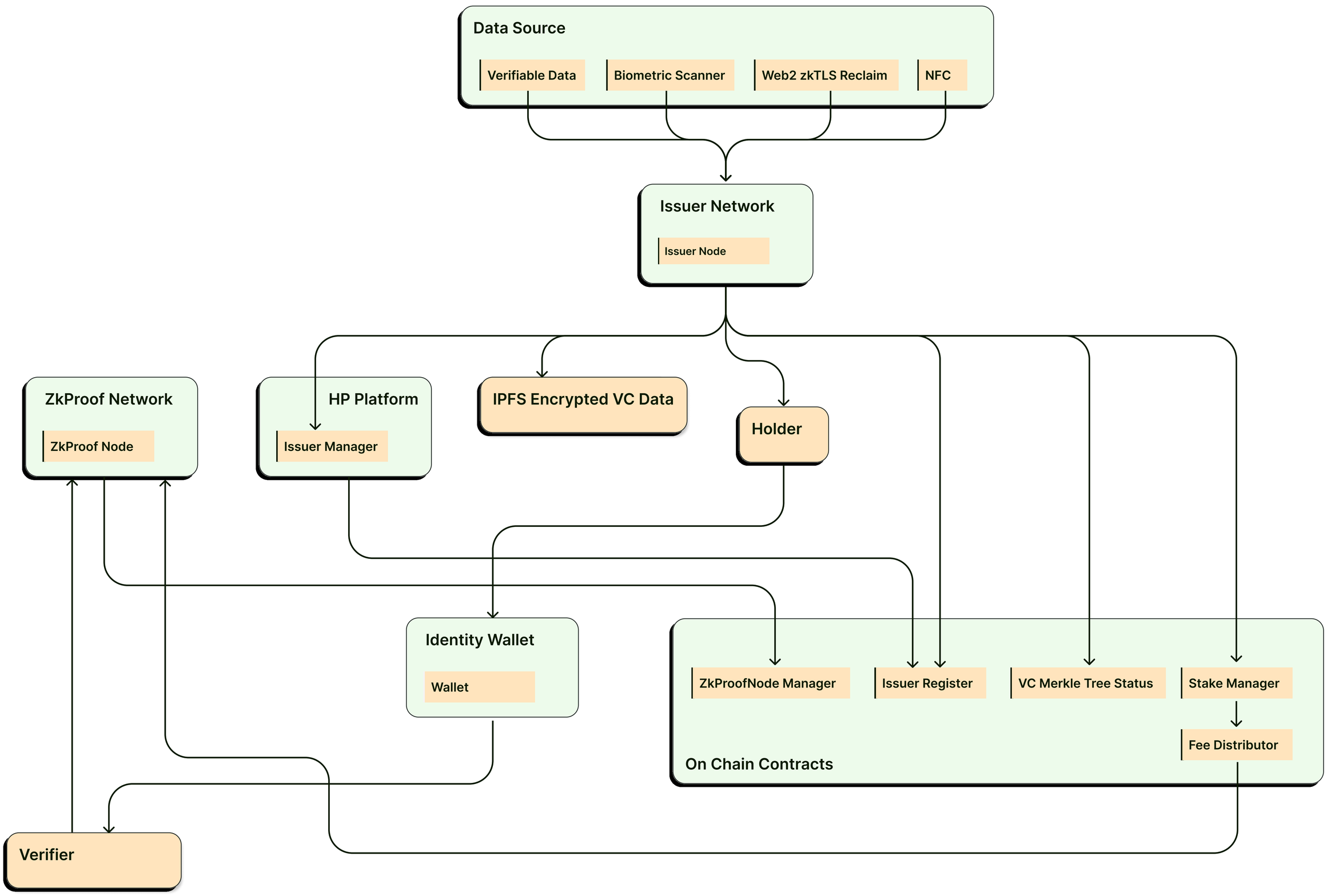
Cross-Platform Interoperability

Universal login & identity: Reuse PoT credentials across apps and platforms without re-verification.
Privacy-respecting credential sharing: Selectively share proofs with different services while retaining full control.

Phase 1:


Wallet (unique human)
Sign Claims
Verifiable Credential
HP Core Platform
Credential Store
Transform / Enrich / Atomize
ZK oracle
Verifiers
HP Mainnet
DApp
Smart Contract
Decentralized Systems
Key-Share Network
IPFS Storage

Phase 2:



What is Proof-of-Trust?

Humanity's Proof-of-Trust leverages non-invasive and inclusive palm recognition, decentralized data storage, zero-knowledge (ZK) proofs, and a self-sovereign identity (SSI) framework.

