WORLD WHITEPAPERS

Updated on March 24th, 2026

This series of whitepapers explores the technical foundations, philosophical underpinnings and economic structures of the World Network.

1. Building World — World Network: Proof of Human, new economic infrastructure and the real human network to maximize individual empowerment.

2. Achieving Proof of Human — How to build Proof of Human in a way that is aligned with individual empowerment.

3. Advancing Decentralization — How to decentralize the World network and minimize central points of failure.

4. Designing for Scale — How WLD powers governance, identity and financial access for every verified human.

Disclaimer: This white paper complies with Title II of Regulation (EU) 2023/1114 and, to the best of the knowledge of the management body, the information presented in the white paper is fair, clear and not misleading and the white paper makes no omission likely to affect its import.

This white paper has not been approved by any competent authority in any Member State of the European Union. The person seeking admission to trading is solely responsible for the content of this white paper.

1. World

World Network: Proof of Human, new economic infrastructure, and the real human network to maximize individual empowerment.

1.1. Motivation

The internet has enormous potential to uplift people all over the world by providing everyone with equitable access to information. But due to recent and accelerating increases in malicious bot activity, the internet is dying which threatens the stability of democracy. At the same time, amplified by AI, the internet could empower people orders of magnitude more if we had:

1. Universal financial infrastructure: Anyone (human or AI) can interact economically with everyone else.
2. Proof of human (PoH): Anyone can know (in a private way) whether they are interacting with a human (or a bot on behalf of a human), which helps increase integrity.

If those existed, they would:

- Expand access and participation in the global economy by enabling billions of people and AI agents to transact.
- Enable positive-sum collaboration by ensuring interactions can be trusted to be from a human or a bot acting on behalf of a human.
- Significantly reduce scaled abuse, impersonation, and fraud.

And as a result, they could transform the Internet in ways that meaningfully:

- Accelerate global progress and prosperity by creating a more trustworthy foundation for the economy.
- Increase global GDP due to improved efficiency and access.

We are approaching a moment that may make such infrastructure essential. The accelerating capabilities of AI agents create an existential challenge for the integrity of digital interaction and the stability of our society. AI-generated content and actions are becoming indistinguishable from human interaction, and automated messages become increasingly personalized and scalable. As a result, the ability to reliably distinguish humans from AI becomes critical. A world without PoH risks mass disinformation, election manipulation, scalable fraud and privacy-invasive tracking, all of which seriously threaten the stability of democracy and human agency. As cost per capability declines and automation enables continuous operation, influence scales with compute rather than people. At the same time, PoH protects freedom of speech by elevating human voices above bots and it empowers people through agents that are not blocked as bots but recognized to act on a human's behalf. Contrary to common perception, (well-implemented) PoH does not enable surveillance but protects against it because it preempts the need for privacy-invasive monitoring.

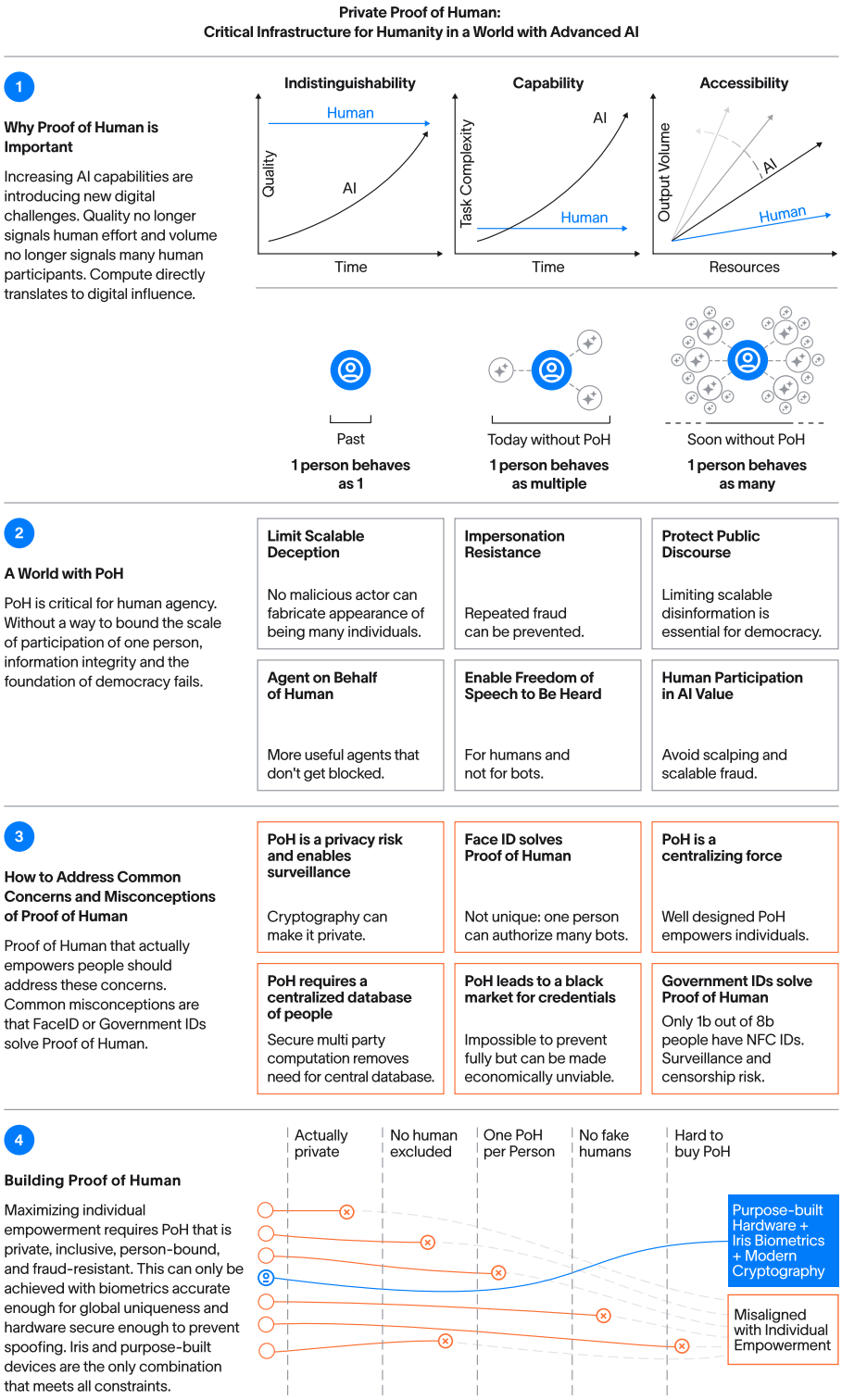

Figure 1: Overview of PoH. (1) AI's growing indistinguishability, capability, and accessibility erode traditional signals of authentic human participation, enabling single actors to masquerade as many. (2) PoH has many benefits including fraud prevention, impersonation resistance, democratic resilience, free speech protection, and enabling benefits distribution (if needed). (3) Common concerns around surveillance, centralized databases, and biometrics can be addressed through cryptography and decentralization. (4) Maximizing individual empowerment requires PoH that is private, inclusive, and fraud-resistant. Iris biometrics and purpose-built hardware are the only known combination that meets all constraints.

But building PoH is unexpectedly challenging. Government IDs are either ineffective or problematic due to surveillance risks, and face-based methods exclude a large portion of the global population. Creating a surveillance-free and effective solution requires new technology. World is an attempt to build a real human network based on PoH using purpose-built hardware and

modern cryptography. We advocate for scaling this infrastructure rapidly to prevent avoidable threats to democracy and avoid less effective, censorship-enabling, privacy-invasive measures that are incentive-misaligned with individual freedom in the long-term.

Bureaucracies tend to address major problems only after significant damage has occurred, which helps focus on what matters most. However, a reactive approach to PoH is highly undesirable. This not only results in avoidable negative consequences but also increases the likelihood of a less considered and simpler implementation, which would likely undermine efficacy, privacy and freedom of speech.

While such infrastructure is unprecedented in scale and extremely difficult to accomplish, the potential upside for humans makes it worth trying. These motivations led to the founding of the World project.

1.2. Introducing World

World is the real human network built to accelerate every human in the age of AI. It is based on decentralized PoH that lets people and applications distinguish humans from AI online, combined with an open financial layer that enables anyone to transact and participate in the global economy. At scale, World becomes a trust and financial layer for the internet, strengthening privacy, reducing abuse, and supporting safe, reliable AI adoption.

1.2.1. A Network Built Around People

The goal of World is to create universal means for verifying humanness and a financial layer that uses that verification to enable participation in the global digital economy. It builds a foundation where anyone can prove they are human without compromising their privacy, and transact with anyone else through open, decentralized infrastructure.

The network is built around a few core tenets.

- Proof of human (PoH): PoH is a missing digital primitive that establishes a person is both a real human and unique from other humans. As AI advances, this will become essential infrastructure for establishing trust online.
- User-owned: PoH enables universal access to network ownership for users, so that everyone directly benefits from the network they are creating.
- Incentive alignment: Distributing network ownership encourages participants to join and grow the network until it becomes self-sustaining.
- Scale: The larger the network, the more useful and valuable it becomes to its participants.

1.2.2. The Vision for the World Network

Like Aadhaar and UPI in India enabled over a billion people to authenticate and transact digitally and accelerated progress as a country, World aims to extend that idea globally. But unlike national systems, it is open source, privacy-preserving, and interoperable across jurisdictions.

In the limit, the World Network is not only a programmable financial and identity layer that is native to the internet, but also a decentralized network between people that is foundational to the internet economy in a world with AI.

The World Network consists of five core technologies: World ID, the Orb, World App, World Chain, and Worldcoin (WLD). Where the Orb and World App are the first but likely not the only implementation of their kind. Together, these core technologies form an open ecosystem that grows through community participation and shared benefit.

The World whitepaper series shares the components, reasoning, and implementation of the World project, its current state and its roadmap for the future. This first whitepaper in the

series provides an introduction and overview of World, while the others detail specific areas of the project.

1.2.3. Requirements for Proof of Human

The implementation of PoH can take many forms, leading to vastly different societal and individual consequences. These potential outcomes span a spectrum, from intrusive, Orwellian surveillance to systems that safeguard privacy and actively enable free expression. Consequently, the core system architecture, along with the resulting capabilities and incentives for all participants, must be designed with extreme care.

To establish design requirements, we first need to define what we value most. We place the highest importance on individual empowerment because we believe this leads to the most beneficial implementation for human society. This means the design requirements should prevent surveillance, maximize privacy, ensure broad participation and accessibility, and uphold freedom of expression and individual agency.

PoH is still nascent and the thinking around requirements will likely evolve from practical experience as adoption increases. Starting from first principles, valuing individual empowerment above all else leads to the following design requirements:

Inclusive and scalable. It must be feasible for every single human on the planet to participate: across geographies, economic conditions, varying levels of digital literacy, and levels of technical access. A global PoH must be maximally inclusive and accessible to everyone. It should be capable of distinguishing billions of individuals, provide a feasible path to implementation at global scale, and enable participation regardless of nationality, race, gender, age, disability, or economic means. Inclusivity is essential because a PoH that excludes large portions of humanity cannot serve as a universal primitive for trust. Identity systems in the past have often reinforced existing inequities by limiting participation to those with specific credentials, technologies, or forms of access.

Unique and high-integrity. Individuals should be able to acquire exactly one PoH credential, and not more. In order for uniqueness to be effective, the uniqueness verification must be extremely difficult to spoof or bypass.

Person-bound. Credentials must be difficult to sell or transfer at scale; otherwise, uniqueness collapses via a black market for credentials.

Privacy-preserving. Proving that one is a unique human should not require revealing identity, and should support unlinkable use across contexts. While there are many situations where identity is important and useful, there are also many situations where it is important that users be able to interact with one another and with internet services in a pseudonymous or even fully anonymous manner. This must also be possible while differentiating humans from bots, so PoH must be capable of providing users with the ability to interact in an anonymous manner.

Recoverable. If someone loses access to their credentials or their credentials are compromised, they need to be able to recover them. However, if users are managing their own keys, this is a significant challenge because there is no central authority to help restore or revoke keys.

Revocable. In instances where an issuer is found to be compromised or malicious, the impact can be mitigated by removing affected PoH credentials from the list of accepted credentials. If issuance is decentralized across multiple issuing locations and only a subset is affected, the respective subset could be revoked by the issuing authority itself.

Decentralized and open source. Most existing identity systems are centralized and rely on trusted entities such as governments, financial institutions, or global social networks. These models limit inclusivity, introduce potential conflicts of interest, and create systemic risks when the supporting organizations change or fail. A global PoH system capable of supporting the World Network must be decentralized, without any single point of control or failure. It should begin with an open source and clearly defined implementation that promotes transparency and allows

anyone to inspect, verify, or build upon the system. The underlying economic model must also be independent and sustainable so that the system can operate without relying on external subsidies or gatekeepers.

Taking the above requirements seriously requires investing in a very sophisticated system, which requires substantial resources to establish but seems likely to lead to the best outcome for humanity. The second whitepaper (Achieving Proof of Human) examines the underlying mechanisms for verifying uniqueness and obtaining a World ID at scale.

1.2.4. Requirements for the Financial Layer

A financial layer for the internet should meet the following key requirements:

Scalability. The network must support high transaction throughput with low latency to enable billions of people to transact seamlessly.

Decentralization. It should be governed and operated through open, permissionless infrastructure that avoids single points of failure or control.

Privacy. Transactions and balances should be secured through cryptographic mechanisms that protect individual data while maintaining the transparency required for network integrity.

Together, these requirements create a financial foundation that is human-centric, resilient, and scalable for the World Network. Today, these remain active work in progress.

1.2.5. Core Components of the World Network

The World Network is built on a set of core components that implement the requirements described above. These include World ID, the Orb, NFC ID credentials, World App and World Chain, each with a distinct function within the ecosystem. Alongside these components, Worldcoin (WLD) serves as the network's native token, which is designed to distribute ownership to all network participants and serve as economic unit of account between actors in the network in the long term.

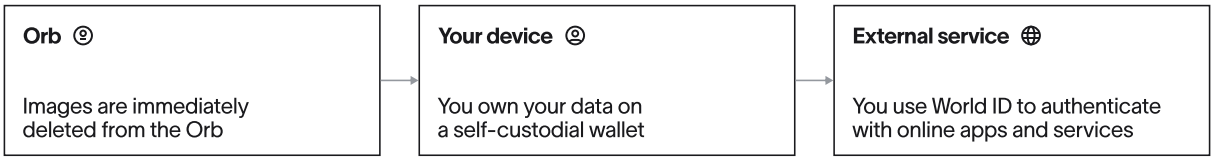

Figure 2: A simplified diagram of how users verify a World ID and present the PoH credential through World App to authenticate with relying parties.

1.2.5.1. World ID

World ID is open source, decentralized infrastructure that enables relying parties to verify credentials of the person they are interacting with, including that they are a real human. Each World ID is designed to be personbound, meaning it can only be used by the individual to whom it was issued. Unlike conventional digital identity systems, World IDs allow individuals to preserve their privacy (including maintaining their anonymity) because the protocol uses personal custody, anonymized multi-party computation (AMPC) and zero-knowledge proofs (ZKP).

The World ID SDK lets any developer directly integrate with the World protocol, so they can both contribute to and benefit from the World Network. The MiniKit SDK makes it easy to build JavaScript web apps that run inside World App. With MiniKit, any web application can request PoH, authentication, and other credentials from World App or other authenticators. Eventually, the Authenticator Kit should also enable developers to integrate their own apps directly as World ID authenticators, giving users more options beyond World App.

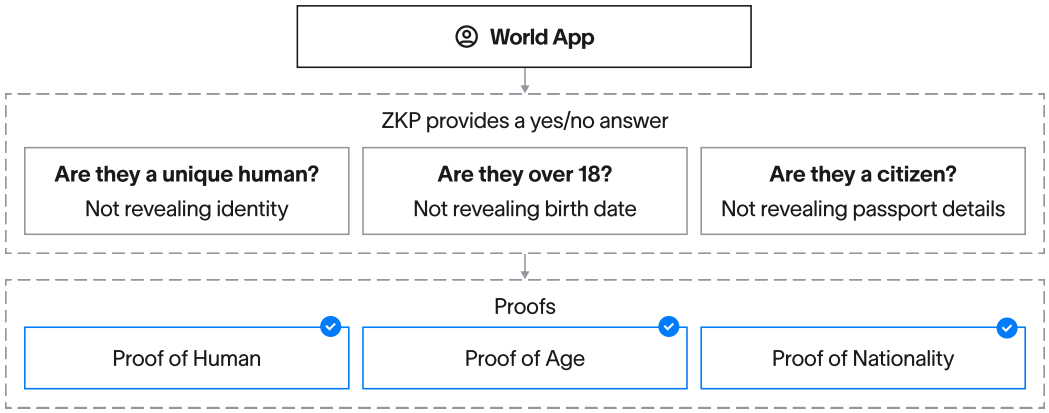

Figure 3: A simplified diagram of World ID presentments as zero-knowledge proofs through World App.

1.2.5.2. Orb

The Orb is a high-security, open source camera that makes it possible to verify you are a unique human without sharing anything else about you. It takes images of your face and eyes, then encrypts and stores them on your phone as a personal custody package so that only you control them. Encrypted, anonymized codes generated by the Orb can then be used by the World protocol to determine that a person is unique and issue a PoH credential. All of this is done simply and easily in a few seconds.

The Orb also produces verifiably human images that are cryptographically signed, creating a new root of trust for the internet. These cryptographically verified signals can strengthen both security and privacy across a range of applications.

- Face Auth builds on the Orb-generated credential to provide privacy-preserving multi-factor authentication. It enables a verified human to confirm that they are taking an action, such as signing in or approving a transaction, adding security without exposing personal data.
- Deep Face also leverages the Orb-generated credential to allow World ID holders to prove that their digital representation, such as a profile photo or live video, matches a real human rather than a deepfake. The verification is done privately, without revealing the original image or identity.

Figure 4: The Orb.

1.2.5.3. NFC ID Credential

A self-custodial credential is derived from valid government identity documents (starting with ICAO-compliant, NFC chip-enabled passports and national ID cards), enabling people to prove things about themselves online—like their age or nationality—without revealing their identity. This credential introduces a new secure, privacy-preserving way for people to interact online without directly uploading and exposing ID data, helping reduce the risk of personal information being compromised while ensuring individuals meet the requirements needed to keep online platforms free from fraud and misuse.

All ID authentication happens locally on the user's phone and the data remains encrypted, stored locally on the device, and managed within World App. No ID data is uploaded, stored, or shared with TFH, World Foundation or any third party.

1.2.5.4. World App

World App is the first frontend client to the World Network. It provides a self-custodial wallet that allows users to access financial services on World Chain and manage their World ID credentials. The app guides individuals through Orb verification and uses cryptography to let them prove facts to third parties without revealing their identity. World App also enables developers to connect to the World Network through Mini Apps and access World ID proofs. While it is the first frontend, developers are encouraged to build their own applications and wallets that integrate with the network. The World ID SDK is designed to make this process open and permissionless.

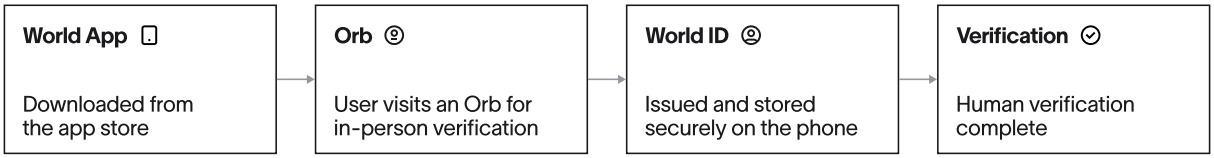

Figure 5: A simplified diagram of how a user joins the World Network. After downloading World App, the users visit an Orb for in-person verification to obtain their PoH credential. A verified World ID is then issued and securely stored on the user's phone. In regions where permitted, verified users can claim their share of the World Network in WLD.

1.2.5.5. World Chain

World Chain is the financial layer of the World Network. It is designed to function as an open, human-centered financial system.

World Chain is implemented as a layer-2 network on Ethereum and is built on the Superchain architecture, which supports high throughput and low-latency transactions. By combining decentralized execution with human-based prioritization, World Chain establishes the financial layer that powers PoH and adds decentralized security to the broader infrastructure of the World Network.

1.2.5.6. Worldcoin (WLD)

WLD is the native digital currency of the World Network, designed to become the most widely used and accessible form of value exchange in the world.

Ownership of WLD represents a proportional share in the value created by the World Network. Unlike traditional platforms where value accrues to a small number of centralized entities, WLD enables decentralized ownership by distributing tokens to verified participants through PoH credentials in World ID. This model ensures that everyone contributing to or participating in the network can share in its success, aligning incentives for growth, sustainability, and responsible governance.

The issuance of WLD is governed by smart contracts that transparently manage on-chain distribution, fees, and incentives (certain distributions are currently administered by the World Foundation). This structure allows the World Network to evolve as a self-sustaining ecosystem that resists centralized control and stays aligned with the interests of its global community.

For further details refer to the Decentralization whitepaper and on the supply model and network fees, see the supply and fees blog posts.

1.3. Applications and Impact

World has the potential to expand equal opportunity worldwide by enabling anyone, regardless of location or socioeconomic status, to participate in the global digital economy. Through universally accessible, decentralized infrastructure, World lowers barriers to access, allowing more people to connect, transact, and create value online. As more verified users join, the network becomes more valuable, which strengthens what already exists and unlocks entirely new applications that rely on a trusted PoH credential.

<table>
<tr><th>Trust and Identity</th><th>Economic Access</th><th>Financial Services</th></tr>
<tr><td>Combating Bots, Spam & Misinformation</td><td>Equal Access & Distribution</td><td rowspan="2">Payments</td></tr>
<tr><td>Deepfake Prevention</td><td>Owning Digital Money</td></tr>
<tr><td>Real Human Interactions (gaming & dating)</td><td>Transferring Digital Money</td><td rowspan="2">Credit</td></tr>
</table>

Figure 6: Examples of how the World network can be applied across a variety of identity, economic, and financial use cases.

1.3.1. Economic Access

Billions of people still live outside the global economy. Even for those included, moving money remains slow and expensive. World Chain connects people through a shared financial layer that works at internet scale. Inside World App, Mini Apps already let users hold digital money, exchange assets, and use fast, low-cost financial rails. The Morpho Mini App, which brings decentralized lending to verified users, shows how human verification can make DeFi safer and more inclusive.

Examples like the COVID Crypto Relief fund for India, which raised over $400 million in digital assets, show how decentralized networks can coordinate and distribute resources globally. World builds on that idea and makes it accessible to everyone. This same infrastructure could one day connect billions through a unified, human-centered network for value exchange.

Whether AI will create the need for broad redistribution systems, such as benefits for impacted individuals, universal basic compute, or comparable per-person allocations, is highly uncertain. However, if such mechanisms become important, there is currently no infrastructure capable of supporting this on a large scale without catastrophic failure modes–especially if it crosses geographical borders. Any system that distributes resources per person is immediately vulnerable to Sybil attacks. Without a reliable way to identify unique humans, redistribution collapses under unlimited duplication and resource drain.

1.3.2. Trust and Identity

Verifying humanness privately introduces a new layer of integrity to the internet. By enabling a way to constrain the number of accounts any one individual can create, PoH can directly address scalable deception at its core. Limiting the number of accounts makes artificial amplification of messages and manufactured appearance of broad consensus much more expensive and ideally

uneconomical. This significantly reduces the reach and impact of disinformation campaigns. Furthermore, this limitation allows existing mechanisms—such as content provenance, moderation, community notes, and polls—to function as they were intended.

The same participation constraint directly limits large-scale fraud and impersonation. Attacks like phishing, account selling, benefits fraud, and identity theft all rely on the ability to cheaply multiply identities. By enforcing per-human access limits, PoH makes these attacks difficult to scale. This is achieved without the need for continuous behavioral monitoring or cross-service data correlation. Consequently, systems can effectively prevent reply bots, reduce rapid re-entry after a ban, and limit the resale of high-influence accounts while still preserving pseudonymity and avoiding persistent surveillance.