This provides a foundational layer for verifiable identity and personal information that is both privacy-preserving and tamper-resistant. By combining biometric uniqueness with cryptographic verification, the system enables users to prove their humanity and identity without exposing personal or biometric data.

How we treat datas?

All sensitive information remains under user control. Verifiers receive a defined, user-consented subset of claims in plaintext, such as eligibility or status, together with cryptographic proofs that attest to their authenticity.

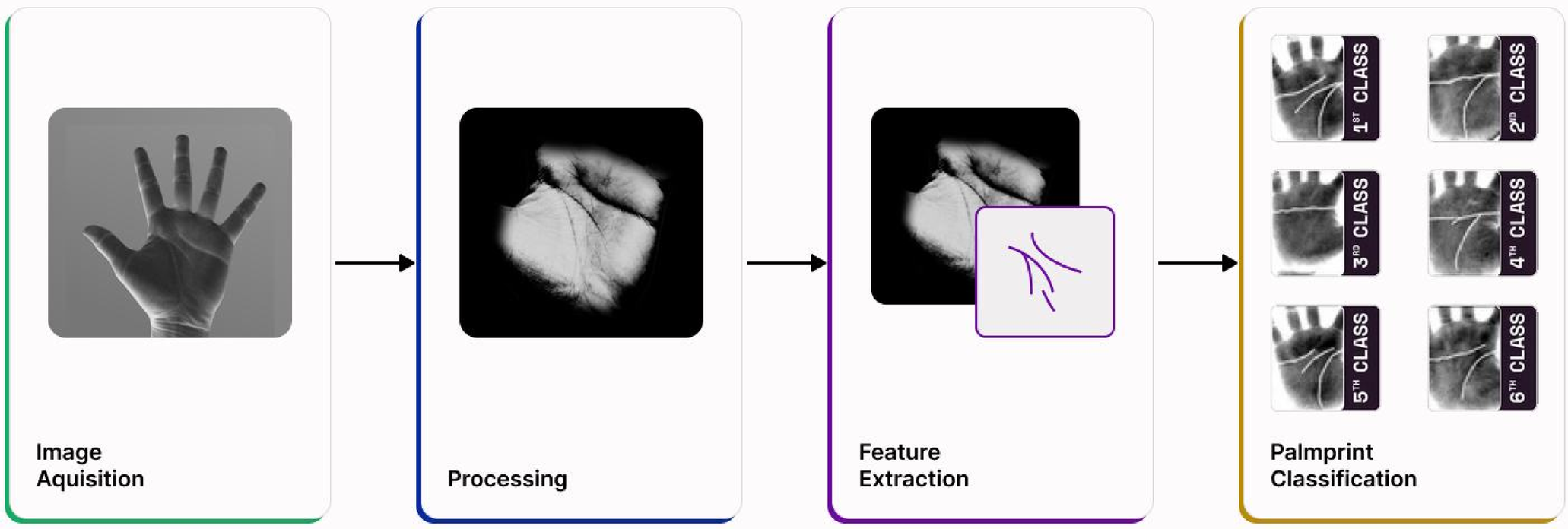
Unlike traditional systems, this access is one-time and scoped, preventing ongoing synchronization or profile tracking.

This architecture establishes the technical basis for a trust infrastructure that can be integrated across digital services, allowing applications, institutions, and networks to confirm authenticity, prevent Sybil attacks, and ensure compliance, all without centralized data custody or surveillance.

One of HP's key innovations is the integration of AI and HP hardware, particularly in the development and deployment of deep learning models for biometric identification.

HP's AI palm recognition algorithm is trained on a diverse dataset of over 500,000 palm print and palm vein features, collected using the easily available HP hardware that works in both visible and infrared light spectra.

The result is a highly accurate and reliable human recognition module that's also cost-effective, inclusive and user-friendly.



The DePIN network empowered by HP hardware, a cornerstone of Humanity's vision, exemplifies the protocol's utility in bridging the on-chain and off-chain worlds.

DePIN facilitates secure, blockchain-verified access to physical infrastructure, enabling a myriad of applications from secure building entry to streamlined hotel check-ins, all authenticated through the Humanity ecosystem.

A verifiable credential is a digital claim related to the subject of the credential — in our context, this is the unique human user.

The type of claims included in VCs can be very broad, but generally include the following:

01

Information related to the status of the VC holder (e.g. human, institution)

02

Information related to the identity of the VC holder (e.g. name, photo)

03

Information related to the issuer of the VC (e.g. HP protocol, government, KYC provider)

04

Information related to the type of VC (e.g. education history, driver's license)

05

Information related to specific attributes or properties being asserted by the issuer about the user (e.g. nationality, the classes of vehicle entitled to drive)

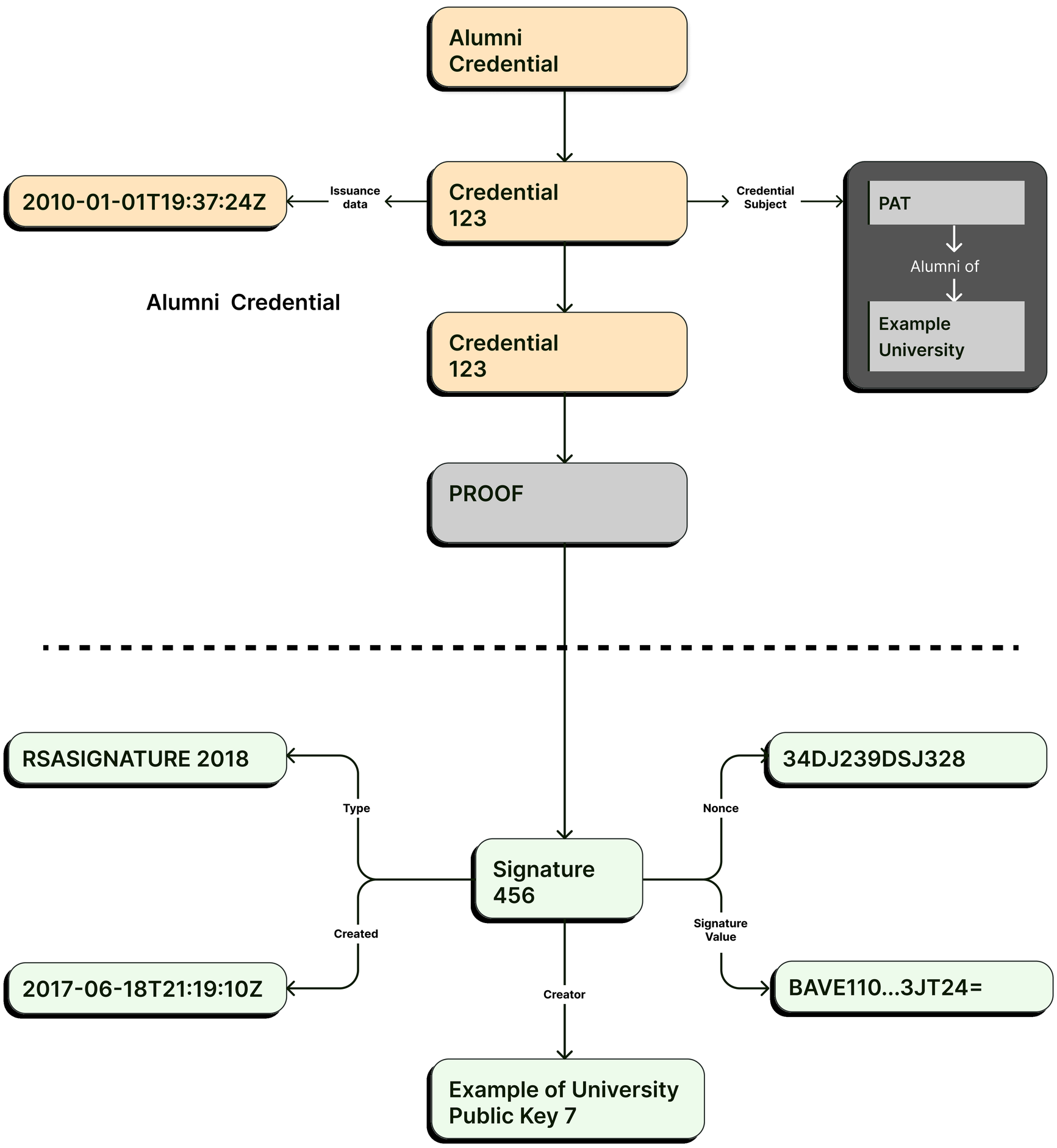
06

Evidence related to how the VCs were derived (e.g. digital signatures and methods)

07

Information related to constraints on the VC (e.g. expiration date, scope)

Compared to their physical counterparts, VCs are more convenient and tamper-resistant because they are cryptographically secured with digital signatures. Once issued, they can also be independently verified via cryptographic proofs, making them ideal for use in the SSI model.



In the HP SSI framework, Identity Validators (Issuers) are the entities that check the private data submitted by users and issue verifiable credentials.

If these data are proven to be valid against the respective claims of the VCs. Identity Validators are considered trusted entities since they are ultimately responsible for the authenticity of the issued VCs (similar to the role of the sequencer in zero-knowledge rollup applications).