Verification also strengthens protection against deception, which is becoming more important as deepfake technology continues to make impersonation increasingly convincing and easy. Many PoH implementations naturally support the creation of locally held (on the user's phone), signed selfie pictures taken during the initial verification. These selfies can be used to sign messages, images, or video streams as originating from a particular human. While this does not detect AI-generated content, it significantly raises the cost of impersonation, in much the same way that two-factor authentication reduces account takeover risk without proving intent. Essentially someone can prove that a particular video stream was authorized by someone that actually looks like the person in the video stream. This makes it very hard to impersonate someone because it is very hard to obtain an authentic signed face picture of someone (assuming the PoH issuer has good security) and then also spoofing a real-time local faceID-like authentication challenge. Applications include authenticating participants in video conferencing, signing emails, and verifying profile pictures and social interactions between individuals. Tools like Deep Face, a Mini App that uses World ID authentication, can accurately confirm that a video or image originates from a real human while keeping identity private.

Practical uses are already emerging. For example, World ID's partnership with Match Group enables age verification on Tinder in Japan, helping users connect safely while maintaining privacy. In gaming, verified human credentials such as Razer ID with World ID support fair play and stronger community standards as AI agents begin to appear in all types of online games.

1.3.3. Prevent Scalable Disinformation and Protect Public Discourse

PoH is essential for enabling authentic public discourse in a world where humans and bots are difficult to distinguish. By preventing bad actors from scaling misinformation and manufacturing the appearance of widespread support for specific beliefs or events, PoH safeguards the integrity of human participation in online opinion formation.

A public "town square" depends on people forming opinions based on engagement with other human participants. When humans cannot be distinguished from bots, individual contributions are harder to surface, and people may give up expressing their opinion when they assume most participants are bots. PoH empowers individuals and enables public debate by elevating human voices above automated noise.

At the same time, as AI lowers the cost of aggregation and analysis, collecting large-scale human input becomes more feasible than before. For governments, this makes real-time policy input more efficient. PoH ensures that such participation can be trusted to come from real people and not bots.

1.3.4. Agent on Behalf of Human

As AI agents become more capable, an increasing share of human-like online activity will originate from bots rather than from humans. Communication, coordination, and economic actions will often be carried out asynchronously, at high frequency, and over long horizons by systems acting on someone's behalf.

To enable the same benefits PoH creates for human-to-human interaction, agent-mediated activity also needs to be anchored to real humans. This can be implemented as revocable delegation of someone's PoH to an agent. Actions taken by an agent can therefore be verified as occurring on behalf of a human, even when the execution is automated. Importantly, this does not enable someone to delegate PoH to a large number of bots — it preserves the core property of PoH: participation and influence are human-bounded and therefore rate-limited.

1.3.5. Financial Empowerment

Programs that depend on human participation like incentives, research studies, or loyalty rewards can operate without being distorted by bots or duplicate accounts. The TBD.vote Mini App enables this by letting unique participants receive rewards for sharing their feedback and opinion without exposing personal data, producing better information and fairer outcomes.

PoH also redefines how credit can function. Instead of depending on collateral or opaque scoring models, lenders can extend credit to verified humans through secure, privacy-preserving credentials. The Credit Mini App is an early example of this, showing how lending can become more accessible and accountable.

1.4. Looking Forward

World was conceived with the mission of building the real human network to accelerate humans in the age of AI. PoH, the foundation of the World Network, introduces a new digital primitive that can redefine how people interact and transact online. By enabling applications and services that are inherently human-centric, such as Mini Apps that integrate privacy-preserving human verification and finance, PoH makes a new class of interactions possible — built on trust, authenticity, and universal access.

Such infrastructure is unprecedented in both scale and complexity. There are many challenges that could prevent its success.

- Scale: Public resistance to biometric verification or the logistical complexity of deploying verification hardware worldwide could impact the project's scale.
- Equitable access: Barriers related to geography, regulation, technology, or cost could create unequal access and undermine the goal of universal participation.
- Governance and incentives: Misaligned incentives or concentration of ownership could distort participation and reduce the effectiveness of decentralized decision-making.
- Security: The system may be vulnerable to technical failures, security breaches, or other unforeseen errors.

There are also risks that demand continuous attention. If implemented poorly, systems like PoH could threaten privacy, limit free expression, or concentrate control. To guard against these outcomes, World is being developed in the open, with transparency, distributed issuance, and privacy as core design principles.

Recognizing PoH as critical infrastructure still requires a meaningful shift in public perception which is likely the biggest limiting factor for proactive adoption and safeguarding humans in a world with advanced machine intelligence. Although awareness of scalable automation is increasing, PoH is usually framed as a narrow anti-bot measure rather than as a foundational layer for human coordination and societal stability. Misconceptions around surveillance and privacy that conflate privacy-preserving uniqueness verification with centralized identity systems that collect and monitor personal data slow down adoption. At the same time, AI capabilities continue to advance in both scale and coordination, and as machine capabilities compound, the absence of widely adopted, high-integrity PoH becomes more consequential. Adoption must accelerate in parallel with AI progress.

The remaining whitepapers in this series outline the current thinking on how to design and evolve the World Network so that it becomes a durable and beneficial piece of global infrastructure for humanity.

1.5. Other Resources

The World roadmap is a dynamic and evolving blueprint that is subject to change and refinement through input and decisions from the World community. Whether you are a developer, a user, an enthusiast or simply someone interested in the future of decentralized systems, please reach out through the appropriate channel:

- Join the community discussion on X or Discord.
- Contribute to open source repositories on GitHub.
- Visit the World developer documentation.
- Reach out directly to the World team for support questions.
- View live on-chain data on the Dune dashboard.

2. Achieving Proof of Human

How to build Proof of Human in a way that is aligned with individual empowerment.

2.1. Introduction

In the previous whitepaper, we introduced the idea of an anonymous Proof of Human (PoH) and its high level building blocks. We detailed the accelerating capabilities of AI agents that create an existential challenge for the integrity of digital interaction and why a globally inclusive, high-integrity, and privacy-preserving PoH mechanism is critical infrastructure for humanity.

This whitepaper, the second in the World whitepaper series, focuses on how to build PoH. It outlines the key design requirements needed to implement a PoH that is optimized for individual empowerment at scale. We then evaluate how to implement those in practice including candidate approaches to establishing a root of trust. Eventually we detail how World implements privacy-preserving PoH via World ID, which includes the Orb, Anonymized Multi-Party Computation (AMPC), and zero-knowledge proof-based authentication.

2.2. Building Proof of Human

The implementation of PoH can take many forms, leading to vastly different societal and individual consequences. These potential outcomes span a spectrum, from intrusive, Orwellian surveillance to systems that safeguard privacy and actively enable free expression. Consequently, the core system architecture, along with the resulting capabilities and incentives for all participants, must be designed with extreme care. This section outlines the key properties that we believe are essential for creating the best possible future for humanity, separate from the World project. World ID is our effort to translate these properties into a working system.

2.2.1. Derivative Design Requirements

To establish design requirements, we first need to define what we value most. We place the highest importance on individual empowerment because we think this leads to the most beneficial implementation for (human) society. This means, the design requirements should be defined such that they: prevent surveillance, maximize privacy, ensure broad participation and accessibility, and upholding freedom of expression and individual agency.

2.2.1.1. Importance of Uniqueness

Counterintuitively, PoH alone is insufficient because, without uniqueness, it is vulnerable to relay attacks. In this scenario, a small group of humans could authenticate repeatedly to serve millions of automated agents—picture a "human call-center" dedicated solely to passing PoH challenges for bots.

Strict uniqueness—exactly one credential per person—is essential to PoH integrity. Even allowing individuals to hold a small number of credentials creates a fatal vulnerability. If PoH becomes critical societal infrastructure, the incentive to bypass it will be enormous. Those who can acquire multiple credentials will likely find it lucrative to sell all but one. If just 1% of the US population sold nine out of ten credentials, a single malicious actor could masquerade as 31 million Americans. Since often only a fraction of people participate in any given online debate, this is usually more than enough to dominate public discourse.

The stakes extend well beyond social media. Elected governments wield immense power, making them high-value targets for manipulation. During elections in particular, bot networks armed with illegitimately transferred PoH credentials could pose as passionate citizens, drown out

real voices, manufacture false consensus, and ultimately shift voter opinion enough to alter outcomes.

To maximize individual empowerment and protect the integrity of democratic society, PoH uniqueness must therefore be exact.

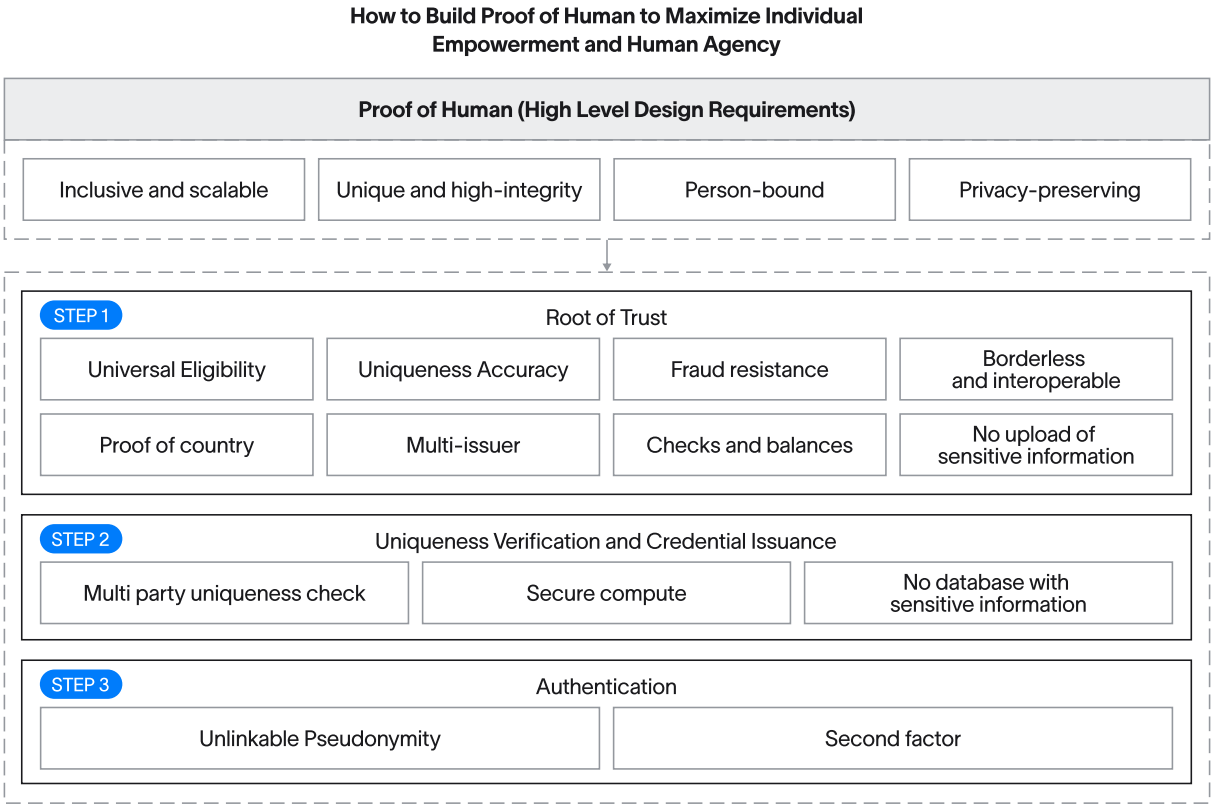

Figure 7: Building PoH in a way that maximizes human agency leads to high level design requirements as explained in the previous whitepaper. Those requirements can be broken down into derivative requirements for the three core components of PoH: root of trust, uniqueness verification and credential issuance, and authentication. These requirements are costly to implement in practice but important to empower individuals and prevent privacy-invasive tracking.

2.2.2. Three Stages of Proving Uniqueness

The process of proving unique humanness involves three distinct stages:

Stage 1: Root of Trust — Proving an individual is human and acquiring verifiable, high-integrity information. This information is then used in the second stage to establish uniqueness.

Stage 2: Uniqueness Verification and Credential Issuance — Verifying uniqueness based on the previously acquired information and issuing a unique human credential.

Stage 3: Authentication — Using the issued credential to prove one's unique human status to other parties.

Based on the initial design requirements, we can deduce derivative design requirements for each of these three stages:

2.2.2.1. Design Requirements for Root of Trust

- **Universal Eligibility.** Anyone needs to be eligible.
- **Uniqueness Accuracy.** In order to be able to establish uniqueness, there needs to be enough entropy to distinguish between O(10B) humans without falsely rejecting a single person.

- **Fake Human Resistance.** The humanness and uniqueness test needs to be very hard to bypass or spoof. This includes the ability for the issuer to act quickly if a compromise becomes known.
- **Borderless and Interoperable.** Citizens from different countries need to be able to prove to each other that they are humans; high-integrity uniqueness means countries need to be able to trust the PoH from citizens of other countries to not be bots, to prevent influence operations.
- **Proof of Country.** In order to trust PoH in certain high-stakes scenarios with national context (e.g., opining on presidential candidates) and to prevent global income arbitrage, it is important for people to be able to prove in which country their credential was issued.
- **Multi-issuer.** To ensure inclusivity and make sure no entity has the power to exclude someone from receiving a PoH, there need to be multiple entities as a root of trust—but importantly, they all need to tie into the same uniqueness set.
- **Checks and Balances.** It needs to be possible to validate one's PoH via another issuer, which can make it game-theoretically uneconomical to create fake identities.
- **No Upload of Sensitive Information.** To preserve privacy, no sensitive information should be uploaded.

2.2.2.2. Design Requirements for Uniqueness Verification

- **Multi-party Uniqueness Check.** The uniqueness check should be performed by multiple parties to prevent any single party from blocking anyone.
- **Secure Compute.** It must be as difficult as possible for any single party to adversarially inject fake identities or deviate from the comparison protocol.
- **No Centralized Database with Sensitive Information.** Sensitive information must not be aggregated or stored in any centralized database.
- **Recovery.** Enable the legitimate owner to reclaim their PoH following theft or sale.

2.2.2.3. Design Requirements for Authentication

- **Unlinkable Pseudonymity.** It should not be possible to identify who someone is or to track someone across different contexts.
- **Illicit Transfer Prevention.** The system needs to ensure that the person using the PoH credential is the one it was issued to, via a person-bound second factor for periodic reauthentication.

2.3. Ideal Root of Trust for PoH

2.3.1. Overview

When evaluated against the design requirements outlined above, most candidate PoH mechanisms fail for structural reasons. Below, we evaluate several approaches.

2.3.1.1. Online Accounts

The simplest attempt to establish PoH at scale uses existing accounts such as email, phone numbers, and social media. This method fails because one person can have multiple accounts. Further, accounts are not person-bound—they can be easily transferred—and CAPTCHAs are ineffective because AI agents are now capable of bypassing them. Current methods for preventing duplicate accounts, such as analyzing activity patterns, tend to fail when users have strong incentives to create multiple identities or commit fraud, as demonstrated by large-scale attacks targeting well-established financial services.

2.3.1.2. Credit Cards

Credit cards have been used in several contexts as a proxy for PoH. Although this method can increase friction for fraudsters, it is far from effective. Beyond not being private, credit cards allow fraudsters to create many duplicates—the simplest method is to pay for many accounts, and fraudsters can acquire large numbers of credit cards either through virtual credit cards or on the dark web. Advances in generative AI let automated agents mass-produce plausible credit identities. Furthermore, many people lack access to financial services. Even in the U.S., 6% of adults don't have a bank account, and credit card ownership is not universal even among those with accounts. In less developed countries, the share without access is significantly higher. Therefore, credit cards are not an inclusive solution for PoH.

2.3.1.3. Official ID Verification (Know Your Customer)

Online services often request proof of ID to comply with KYC requirements. In theory, a similar mechanism could be used to issue a PoH based on government documents, but this faces multiple challenges (discussed in depth in Section X). More than 50% of the global population does not have an ID that can be verified digitally, and building KYC verification while preserving anonymity is inherently contradictory. Zero-knowledge proofs and digitally signed IDs can partially address the privacy concern, but NFC-readable IDs are far less prevalent and people can hold multiple government IDs, so perfect uniqueness cannot be achieved.

2.3.1.4. Web of Trust

The underlying idea is to verify identity claims in a decentralized manner—for example, PGP key-signing parties or projects like Proof of Humanity that use face photos and video calls. However, these systems heavily rely on individuals and are susceptible to human error and Sybil attacks. Staking assets can increase security but decreases inclusivity, and these systems carry privacy concerns (e.g., publishing face images) and susceptibility to fraud using deepfakes.

One could also use information about relationships between people to infer which users are real. Projects like EigenTrust, BrightID and soulbound tokens (SBTs) propose more sophisticated rules based on the observation that social relations can constitute a unique identifier.[1] However, the required relationships are slow to build on a global scale, and it seems inevitable that AI, possibly assisted by humans acquiring multiple "real world" credentials, will be able to create such profiles at scale. Ultimately, these approaches require giving up the notion of a unique human entirely.

2.3.1.5. Biometrics

Approaches based on online accounts, social graphs, webs of trust, or financial credentials can be mimicked by AI systems and ultimately require accepting multiple identities per person. Biometric verification is the only class of mechanisms that can simultaneously satisfy all design requirements at global scale when implemented correctly. Biometrics are universal, enabling access irrespective of nationality, race, age, gender, or economic means. They provide a natural recovery mechanism and can be used for authentication, making the PoH credential person-bound. Among biometric modalities, iris recognition uniquely satisfies the accuracy, scalability, and privacy requirements, as shown in Fig. 2.

[1] SBTs are not designed to be a PoH mechanism. Rather, they complement applications where proving *relationships* rather than *unique humanness* is needed. However, they are sometimes mentioned in this context and are therefore relevant to discuss.

Proof of Human Mechanisms						
	Online Accounts	Credit Cards	KYC	Web of Trust	Social Graph Analysis	Biometrics
Inclusivity & Scalability	Possible	No	No	Possible	Possible	Possible
Uniqueness & Integrity	No	No	Possible	No	No	Possible
Personbound	No	No	Possible	Possible	Possible	Possible
Decentralization	Possible	Possible	No	Possible	Possible	Possible
Privacy-Preserving	Possible	No	Possible	Possible	Possible	Possible

Figure 8: An overview of candidate PoH mechanisms evaluated against the core design requirements established in the previous whitepaper. Only biometrics satisfy all five requirements when implemented correctly.

2.3.2. Deep Dive: Why a Document-based Root of Trust is Not Ideal for Individual Empowerment

In a future shaped by highly capable machine intelligence, the foundations of economic and social power shift. As automation increases, control over bots as well as the ability to determine who counts as a unique human will become an increasing source of power. Any entity that controls PoH gains significant influence over access to platforms, economic participation, and collective decision-making. Therefore, any incentive misalignment between issuer and participants can lead to catastrophic failures. The inherent nature of how documents are issued suggests that any PoH system based on them will result in long-term incentive misalignment.

Despite benefits—such as legal incentives against hacking and the fact that one billion people already have a verifiable document—the structural limitations of document-based PoH make it unviable on a global scale.

Properties of Document-Based Proof of Human	
Universal Accuracy	Not possible
Universal Eligibility	Not possible
Fraud resistance	Possible
Borderless & interoperable	Not possible
Proof of country	Possible
Multi-issuer	Not possible
Checks & balances	Not possible
No upload of sensitive information	Possible

Figure 9: Properties of document-based PoH evaluated against core design requirements. Five of eight requirements (red) cannot be met by document-based approaches.

Evaluating against design requirements:

2.3.2.1. Universal Accuracy

Establishing uniqueness using government documents is challenging. Names are insufficient for deduplication due to high collision rates (e.g., nearly 40,000 James Smiths in the US), and

the birthday problem further complicates uniqueness checks. A document's numerical identifier is the only viable uniqueness signal, but this creates a vulnerability where individuals could acquire multiple PoH simply by reporting their document "lost" and obtaining a new one. If 1% of the US population participated, this could easily lead to tens of millions of "authentic human" bot accounts.

2.3.2.2. Universal Eligibility

Only about one in eight people possess documents that can be cryptographically verified. Basing PoH on documents would exclude many billions of people.

2.3.2.3. Fake Human Resistance

Some documents are cryptographically verifiable, making them relatively fraud resistant. However, document-based PoH incentivizes the theft of physical documents like passports. Stolen documents can be used to generate PoH or, in some implementations, be cloned without the owner's knowledge. As AI capabilities grow, the issuing infrastructure will need increasingly advanced capabilities—securing the root of trust, anomaly detection, cross-issuer verification, revocation mechanisms, and dynamic expiration dates. Developing these capabilities is likely better suited to publicly auditable and mutually verifiable companies rather than governments.

2.3.2.4. Borderless & Interoperable

Interoperability is relatively straightforward since verifiable documents are already standards-based. However, the fact that governments could create fake documents and inject fake PoH credentials makes it hard to trust foreign credentials. This leads to a replication of geographical borders on the internet and may lead to exclusion of free exchange between people from different countries.

2.3.2.5. Proof of Country

Documents include the issuing country, which makes proof of location straightforward.

Multi-issuer. Wherever PoH becomes a prerequisite for interaction, the issuer gains leverage. Loss of PoH will eventually imply exclusion from large parts of the internet, including significant limits on freedom of speech. This can be mitigated if no single entity has a monopoly over issuance, which is not possible for government documents.

Checks & Balances. The ability to issue PoH credentials directly translates to power. For government documents, no second issuer exists for cross-checking and validation. For biometric-based PoH, there can be a diverse set of hardware devices from different manufacturers that can be cross-checked against each other.

No Upload of Sensitive Information. It is possible to verify the integrity of cryptographically verifiable documents without uploading sensitive information.

2.3.3. Deep Dive: Why Iris-based Root of Trust Maximizes Individual Empowerment

To our knowledge, a set of secure hardware devices from different companies (based in different countries) that issue a root of trust based on the entropy of the iris is the root of trust that maximizes individual empowerment and is the only root of trust that fulfills all design requirements. Note: this is not where World ID is today, but it should get there eventually. Iris-based hardware—while able to fulfill all requirements—also comes at the cost of being very capital intensive and operationally complex to scale.

Advantages of Iris-based Root of Trust	
Universal Accuracy	Possible
Universal Eligibility	Possible
Fraud resistance	Possible
Borderless & interoperable	Possible
Proof of country	Possible
Multi-issuer	Possible
Checks & balances	Possible
No upload of sensitive information	Possible

Figure 10: Unlike document-based approaches (Fig. 3), an iris-based root of trust satisfies all core design requirements for PoH that maximizes individual empowerment.

2.3.3.1. Why Iris Biometrics Specifically

Among biometric modalities, iris recognition uniquely satisfies the accuracy, scalability, and privacy requirements of global uniqueness verification. There are two modes to consider: 1:1 authentication (comparing a user's template to a single enrolled template, like Face ID) and 1:N verification (comparing against a large set of templates to prevent duplicates). Global PoH requires the latter—comparing biometrics against eventually billions of previously verified humans. If the mechanism is not accurate enough, an increasing number of users will be incorrectly rejected. Face biometrics are not accurate enough and billions of people would be falsely denied a Proof of Human.

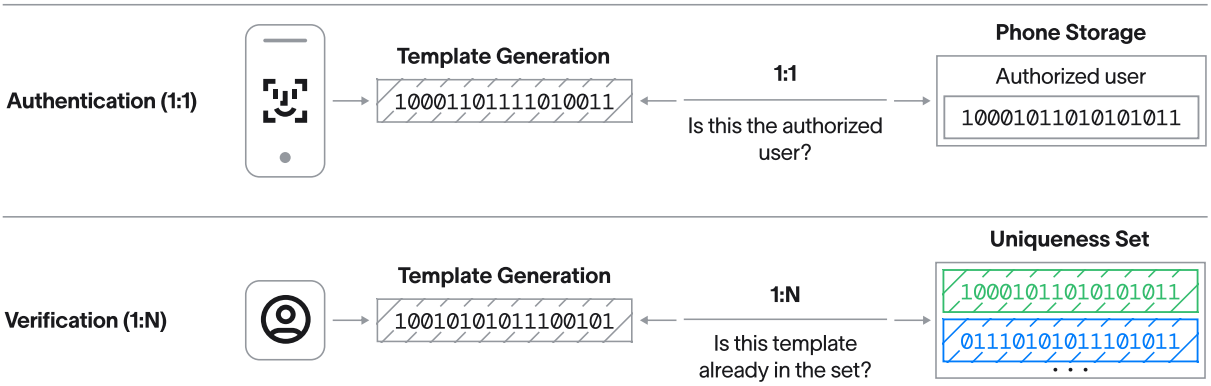

Figure 11: There are two different modes for biometrics. The simpler mode is 1:1 authentication, which involves comparing a user's template against a single previously enrolled template. This is commonly used in technologies such as Face ID, which compares an individual against a single facial template. However, for global Proof of Human, 1:N verification is required. This mode involves comparing a user's template against a large set of templates to ensure that there are no duplicate registrations.

Iris biometrics can achieve false match rates beyond 2.5×10-14 (one false match in 40 trillion), which is several orders of magnitude more accurate than the current state of the art in face recognition, while maintaining a suitable false non-match rate. The structure of the iris is remarkably stable over time, difficult to alter, and essentially unique to each individual. The iris texture is formed by random morphogenesis during gestation—an epigenetic development independent of personal factors—so even genetically identical individuals (identical twins or a person's two irises) have completely uncorrelated iris patterns.

Other biometric modalities exhibit fundamental limitations:

- **Fingerprints** can be unreliable since cuts or wear alter ridge patterns, and capturing high-quality images becomes difficult as fingerprints degrade over time. Using all ten fingerprints or combining modalities is vulnerable to combinatorial attacks.
- **Facial recognition** offers better liveness detection than DNA, but its accuracy is far below that of iris biometrics. At global scale with billions of people, the error rates would lead to double-digit percentage false rejection rates, falsely rejecting billions.
- **DNA sequencing** could in theory be highly accurate, but reveals extensive private information, collection is intrusive, difficult to scale, and there is no practical way to ensure liveness.

Biometric Modalities				
	Fingerprint	**Face**	**DNA**	**Iris**
Privacy	Possible	Possible	Hard	Possible
Accuracy for global scale	Not enough	Not enough	Sufficient	Sufficient
Scalability	High	High	Low	High
Integrity	Low	Medium	High	High

Figure 12: Overview of how different biometric modalities impact key considerations such as privacy, accuracy, scalability, and integrity (red indicates insufficient or problematic). Iris biometrics is the only modality that enables all of them.

2.3.3.2. Why Purpose-Built Hardware Is Needed

Meeting the design requirements necessitates guarantees that cannot be achieved through software or general-purpose hardware alone. Reliable verification depends on:

- **Compute integrity:** Image capture and processing must occur within a tamper-resistant environment and cannot be emulated, replayed, or modified. This requires hardware-backed signing, secure execution, and protections against compromised enrollment flows.
- **Multispectral imaging and active liveness detection:** Single-sensor consumer devices lack the signal diversity to reliably distinguish genuine presentations from high-quality spoofs in adversarial settings.
- **High-resolution infrared imaging:** Required to capture sufficient iris entropy across eye colors. Visible-spectrum cameras suffer from reflections and low contrast, particularly for darker irises.

While smartphones provide the most straightforward and scalable option, the correlation between image quality and biometric accuracy is well established. Both smartphones and existing imaging devices lack sufficient resolution to accurately capture iris biometrics, resulting in unacceptably high error rates. Furthermore, phones and existing iris cameras lack multi-angle and multispectral cameras as well as active illumination to detect presentation attacks with high confidence. A widely viewed video demonstrates an effective method for spoofing Samsung's iris recognition and underscores how easily such attacks succeed without sufficiently advanced hardware.

Additionally, an on-device trusted execution environment (TEE) is needed to guarantee that verifications originate from fully compliant devices rather than emulators. While some smartphones include specialized hardware (Apple's Secure Enclave, Google's Titan M), many do not or can only be accessed by the device manufacturer. Without such protections, attackers could spoof both image capture and enrollment requests, creating unlimited fraudulent PoH credentials.

2.3.4. Walking Through the Design Requirements

2.3.4.1. Universal Accuracy

Global uniqueness requires false match rates on the order of 10-20 to ensure no single person on Earth would mistakenly be excluded. Iris-based algorithms achieve error rates on the order of 10-14 today. Those can be further improved. If improvements aren't sufficient, they can be combined with face-based entropy which would already today achieve error rates below 10-20.

2.3.4.2. Universal Eligibility

Iris biometrics far surpass the inclusivity of alternatives like verifiable documents by many orders of magnitude. Many health conditions, like cataracts to a degree, do not impede iris biometrics. Specialized verification centers could facilitate alternative verification for individuals with severe eye conditions, via e.g., facial biometrics.

2.3.4.3. Fake Human Resistance

A purpose-build biometric camera can include multispectral cameras, a TEE, verifiable software, and multiple secure elements to make spoofing very expensive. Any root of trust issued by a particular hardware device can be revoked through a governance mechanism. Implementing incentive mechanisms for decentralized audits can raise the bar far beyond what hardware security alone could achieve.

2.3.4.4. Borderless & Interoperable

Biometrics and hardware are inherently borderless and it is straightforward to build interoperable infrastructure.

2.3.4.5. Proof of Country

Hardware devices can verify location via celltower and GPS connectivity plus continuous audits. With ongoing reauthentication, continuous travel to spoof PoH country credentials becomes expensive.

2.3.4.6. Multi-Issuer

Multiple companies across different jurisdictions can build auditable and verifiable hardware devices to the same specifications. This prevents censorship.

2.3.4.7. Checks & Balances

Hardware devices from different companies can issue iris-based roots of trust to the same specifications, enabling cross-checks. With staked security deposits and periodic reauthentication across different devices, it can become game-theoretically uneconomical for a manufacturer to inject fake identities.

2.3.4.8. No Upload of Sensitive Information

It is possible to issue an iris-based root of trust without uploading sensitive information.

Therefore, we conclude that an iris-based root of trust fulfills all design requirements.

2.4. The Orb

Based on the conclusion that iris biometrics via purpose-built hardware is the ideal root of trust, Tools for Humanity (TFH) built the Orb: a high-security, open-source camera that anonymously issues an AI-safe PoH credential. The Orb is purpose-built to verify humanness and ensure uniqueness in a fraud resistant and inclusive way. The humanness check is performed locally on the device, without requiring any images to be stored or uploaded. World Foundation's vision is for device development, production, and operation to be decentralized over time so that no single entity will be in sole control of World ID issuance.

2.4.1. Top Level Requirements

The Orb's primary use case of verifying unique humanness led to the following requirements:

- **Privacy:** The Orb must process images locally on-device and then securely transfer them to the user's custody. This eliminates any requirement for storing images on the Orb or uploading them to a central backend.
- **Security:** The Orb must only verify World IDs of genuine humans, meaning it must be highly resistant to spoofing and tampering, even in adversarial environments.
- **Transparency and Verifiability:** The Orb must require minimal trust in its manufacturers and operators. There must be a way for the public to audit Orbs, including transparency into its design, and the state of software and cryptographic keys (see the Decentralization whitepaper).
- **Scalability:** The Orb must generate iris codes consistently and accurately enough to allow for 8+ billion unique World IDs without significant false matches or false non-matches.

The Orb was designed to maximize trust, user experience, and scalability, with minimal compromises on imaging quality and security. The device's key imaging components include a wide-angle RGB/Infrared (IR) imaging for capturing high-quality face images, a telephoto IR camera with a steerable focus using custom lenses that can capture high-quality iris images, 2-D Time of Flight (2D-ToF) for face depth mapping, high-resolution thermal imaging for liveness detection, and imaging at orders of magnitude higher resolution than the industry standard.

Additional software and hardware components to highlight include secure on-device biometrics image processing that ensures the images are authentic and generates a signed iris code, fraud and presentation attack detection (PAD) measures to ensure liveness and humanness (see more below), and, lastly, images are only analyzed in local memory, and are deleted after verification.

2.4.2. Hardware Design

The Orb's design is open sourced so others can trust, learn from, and improve the design. The work is intended to serve as an inspiration and starting point for other protocol-compatible verification devices.

The Orb consists of two hemispheres separated by a retaining ring tilted at 23.5° (inspired by the angle of Earth's rotational axis). Once the shells are removed, the Orb divides into four core parts:

- **Front:** Optical system
- **Middle:** Mainboard and Powerboard
- **Back:** Computing unit and cooling
- **Bottom:** Speaker and docking chamber for an exchangeable battery

The optical system consists of several multispectral sensors behind a 2D mirror gimbal to capture high-resolution iris and face images, along with additional liveness signals. Key imaging components include:

- Multi-camera, multi-spectral optical system featuring wide-angle RGB/Infrared (IR) imaging for high-quality face images
- Telephoto IR camera with steerable focus using custom lenses for high-quality iris images
- 2-D Time of Flight (2DToF) for face depth mapping
- High-resolution thermal imaging for liveness detection
- Imaging at orders of magnitude higher resolution than industry standard

The mainboard holds a powerful computing unit enabling secure on-device image processing. The rear hemisphere contains the cooling system and compute module. An exchangeable battery can be inserted from the bottom for mobile operation; constant power via USB-C is also available for stationary use.

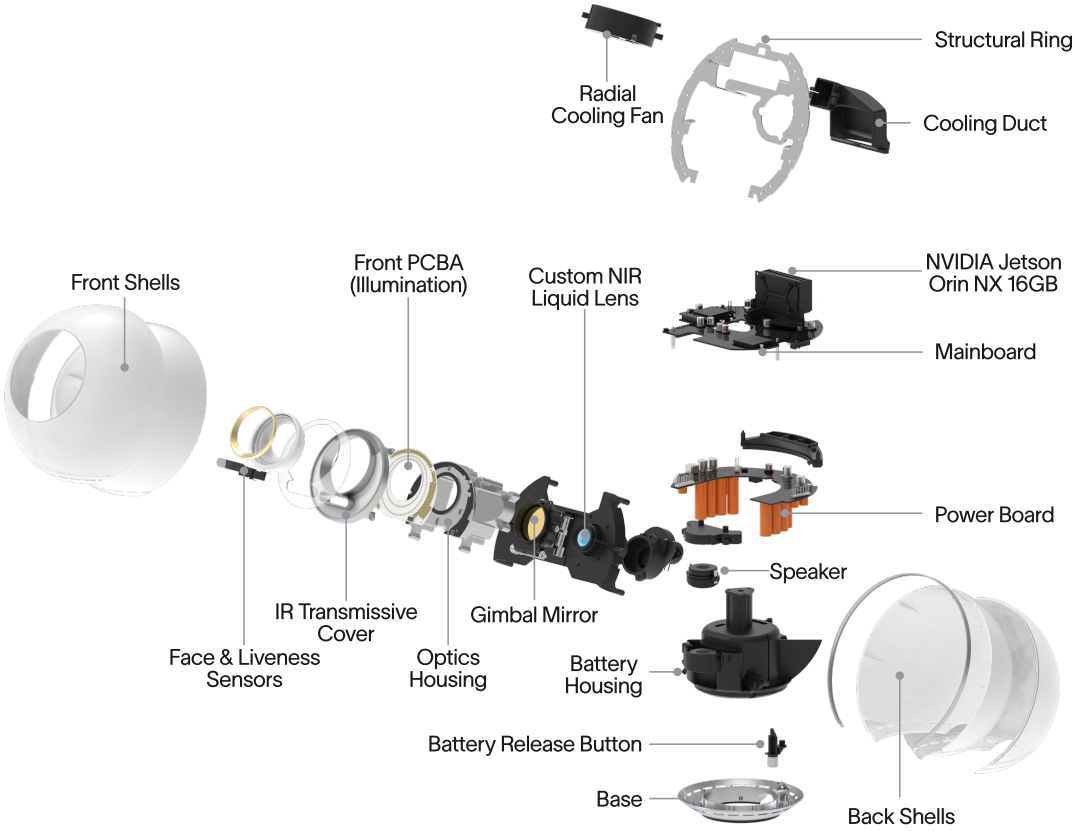

Figure 13: All relevant components of the Orb.

2.5. Security and Privacy

2.5.1. Presentation Attacks and Liveness Detection

The Orb's presentation attack detection (PAD) system runs in real time to distinguish genuine presentations from attack attempts. For enhanced privacy, all PAD checks run locally—images are never uploaded for PAD processing. The Orb layers multiple complementary checks across a diverse sensor suite to maximize the cost and complexity of attacks:

- Challenge-response and passive liveness checks ensure that biometric images on screens, printouts, or simulations are rejected
- A thermal sensor verifies the heat signature matches that of a live human
- Additional checks for fraudulent biometrics (e.g., patterned contact lenses) and obscured biometrics (e.g., looking away from the camera)
- Continuous hardening through internal red teaming and external programs

2.5.2. Hardware Security

Two unique cryptographic keys are permanently burned into the Orb's hardware: one provisioned into the main SoC during manufacturing and another in a hardware secure element that cannot be exported. The Orb will not operate unless both keys are valid and their environments are intact, and no code can run without a valid cryptographic signature. Additional features include active device tamper monitoring, fraud detection, secure element for authenticity, and an accessible SD card for auditors to validate code.

2.5.3. Third-Party Audits & Testing

The Orb sets a high bar for defending against scalable attacks. However, any hardware system interacting with the physical world requires continual enhancements. Contributor red teams test various attack vectors. Several audits (Theori, Trail of Bits, Least Authority) have been conducted, and a bug bounty program establishes incentives for external findings.

2.6. Distribution

2.6.1. Current

Wide-scale Orb distribution is paramount to bootstrapping PoH from an abstract protocol into something relying parties can actually use. Today, the operational model combines trained operators, large-scale partnerships, and TFH-led flagship locations. Dedicated operators provide predictable hours and high-quality sessions. TFH is integrating with established retail and venue partners to reach people where they already are: transit hubs, shopping corridors, campuses, and civic spaces. TFH continues to run flagship sites to set the bar on safety, privacy, and user experience, and to validate operational playbooks before handing them to partners. TFH is targeting mass deployments globally, prioritizing high-density areas and layering mobile and pop-up routes to close gaps.

2.6.2. Future

The target state is a way to verify your World ID within easy reach of every person across the globe. The network will grow from professional operators into a broad ecosystem including retail counters, service desks, campus groups, community organizations, and independent providers. As the technology standardizes and decentralizes, the operator role becomes more lightweight. The hardware footprint will follow the same arc: form factors enabling mobility and others optimized for unattended use. As consumer hardware evolves and begins to offer widely available secure execution and camera pipelines that meet liveness and imaging quality thresholds, PoH verification will extend beyond dedicated Orbs to consumer-level hardware.

Distribution Roadmap					
Privacy	**Operator model**	**Form factor**	**Primary sites**	**UX mode**	**Distribution goal**
Seed	TFH-run pilots	Orb	Pop-ups, events, flagships	Supervised	Prove throughput & safety
Urban scale	TFH + selected partners	Orb	Malls, transit, campuses	Supervised + assisted	City-level density
Broad access	Independent operators	Orb, Orb Mini	Retail counters, kiosks	Assisted + self-serve	Nationwide coverage
On-demand	Mixed (incl. gig-style)	Orb, Orb Mini	Mobile, micro-kiosks	Self-serve + Community operator	15-20 min access in most regions
Ambient	Fully decentralized	Embeddable modules & new consumer hardware	Phones, PCs, ATMs	Self-serve	"Verify anywhere"

Figure 14: A view of the planned distribution roadmap for the Orb as well as new device form factors to scale PoH verifications across the globe.

2.7. Verification of Uniqueness

As established earlier, uniqueness must be absolute—exactly one credential per person. The two hardest parts are making sure every human can receive a PoH and minimizing false acceptances of users that have previously verified. This section describes the generic architecture for achieving both, followed by World's specific implementation.

Determining whether a person has already verified requires global information from all prior verifications, so this process cannot happen locally on verification devices. Instead, a global uniqueness check service is required, complementing the verification hardware in the PoH issuance process. The critical properties are:

- **Multi-party uniqueness check:** The uniqueness check should be performed by multiple parties to prevent any single party from blocking anyone.
- **Secure compute:** It must be as difficult as possible for any single party to adversarially inject fake identities or deviate from the comparison protocol.
- **No centralized database with sensitive information:** Sensitive information must not be aggregated in any centralized database.
- **Recovery:** Enable the legitimate owner to reclaim their PoH following theft or sale.

One way to implement these requirements is through a secure multi-party computation (SMPC) protocol that verifies uniqueness in an anonymous manner without revealing biometric data to any entity. At enrollment, biometric information is processed locally in a TEE on a custom biometric camera and transformed into encrypted, statistically random fragments by verifiable software. Those fragments are sent to the user's phone. The user can then choose to send them to multiple independent node operators. Those nodes have private state and jointly determine whether someone has verified before—crucially, in such a manner where no party learns any statistically meaningful information about the underlying data whatsoever, except whether the entry is unique.

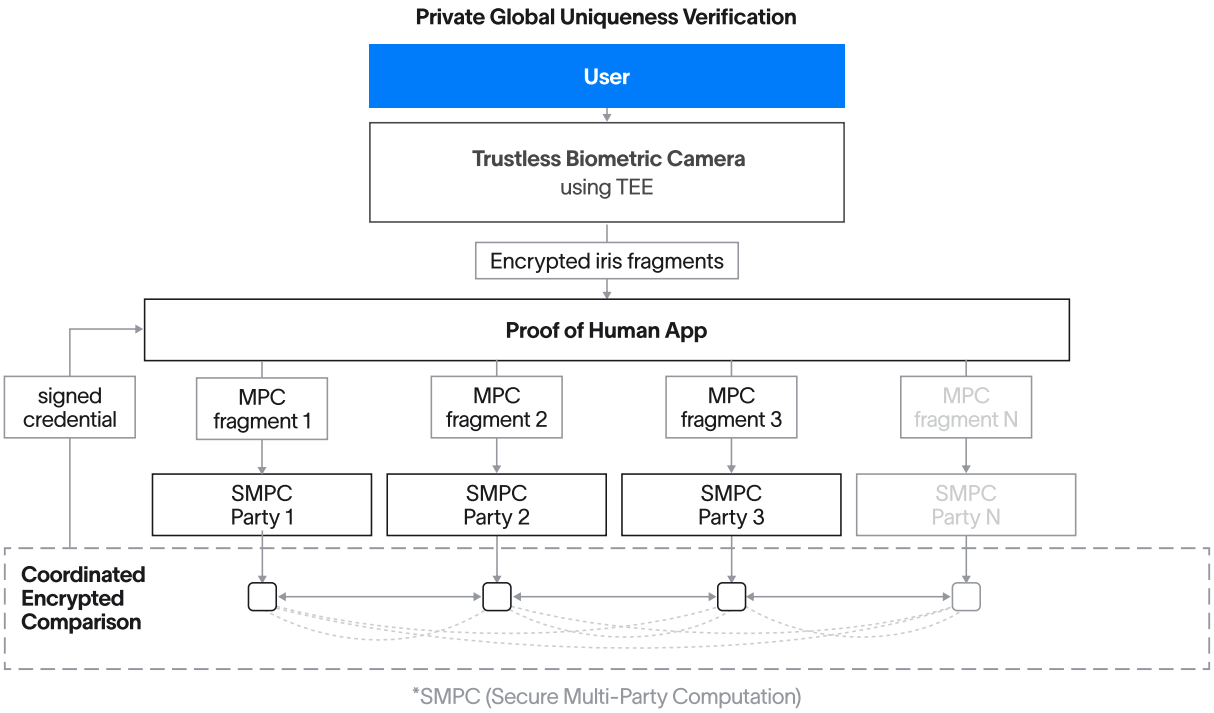

Figure 15: A diagram of a secure multi-party uniqueness (SMPC) check. When a new person verifies through the biometric hardware device, their iris data is converted into a unique code and split into multiple encrypted, statistically random fragments. Each SMPC party independently compares the new fragment against their set of existing encrypted fragments, and together, determine the existence of potential duplicates without revealing the underlying data to any party. If all SMPC results indicate that the fragment is unique, a signed Proof of Human credential is returned to the user. This process ensures that each Proof of Human corresponds to a single, unique human while preserving user anonymity.

If the uniqueness check is successful, the encrypted fragments are stored in the respective SMPC node and a signed PoH credential is returned to the user. Importantly, the credential should not be used directly to prove humanness, in order to prevent tracking across applications.

As PoH becomes more widely relied upon for platform access, economic participation, and public discourse, losing access to one's credential becomes a serious problem. However, enabling recovery conflicts with the uniqueness of PoH, making credential recovery challenging.

Any recovery mechanism must meet strict criteria: it must preserve the owner's privacy, and only the legitimate owner can be allowed to trigger it. This places severe requirements on the root of trust for recovery. Relying solely on a document like a passport is insufficient, as it would be too easy to impersonate the owner.

Crucially, recovery must deactivate the old access and issue new access without resetting the PoH's unique property. This is necessary to prevent individuals from fraudulently presenting as multiple people or circumventing a block issued due to misuse.

One way to implement this recovery is to store the PoH key in an SMPC system, accessible via user-stored authentication keys. If these authentication keys are compromised, the user can undergo a trusted verification process (e.g., via a secure biometric camera). This process would temporarily enable the user to deactivate the compromised keys, add new ones, and thus regain access.

2.7.1. World's Implementation: Creating a Unique Iris Code

This section details how World implements the generic uniqueness architecture described above, beginning with how the Orb generates a unique iris code.

Iris recognition was first developed in 1993 by John Daugman. Unlike 2D face images that are mostly defined by landmarks, feature proportions and shapes, iris images present rich and complex texture with semi-periodic variations in image intensity. As a result, they contain strong signals in both the spatial and frequency domains, and effective analysis must take both into account. Examples of iris images can be found on John Daugman's website.

Although the field has advanced since the turn of the millennium, it continues to be heavily influenced by legacy methods and practices. Historically, the morphology of the eye in iris recognition has been identified using classical computer-vision methods such as the Hough Transform or circle fitting. In recent years, deep learning has brought about significant improvements in the field of computer vision, providing tools for understanding and analyzing the eye physiology with unprecedented depth

Rather than using raw images directly, the Orb derives unique codes from iris texture patterns via frequency-based feature extraction (e.g., applying multi-scale Gabor wavelet filters and quantizing their phase response).

Although the iris code is essentially random data not known to reveal any information about the person, the Orb also anonymizes the iris code to create fragments for the AMPC system. This is done on the Orb so that the uniqueness check can later be performed without any exposure of personal or personally identifiable information.

2.7.2. Scale and Error Rates

A false match occurs when two different people are incorrectly judged to be the same. A false non-match occurs when two samples from the same person are incorrectly judged to be different. These two metrics are the key performance indicators for any biometric system and constrain its scale.

At the beginning of the project, World established that in order to scale to a billion people, there must be a false match rate (FMR) — or the probability of falsely matching two individual identities — of 1x10-12, so that even when matched against a billion unique identities, a new genuine user would only have a 1 in 1000 chance of getting falsely rejected and having to perform another signup. To reach this number, we need a FMR of 1x10-6 per iris (as detailed further in a blog post).

The verification system needs to reach these acute precision levels, while maintaining a false non-match rate (FNMR) — the probability of accepting someone in the system a second time — below 5x10-3.

These targets were exceeded in extensive, purpose-built test sets conducted prior to launch, where the project achieved an FMR of 2.25×10^{-14} at approximately 1×10^{-3} FNMR.

2.7.3. Limitations

Biometrics are probabilistic, and biometric verification has inherent error rates. In real-world operations, the measured error rate of the system for confusing any two people to be the same (false match rate) is approximately 1×10^{-12}, or about 1 in a trillion. On a billion-person scale, this translates to roughly a 99.999% true acceptance rate and a 0.001% false rejection rate, which remains significantly better than known alternatives.

As PoH becomes more important to everyday life, universal accessibility will matter. Everyone should be able to verify if they choose to do so. Many common eye conditions, including cataracts, do not meaningfully affect the accuracy of iris biometrics but there are some more severe eye conditions that can affect accuracy. In time, specialized centers could support alternative verification for individuals with severe eye conditions, for example through facial biometrics. Such extensions, however, would need careful design to preserve the system's integrity.