In Phase 1:

The Humanity Core

Platform processes biometric inputs (e.g., palm signatures) via the Human Recognition Module.

Unique-human VCs

issued only when the signatures pass uniqueness and validity tests (non-membership proofs in the PoT universe).

The Core Platform

generates zero-knowledge Verifiable Presentations (VPs) for authorized queries from third-party applications.

Identity Validators (Phase 1 → Phase 2 Transition)

Given the Issuers' critical role in attesting to verified user data, a fully permissionless model, where anyone can issue Verifiable Credentials, would pose substantial privacy and trust risks. Accordingly, Humanity begins with a Phase 1 centralized issuance model, where the Humanity Core Platform acts as the sole issuer for unique-human VCs. This controlled setup ensures data accuracy, compliance readiness, and security while the underlying cryptographic and governance mechanisms are fully validated.

However, Phase 1 centralization is strictly temporary. The protocol is designed with a defined and transparent migration pathway toward a partially decentralized issuance network, where accredited Issuers independently validate and issue domain-specific credentials (e.g., education, KYC, employment).

In Phase 2:

Accredited Issuers

A diverse set of accredited Issuers will be selected through staking, governance elections, and institutional verification.

Manage domain-specific credential issuance

(e.g., financial, educational, professional), supported by sharded storage and collaborative ZK proof generation with the Core Platform.

The governance framework

will regulate term limits, revocation procedures, and the continuous evaluation of decentralization metrics.

The Humanity’s Self-Sovereign Identity (SSI) framework is an intricate and vital component of its overarching network, designed to facilitate secure and private transactions.

0.2 /

Within this sophisticated architecture, zkProofer Nodes stand as pivotal entities. These nodes are tasked with the critical function of receiving, processing, and authenticating a variety of verifiable credentials (VCs) or the more privacy-centric Zero-Knowledge Verifiable presentations (VPs).

Their role is indispensable in the network's operations, especially when an authenticated transaction demands the verification of these credentials or presentations, such as during interactions between Users and third-party Decentralized Applications (DApps). zkProofer Nodes operate under stringent privacy considerations. They are deliberately structured to interact with the network without having direct access to unencrypted User metadata.

This design choice serves a dual purpose: it upholds the privacy of the users and, by enabling a broad network of Verifier Nodes, it significantly bolsters the decentralization and community engagement within the Proof of Trust (PoT) verification process. The HP Core Platform, in its commitment to privacy and security, exclusively shares the Zero-Knowledge (ZK) Proofs of VCs and VPs with this network of Verifier Nodes, ensuring that sensitive information remains confidential.

Node Distribution

The node distribution method for HP is crafted to be fully decentralized. Upon launch, the three types of zkProofer Node Licenses - Basic, OG, and Founder -

will be made available through a random draw system, ensuring that every buyer has an equal chance at obtaining the various tiers of zkProofer Nodes.

A maximum total of

100,000 zkProofer Node

will be made available to interested operator

Rewards	Allocation	Reward Share
Basic Nodes	75%	**53.57%**
OG Nodes	20%	**28.57%**
Founder Nodes	5%	**17.86%**

Tokenomics

Humanity introduces a comprehensive tokenomics model centered around the $H token

An ERC-20 token with a fixed supply of 10 billion units, designed to fuel the ecosystem's operations and incentivize participation. The $H token facilitates a variety of critical functions, including humanity attestation, identity verification, and credential validation, and serves as the primary medium for verification rewards for zkProofer Nodes and staking rewards for Identity Validators, as well as for DAO governance participation.

Furthermore, it underpins the Community Incentives pool, driving engagement through fairdrops, the Humanity Scanner DePIN network, and collaborations with ecosystem projects. A significant aspect of Humanity’s tokenomics is the distribution of verification fees to zkProofer Node operators and Identity Validators, ensuring a fair and sustainable reward system.

This model aims to create a balanced economic environment that secures the network's integrity, encourages community involvement, and sustains the token's value, laying the foundation for a decentralized digital identity verification ecosystem.

The Humanity economic model is meticulously designed to encourage a secure, functional, and valuable token ecosystem, underpinned by a well-structured incentive system. Central to the Humanity Protocol ecosystem is the $H token, an ERC-20 token with a fixed supply cap of 10 billion divisible to 8 decimal places. The $H token not only fuels the blockchain operations as the gas token but also facilitates a wide array of essential functions within the ecosystem:

Token Utility

This model aims to create a balanced economic environment that secures the network's integrity, encourages community involvement, and sustains the token's value, laying the foundation for a decentralized digital identity verification ecosystem.