2.8. World's Implementation: Anonymized Multi-Party Computation (AMPC)

AMPC is World's specific implementation of the generic SMPC architecture described previously. It is an open-source, multi-party computation system that anonymizes and securely protects MPC fragments of Orb-verified World IDs. AMPC is not only one of the largest MPC-based systems in production but also breaks new ground by leveraging high-end GPUs to significantly increase performance. These technologies set a new standard for privacy, security, and scalability in biometric verification.

2.8.1. Privacy Protections

AMPC offers additional privacy protections by eliminating the need for storing iris codes and avoiding plaintext Hamming distances during verification. It incorporates the latest advances in cryptographic multiparty protocols and ensures that no biometric data ever leave the user's device. Iris data is cryptographically processed directly on the Orb, rendering a single iris code into multiple encrypted fragments that do not individually reveal any information about the original. The fragments are end-to-end encrypted and transmitted to each compute node so that at no point is user data visible to any party.

One key privacy enhancement is how similarity comparisons are handled. Although iris codes are matched based on Hamming distance, AMPC does not reveal any information about the distances—only a binary result: whether the user is a match or not. The AMPC system reveals only a single bit per invocation: whether the individual has previously verified.

In addition, masks used to filter out noise and highlight relevant features during verification are also broken into fragments, ensuring they never exist in plaintext. This eliminates another piece of information and further enhances privacy.

2.8.2. Decentralization and Transparency

AMPC marks an important step toward decentralization and transparency. It also operates with reputable third-parties like Nethermind, a trusted and reputable blockchain and research engineering company, to operate an independent database in which the anonymized data is stored. Other independent operators include the University of Erlangen-Nuremberg (FAU) and UC Berkeley Center for Responsible Decentralized Intelligence (RDI), with two additional institutions — the Korea Advanced Institute of Science and Technology (KAIST) and the University of Engineering and Technology in Peru (UTEC) — set to join the network. Today, AMPC is operated exclusively by these independent, trusted organizations, and neither World Foundation nor Tools for Humanity serve as parties in AMPC.

A governance board has been established, including independent external domain experts, to coordinate and supervise updates, ensure accountability, and govern onboarding of third parties to operate compute nodes.

2.8.3. Roadmap

Future improvements aim at scaling the system and reducing compute requirements to make it easier for new third parties to join. Trusted execution environments (TEEs) are in development to minimize potential manipulation. Further, AMPC is open source, and the community is encouraged to review, contribute to, and build upon this work. Looking ahead, the World ID 4.0 protocol upgrade introduces changes that strengthen the uniqueness and privacy layer, including abstract on-chain accounts with multi-key support, a distributed OPRF network for nullifier computation, enforced one-time-use nullifiers, and credential recovery via designated Recovery Agents.

2.9. World's Implementation: Semaphore Set Registration

With AMPC, it is possible to prove that an individual is a member of a set—but that single bit of information is not sufficient for the more complex interactions envisioned for PoH. To enable those interactions, World uses another privacy technology: Semaphore.

Semaphore is a generic, open-source privacy layer for Ethereum applications based on zk-SNARKs (zero-knowledge succinct non-interactive argument of knowledge). Using zero knowledge, Semaphore allows Ethereum users (or users of any chain capable of verifying Groth16 proofs) to prove their membership of a group and send signals (e.g., perform actions, cast votes) without revealing their original identity.

World's version of Semaphore is deployed as a smart contract on Ethereum, with a single set containing the hashes of the World ID secrets for all Orb-verified users. A commitment to this set is replicated to other chains using state bridges so that corresponding verifier contracts can be deployed there.

Individuals interact with the protocol through a wallet containing a Semaphore key pair specific to World ID. Semaphore does not use an ordinary elliptic curve key pair, but leverages a digital signature scheme using a ZKP primitive. The World ID secret is a series of random bytes. The signature is a ZKP that proves the person holds a secret that, when hashed, corresponds to an entry in the identity set. Specifically, the hash function is Poseidon over the BN254 scalar field. The hash of the World ID secret is not revealed or disclosed after initial enrollment.

2.9.1. Authenticating Using Proof of Human

2.9.1.1. Generic Architecture

A robust authentication mechanism is needed to prove that an action originates from a human. This mechanism must be privacy-preserving and prevent cross-context tracking:

- **Unlinkable Pseudonymity:** It should not be possible to identify who someone is or to track someone across different contexts.
- **Illicit Transfer Prevention:** The system needs to ensure the person using the PoH credential is the one it was issued to, via a person-bound second factor for periodic reauthentication.

One way to address unlinkable pseudonymity is through a combination of self-custody (user-held key material) and zero-knowledge proofs. Credentials are held locally by users and can be presented without revealing identity or linking activity across contexts. A public, tamper-resistant registry enables verification and revocation without exposing personal data.

Additionally, a second factor is required. The initial verification alone is insufficient to maintain integrity over time. Without continuous authentication, a credential holder could temporarily delegate access to a malicious actor while retaining the ability to reclaim it—making short-term rental economically attractive. Continuous authentication, like face-based checks against embeddings from the initial verification, can be performed locally on the user's device. By requiring frequent reauthentication, the original owner cannot hand off their credential for extended periods. For high-stakes use cases, users can return to a purpose-built biometric camera for high-assurance authentication (an "anonymous notary").

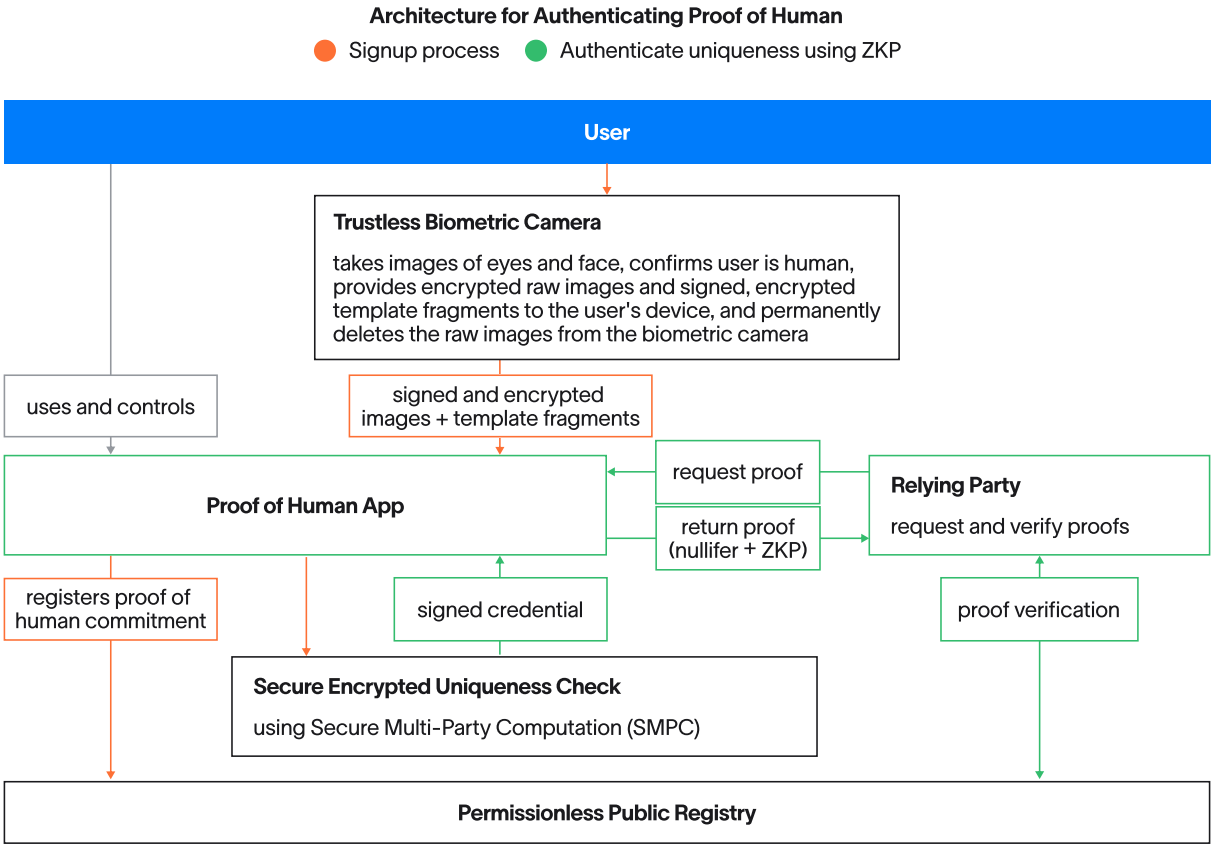

Figure 16: During enrollment (orange), a biometric camera captures images to confirm the user is a real human, then provides signed and encrypted template fragments to the user's device before permanently deleting the images. A SMPC network performs an encrypted uniqueness check to ensure the user has not previously enrolled, and the app publishes the proof of human commitment to a public registry. During verification (green), a relying party requests proof of humanness from the user's app, which generates and returns a zero-knowledge proof (ZKP) paired with a nullifier. The relying party verifies this proof against the public registry, confirming the user is a unique human without revealing their identity.

2.10. World's Implementation: Personal Custody Package

World's specific implementation of the generic authentication architecture begins with the Personal Custody Package (PCP). The data used by the Orb to determine a person is a real human is immediately packaged into a PCP, encrypted, sent to the user's device, and permanently deleted from the Orb.

World publicly announced personal custody in March 2024. At a high level, personal custody ensures that images taken by the Orb are not exposed to World Foundation's (or any third party's) backend systems, but are stored locally and readily available for the user.

As detailed in the Protocol whitepaper, PCP has evolved over time to generally describe a self-custodial credential. There are now multiple types of PCPs, and as the World protocol becomes more established, the PCP format is expected to be publicly documented and standardized for interoperability between credential issuers and the protocol.

Currently, the Orb-specific PCP contains:

- Iris and face embeddings generated by the Orb
- Raw iris and face images
- MPC fragments for the AMPC system

Many data fields are individually encrypted with a key specific to the use case—for example, each MPC fragment is encrypted with the public key of the specific AMPC party. The entire

PCP is then encrypted on the Orb with a key provided by the user, ensuring only the user can access it on their own device.

The PCP provides two primary functions:

1. **Face Auth:** A trusted face image from the verification process is compared against a selfie generated by the device.
2. **Uniqueness enrollment:** The included MPC fragments can be checked to determine whether the user has enrolled in the uniqueness service. Users can only enroll once to receive a unique PoH credential.

2.11. How to Address Common Concerns of PoH

Poorly implemented PoH creates severe risks. However, in a rigorous implementation (see section X), those risks can be contained:

2.11.1. Concern: PoH is a privacy risk and enables surveillance

Poorly designed PoH systems can be privacy invasive, enabling tracking across applications. However, a well-designed PoH implementation can be strongly privacy preserving by design. Without PoH, systems must infer legitimacy indirectly through continuous tracking: behavioral monitoring, device fingerprinting, cross-service correlation, and identity checks. These approaches require persistent visibility into user behavior and create strong incentives for surveillance. PoH shifts the model from invasive monitoring to a privacy-preserving proof. PoH can be implemented private-by-design. Secure multi-party computation protects privacy when establishing uniqueness, having multiple issuers minimizes the risk for censorship and zero-knowledge proofs and unlinkable nullifiers preserve anonymity when proving humanness to others. This way no cross-service profile can be established and surveillance can be prevented.

2.11.2. Concern: PoH requires a centralized database of people

This is the case for traditional identity systems. However, for a well designed PoH system, uniqueness can be verified using encryption techniques that avoid exposing biometric or identifying data and distribute trust across multiple independent parties such that there is no need for a centralized database.

2.11.3. Concern: PoH is a centralizing force

PoH can be designed such that the opposite is the case. Without PoH, influence concentrates among actors who leverage bots, coordinated networks, or purchased accounts. This centralizes power in the hands of those with resources to manufacture participation. PoH inverts this dynamic by making participation human-bounded, which prevents authentic voices from being drowned out and empowers individuals. At the same time, for any PoH there will be an implementation and bootstrapping phase in which in almost all cases will lead to temporary centralization which needs to be iteratively eliminated over time. Initially, there is a small group of people that builds the first version and has decision-making authority. The class of PoH systems we are advocating for can be and need to be progressively protected against incompetence and malice of this initial group of people. The world decentralization whitepaper describes one potential implementation.[2]

2.11.4. Concern: PoH leads to a black market for credentials

When PoH becomes critical, malicious actors will be strongly motivated to amass credentials, which would undermine PoH's effectiveness. While complete prevention of PoH delegation to

[2]https://whitepaper.world.org/advancing-decentralization

bad actors is likely impossible, several measures can significantly increase the difficulty and economic cost of such actions.

Key security and recovery mechanisms include:

- **Strong Authentication:** Using phone-based methods similar to FaceID, combined with regular reauthentication, can ensure that the credential remains under the control of its rightful owner.
- **Recovery Mechanisms:** Enable the legitimate owner to reclaim their PoH following theft or sale, reducing the long-term utility of illicit transfers.
- **Geographic Association:** Optionally disclosing the country of issuance of a PoH can help prevent arbitrage based on income disparities.

Furthermore, as long as each person can only acquire a single PoH, renting it out carries significant risk: if the malicious actor uses the PoH against the terms of use of applications the original owner risks being locked out of essential applications.

Ultimately, if PoH achieves the importance we anticipate, the delegation or misuse of another person's PoH may reasonably be made illegal, mirroring existing laws against the misuse of a passport.

2.12. World ID: Bootstrapping PoH

World is an effort at implementing PoH as described above, with the design goal to maximize individual empowerment.

This whitepaper evaluates multiple approaches to achieving a global PoH mechanism and concludes that biometrics — and specifically iris biometrics — best satisfy the core requirements of inclusivity, uniqueness, person-bound credentials, decentralization, and anonymity. To operationalize iris verification at global scale, TFH built the Orb, a custom, open-source imaging and processing device that prioritizes privacy (local processing and Personal Custody Packages), robust liveness and presentation-attack detection, and auditable security features. In addition to the Orb, Anonymized Multi-Party Computation (AMPC) enables uniqueness checks without exposing biometric data, while Semaphore and zero-knowledge proofs let holders present only the facts they consent to share. These design choices together make a privacy-preserving, auditable pathway to a verified World ID. Iris biometrics offer orders-of-magnitude lower false-match rates than face recognition, and the Orb's engineering and operational model are aimed at producing a reliable personbound credential that scales. The result is a practical technical foundation for systems and services that need to know *"is this a unique human?"* while preserving user anonymity and removing central points of trust.

2.12.1. Proactively Implementing PoH

Bureaucracies tend to address major problems only after significant damage has occurred, which helps focus on what matters most. However, a reactive approach to PoH is highly undesirable and lead to surveillance. This not only results in avoidable negative consequences but also increases the likelihood of a less considered and simpler implementation, which would likely impact efficacy, privacy and freedom of speech. By the time a crisis makes PoH seem necessary —potentially involving extreme outcomes like meaningful increases in societal unrest or other threats to democracy like outcome-altering election interference—the resulting PoH would most likely be implemented in haste. A rush would likely lead to prioritizing speed and functionality above all else, compromising critical elements such as individual empowerment, privacy and resilience to adversarial actors, making the final system far less beneficial than a proactive solution in ways that cannot be addressed iteratively afterwards (local optimum).

The World project is a proactive effort to address these challenges. In order to bootstrap PoH ahead of time and avoid some of the negative consequences, World employed one particular approach to try to counteract the described dynamics: It used its token as an economic

bootstrapping mechanism while PoH is new and adoption is nascent and provides an incentive to verify. Analogous mechanisms have been used historically to grow networks at a smaller scale: for example, in PayPal's early years, the company invested in user incentives to rapidly expand user adoption and achieve network scale, which was critical to its transition from a niche startup to a global platform. The token further gives all network participants a native ownership share for their participation, because the overall system becomes more useful as more people are verified.[3]

2.12.2. Multiple Uniqueness Credentials

In practice, supporting multiple forms of uniqueness can be useful in the short term to accelerate adoption and improve coverage. Therefore, World ID supports not only PoH credentials through the Orb but also credentials through passports and face based verification.

However, when evaluated against the requirements for global PoH, these alternatives exhibit structural limitations. Cryptographically verifiable identity documents with embedded chips (e.g., NFC-enabled IDs) depend on inhomogeneous availability, heterogeneous security infrastructure, and document issuance processes rather than the person themselves. Uniqueness degrades through issuance by multiple authorities (e.g. dual citizenship), re-issuance or replacement, and robust recovery is incompatible with privacy without introducing avenues for serious government surveillance. In more extreme cases, not all governments might be trusted to not create fake IDs (to potentially disseminate disinformation in other countries or even their own).

Similarly, face-based verification on consumer devices provides limited assurance and does not scale to global uniqueness. Camera quality and sensor diversity limit entropy and therefore the ability to distinguish lookalikes. This makes it practically impossible to distinguish real people from high resolution displays showing deep fakes. Compute integrity is also insufficient to prevent attacks.

For these reasons, while multiple credential types should coexist as transitional or complementary mechanisms, purpose-built biometric hardware appears to be the most beneficial long term approach that satisfies the full set of requirements for robust and privacy-preserving PoH.

2.12.3. World ID Today

Most of the security and privacy measures outlined previously—such as the secure hardware device (the Orb), Secure Multi-Party Computation (SMPC), Zero-Knowledge Proofs (ZKPs), and face authentication—are already integrated into World ID. This is complemented by numerous other privacy-enhancing features and ongoing development to further strengthen the system, including World ID 4.0.

World ID is progressing towards global adoption. At the time of this writing, there are about 40M people on World App (the first of ideally many World ID authenticator apps) and about 18M people verified as human with an Orb. At the same time, current projections for advanced machine intelligence require accelerating adoption in order to enable the benefits of PoH when they are needed.

2.13. Other Resources

The World roadmap is a dynamic and evolving blueprint that is subject to change and refinement through input and decisions from the World community. Whether you are a developer, a user, an enthusiast, or simply someone interested in the future of decentralized systems, please reach out through the appropriate channel:

- Join the community discussion on X or Discord.

[3]For more information on WLD, please see this.

- Contribute to open source repositories on GitHub.
- Visit the World developer documentation.
- Reach out directly to the World team for support questions.
- View live on-chain data on the Dune Dashboard.

3. Advancing Decentralization

How to decentralize the World network and minimize central points of failure.

3.1. Introduction

World is a protocol, not a company. This makes decentralization an axiomatic end goal.

If World is to become critical, global-scale infrastructure, it must not—and cannot —be controlled by a single organization or small number of contributors. In that case, the political and economic pressures placed on any single entity would likely be too high: the network would either be corrupted or collapse entirely.

By contrast, decentralization of the World protocol so that it is sustained by a community with dozens, hundreds, or even more independent organizations that use and support the protocol, will enable the network to scale to billions of people while increasing utility and preventing fraud.

In the blockchain community, decentralization often refers to core infrastructure properties like transparency, verifiability, and permissionless access—conferring the network the ability to recover from local participant failures. Additionally, decentralization requires many independent participants to have a sustainable economic interest (e.g. a stake) in maintaining the infrastructure. Those properties are all important for World to function as a true public good. They are also important for adoption and continuous improvement of the protocol by application developers building on the protocol. Without them, the network cannot scale and it cannot be sustainable—that means failing its promise of becoming a trusted, global utility.

Because World is a complex system with multiple technologies that operate together, World Foundation has defined a series of critical use cases and tests to evaluate the stage of decentralization that has been achieved for those use cases.

This whitepaper explores avenues for decentralization of various components of World protocol, including software, hardware and governance.

3.2. Basic World Protocol Glossary

The Orb: The Orb is a verification device which takes pictures of a person, uses on-device analysis to determine that the person is a real, live human, and generates a privacy-preserving enrollment code that can be used to determine if they've previously enrolled—and therefore, whether they are unique. This enables the creation of a "Proof of Human," perhaps the most important new property enabled by the World Protocol.

Relying Party: At its core, the World protocol allows applications to request a user-generated proof (such as Proof of Human, to confirm that they are a verified, unique human). The application requesting a proof is known as the "Relying Party." The Relying Party is often an application on the user's phone, a web application, or a smart contract.

World ID : World ID is a privacy-preserving digital ID. Discrete, unlinkable statements about the user can be generated with a secret value held only by the user—these are known as "Proofs". Proof of Human, as an example, ensures that each human can only have a single "Verified World ID". The World ID can also be used with other credentials to produce other proofs, such as Proof of Age, or Proof of Citizenship. An important property of the World ID is that proofs provided to two different Relying Parties cannot be linked together unless the user wants to do so.

Credential and Credential Issuer: World ID Proofs are generated using information from a credential. Every credential is produced and cryptographically signed by an issuer. For example,

the World Foundation authorizes Orbs to produce the credential that is central to generating the Proof of Human, so the Orb credentials and Proof of Human are issued by the World Foundation.

Authenticator: The "World ID Authenticator" is software authorized by the user to generate World ID proofs. The authenticator may be a single purpose application, but it is more often provided as part of a larger application with other functionality. For example, the World App includes a World ID Authenticator while also bundling financial products and a mini-app ecosystem that extends functionality. Users may have multiple authenticators.

User Agent: Where the authenticator is bundled with other application functionality, it may be referred to as a User Agent. These User Agents may support a wide set of capabilities, as with the previously mentioned World App, or they may be an application with a specific purpose (for example, an application accessing a specific social media service, a gaming client, or an application to purchase concert tickets). User Agents may not necessarily run on a device that is controlled by the user – for example, "AI User Agents" are likely to run on infrastructure provided by an AI provider. As AI capabilities advance, we expect that humans may want to delegate the use of their World ID for certain purposes by providing the AI Agent with an Authenticator.

WLD / Worldcoin: A token governed by the World Foundation that will be used to pay for fees in the World Network such as the World ID Fees.

3.3. Tests to Evaluate Technical Decentralization

Progress in decentralizing the protocol can be measured with three major test cases:

1. **Test 1 – Permissionless Market Launch:** Any operator can *introduce the protocol* to users in a new market without any dependency on any one (other) party.
2. **Test 2 – Protocol Use by Relying Party:** Any relying party can *use the protocol* without dependency on any one (other) party.
3. **Test 3 – Enhancing the Protocol by Issuer:** Any issuer can *enhance the protocol* with new credentials and proofs (including uniqueness modalities) without dependency on any one (other) party.

To further quantify progress, we defined decentralization stages for each of these test cases.

3.3.1. Test 1: Permissionless Market Launch

Much of the global population lives in areas that World Foundation and its existing contributors, such as Tools for Humanity (TFH), cannot directly service due to isolation, regulatory complexity, or mistrust. To allow these people to use the protocol, other parties must be able to provide access without needing World Foundation's support or permission.

The use case: An individual within a new market should be able to go through the verification process (install a World Network-enabled wallet application, verify at an Orb) and then provide proof of human (PoH) without receiving World Foundation's permission or using any technology controlled by World Foundation.

- **Current:** World Foundation governs the development and operation of PoH verification devices (Orbs) and wallets. These wallets use World Foundation authorized or managed backend systems.
- **Stage 1:** World Foundation-managed operation of verification devices will transition to Independent, arms-length operations using TFH/World Foundation front/backend systems.
- **Stage 2:** Stage 1 is achieved, and independent operations can be conducted without direct reliance on World Foundation managed or operated backend systems.

- **Stage 3:** Stage 2 is achieved, and there are multiple World-enabled wallets that can request WLD airdrops from World Foundation.
- **Stage 4:** Both Orb and wallet are provided by multiple parties. Airdrops are managed via smart contracts that are immutable or under decentralized governance.

Achieving Stage 4 will require technical changes to the World protocol, operations and governance. Some of these changes are already underway.

3.3.2. Test 2: Protocol Use by a Relying Party

Many enterprises and large applications hesitate to adopt a protocol that requires third-party permission, especially when long-term business interests may not align.

The use case: Any application or service provider that would like to leverage World Network and proof of human as a relying party should be able to deploy all parts of the technology stack for user enrollment, credential issuance and management, and proof verification without permission from or support of World Foundation (or any other third party). People who have a verified proof of human—originally issued for one relying party—should also be able to use the credential with other relying parties, such as the WLD airdrop highlighted in Test
1.

- **Current:** To prevent phishing and namespace collisions, applications and Mini Apps require a developer account overseen by Tools for Humanity. Users must have World App installed and use a World Foundation-authorized Orb to verify and generate their Proof of Human.
- **Stage 1:** Using a decentralized mechanism, developers can release apps that can request proofs from World App without needing a developer account or reduced trust.
- **Stage 2:** Stage 1 is achieved, multiple User Agents with World ID capable authenticators are connected to the World Network, including ones that are not developed by TFH or World Foundation. So a relying party can request and/or generate proofs without use of any User Agent managed by World Foundation or TFH.
- **Stage 3:** Stage 2 is achieved, and a relying party can deploy their full use case from user enrollment to credential issuance, proof generation and verification by the relying party without any dependency on World Foundation-managed technology or infrastructure.
- **Stage 4:** Stage 3 is achieved, and World Foundation authorization or support are not required for interoperability. Relying parties can independently assess third-party World-enabled applications and verification devices to determine whether they are trustworthy.

Achieving Stage 4 will require technical changes to the World Network protocol, operations and governance. Some of these changes are already underway.

3.3.3. Test 3: Credential integration with the protocol

Today's digital identity infrastructure is fragmented and inefficient. Many discussions with potential relying parties (e.g., governments, identity companies, hardware manufacturers, etc.) are about enhancing the protocol to connect World Network to existing identity infrastructure and systems. World Network can provide a global, privacy-preserving way for users to manage and present credentials when using digital services online. Currently, only World Foundation and Tools for Humanity (via World App) can create a new credential that integrates with World ID.

The use case: Any credential provider can offer a new credential that can be integrated with World ID to be presented by the World ID user directly to relying parties or through privacy-preserving zero-knowledge proof (ZKP) attestations. This requires no permission from World Foundation (or any other party), and relying parties are able to use these credentials to enhance their services.

This enables the existence of a rich ecosystem of potential third-party credentials and proofs that can enhance the protocol.

- **Current:** Multiple credentials (Orb, NFC-enabled identity document, and device uniqueness) exist within World App.
- **Stage 1:** Credential formats are publicly documented. New credentials and ZKP attestations can be added by third parties with permission of World Foundation.
- **Stage 2**: User-controlled API for managing 3rd party credentials/attestations in World App (and other authenticators).
- **Stage 3:** Third-party unique credentials can be permissionlessly introduced using AMPC-based uniqueness services.
- **Stage 4:** World ID fees are deployed: relying parties pay credential issuers and the protocol to create a sustainable economic model for the protocol.

Achieving Stage 4 will require technical changes to the World Network protocol, operations and governance. Some of these changes are already underway.

3.4. Technical Roadmap for Decentralization

The following sections outline several different areas of World—User Agents (e.g., World App), verification hardware (e.g., Orbs), hardware operations, protocol, and governance—and how they can be improved through decentralization. The optimal mechanisms to increase decentralization may evolve over time, and suggestions for improvements are welcome.

3.5. User Agent

World App was the first application designed to work with the World Network, and it consists of three primary components:

- An *authenticator* that manages the user's identity on the network and provides proofs to relying parties.
- A self-custody *wallet* that provides access to the financial functionality within World App.
- A *miniapp* platform that allows Third-Party applications to be deployed within the World App.

World App was launched as the first user agent to support World Network, enabling people to verify their World ID at an Orb and interact with relying parties. World ID is already available through the IDkit and Minikit (see developer portal), so any developer who wants to use Sybil protection in their application can connect to World Network via World App.

While currently users must first download World App to interact with the World Network, World Foundation is encouraging the development of other applications that connect to World Network. These applications are called *User Agents*, and, like World App, they connect to the network as an *authenticator*. World Network is designed so that any developer will be able to build their own user agent without requiring permission from World Foundation or any other contributor to the World project.

Research is currently underway to develop Authenticator SDKs that will make it easy for any application to connect directly to World Network while still serving the high level of privacy and security required by relying parties. This gives the user more choice of which user agent to use.

3.5.1. Enabling Decentralized Trust

There should be multiple user agents for people to choose from at the time of verification at an Orb, or when using World ID to provide a proof to a relying party. To enable a diverse range

of trustworthy user agents, Tools for Humanity is currently working to improve the following components:

3.5.1.1. Integrity Services

Relying parties must be able to evaluate the authenticator environment that provides World ID proofs to determine whether they can trust the integrity of the provided proof. The World ID zero-knowledge proof itself is independent of the authenticator, however, additional security features (e.g., World ID Face Auth) require verifying the integrity of the User Agent and its authenticator. This is the result of privacy requirements which encourage local computation on the user's phone. While local computation could potentially be secured through zero-knowledge proofs and the Orb's image is signed, additional credential sources (including objects like a second input image taken through the user phone's camera) may not maintain a similar level of data integrity. Until manufacturers begin attaching hardware attestations to those images, comparison to an image from the phone's camera fully relies on trusting the integrity of the phone's hardware and software. Thankfully, OS-level attestations already exist on an app level (e.g., Apple App Attest or Google Play Integrity) and can be used as a lower level integrity assurance signal. The verification of those can be handled by services that sign off on individual requests and enhance trust.

3.5.1.2. World ID Authenticator Kit (previously referred to as Wallet Kit)

World App already contains all the logic for handling an Orb verification and using World ID to generate and submit proofs (such as when receiving WLD grants). This process can be made simpler and quicker for new teams building their own applications. Authenticator Kit will handle the connection with the Orb and establish the privileged execution environment on the phone through the integrity services. Importantly, it should also contain a mobile-optimized proof-generation library.

3.6. Verification Devices

In the context of World, specialized verification devices (Orbs) enable the verification of humanness and the issuance of World IDs. There are several ways to make Orbs more transparent, verifiable and accessible. Increasing transparency and verifiability of the Orb's functionality can help align the incentives of manufacturers not to be malicious. Furthermore, letting anyone develop alternative Orbs democratizes the solution space and accelerates decentralization.

The following sections walk through different milestones that can contribute to the robustness of Orb infrastructure.

3.6.1. Core Orb Engineering open source

To allow Orb functionality to be verifiable by the public and enable anyone to build their own Orb, the firmware and hardware have been made open source.

3.6.1.1. Hardware Source-Available

Today, hardware components that aren't security critical (e.g., tamper detection and security board) have been made publicly available. Eventually, *as much as possible* should be made publicly available, but it is unclear whether publishing all Orb components is desirable given the security considerations described in the next section. There should be a continuous evaluation of which sensitive components can be made open source.

3.6.1.2. Core Firmware Components Are Open Source

Publishing core firmware components makes the functionality of the Orb more transparent and is a requirement to achieve verifiable Orb provenance and firmware. Therefore, a large part of the firmware of the Orb has been open-sourced.

Making these core components open source enables others to understand the functionality of the Orb in more detail and build alternative Orb firmware implementations. Potential vulnerabilities can be submitted through a public bounty program.

Given no hardware device can be perfectly secured, other sensitive components (like spoof-prevention algorithms and fraud models) that may pose a direct integrity or security risk to the ecosystem if exposed will likely not be made open source. Importantly, World doesn't need to rely on perfect hardware security when complemented with mechanisms like auditing of Orb operations. To reduce trust requirements on non-open-source parts of the code, the open-source code defines software "sandboxes" for some closed-source components. For example, consider a closed-source fraud-detection module that ingests biometric data. The open-source code that interfaces with this module can provide strong evidence that the closed-source code cannot save/upload any biometric data.

3.6.2. Enabling Decentralized Trust

In a decentralized World Network, relying parties have access to the information they need in order to assess the trustworthiness of any credentials or proofs they verify. Orbs are one of the most important roots of trust for credentials in the network and must meet exceptional standards for trustworthiness. To ensure the integrity of the network and reduce trust in provisioning, Orbs should fulfill certain requirements (see Secure Provisioning Standard). However, no provably secure hardware exists, and certain points of trust remain as described in Orb Provenance Verification. Importantly, World Network doesn't rely on perfectly secure hardware, and audit logging and in-person auditing of Orb locations can help decrease incentives for malicious actors.

The following technologies are currently being improved to help reduce trust assumptions; they provide relying parties and the broader community with the ability to evaluate the trustworthiness of any verification device.

3.6.2.1. On-chain Orb Registry

The "Orb Registry" refers to the set of active Orbs currently endorsed by World Foundation. If an entity's process can be sufficiently trusted (e.g., by implementing a secure provisioning standard and conducting regular audits), the insertion of public keys from that entity in the Orb registry could be delegated to that entity. To limit the harm caused by a malicious Orb, World IDs registered with different Orb manufacturers (and ideally with different Orbs) should be distinguishable from each other. This makes it possible for the ecosystem to respond to (inevitable) attacks by removing individual Orb manufacturers, and perhaps even individual Orbs, from the whitelist on demand. Optionally, World IDs associated with fraudulent Orbs could be revoked. This information can be private and only stored on the World ID holder's device as long as it is provable on demand. If anyone were mistakenly affected by such action, they could re-verify through an active Orb. As a last resort, disagreement in the set of trusted provisioning entities could be resolved by forking the protocol and adding or removing provisioning entities.

3.6.2.2. Secure Provisioning Standard

"Secure provisioning" refers to the process of setting up the cryptographic keys of an Orb. One part of such a standard could, for example, specify that only certain approved secure element models can be used and require proofs of authenticity from each secure element (via die-unique

certificates signed by the secure element vendor) to be reported alongside the public keys. Orbs generated by this process can then be considered securely provisioned.

Today, a secure provisioning process is in place that involves generating private keys on a secure element as well as burning secrets generated on an air-gapped machine connected to a hardware security module into private fuses (only accessible by TrustZone applets). These secrets are derived using a NIST-SP-800-108 KDF algorithm into two keys transmitted to the backend used for future device attestation, and then are immediately destroyed. The original key material only exists in the restricted fuse banks on the NVIDIA Jetson and within the secure element. Continual auditing of the process can help maintain a high security bar.

3.6.2.3. Auditing of Orb Operations

Auditing operations can help detect malicious operators and malicious Orbs, thereby disincentivizing malicious behavior. No entity in World Network should have to be trusted. Therefore, all operations need to be audited in a distributed manner.

One primary concern is someone being able to inject fake iris codes. In this case, "fraudulent" means the entity has a way to spoof requests to the uniqueness service to make them seem as if they came from a legitimate Orb. Security measures on the Orb should make such an attack very difficult. However, the risks associated with malicious individuals involved in provisioning and/or flaws in digital security can't be entirely eliminated.

The auditing of Orb operations by incentivized users and dedicated auditing organizations, when combined with software- and hardware-security measures, can make generating fake IDs very hard. Today, operations are already audited by third-party organizations. To increase the robustness of this process, a list of all Orbs, their locations and operational information about the Orbs could be made public.

3.6.2.4. Incentivized Re-Verification

Similar to auditing of Orb operations, verified users can be incentivized to re-verify at a different Orb. For any attacker who compromised an Orb or spoofed verifications, such a second verification at a different Orb would be very difficult to also spoof. Therefore, statistically, the fraction of incentivized users that end up verifying a second time with a different Orb would be lower for a compromised Orb, allowing anomalies to be detected.

3.6.3. Orb Security Transparency

Below are steps toward making the security of the Orb more transparent:

3.6.3.1. Publish Audits

World Foundation regularly conducts and publishes hardware and firmware audits like this one to help ensure that the systems being built are as secure as possible, and to increase transparency into those systems. Such audits entail both security and privacy considerations.

3.6.3.2. Public Bug Bounty Program

A bounty program can raise the security bar by finding vulnerabilities early. In collaboration with Tools For Humanity and HackerOne, World launched a public bug bounty program in February, 2024. The program is being continuously extended with additional endpoints, source code and new categories of attacks.

3.6.3.3. Verifiable Orb Provenance and Firmware

While there is significant research involved, ideally, the public would be allowed to verify properties of an active Orb, including that it is:

- not counterfeit and is from an Orb vendor that meets manufacturing and security standards
- configured to only boot signed firmware
- running a specific version of the firmware

These verifications can help mitigate important privacy concerns related to biometrics. The public should not need to blindly trust an Orb vendor to faithfully/correctly implement privacy-preserving firmware.

Eventually, there may be a path to allow for firmware that hasn't been approved by World Foundation governance, though it is unclear whether this would be desirable given the potential downsides. This would require appropriate incentive and audit mechanisms to disincentivize malicious behavior, which could turn out to be unviable in practice.

3.6.3.4. Orb Provenance Verification via User Agent

A first step towards verifying an Orb as non-counterfeit could be implemented through provenance verification via the user agent. Such a mechanism could help verify that an Orb is from a vendor that has been approved by World governance and therefore is running approved firmware. Such a feature can be integrated into other protocol-compatible apps.

One possible path for such a verification could be to ask the Orb to sign a challenge that has been generated by the App. Orbs contain two mechanisms for cryptographically attesting they are in the Orb registry: private keys in the secure element and private keys derived from fuses on the NVIDIA Jetson. Verifying signatures from both sources provides strong evidence that an Orb was manufactured by a vendor that has been approved and was not subsequently tampered with. Verification of the NVIDIA Jetson fuse state can provide strong evidence that Orbs can only boot firmware that has been signed. The user agent could also request an Orb's firmware version from the Trusted Execution Environment's (TEE) secure storage. As part of a normal boot, the root hash for dm-verity can be delivered to the bootloader by the TEE, ensuring that only code authorized by the TEE is able to boot. Inside of secure storage, these hashes would be associated with version numbers, allowing an entity (e.g., the World App) to request attestation of the current hashes and version numbers existing in the secure storage.

This mechanism assumes that an Orb's private key only exists in its secure element (i.e., there are no other copies), a constraint which should be specified by the secure provisioning standard. Private keys are generated on the secure element directly and never leave, and a series of transparent certificate attestations during generation and export can prove that a particular key originated from a legitimate secure element. Therefore, physically attesting an Orb has a private key provides strong evidence that the same private key is not in the control of an attacker. Extracting private keys from the Orb's secure element is assumed to be extremely difficult.

It is important to note that it is impossible to fully eliminate attack vectors of Orb hardware vendors/manufacturers or upstream vendors. The following attack vectors remain:

- The Orb vendor could bypass parts of the secure provisioning process (due to malice or incompetence), invalidating the guarantees of the proposed verifications. Therefore, Orb manufacturers should be audited to ensure the secure provisioning standard is maintained, and World Foundation is sponsoring research on other ways to harden the software supply chain..
- NVIDIA firmware could have security vulnerabilities or backdoors, which could threaten the Jetson fuse attestation.
- The secure element vendor could be compromised/incompetent/malicious, which would threaten the integrity of the corresponding attestation.

- The World Foundation could sign malicious firmware. Hardware support for firmware verification helps enable procedures to verify the actual firmware running on an Orb.

Therefore, there should be mechanisms to mitigate the risk of fraudulent manufacturers or compromised Orbs. In-person auditing of Orb locations and incentivized re-verification can make exploiting backdoors significantly harder and help detect malicious verification of World IDs in retrospect.

3.6.3.5. Reproducible Builds

Without reproducible builds, the public is required to trust that compiled firmware wasn't maliciously modified during/after the build. Reproducible builds provide a mechanism to verify that Orb firmware was compiled from a specific state of the public repositories. To verify the integrity of the firmware, third parties should be able to build it from source on their own infrastructure. Full reproducibility means the resulting artifacts should be identical to those deployed to Orbs, and the signature from the signed firmware should be valid for the self-built firmware. The initial priority should be to make privacy-sensitive components of the firmware open source and reproducibly built.

However, there are some limitations. The firmware should (at least initially) include closed-source components, which are opaque parts of the system. Some of these are from Tools for Humanity (e.g., spoof-detection models) and some are from vendors (e.g., NVIDIA firmware components). Additionally, some components may be hard to make reproducible. These can be built separately and pulled in as compiled components to the main build.

3.6.3.6. Hardware Support for Firmware Verification

The most transparent way to verify firmware is by having read access to the storage of the main computing unit. The new generation Orb has a removable SD card that is easily accessible from the outside, and no persistent storage. Public auditors can use this mechanism to verify the integrity of a particular Orb's firmware. The integrity verification of the dumped memory could optionally reuse the Orb's internal integrity verification mechanism (dm-verity). This can provide stronger guarantees than Orb provenance verification via user agent, as there are fewer attack surfaces for spoofing direct physical access relative to remote attestation schemes.

While this mechanism provides strong guarantees for the firmware state, it is still possible to spoof the auditor at the hardware level. For example, there could be a second hidden flash chip that the Orb is actually booting from. This risk could be mitigated by additional audits that inspect the hardware directly on a random subset of devices. Further, in-person audits of Orb locations can make attacks significantly easier to detect and can create disincentives for malicious behavior.

3.6.4. Operations

Operations, in the context of World, refers to procedures in the "analog world" that allow people to get their World ID verified. The primary participants are Orb operators (i.e., independent entrepreneurs and their organizations around the world) who provide Orbs in physical locations for people to verify. Currently, all Orb operators have a commercial relationship with World Foundation. In the future, we expect that Orb operators will be able to acquire, deploy and manage operations without permission from World Foundation or any other entity. Certain infrastructure primitives can help reduce trust assumptions and align the incentives of all participants.

3.6.4.1. Community Operators

In 2025, Tools for Humanity (TFH) expects to provide the general public with the ability to become an Orb operator. They should be able to acquire an Orb and use it as part of a standalone operation to extend the protocol (as described in Test 1) or to develop a new use

case (as described in Test 2). These new operators will complement the existing World Spaces and flagship operations that are overseen by TFH and other partners of World Foundation.

3.7. Protocol

The protocol contains off- and on-chain components that are responsible for handling, for example, verification or authentication requests from users. Since privacy is central to World ID, it is especially important to not sacrifice it in favor of accelerated increases in transparency, verifiability and resilience. One example of this is the uniqueness service, which still requires more research before it can be made more permissionless.

The following sections describe possible improvements to further increase transparency, verifiability and robustness of the protocol:

3.7.1. Protocol Open-Source

All of the components of the protocol are already open source (see the open source tree).

3.7.2. Protocol Security Transparent

Over the course of several months beginning in April 2023 prior to World's public launch, audit firms Nethermind and Least Authority conducted two separate security assessments on the off-chain and on-chain components of World Network, including the following parts of the protocol:

- Correctness of the implementation, including cryptographic constructions and primitives and appropriate use of smart contract constructs
- Common and case-specific implementation errors
- Adversarial actions and other attacks on the code
- Secure key storage and proper management of encryption and signing keys
- Exposure of any critical information during user interactions
- Resistance to DDoS (distributed denial of service) and similar attacks
- Vulnerabilities in the code leading to adversarial actions and other attacks
- Protection against malicious attacks and other methods of exploitation
- Performance problems or other potential impacts on performance
- Data privacy, data leaking and information integrity
- Inappropriate permissions, privilege escalation and excess authority

Of the issues detected by Nethermind, which performed a comprehensive audit of World's smart contracts, 92.6% were identified as fixed after the re-audit stage, while 3.7% were mitigated and 3.7% were acknowledged.

Details of these audits can be found in the Nethermind and Least Authority reports.

Since its launch, the World Protocol has continually evolved, with audits performed whenever sensitive or complex updates are introduced. For example, the uniqueness service, now based on an SMPC protocol, has undergone multiple audits from Least Authority which can be found here, here, and here.

3.7.3. Publicly Available Merkle Tree

The set of World ID public keys is already publicly available and committed to by the sequencer on Ethereum. The public keys are available as calldata, and the current state of the Merkle tree is committed as a Merkle root. Its validity is enforced through a ZK validity proof of batch insertions of public keys. While this ensures that the committed root actually corresponds to a Merkle tree, it's not yet ensured in the validity proof that the public keys actually originate from an Orb. Even though the leaves are publicly available, it's practically infeasible for the client to download all of this data and reconstruct the tree to be able to compute a Merkle

inclusion proof. The tree availability service serves those Merkle inclusion proofs to clients. Clients can check the correctness of the Merkle proof against the on-chain root. However, this request can leak additional metadata about the client (e.g., IP address). This can be addressed by routing those requests through mixnets or through private information retrieval.

3.7.4. Permissionless Merkle Tree

As mentioned above, the validity proof of the Merkle tree needs to be enriched by a signature check of the public key. Once this check is added, trust in the identity sequencer is no longer required. Similar to the uniqueness service, this sequencer also needs to actually implement coordination to rotate between multiple sequencers so there is no possibility of censorship.

3.7.5. World ID Fees

The World Foundation is extending the World ID protocol to introduce World ID fees, payable in WLD. Usage will remain free for end users while applications will be charged for using World ID services. Each credential issuer will be able to set and retain their own credential fee, while a separate protocol fee will flow back to the protocol itself. More details were provided in a blog post on April 30, 2025 and technical specifications are expected to be released in 2025.

3.7.6. Decentralized Trust: Attestation and Auditability

Tools for Humanity and World Foundation are currently working to provide an update to the protocol that incorporates hardware and software security attributes (e.g., "attestations") that allow for a decentralized trust model for authenticators, verification devices (Orbs), uniqueness services and relying parties. This will be released as open source and as a public standard that can be used by any third party to build or deploy infrastructure on the network.

3.7.7. Decentralization of Uniqueness Service

Increasing the resilience of the uniqueness service is challenging because a permissionless operation of the service would require iris codes to be public. A permissioned set of nodes that run the computation and agree on the result through consensus—or run the comparison on a reduced version of the iris codes so that no node has the full code—improves the verifiability of the system. As of 2024, such a system (known as AMPC) has been introduced.

3.7.7.1. AMPC

AMPC, or anonymized multi-party computation, is a quantum secure multi-party computation (SMPC) setup that anonymizes and securely protects the iris codes of Orb-verified World ID holders. It leverages NVIDIA H100 GPUs as the main compute platform to enable up to 50 million pairwise uniqueness comparisons per second.

AMPC incorporates the latest advances in cryptographic multiparty protocols and further improves on state-of-the-art techniques. This ensures that no iris codes ever leave the user's device. Instead, iris data is cryptographically processed directly on the Orb and rendered anonymous. Only anonymous data, which are secret shared and end-to-end encrypted, are transmitted separately to each compute node of the AMPC setup.

AMPC improves the way similarity comparisons are handled. In the previous version, pairwise Hamming distances were used in plaintext to determine the outcome of the enrollment process. In AMPC, only a binary result is revealed: whether the user is a match or not. This approach improves privacy even further.

In addition, iris masks, which are used to filter out noise and highlight relevant features of the iris for the uniqueness check, are now also secret shared, ensuring that they never exist in plaintext at any stage. This eliminates another piece of information and further enhances

privacy protections for users. The architecture allows users' biometrics to remain secure, private and anonymous throughout the entire process.

Leveraging high-end hardware for superior performance

To achieve the high throughput required for global-scale biometric verification, AMPC leverages GPUs as the main compute platform. The AMPC protocol has been fully implemented using NVIDIA CUDA, enabling approximately 50 million pairwise comparisons per second overall.

Each compute node consists of an AWS p5.48xlarge instance with eight NVIDIA H100 GPUs. These instances provide around 3200 Gbps of bandwidth through Remote Direct Memory Access (RDMA) and 20 exaflops of compute performance.

Not only the uniqueness check itself, but also the transition from SMPC to AMPC was designed with the highest security and privacy in mind. This migration process, which involves changes in how the underlying cryptographic secret sharing works, is fully SMPC-based itself, meaning that no biometric data is ever processed or exposed during the upgrade. This ensures that user privacy is maintained throughout the entire transition process.

A decentralized and transparent approach

AMPC marks an important step toward decentralization and transparency.

World Foundation has partnered with Friedrich-Alexander-Universität Erlangen-Nürnberg in Germany, UC Berkeley Center for Responsible Decentralized Intelligence (RDI) in the U.S, and Nethermind, a trusted and reputable blockchain and research engineering company to operate a Multiparty Computation Setup, in which the anonymized data will be stored.

Figure 17: AMPC universities

Additionally, the Blockchain Center of the University of Zurich in Switzerland and the Korea Advanced Institute of Science & Technology (KAIST) have committed to assisting in advancing the secure storage of the anonymized data. This shift will help create a global and decentralized system, ensuring that no entity has access to biometric data.

To further enhance community oversight, a governance board has been established, which will include independent external domain experts. This board will coordinate and supervise updates, ensure accountability, and govern the onboarding of third parties to operate compute nodes in the AMPC setup.