Humanity Attestation

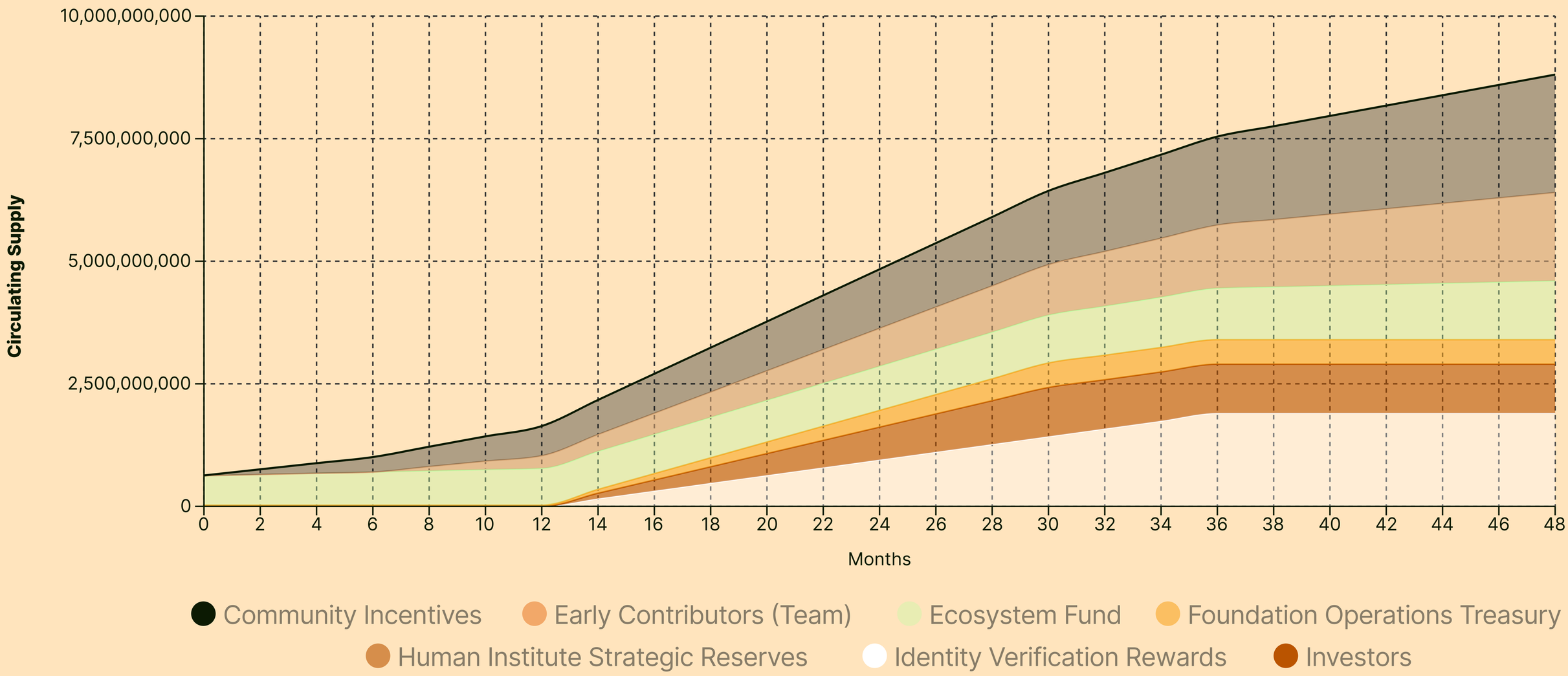
Identity Verification

Staking Rewards

DAO Governance

Credential Validation

Coins for Humanity Rewards


10,000,000,000
7,500,000,000
5,000,000,000
2,500,000,000
0
Circulating Supply
0
2
4
6
8
10
12
14
16
18
20
22
24
26
28
30
32
34
36
38
40
42
44
46
48
Months
Community Incentives
Early Contributors (Team)
Ecosystem Fund
Foundation Operations Treasury
Human Institute Strategic Reserves
Identity Verification Rewards
Investors

Category	Allocation	Cliff (Months)	Vesting (Months)	% Unlocked
Early Contributors (Team)	19.00%	12	24	0%
Investors	10.00%	12	18	0%
Human Institute Strategic Reserves	5.00%	12	18	5%
Foundation Operations Treasury	12.00%	0	48	50%
Ecosystem Fund	24.00%	0	48	0%
Identity Verification Rewards	18.00%	6	42	0%
Community Incentives	12.00%	0	0	100%

Introducing the internet's trust layer

humanity