Scaling for the future

The future roadmap for AMPC includes numerous improvements aimed at scaling the system for future growth. These also ultimately serve to reduce the compute requirements, making it easier for new third parties to join the network. Additionally, trusted execution environments are in development to minimize potential room for manipulation of those trusted AMPC parties.

Like its predecessor, AMPC is open source. Transparency is essential for building trust in privacy-preserving technologies. Anyone is invited to review, contribute and build upon the codebase.

Unprecedented privacy in biometric systems

AMPC is not only one of the largest SMPC-based systems in production but also breaks new ground by leveraging high-end GPUs to significantly increase performance. These technologies set a new standard for privacy, security and scalability—all while advancing the state of biometric verification.

For a detailed description of the techniques used in AMPC, please refer to the paper, Large-Scale MPC: Scaling Private Iris Code Uniqueness Checks to Millions of Users.

3.8. Governance

A global community of developers, individuals, economists and technologists conceived and made early contributions to World Network. The original idea started with co-founders Sam Altman, Alex Blania and Max Novendstern, who founded Tools for Humanity and assembled a team to begin developing the technology to support World.

Tools for Humanity is a technology company building for humans in the age of AI. . It is a Delaware (U.S.) corporation headquartered in San Francisco, California, with a wholly-owned subsidiary, Tools for Humanity GmbH, based in Germany. Tools for Humanity supported World's multi-year beta testing phase, during which it developed the Orb and the World App.

Tools for Humanity and other early contributors are committed to providing every person on the planet access to the global economy, regardless of country or background.

Today, the governance of World is overseen by World Foundation, an independent entity that is committed to transitioning World governance to all of humanity. It is important that this happens in a deliberate way. Therefore, governance (e.g., voting) must be well-studied and tested before this transition.

The following sections describe different improvements that are either already occurring or can contribute to this objective:

3.8.1. World Foundation Setup

On October 31st, 2022, World Foundation was established as the non-profit steward of World, supporting and growing the ecosystem as it becomes self-sufficient. The Foundation's main objective is to scale an inclusive identity and financial network as a public utility and to expand the governance thereof. This infrastructure has the potential to empower everyone to participate in the global economy in the age of AI.

The Foundation is an exempted limited guarantee foundation company, which is a type of non-profit incorporated in the Cayman Islands. It has a wholly owned business company subsidiary in the British Virgin Islands called World Assets Limited. This is "one of the most often used, and internationally recognized structures" for decentralized blockchain projects.[4] World Foundation is "memberless"; it has no owners or shareholders.

This entity setup was a good fit for World due to the Foundation's separate personhood, limited liability, tax efficiency, support for compliance with virtual asset regulations and suitability for long-term community governance. That last point is especially important. Cayman foundation companies can be structured to be "memberless" (that is, have no owners or shareholders) and instead to take instructions from token holders and/or World ID holders. They can therefore gradually steer matters such as running a grant program, open sourcing intellectual property (IP), entering into service agreements and managing a treasury. In the case of World, the shared governance model is all the more critical so that, in the long term, decisions can reside with the community.

At the same time, the Foundation can aid the community's governance by safeguarding protocol IP. In most legal systems today, a traditional legal entity is needed to protect IP such as trademarks, open-source copyrights and domains. Tools for Humanity has already transferred core protocol IP to the Foundation, including smart contracts, the World ID SDK, patents for the Orb design and iris recognition technology, brand assets, domains and social media

[4]To learn more about this arrangement, check out this Guide to the Cayman Islands Foundation Company from the Foundation's outside counsel at the law firm Ogier.

accounts. And the Foundation has open-sourced several core tech repositories and made the Orb's hardware available under its Responsible Use License.

3.8.2. Transfer of Control and Ownership to the Foundation

In order to facilitate future governance models, several assets and key components have been transitioned to World Foundation:

- Treasury: World Foundation (and/or its affiliate entities) manages the treasury of tokens once they are unlocked. This includes World grants, operator rewards, and other contributor grants.
- Orb IP: Tools for Humanity has transferred the Orb IP to World Foundation. The Orb hardware and software will be made publicly available under a restricted use license, prohibiting the misuse of the technology. This allows the Foundation to onboard other organizations building Orbs or similar devices.
- Ability to Whitelist Orb Provisioning Entities: The Foundation manages the permissions for adding Orbs to the network, balancing hardware distribution, security and growth.

In order to grow the network and ultimately enable all of humanity to participate in the governance of World, the issuance of World ID and allocation of the WLD token (in certain countries) is ongoing.

3.8.3. Support Future Development

To encourage individuals and organizations to contribute to World Network through research, the development and production of Orbs or auditing of the system, World Foundation is setting up a grants program. Further, the World Improvement Proposals process is currently being created and will be open for proposals soon.

Separately, the Foundation intends to work on common standards and ecosystem-wide proposals. For example, today, Orbs are developed and produced by Tools for Humanity. Orb operations are managed by several organizations around the world. With support from Tools for Humanity, the Foundation will work on standards and incentives for organizations to develop, produce and operate Orbs such that production of Orbs and their operation can be further distributed. More details can be found in the Orb whitepaper.

3.8.4. Initial Community

World maintains a dynamic and evolving blueprint that is subject to change and refinement through input and decisions from the World community.

To enhance transparency and facilitate community involvement, regular community calls should be established with the aim of providing a platform for open dialogue and updates on World's progress. Additionally, a dedicated forum similar to ethresearch should be set up to further foster meaningful discourse and engagement around World. This forum can serve as a hub for ideas, suggestions and discussions among community members and the project team. Lastly, the Foundation has already hosted several developer meetups and strives to create more opportunities for developers to collaborate, innovate and contribute to World.

3.8.5. Decisions by Community

Increasing the resilience of the governance of World Network is both imperative and unprecedented, given the foundational nature of proof-of-personhood infrastructure and the ambition to scale it to billions of people. Building a community-based governance system for World represents perhaps the most formidable challenge of the entire project, and this process is still in its earliest stages.

The Foundation should ultimately have a limited role in the protocol's governance. To this end, the Foundation's founding documents have provisions for community-driven governance. These provisions make it possible, through a prescribed process, for the community to make recommendations to the Foundation's board of directors. For further details, see the Foundation's Memorandum of Association and Articles of Association.

World ID provides unique infrastructure for distributed governance and presents the opportunity to harness input from a large and diverse set of individuals for community-driven governance. The reach of World ID is unprecedented. As a proof-of-personhood protocol, World ID naturally supports "one-person-one-vote" voting, in contrast to token-based voting commonly used by other blockchain projects. Notably, this adds more democratic options to the design space of voting mechanisms for World. However, the exact structure of delegating decisions to the community needs careful iteration and consultation with experts. Further, many governance decisions notoriously lack engagement from participants. Therefore, it will be important to encourage a large set of people to participate and explore the decisions. In the future, the user agent should serve as an entry point for using World as well as the governance of it. Additionally, multi-stakeholder governance models akin to ICANN should be explored.

3.8.5.1. Full Handover to Community

World Foundation is committed to continuously transitioning governance toward a model that sustainably enables World to benefit all humanity. This is an unprecedented endeavor in scale and complexity for a decentralized system, which will require a methodical and gradual approach. Key aspects like voting mechanisms should be thoroughly researched, validated with experts and tested before meaningful control is transferred. Transparency, inclusivity and neutrality are essential. However, these attributes contribute to intricate governance structures like today's democracies, which can lead to often slow and expensive decision-making. While this deliberateness is beneficial for making long-term strategic decisions, such as amending a constitution, it can hinder the ability to quickly adapt to new challenges during the initial growth phases. Hence, prematurely adopting a governance model that fully transitions governance to the community without a well-vetted plan is itself a failure mode to be avoided.

The Foundation seeks input from contributors, the community and experts in the field as it increases the robustness of the governance of World Network

3.9. Other Resources

The World roadmap is a dynamic and evolving blueprint that is subject to change and refinement through input and decisions from the World community. Whether you are a developer, a user, an enthusiast or simply someone interested in the future of decentralized systems, please reach out through the appropriate channel:

- Join the community discussion on X or Discord.
- Contribute to open-source repositories on GitHub.
- Visit the World ID Developer Docs and Portal.
- View live on-chain data on the Dune Dashboard.
- View the Decentralization and Open Source Roadmap.

---

4. Designing for Scale

How WLD powers governance, identity and financial access for every verified human.

4.1. Mission: Building a global identity and financial network

The mission of World is to build the world's largest identity and financial network as a public utility, giving ownership to everyone. The project's goals regarding the Worldcoin token, WLD, are as follows:

1. The majority of WLD tokens will be claimed by individuals simply for being verified unique humans.
2. The majority of humans alive today will claim WLD tokens, which may result in WLD becoming the most widely distributed digital currency.
3. The WLD token, alongside World ID, will be used for protocol governance.
4. The WLD token will form the basis of the largest anonymous identity and financial network.

4.2. Introducing WLD

WLD is designed as a cryptocurrency with governance properties, with the goal of eventually empowering users by giving them a say over the future of the protocol. Beyond conventional "one-token-one-vote" governance mechanisms, the introduction of World ID paves the way for "one-person-one-vote" mechanisms. These two mechanisms can be combined in many ways to enable new ways of governance. While World Foundation currently acts as the steward of the protocol, it plans to solicit proposals and interface with community-governance projects on how World ID and the WLD token should interact in World's future governance model.

The community of users may determine the token's utility for governance, but a few other use cases could emerge. For example, users may decide to use WLD within the World Network ecosystem to access features within World App or another wallet app, such as tipping, buying and selling goods, or signaling their support for causes or initiatives.

World Foundation is currently governing the project and is working toward progressively decentralizing governance and the ecosystem. The goal of decentralization will be aided by World Foundation's unique approach of giving the majority of the WLD token supply to participants of World Network—simply for being humans.

4.2.1. The WLD Token

Launch Date	July 24, 2023
Network Information	Worldcoin (WLD) is an ERC-20 token on **Ethereum Mainnet.**** **** **Individuals claiming user tokens will receive bridged WLD tokens on World Chain Mainnet, an OP Stack layer-2 network on top of Ethereum**.** Therefore, most WLD token transactions will likely take place on World Chain. If needed, the token can be bridged back to Ethereum through the OP Stack Superbridge.
Address: Ethereum	0x163f8C2467924be0ae7B5347228CABF260318753
Address: World Chain** **(main venue for access and use)**	0x2cFc85d8E48F8EAB294be644d9E25C3030863003
Address: Optimism** **	0xdC6fF44d5d932Cbd77B52E5612Ba0529 DC6226F1 Between July 24, 2023, and October 17, 2024, Optimism was the main venue for access and use of WLD. While WLD remains available on Optimism, the main venue for access and use is now World Chain.
Upgradability	None. No control, except inflation starting 15 years after token launch (see Inflation below).
Token allocation entity	World Assets, Ltd., based in the British Virgin Islands. World Foundation is its sole member and director.
Initial supply cap	10B WLD tokens (also see Inflation below)
Inflation	Any inflation of the WLD supply beyond the initial 10B token amount can only start, at the earliest, 15 years after launch (specifically, on July 24, 2038, 4am UTC). The rate of inflation is to be determined by protocol governance. The allocation of any newly-minted tokens is to also be decided by governance. The inflation cap, enforced by the WLD token smart contract, is 1.5% annually. The default inflation rate = 0%.

4.2.2. Availability

Worldcoin tokens are not available to people or companies who are residents of, or are located, incorporated or have a registered agent in, the State of New York or certain other restricted territories. More details can be found in the Terms of Use, including additional restrictions on eligibility.

4.2.3. Safety reminder

Watch out for fake apps claiming to be associated with World, and platforms or third parties that may try to sell or provide you with fake WLD tokens! Ensure that whenever you are transacting in WLD that it has the correct token address listed above. If the WLD have been "bridged" to another chain that is not Ethereum, World Chain, or Optimism, make sure this bridged version is secure and can always be redeemed or bridged back for WLD on Ethereum, World Chain, or Optimism. World Foundation and its affiliates are not responsible for the creation, operation, or security of any bridges deployed by third parties, nor any WLD that is bridged through them.

4.2.4. Important User Information

Cryptocurrencies, tokens, and blockchain applications are highly risky. They are novel and rapidly-evolving technologies whose availability, usage, utility, value, and functionality is dependent on and affected by third party actors, market forces, regulatory environments, and emergent or changing technologies and behaviors. These factors create significant complexity and introduce new and unanticipated risks or consequences. WLD may never increase in value and/or utility, or it may lose all value and/or utility. For more information, visit https://world.org/risks.

4.3. WLD Token Allocation

The following figure shows the allocation of WLD's total supply to the four high-level stakeholder groups. Note that, since launch, the token allocation has changed within the 25% of the TFH Investors + Team + TFH Reserve allocation of tokens. The 75% World Community tokens are unaffected by this.

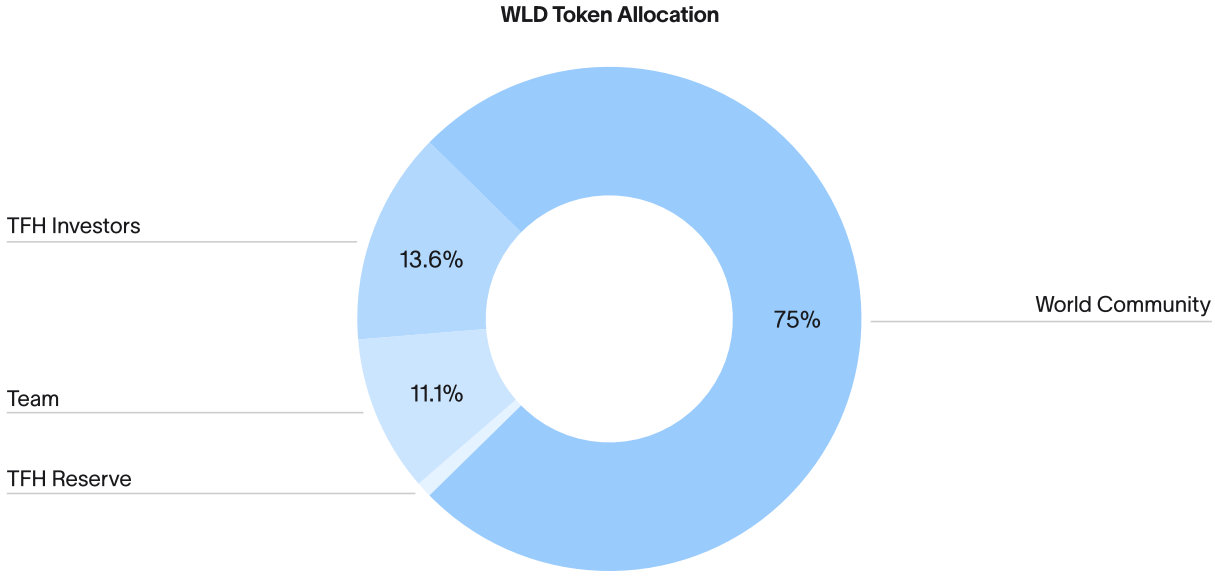

Figure 18: Current WLD token allocation (percent of 10B initial total supply) as of April 28, 2025

The following table provides details on the token allocation.

Percentage	Category	Description
75%	World Community	World Foundation governs the allocation of these tokens in line with its Articles of Association and a mandate to continue decentralizing governance of token management decision-making. Most of these tokens are allocated to users; some will be used for the ecosystem fund and network operations (details below).
11.1%	Team	These tokens go to the TFH team and other service providers that took the steps to develop World.
13.6%	TFH Investors	TFH investors provided funding that enabled TFH to support the multi-year pre-launch phase of World.
0.3%	TFH Reserve	TFH retains a reserve of WLD tokens to address future needs of TFH.

4.3.1. Unlocked Supply and Circulating Supply

This section discusses token lock-ups and how WLD comes into circulation. Here are two terms to understand:

- **Circulating supply** denotes the total amount of WLD tokens that are freely circulating, meaning they do not have any specific transfer restrictions imposed upon them, and are not subject to the protocol's governance discretion. This also includes tokens that could be acquired by external parties at any time, e.g., liquidity positions.
- **Unlocked supply** denotes the total amount of WLD tokens that are either part of the circulating supply or are unlocked but subject to the protocol's governance discretion on their rate of release into the circulating supply.

4.3.1.1. Unlocked Supply Schedule

An important feature of the *unlocked supply schedule* is that (a) team and investor tokens are subject to lock-ups, while (b) tokens claimed by users are *not* locked up. The following figure shows the 15-year WLD token unlock schedule. Importantly, governance will determine the rate at which WLD tokens from the World community category are introduced into the circulating supply. This will depend on several factors, particularly the speed at which the number of World users grows. Thus, **the unlocked supply represents an upper bound on the maximum circulating supply.**

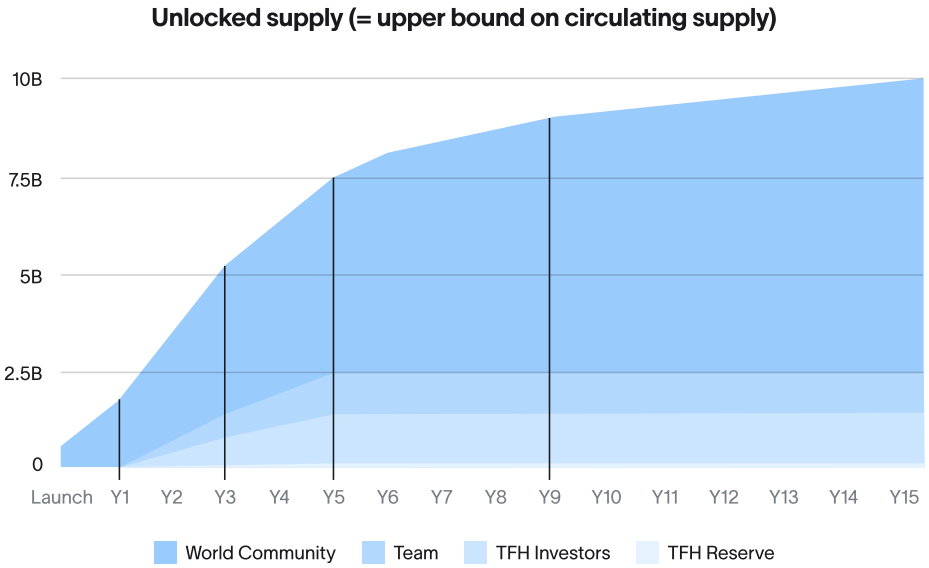

Figure 19: 15-Year WLD token unlocked supply schedule (representing an upper bound on circulating supply). Governance controls the rate at which the unlocked World Community tokens are introduced into the circulating supply. After year 15, governance may enact an inflation rate of up to 1.5% per year.

Note: For simplicity, the figure above assumes that the tokens contained in the TFH Reserve unlock according to, a one-year full lockup starting 2025-04-27 plus two years of linear unlock (see below). Given that these tokens are currently unassigned, they may be subject to additional lock-up periods and may unlock somewhat later than shown in the figure. A live version of the unlocked schedule can be found on Dune.

Below are details about the unlocked supply schedule for each category of recipient:

4.3.1.1.1. World Community Tokens

Ahead of launch, all 7.5B WLD tokens allocated to the World Community were minted. However, the vast majority of those tokens unlock over a 15-year span (details below). This unlock schedule constrains the pace at which these tokens can be made available for ecosystem participants. The unlock schedule of tokens is enforced by four smart contracts (1,2,3,4). Importantly, the tokens allocated to users and operators are not locked up.

The WLD token amounts shown in the following table unlock across the specified periods. During each period, an equal number of tokens are unlocked each calendar day.

Time Period	Amount of WLD Unlocked During Period	Cumulative WLD Unlocked at End of Period
At Launch	0.5B WLD	0.5B WLD
Launch – End of Year 3	3.5B WLD	4B WLD
Start of Year 4 – End of Year 6	1.75B WLD	5.75B WLD
Start of Year 7 – End of Year 9	0.875B WLD	6.625B WLD
Start of Year 10 – End of Year 15	0.875B WLD	7.5B WLD

Note: World aims to scale the network to every human. As the project grows, the number of people who are not part of the community necessarily becomes smaller. Given these dynamics, a substantial quantity of tokens are available for the World community within the first few years after launch, when the number of people who can join is highest and the rate of growth is the fastest. This is why 4B of the World Community tokens unlock over the initial three years. However, the rate at which these tokens enter the circulating supply depends on the speed of the network's growth.

4.3.1.1.2. TFH Team and Investor Tokens

The tokens allocated to TFH investors were contractually fully locked up for 12 months after those investors exercised their respective token warrants (which they were able to do at launch). The team tokens had the same 12-months full lockup in place. After the full lockup period, approximately 80% of the TFH team and investor tokens started unlocking linearly over a 48-month period while approximately 20% unlock linearly over a 24-month period. Unlocking for nearly all of these tokens therefore concludes by the end of July 2028—five years after protocol launch. Originally, all unlock schedules were over 24 months, but they were extended to 48 months for the majority of tokens in July 2024. The World Foundation previously shared information about these unlocks (see here), as this very gradual unlock schedule is longer than that of many projects and aligns with the long-term nature of World's mission. Note that team members' tokens may additionally be constrained by vesting schedules, which have their own timelines, typically tied to a person's tenure at TFH.

4.3.1.1.3. TFH Reserve

The tokens in the TFH Reserve are contractually locked up for at least one year of full lockup plus two years of linear unlock from the time they are allocated. The exact lock-up period will depend on when these tokens are allocated.

4.3.1.2. Circulating Supply at Launch

Figure 4.2 shows the amount of unlocked WLD tokens over time. This is different from circulating supply, which excludes unlocked WLD tokens that are held in the Foundation's treasury but have not been allocated for any specific purpose.

The circulating supply of WLD primarily grows with network size and usage. At launch, there were about 2M humans who had verified and were allocated a total of 43M Beta WLD tokens during the pre-launch phase of the project. In line with World's goal of creating a network of as many humans as possible, the circulating supply of WLD was quite low at 100.7M WLD (1% of total supply), consisting of the following parts:

- 700k WLD tokens had been migrated by users from the pre-launch phase at launch. The remaining 42.3M WLD from the pre-launch phase remained available for migration for a period of time after launch.
- 100M WLD tokens had been loaned to trading firms operating outside of the US.

Since launch, the circulating supply of WLD has grown steadily. As of April 28, 2025, it stands at about 1.3B WLD (i.e., 13% of total supply). See the dune dashboard for live numbers.

4.4. Foundation's Token Allocation Goal

Until the protocol is self-sufficient, the World Foundation acts as the steward of the World Community tokens. As part of its role, the Foundation has allocated those tokens towards three purposes: (1) user tokens, (2) network operations, and (3) an ecosystem fund.

World's evolution over time may be affected by a variety of factors, each of which could be significant. These factors include the number of Orbs deployed in the field, the number of new verifications per week, the activity of World's users, the number and location of merchants, platforms, developers, and others seeking to utilize the functionalities of World, future governance decisions, and numerous other known and unknown factors. Therefore, the final allocation of the World Community tokens cannot yet be determined. Nonetheless, taking into account the project's objectives and current scale, the World Foundation has formulated an **aspirational token allocation goal,** as shown in the following figure:

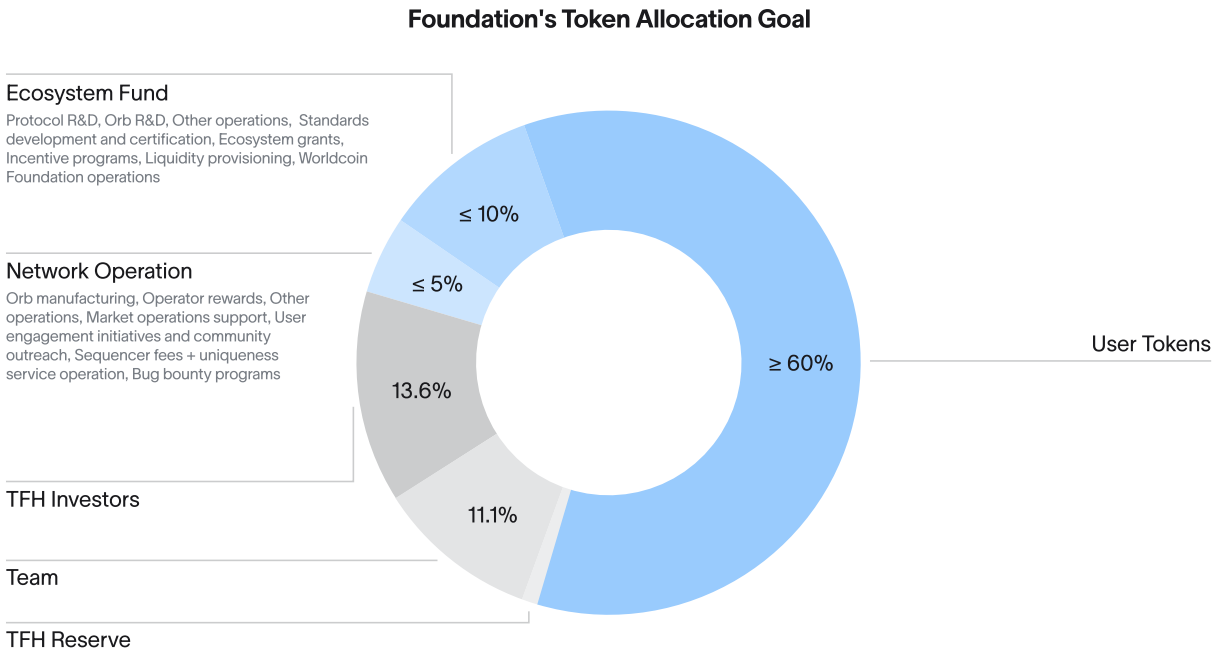

Figure 20: Foundation's Token Allocation Goal. For the Network Operation and Ecosystem Fund category, the major cost items are also shown.

World Foundation seeks to maximize the number of WLD tokens allocated to users in line with the various factors that affect World Network's growth. This may mean that the Foundation allocates fewer tokens to network operations and the ecosystem fund over time than shown in the above figure.

4.4.1. User Tokens (target allocation: ≥ 60%)

Worldcoin's tokenomics is unique in that the majority of WLD tokens will be freely available to claim by individuals over time in the form of *user tokens (previously known as "user grants" or the "WLD airdrop").* Individuals can claim these tokens simply for engaging in World Network and verifying their unique humanness. Because of this, **the circulating supply of WLD primarily grows with network size and usage.**

Given that *equality* is one of the project's guiding values, there was not a large one-time airdrop at launch, as such an event would have likely resulted in tokens flowing to a small group of people. Instead, the availability of WLD tokens is based on the following three principles:

- **Unique humanness.** Every verified unique *human* is eligible to claim user tokens (subject to the availability noted above).

- **Fairness.** At any given point in time, all verified individuals, across all applicable countries, can claim the same amount of tokens (subject to availability).
- **Incentives**: User tokens are given out over time, and the claimable user token amount decreases over time. This gives users an additional incentive to join the network early and to regularly engage with the protocol, thereby addressing the cold-start problem inherent to launching a new network.

The user tokens are not an investment. If you already have an eligible credential (see below) attached to your World ID, you may claim user tokens without providing anything of value to World as the claim is in and of itself a simple check (using zero-knowledge proofs) to determine that you are in fact eligible. No appreciation or receipt of value is guaranteed or implied–and you don't have to claim user tokens at all to participate in World Network.

4.4.1.1. How users can claim WLD tokens

To be eligible to claim user tokens, a user needs to have a *credential attached to their World ID* that is recognized by the protocol for the claiming of user tokens. Currently, two credentials are recognized for this purpose. The first is the *proof of human* credential, which individuals obtain by verifying their uniqueness at an Orb; this automatically attaches the credential to their World ID. The second is the passport credential (or in some countries a government ID credential), which individuals can attach to their World ID by connecting their phone to a compatible NFC-enabled government issued ID, such as a passport. Note that these credentials may not be available in some jurisdictions.

Eligible individuals can then make a claim for the following two types of user token amounts via a compatible app, such as World App, by checking if their credential is in the protocol:

- **First User Token Amount:** 24 hours after the credential is added, they can claim their *first user token amount*. As of August 1, 2025, the first user token amount is 25 WLD for the proof of human credential and 12.5 WLD for the passport credential. The amounts are expected to decrease over time.
- **Recurring User Token Amounts:** Starting one month after the credential is added, individuals can claim their first *recurring user token amount*. Each recurring user token amount is available to claim for one month to every (eligible) individual in the world. Recurring user token amounts are the same for everyone at a given point in time but decrease over time. The recurring amount for August 2025 is 3.22 WLD for the proof of human credential and 1.61 WLD for the passport credential. The ability to claim recurring user token amounts does currently not expire, though governance could change that at a later time.

If the same individual has attached both the proof of human and the passport credential, they can claim *both* of the respective (first and recurring) user token amounts. For example, an individual who attaches both credentials in April 2025 can claim a total first user token amount of $25 + 12.5 = 37.5$ WLD.

For a user who becomes eligible today, one can compute how much WLD they may be able to maximally claim over the following year. To do this, one fetches the first user token amount and the currently configured future recurring user token amounts for one year (see Technical Information) and sums them up. The Worldcoin Mini App in World App currently displays the result to the user as their total user token amount to abstract away the intricacies of the schedule of recurring amounts.

As of 2025-08-01, the future recurring user token amounts (as currently configured in the smart contract) are as follows. Note that governance may change these amounts.

Year	Month	Recurring user token amount, proof of human credential (WLD)	Recurring user token amount, passport credential (WLD)
2025	August	3.22	1.61
2025	September	3.20	1.60
2025	October	3.18	1.59
2025	November	3.16	1.58
2025	December	3.14	1.57
2026	January	3.12	1.56
2026	February	2.68	1.43
2026	March	2.60	1.30
2026	April	2.34	1.17
2026	May	2.08	1.04
2026	June	1.82	0.91
2026	July	1.56	0.78
2026	August	1.36	0.68

Unclaimed WLD tokens remain in the World community pool. Importantly, "claim" refers to the process described above by which user token amounts are received and is not intended to create or imply any legal relationship between any individual and World Foundation or any other entity.

Governance over user token amounts. The user token amounts are set by the protocol's governance. Currently, governance is implemented via World Foundation, but it is expected that over time, governance will be increasingly decentralized. This means that governance could also alter the emission mechanism for user tokens. For example, once the system has stabilized, governance may decide to automatically update the user token amounts according to some rule implemented in a smart contract.

Long-term sustainability of the user token emission. To achieve the goal of providing WLD tokens to every living human being (subject to availability and eligibility), governance may also decide to phase out the recurring user token amounts after a few years and only keep the first amount, thereby reserving the remaining tokens for new users in the future. As explained below, governance may also decide to direct a portion of the future fee revenue from World ID fees towards user tokens. Finally, as explained above, 15 years after launch, governance may also decide on enacting an inflation rate of up to 1.5% per year, if this is deemed necessary to continue the user token mechanism into the future.

Historical note: user token reservations for unverified individuals. For a period after launch, individuals were able to *reserve* user token amounts prior to verification and they would receive their reserved amounts once they verified at an Orb. Reservations have now been phased out and redemptions of these reservations close in July 2025.

Historical note: User token allocations during the pre-launch phase. During the pre-launch phase of World, which lasted from May 2021 until July 2023, Beta WLD tokens were allocated to users in different stages (subject to availability). Users were able to migrate their Beta WLD to WLD at or after launch.

The remainder of this section discusses the other categories in the Foundation's token allocation goal.

4.4.2. Network Operation (target allocation: ≤ 10%)

A portion of the WLD token supply allocated to the World Community is intended to be used to fund *network operations*. This section describes the main operational costs for the network, though this list is not intended to be exhaustive. Where necessary, these costs may be covered by World Foundation converting a portion of WLD tokens allocated to network operation into fiat or other currency.

Areas and responsibilities for network operations. The World Foundation is the steward of the World project, supporting and growing the community. The World Foundation owns the IP for the World ID protocol, the Orb, World Chain, and the Worldcoin token protocol. The World Foundation also governs the 75% of all Worldcoin (WLD) tokens that have been allocated to the World Community. In line with the project goals, the Foundation is allocating part of these tokens towards network operations and ecosystem building.These include the operation of the World ID sign up sequencer and uniqueness services, entities supporting World Chain, user engagement, and community outreach.

Other areas of network operations are the responsibility of ecosystem contributors. These areas include Orb manufacturing and operations. One of these ecosystem contributors is Tools for Humanity (TFH), the initial development company that launched World Network.

The World Foundation plans to further decentralize network operations, for example, through additional service providers and decentralized structures that ensure the long-term sustainability of the operations of the network.

4.4.2.1. Orb Manufacturing

Part of the WLD token supply is used to fund ongoing manufacturing costs. To this end, World Foundation engages TFH to oversee manufacturing of the Orb. In the future, other service providers may also be engaged to manufacture the Orb or devices similar to the Orb.

4.4.2.2. Orb Operations

Orb Operators are independent ecosystem participants who operate the Orbs and receive *Operator rewards* for verifying individuals at the Orb. It is important that Operators provide users with a high-quality experience by educating them about the project and supporting them during the verification process. To align the Operators' financial interests with the objectives of World, Operator rewards are impacted by measures of sign-up quality.

To ensure the long-term financial viability of World (given the Foundation's long-term goal of deploying 50,000 Orbs), competitive mechanisms have been trialed to determine fair Operator rewards. This also encourages Operators to innovate and quickly adapt to the changing needs of the project. The vast majority of Operator rewards is paid in WLD tokens (subject to the availability noted above), while a small share is paid in USDC.

4.4.2.3. Other Operations

Part of the WLD token supply is used by World Foundation to fund other operational costs, which includes logistics associated with Orb deployment, production of equipment provided to Operators, etc.

4.4.2.4. Market Operations Support

Part of the WLD token supply will be used by World Foundation to fund market operations support, which includes the recruitment, training and coordination of the network of Operators around the world.

4.4.2.5. User Engagement Initiatives and Community Outreach

When launching in a new country or region, part of the WLD token supply can be used by World Foundation to fund user engagement initiatives and community outreach programs (e.g., partnering with local organizations).

4.4.2.6. Sequencer and Uniqueness Service Operation

When a person verifies with an Orb, the uniqueness of their biometric information needs to be verified, and the proof of uniqueness needs to be written to the blockchain. The corresponding service is operated by World Foundation. World Foundation also supports the operation of a sequencer for World Chain that writes the state of the World Chain to Ethereum. Part of the token supply is allocated toward covering the cost of these services.

4.4.2.7. Bug Bounty Programs

While the hardware and software have been extensively audited by external security auditing companies (see the Orb audit and protocol audits), additional bug bounty programs have been set up for the smart contracts and other software. These bug bounty programs may also function as tools for the progressive decentralization of the project.

4.4.3. Ecosystem Fund (target allocation: ≤ 5%)

The ecosystem fund is intended to be used by World Foundation to support activities for the continued development and decentralization of World. These costs are largely independent of the network size or the size of the on-the-ground operations.

4.4.3.1. Protocol R&D

Some funds are used by World Foundation for continued development of World and related software. This includes, for example, the development of the World ID protocol, World Chain, and may in the future include the development of client apps.

4.4.3.2. Orb R&D

Ecosystem funds are also used for continued research and development of Orb hardware and software, including security mechanisms and new features.

4.4.3.3. Standards Development, Audits, and Certification

Some funds are used by World Foundation to foster standardization of the different parts of World, including different wallet apps, the Orb and the on-chain protocol. Standards help decentralization by making it easier for different parties to become part of the network. In the future, some funds are expected to be used for audits (e.g., of new biometric devices or new wallet apps) and certifying new service providers.

4.4.3.4. Ecosystem Grants

Some funds are used for ecosystem grants, which are issued for the development of new protocols, systems and integrations that are part of World, as well as for additional research and development.

4.4.3.5. Incentive Programs

Some funds are used for programs that directly incentivize activities by persons, companies and protocols that contribute to the ecosystem's growth.

4.4.3.6. Liquidity Provisioning

World Assets,, Ltd. entered into loan agreements with several trading firms operating outside of the US. These loans enable trading firms to independently assess and provide liquidity for WLD tokens.

As of 2025-04-28, these entities collectively hold loans worth 13M WLD. Out of this amount, 10M WLD expire on 2025-06-14, 1M WLD expire on 2025-09-26, and 2M WLD are currently not marked for expiry. The loans must be repaid in full in WLD – in particular, there is no call option.

4.4.3.7. World Foundation Operations

Part of the ecosystem fund will be used to fund a small staff working at World Foundation, along with associated operational costs (e.g., legal, administration).

4.4.4. World ID Fees

World ID is a protocol enabling a global, privacy-preserving identity network. At its core is the proof of human credential provided by the Orb. Additionally, the World ID protocol enables any entity (e.g., enterprises or governmental institutions) to create a new *World ID Credential* (e.g., a credit report or a university certificate), which individuals can attach to their World ID. Individuals can then share things about themselves without revealing their real identity. For example, Orb-verified individuals can prove to an application (aka a *relying party*) "I am a unique human", while individuals who have added a passport credential can prove "I am over 18" or "I am a US citizen". Credentials can also be combined to make composite proofs, for example "I am a unique human who is over 18", without revealing any other information. Given the importance of knowing whether a credential (like the age credential) has only been used once for a given application, it is expected that most World ID proofs will include the proof of human credential in this way.

Applications that integrate World ID can request and use such proofs, for example, to avoid bot accounts, to prevent AI impersonation and fraud, or to implement age controls. Furthermore, AI Agents may soon require a technology like World ID for humans to delegate authority to agents.

As part of its mission, the World Foundation aims to progressively decentralize the ecosystem and make the project self-sufficient. In the context of the World ID protocol, this has two primary components:

- **Incentives for credential issuers**: Enable credential issuers to generate sufficient revenue such that they are incentivized to issue and maintain their credentials.
- **Protocol sustainability**: Generate sufficient revenue to make the protocol sustainable.

To this end, the Foundation is currently designing changes to the World ID protocol that will enable the option to charge fees, payable in WLD, to applications using World ID proofs.

4.4.4.1. Charging Applications, not Users

World ID fees will be charged to applications, not to end users. The motivation for this is that value creation is most directly measurable by the applications. The value of World ID is realized when applications integrate it to either enhance their existing services or enable entirely new services—potentially even spawning new business models previously impossible to implement. It is therefore natural for the protocol to charge applications for consuming World ID services. Applications are accustomed to paying for the components they integrate and can be expected to recognize the value World ID brings to their offerings. This approach ensures that a portion of the value created for applications flows back to the credential issuers and the protocol.

4.4.4.2. Details on World ID Fees

World ID fees will consist of two components:

1. **Credential fee**: Each credential issuer (e.g., the World Foundation for the Orb credential, enterprises or governmental institutions for their credentials) will be able to set a

fee for their credential, and they will receive the corresponding fee revenue. This ensures that credential issuers have an incentive to create and maintain their credentials.

2. **Protocol fee**: The protocol will set a *base fee* and additionally charge a small *premium* on top of the credential fee. This will ensure that enough revenue is generated to make the protocol self-sufficient.

From an application's perspective, there will only be one World ID fee – the sum of the credential fee and the protocol fee. The World ID fee will be charged when an application (identified via a unique app id) requests a World ID proof.

Fee payment will be enforced at the protocol level. This is one of the features enabled by the *private state blockchain* employed by the future World ID architecture (see here for a technical background on the underlying cryptography used). Informally speaking, a private state blockchain can update its internal state without anyone being able to observe it, while still being permissionless: anyone can operate a node, but certain state variables are only available within the computation of the private state blockchain itself, not observable in clear text outside of it.

Employing a private state blockchain will enable various features for the World ID protocol (e.g., World ID recovery and multi-wallet usage). Importantly, it will also store part of the application state belonging to each verified user. The World ID smart contract will programmatically check whether the fee has been paid before providing a receipt of the state change from the private state blockchain that enables the user to then generate the proof. In this way, using a private state blockchain also ensures that applications cannot circumvent World ID fees, as they cannot observe the state of the blockchain.

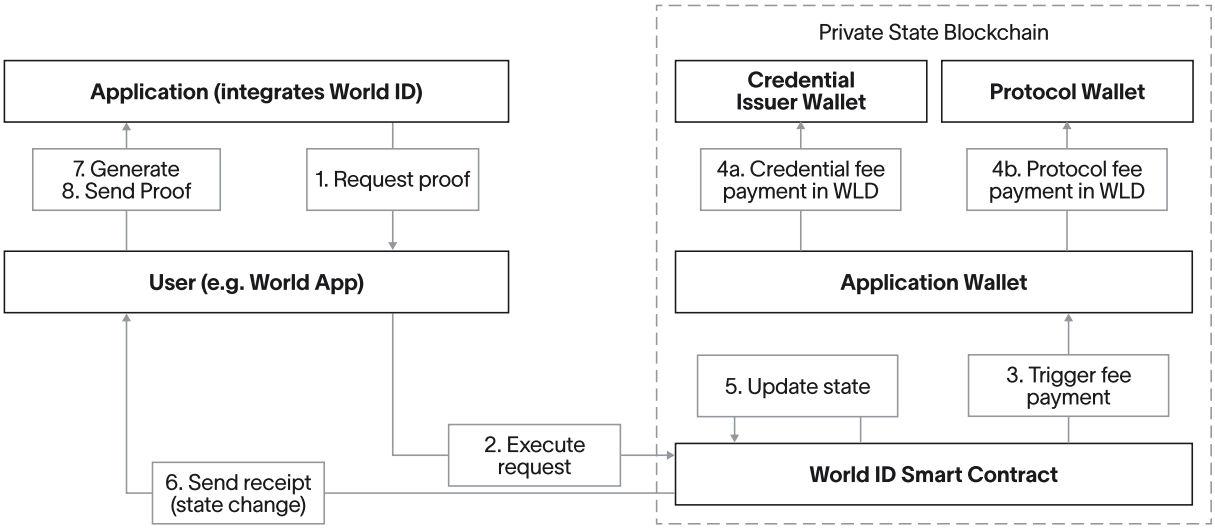

Figure 21: High-level overview of the planned World ID fee implementation

Figure 4.4 presents a high-level overview of the planned World ID fee implementation, using the example of a user who has already enrolled with a credential issuer and had their credential registered on the private state blockchain. World ID fees then work as follows: (1) An application that has integrated with World ID requests a proof (e.g., of unique humanness) from the user. (2) The user (via a World ID app like World App) decides to execute the request towards the World ID smart contract on the private state blockchain. (3) The smart contract automatically triggers the WLD fee payment from a wallet associated with the requesting application. (4) The corresponding credential fee is paid to the credential issuer wallet, and the protocol fee is paid to the protocol wallet. (5) The World ID smart contract updates its own state. (6) The World ID smart contract sends a receipt of the state change to the user. (7) The user's app generates and sends the World ID proof to the application.

The World ID smart contract will require fees to be paid in WLD, meaning applications' wallets on the private state blockchain must be pre-funded with WLD. Web3-native applications

can directly pre-fund their wallet on the blockchain. Alternatively, applications (e.g., Web2 platforms) might use a third-party pre-funding service that handles the wallet pre-funding for them and charges the application in fiat. Either way, WLD tokens are ultimately used to pay all fees.

4.4.4.3. Pricing Mechanisms

Figure 4.4 implicitly assumes that World ID fees are paid for every World ID proof. In practice, each credential issuer will be able to choose any pricing mechanism compatible with the architecture shown in Figure 4.4. Because pricing mechanisms are implemented as smart contracts on the private state blockchain, a wide array of options becomes possible, including:

- **Per-proof**: A fee could be charged for every World ID proof.
- **Per-monthly-active-user**: A fee could be charged for every monthly active user (per app-id). For each user, the fee would be collected the first time a proof is requested for that user in a given month. Since the computation happens inside the private state blockchain, per-monthly-active-user pricing models can be implemented without revealing the identity of users.
- **Free tiers**: The first 1000 users or the first 1000 proofs could be free.
- **Volume discounts**: The per-user or per-proof fee could decrease with volume.
- **Discounts for specific applications**: A credential issuer could offer discounts to specific applications (e.g., NGOs), or even offer their credentials for free.
- **Fees proportional to economic value:** A credential issuer could offer multiple proof variants at different fee levels, with some variants intentionally providing a lower level of proof assurance, allowing applications to select the level that best fits their needs.

For the base fee component of the protocol fee, governance will similarly be able to decide on a suitable pricing mechanism. While several different pricing mechanisms are possible, it is likely that most applications will prefer a per-monthly-active-user fee, as it allows applications to compare that fee with the value that World ID generates for them per user per month (e.g., due to an increase in ARPU).

For composite proofs like "I am a unique human who is over 18 years old," fee amounts could potentially depend on the combination of credentials required by a World ID proof. For example, the fee for a "uniqueness" proof could be lower than the fee for a "uniqueness + age" proof.

4.4.4.4. Fee usage

Each credential issuer will have discretion over how to use their credential fees. As for protocol fees, the World Foundation will initially govern their allocation. Over time, as governance becomes more decentralized, the World community will take over this responsibility. The community may choose to direct a portion of the fees toward continued network growth—for example, by supporting Operators or funding the User Tokens—or even decide to burn a share of the fees. As the World ID protocol grows (with more participants, more applications, and more proof verifications), more fees will be generated, which can then flow back into the ecosystem to create further growth, leading to a self-reinforcing growth mechanism.

4.4.4.5. Next steps on World ID Fees

The World Foundation is currently working on the protocol changes necessary to enable World ID fees. The Foundation expects to complete this work and run a first pilot to test the fee mechanism during Q3
2025. The Foundation believes that demonstrating a path towards World ID

fees early on is important to incentivize other parties in the ecosystem to issue and maintain their credentials, and to show how the protocol can become self-sufficient.

While the Foundation prepares to launch World ID fees, its primary focus remains squarely on growing World Network. The Foundation will also continue providing ecosystem grants to support the community of mini app developers, credential issuers, and applications integrating with World ID.

4.4.5. Technical Information

4.4.5.1. Contracts and Addresses

4.4.5.1.1. Smart Contracts

Contract	Network	Address
WLD Token Contract	Ethereum	0x163f8C2467924be0ae7B5347 228CABF260318753
WLD Token Contract	World Chain	0x2cFc85d8E48F8EAB294be644 d9E25C3030863003
WLD Token Contract	Optimism	0xdC6fF44d5d932Cbd77B52E56 12Ba0529DC6226F1
Community Tokens Unlock Contracts	Ethereum	0x1770bd8186AAd27Df9B050D6 5f86CF2cdC92C296 0xaEE0360b 73B5D01dad134f234d3a93ad c1680e57 0x938ceD2D1eE4AFB2 20929F96c2eB754C053C77F7 0x5B5442C5fcEaE3b40C230C32 a3Ffe924BcBe7D93
Recurring User Token Amounts Allocation Contract, Orb	World Chain	0x2c1Ca1FBbD5f28e5492Cc6bF 8C4e8c57354eb162
Optimism (deprecated)	0xe773335550b63eed23a6e60d cc4709106a1f653c	
Recurring User Token Amounts Allocation Contract, Passport Credential	World Chain	0x85C0BEb46E91D18dFeA0294E 6FC46A8c8AF2BeaD
First User Token Amounts Allocation Contract, Orb	World Chain	0xf4d26620B6d9AE07F2495757 C8Bd00090cE2A172
First User Token Amounts Allocation Contract, Passport Credential	World Chain	0x008177c4F0C0c64334D7CC27 02b783387fCe6d62
Beta WLD Token Contract (deprecated)	Optimism	0x0346c32E5d7e98bD57100b6F 7002a0Ae17188048

User token amounts can be fetched as follows: the currently active grant IDs and future recurring user token amounts can be fetched from the WLDGrant contract available at *(Recurring User Token Amounts Allocation Contract).grant()* where one chooses the *Recurring User Token Amounts Allocation Contract* corresponding to the respective credential (Orb or Passport). The current first user token amount can be fetched from API endpoint at: `https://api.airdrop.world.org/v1/grants/first-claim-amount?grantId=`*<current_grant_id>*

4.4.5.1.2. Main Wallets

Wallet	Network	Address
World Foundation Cold Wallets	Ethereum	0xc534a745bFfaF9466Ed7B47f A23B0177b99A3e77
Optimism	0xc534a745bFfaF9466Ed7B47f A23B0177b99A3e77	
World Chain	0xc534a745bFfaF9466Ed7B47f A23B0177b99A3e77	
World Assets, Ltd. Cold Wallets	Ethereum	0x59a0f98345f54bAB245A0434 88ECE7FCecD7B596
Optimism	0x59a0f98345f54bAB245A0434 88ECE7FCecD7B596	
World Chain	0x59a0f98345f54bAB245A0434 88ECE7FCecD7B596	
World Assets, Ltd. Hot Wallets	Ethereum	0xc4151Dd19A38E7224793F5aD 8fBDD912750e3565
World Chain	0x8C00371AEf2482477c15c878 D58044d64A7FCcA3	
World Assets, Ltd. Hot Wallet: Recurring User Token Amounts	World Chain	0x30672EbB8D3c3b62C261a23B 4a225712FF2CAdBC
Optimism (deprecated)	0x7f26A7572E8B877654eeDcBc 4E573657619FA3CE	
World Assets, Ltd. Hot Wallet: First User Token Amount	World Chain	0x1c288c748F368E8dcD87dB0d 29888666842502aA
World Assets, Ltd. Hot Wallet: Reservations	World Chain	0xDAA7BbAD496c4D44 31423bE64d878a769FbDEBc8
WLD Vault	World Chain	0x14a028cC500108307947dca4 a1Aa35029FB66CE0
Optimism (deprecated)	0x21c4928109acB0659A88AE53 29b5374A3024694C	
Optimism – World Chain Migration	Optimism	0x6CE3A5478232F0DfAE37D717 8C24F984cCa696a8
World Chain	0xC6968c6DF1a2C31Ac66B4294 5BbaD91635a0095B	
World Assets, Ltd. Hot Wallet: Welcome Grants and Beta Token Migration (deprecated)	Optimism	0x074a9ed58d11e3f0f589072c 99de86f80971a844
World Assets, Ltd. Hot Wallet: Temporary holding wallet	Optimism	0xF8Cf291d92e52B722C31af1F DE9F0D7E890E0E0A
World Assets, Ltd. Hot Wallet: Beta Token Migration 2 (deprecated)	Optimism	0x46DcEC50647abFb2905Af8Da 4e670051653A5FBC
Polygon Bridge (Beta User Migration, deprecated)	Optimism	0xe710657bEbDBd75fBDaCA07D 57c2A5aE04085507

4.5. FAQ

How do the World Chain contracts relate to the Ethereum contracts?

The WLD token contract is deployed on Ethereum mainnet, and the token is bridged to the World Chain "layer 2" network. However, World Foundation expects that most of the activity in WLD tokens will happen on World Chain, where verified individuals receive their user token amounts. In addition, World App primarily interacts with the World Chain network. The reasons for choosing World Chain over Ethereum as the primary venue were scalability and transaction costs. A legacy bridged version of WLD also still exists on Optimism.

Who pays the transaction costs (gas fees)?

World App users generally do not currently incur gas costs; the gas fees for claiming WLD tokens, performing swaps, and other transactions are currently funded by TFH. In the future, World App could require users to pay gas fees for certain actions, e.g., transfers made to other wallets. When users verify their identity to a third-party application via World ID, this does not incur gas costs for the protocol. However, the third-party applications may charge users gas fees (depending on whether they verify the proof on-chain or off-chain) or other fees. For instance, when using the swap feature in World App, users *do* pay any fees incurred on third-party platforms. Users may incur gas fees for transactions that are not made through World App that are dependent on the platform and chain on which the transaction is occurring.

How are the World Community tokens stored? Do you use a custody provider?

The majority of the World Community tokens are stored in a cold wallet. Additionally, several hot wallets are used by World Foundation and World Assets, Ltd., to manage everyday operations. Tokens are typically only stored in these hot wallets for a short period of time, and these wallets only store as many tokens as needed.

Who controls the WLD token contract? Is it upgradable? Does anyone have minting rights?

The WLD token contract is not upgradable. No control can be exercised over the contract, except for setting the "minter" address in case the community decides to activate inflation. For 15 years following the launch, no address is able to mint any new tokens. After 15 years, a "minter" address (controlled by protocol governance) can mint up to 1.5% new WLD tokens per year, with governance deciding how to allocate them.

What are the involved entities and where are they incorporated?

The World Foundation is an exempted limited guarantee foundation company, incorporated in the Cayman Islands. It is "memberless," meaning it has no shareholders or beneficial owners. Its registered office is located at Suite 3119, 9 Forum Lane, Camana Bay, George Town, Grand Cayman KY1-9006, Cayman Islands. World Foundation's principal purpose, as set forth in its Articles of Association, is to support and encourage the growth of those building in the World ecosystem, support and foster the decentralization of World technologies and governance, hold and license intellectual property relating to the World Network, and to receive, sell, hold, loan, and spend assets to support these purposes.

World Assets, Ltd. is a company registered in the British Virgin Islands on December 7, 2022 with BVI Company Number 2113558. The World Foundation is the sole member/director of World Assets, Ltd. World Assets, Ltd.is responsible for issuing the 7.5B Worldcoin tokens (WLD) that have been allocated to the World community.

World Chain LLC is a limited liability company formed in the Cayman Islands. World Foundation is its sole member and manager. World Chain LLC is responsible for the ownership and operation of World Chain infrastructure.

More information about these entities, including incorporation documentation and equity composition, can be found at foundation.world.org/about.

Tools for Humanity (TFH) is a Delaware corporation headquartered in San Francisco, California (US), with a wholly-owned subsidiary, Tools for Humanity GmbH based in Germany. Its registered office is located at CSC 251 Little Falls Drive, Wilmington, Delaware 19808. It registered on June 26, 2019 and its legal entity number is 7487684. TFH supported World's multi-year pre-launch phase, during which it developed the Orb, the first version of the protocol, and the World App, the first wallet for World Network, which it still operates today. It is governed entirely independently of World Foundation. Founded in 2019, TFH has grown to a team of approximately 500 people today. However, World is an open protocol that anyone can contribute to and build on.

4.6. Disclaimer

PLEASE READ THE ENTIRETY OF THIS "NOTICE AND DISCLAIMER" SECTION CAREFULLY. NOTHING HEREIN CONSTITUTES LEGAL, FINANCIAL, BUSINESS, INVESTMENT OR TAX ADVICE AND YOU SHOULD CONSULT YOUR OWN LEGAL, FINANCIAL, BUSINESS, INVESTMENT, TAX OR OTHER PROFESSIONAL ADVISOR(S) BEFORE ENGAGING IN ANY ACTIVITY IN CONNECTION HEREWITH. NEITHER THE WORLD FOUNDATION (THE **FOUNDATION**) AND ANY OF THE PROJECT PARTICIPANTS (TOGETHER WITH THE PROJECT PARTICIPANTS, THE **WORLD NETWORK**) WHO HAVE WORKED ON WORLD NETWORK (AS DESCRIBED HEREIN) OR DEVELOPERS OF WORLD NETWORK IN ANY CAPACITY WHATSOEVER, NOR ANY SERVICE PROVIDER SHALL BE LIABLE FOR ANY KIND OF DIRECT OR INDIRECT DAMAGE OR LOSS WHATSOEVER WHICH YOU MAY SUFFER IN CONNECTION WITH ACCESSING THIS WHITEPAPER, THE WEBSITE AT HTTPS://WORLD.ORG (THE **WEBSITE**) OR ANY OTHER WEBSITES OR MATERIALS PUBLISHED BY THE FOUNDATION.

4.6.1. Crypto Products

Crypto products can be highly risky and their regulatory treatment is unsettled in many jurisdictions. There may be no regulatory recourse for any loss from transactions in WLD tokens. Any value ascribed to WLD tokens may change quickly and may be lost in its entirety. Further, the technologies comprising World Network, including the WLD token, are experimental in nature. There is no guarantee that the network will operate as planned. For more information, visit www.world.org/risks. Holding, buying, or selling WLD tokens may not be permitted where you live, and it is your responsibility to comply with all applicable laws. Worldcoin (WLD) tokens are not intended to be available to residents of the State of New York or certain other restricted territories. More details can be found at http://www.world.org/tos.

As described further below, this document contains forward-looking estimates and statements regarding the intended actions and objectives of World Foundation and World Network, based largely on current expectations and projections about future events for which the outcome is uncertain. It is therefore subject to a number of known and unknown risks, including those described at www.world.org/risks, that could cause the actual outcomes to differ materially from what is expressed or implied herein. Readers are cautioned not to put undue reliance on these future-looking estimates and statements. The content of this document speaks only as of the date thereof.

4.6.2. Nature of the Whitepaper

The Whitepaper and the Website are intended for general informational purposes and community discussion only and do not constitute a prospectus, an offer document, an offer of securities, a solicitation for investment, or any offer to sell any product, item or asset (whether digital or otherwise). Nothing contained in the Whitepaper or the Website is or may be relied upon as a promise, representation or undertaking as to the future performance of World Network. The information herein may not be exhaustive and does not imply any element of a contractual relationship commitment in relation to the acquisition of WLD Token, and no virtual currency or other form of payment is to be accepted on the basis of the Whitepaper or the Website. There is no assurance as to the accuracy or completeness of such information and no representation, warranty or undertaking is or purported to be provided as to the accuracy or completeness of such information. Nothing contained in the Whitepaper or the Website is or may be relied upon as a promise, representation or undertaking as to the future performance of World Network. Any agreement between any third party and you, in relation to any sale, purchase, or other distribution or transfer of WLD Token, is to be governed only by the separate terms and conditions of such agreement, and such agreement must be read together with the Whitepaper. Where the Whitepaper or the Website includes information that has been obtained from third party sources, the Foundation, their respective affiliates and/or World Network have not inde-

pendently verified the accuracy or completion of such information. Further, you acknowledge that circumstances may change and that the Whitepaper or the Website may become outdated as a result; and the Foundation is not under any obligation to update or correct this document in connection therewith.

The information set out in the Whitepaper and the Website is for community discussion only and is not legally binding. No person is bound to enter into any contract or binding legal commitment in relation to the acquisition of any WLD token, and no virtual currency or other form of payment is to be accepted on the basis of the Whitepaper or the Website. Any agreement governing the sale or acquisition of WLD tokens shall be governed by a separate set of Terms of Service, available at www.world.org/tos. The Terms of Service must be read together with the Whitepaper and further information available at www.world.org/risks. In the event of any inconsistencies between the Terms of Service and the Whitepaper or the Website, the Terms of Service shall prevail.

4.6.3. Token Features

The native digital cryptographically-secured cryptocurrency of World Network (**WLD Token**) is a transferable representation of attributed functions specified in the protocol/code of World Network, designed to play a major role in the functioning of the ecosystem on World Network, and intended to be used solely as the primary utility and future governance token on the platform. The goal of introducing WLD Token is to provide a convenient and secure mode of payment and settlement between participants who interact within the ecosystem on World Network, and it is not, and not intended to be, a medium of exchange accepted by the public (or a section of the public) as payment for goods or services or for the discharge of a debt; nor is it designed or intended to be used by any person as payment for any goods or services whatsoever that are not exclusively provided by the issuer. WLD Token may only be utilized on World Network, and ownership of WLD Token carries no rights, express or implied, other than the right to use WLD Token as a means to enable usage of and interaction within World Network. WLD Token is not intended to be an investment, and no value appreciation is guaranteed or implied.

4.6.4. Deemed Representations and Warranties

By accessing the Whitepaper or the Website (or any part thereof), you shall be deemed to represent and warrant to the Foundation, their respective affiliates, and World Network as follows:

- in any decision to receive and/or purchase any WLD Token, you shall not rely on any statement set out in the Whitepaper or the Website;
- you will and shall at your own expense ensure compliance with all laws, regulatory requirements and restrictions applicable to you (as the case may be);
- you acknowledge, understand and agree that WLD Token may have no value, there is no guarantee or representation of value or liquidity for WLD Token, and WLD Token is not an investment product including for any speculative investment;
- WLD tokens may not always be transferable or liquid;
- WLD tokens may not be exchangeable against any goods or services contemplated in the Whitepaper, especially in case of failure or discontinuation of the project;
- none of the Foundation, their respective affiliates, and/or World Network members shall be responsible for or liable for the value of WLD Token, the transferability and/or liquidity of WLD Token and/or the availability of any market for WLD Token through third parties or otherwise; and

- you acknowledge, understand and agree that you are not eligible to purchase any WLD Token if you are a citizen, national, resident (tax or otherwise), domiciliary and/or green card holder of a geographic area or country (i) where it is likely that the sale of WLD Token would be construed as the sale of a security, financial service or investment product and/or (ii) where participation in token sales is prohibited by applicable law, decree, regulation, treaty, or administrative act; and to this effect you agree to provide all such identity verification document when requested in order for the relevant checks to be carried out.

The Foundation disclaims all representations, warranties or undertakings to any entity or person (including without limitation warranties as to the accuracy, completeness, timeliness or reliability of the contents of the Whitepaper or the Website, or any other materials published by the Foundation). To the maximum extent permitted by law, the Foundation, their respective affiliates and service providers, and the World Network shall not be liable for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including, without limitation, any liability arising from default or negligence on the part of any of them, or any loss of revenue, income or profits, and loss of use or data) arising from the use of the Whitepaper or the Website, or any other materials published, or its contents (including without limitation any errors or omissions) or otherwise arising in connection with the same. Prospective purchasers of the WLD Token should carefully consider and evaluate all risks and uncertainties (including financial and legal risks and uncertainties) associated with the WLD Token sale, the Foundation, and World Network.

4.6.5. Disclaimers Relating to the WLD Token

It is expressly highlighted that WLD Token:

- does not have any tangible or physical manifestation, and does not have any intrinsic value (nor does any person make any representation or give any commitment as to its value), and may lose its value in part or in full;
- is non-refundable and cannot be exchanged for cash (or its equivalent value in any other virtual currency) or any payment obligation by the Foundation, the World Network, or any of their respective affiliates, and may not always be transferrable or liquid;
- does not represent or confer on the token holder any right of any form with respect to the Foundation, the World Network (or any of their respective affiliates), or its revenues or assets, including without limitation any right to receive future dividends, revenue, shares, ownership right or stake, share or security, any voting, distribution, redemption, liquidation, proprietary (including all forms of intellectual property or license rights), right to receive accounts, financial statements or other financial data, the right to requisition or participate in shareholder meetings, the right to nominate a director, or other financial or legal rights or equivalent rights, or intellectual property rights or any other form of participation in or relating to World Network, the Foundation, and/or their service providers;
- does not entitle token holders to any promise of fees, dividends, revenue, profits or investment returns, and are not intended to constitute securities in any relevant jurisdiction;
- is not intended to represent any rights under a contract for differences or under any other contract the purpose or pretended purpose of which is to secure a profit or avoid a loss;
- may not be exchangeable against the good or service described herein, especially in case of failure or discontinuation of World;
- is not intended to be a representation of money (including electronic money), security, commodity, bond, debt instrument, unit in a collective investment scheme or any other kind of financial instrument or investment;

- is not a loan to the Foundation, the World Network, or any of their respective affiliates, is not intended to represent a debt owed by the Foundation, the World Network, or any of their respective affiliates, and there is no expectation of profit; and
- does not provide the token holder with any ownership or other interest in the Foundation, the World Network, or any of their respective affiliates.

4.6.6. Informational Purposes Only

The project roadmap in the Whitepaper is being shared in order to outline the current status of World as well as some of the plans of World Network and is provided solely for informational purposes and does not constitute any binding commitment. Please do not rely on this information in making purchasing decisions because ultimately, further development, release, and timing of any products, features or functionality remains at the sole discretion of the Foundation, the World Network, or their respective affiliates, and is subject to change. Further, the Whitepaper or the Website may be amended or replaced from time to time. There are no obligations to update the Whitepaper or the Website, or to provide recipients with access to any information beyond what is provided herein.

4.6.7. Regulatory Approval

The legal and regulatory treatment of digital assets in the United States and globally continues to evolve. The Foundation actively monitors applicable laws and may adjust its operations and distribution mechanisms to maintain compliance with future regulatory developments.

No regulatory authority has examined or approved, whether formally or informally, of any of the information set out in the Whitepaper or the Website. No such action or assurance has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction. The publication, distribution or dissemination of the Whitepaper or the Website does not imply that the applicable laws, regulatory requirements or rules have been complied with. World Foundation is solely responsible for the content of this Whitepaper. This Whitepaper has not been reviewed or approved by any competent authority in any Member State of the European Union.

4.6.8. Cautionary Note on Forward-Looking Statements

All statements contained herein, statements made in press releases or in any place accessible by the public and oral statements that may be made by the Foundation and/or the World Network may constitute forward-looking statements (including statements regarding intent, belief or current expectations with respect to market conditions, business strategy and plans, financial condition, specific provisions and risk management practices). You are cautioned not to place undue reliance on these forward-looking statements given that these statements involve known and unknown risks, uncertainties and other factors that may cause the actual future results to be materially different from that described by such forward-looking statements, and no independent third party has reviewed the reasonableness of any such statements or assumptions. These forward-looking statements are applicable only as of the date indicated in the Whitepaper, and the Foundation, as well as World Network expressly disclaim any responsibility (whether express or implied) to release any revisions to these forward-looking statements to reflect events after such date.

4.6.9. English Language

The Whitepaper and the Website may be translated into a language other than English for reference purpose only and in the event of conflict or ambiguity between the English language version and translated versions of the Whitepaper or the Website, the English language versions shall prevail. You acknowledge that you have read and understood the English language version of the Whitepaper and the Website.

5. Disclaimer

PLEASE READ THE ENTIRETY OF THIS "NOTICE AND DISCLAIMER" SECTION CAREFULLY. NOTHING HEREIN CONSTITUTES LEGAL, FINANCIAL, BUSINESS, INVESTMENT OR TAX ADVICE AND YOU SHOULD CONSULT YOUR OWN LEGAL, FINANCIAL, BUSINESS, INVESTMENT, TAX OR OTHER PROFESSIONAL ADVISOR(S) BEFORE ENGAGING IN ANY ACTIVITY IN CONNECTION HEREWITH. NEITHER THE WORLD FOUNDATION (THE **FOUNDATION**) AND ANY OF THE PROJECT PARTICIPANTS (TOGETHER WITH THE PROJECT PARTICIPANTS, THE **WORLD NETWORK**) WHO HAVE WORKED ON THE WORLD NETWORK (AS DESCRIBED HEREIN) OR DEVELOPERS OF THE WORLD NETWORK IN ANY CAPACITY WHATSOEVER, ANY DISTRIBUTOR/VENDOR OF WLD TOKENS (THE **DISTRIBUTOR**), NOR ANY SERVICE PROVIDER SHALL BE LIABLE FOR ANY KIND OF DIRECT OR INDIRECT DAMAGE OR LOSS WHATSOEVER WHICH YOU MAY SUFFER IN CONNECTION WITH ACCESSING THIS WHITEPAPER, THE WEBSITE AT HTTPS://WORLD.ORG (THE **WEBSITE**) OR ANY OTHER WEBSITES OR MATERIALS PUBLISHED BY THE FOUNDATION.

5.1. Crypto Products

Crypto products can be highly risky and their regulatory treatment is unsettled in many jurisdictions. There may be no regulatory recourse for any loss from transactions in WLD tokens. Any value ascribed to WLD tokens may change quickly and may be lost in its entirety. Further, the technologies comprising the World Network, including the WLD token, are experimental in nature. There is no guarantee that the network will operate as planned. For more information, visit www.world.org/risks. Holding, buying, or selling WLD tokens may not be permitted where you live, and it is your responsibility to comply with all applicable laws. Worldcoin (WLD) tokens are not intended to be available to residents of the United States or certain other restricted territories. More details can be found at https://www.world.org/tos.

As described further below, this document contains forward-looking estimates and statements regarding the intended actions and objectives of the World Foundation and the World Network, based largely on current expectations and projections about future events for which the outcome is uncertain. It is therefore subject to a number of known and unknown risks, including those described at www.world.org/risks, that could cause the actual outcomes to differ materially from what is expressed or implied herein. Readers are cautioned not to put undue reliance on these future-looking estimates and statements. The content of this document speaks only as of the date thereof.

5.2. Nature of the Whitepaper

The Whitepaper and the Website are intended for general informational purposes and community discussion only and do not constitute a prospectus, an offer document, an offer of securities, a solicitation for investment, or any offer to sell any product, item or asset (whether digital or otherwise). Nothing contained in the Whitepaper or the Website is or may be relied upon as a promise, representation or undertaking as to the future performance of World Network. The information herein may not be exhaustive and does not imply any element of a contractual relationship commitment in relation to the acquisition of WLD Token, and no virtual currency or other form of payment is to be accepted on the basis of the Whitepaper or the Website. There is no assurance as to the accuracy or completeness of such information and no representation, warranty or undertaking is or purported to be provided as to the accuracy or completeness of such information. Nothing contained in the Whitepaper or the Website is or may be relied upon as a promise, representation or undertaking as to the future performance of World Network. Any agreement between the Distributor (or any third party) and you, in relation to any sale,

purchase, or other distribution or transfer of WLD Token, is to be governed only by the separate terms and conditions of such agreement, and such agreement must be read together with the Whitepaper. Where the Whitepaper or the Website includes information that has been obtained from third party sources, the Foundation, the Distributor, their respective affiliates and/or World Network have not independently verified the accuracy or completion of such information. Further, you acknowledge that circumstances may change and that the Whitepaper or the Website may become outdated as a result; and neither the Foundation nor the Distributor is under any obligation to update or correct this document in connection therewith.

The information set out in the Whitepaper and the Website is for community discussion only and is not legally binding. No person is bound to enter into any contract or binding legal commitment in relation to the acquisition of any WLD token, and no virtual currency or other form of payment is to be accepted on the basis of the Whitepaper or the Website. Any agreement governing the sale or acquisition of WLD tokens shall be governed by a separate set of Terms of Service, available at www.world.org/tos. The Terms of Service must be read together with the Whitepaper and further information available at www.world.org/risks. In the event of any inconsistencies between the Terms of Service and the Whitepaper or the Website, the Terms of Service shall prevail.

5.3. Token Features

The native digital cryptographically-secured utility token of World Network (**WLD Token**) is a transferable representation of attributed functions specified in the protocol/code of World Network, designed to play a major role in the functioning of the ecosystem on World Network, and intended to be used solely as the primary utility and future governance token on the platform. The goal of introducing WLD Token is to provide a convenient and secure mode of payment and settlement between participants who interact within the ecosystem on World Network, and it is not, and not intended to be, a medium of exchange accepted by the public (or a section of the public) as payment for goods or services or for the discharge of a debt; nor is it designed or intended to be used by any person as payment for any goods or services whatsoever that are not exclusively provided by the issue. WLD Token may only be utilized on World Network, and ownership of WLD Token carries no rights, express or implied, other than the right to use WLD Token as a means to enable usage of and interaction within World Network.

5.4. Deemed Representations and Warranties

By accessing the Whitepaper or the Website (or any part thereof), you shall be deemed to represent and warrant to the Foundation, the Distributor, their respective affiliates, and World Network as follows:

- in any decision to receive and/or purchase any WLD Token, you shall not rely on any statement set out in the Whitepaper or the Website;
- you will and shall at your own expense ensure compliance with all laws, regulatory requirements and restrictions applicable to you (as the case may be);
- you acknowledge, understand and agree that WLD Token may have no value, there is no guarantee or representation of value or liquidity for WLD Token, and WLD Token is not an investment product including for any speculative investment;
- WLD tokens may not always be transferable or liquid;
- WLD tokens may not be exchangeable against any goods or services contemplated in the Whitepaper, especially in case of failure or discontinuation of the project;
- none of the Foundation, the Distributor, their respective affiliates, and/or World Network members shall be responsible for or liable for the value of WLD Token, the transferability and/or liquidity of WLD Token and/or the availability of any market for WLD Token through third parties or otherwise; and

- you acknowledge, understand and agree that you are not eligible to purchase any WLD Token if you are a citizen, national, resident (tax or otherwise), domiciliary and/or green card holder of a geographic area or country (i) where it is likely that the sale of WLD Token would be construed as the sale of a security, financial service or investment product and/or (ii) where participation in token sales is prohibited by applicable law, decree, regulation, treaty, or administrative act; and to this effect you agree to provide all such identity verification document when requested in order for the relevant checks to be carried out.

The Foundation disclaims all representations, warranties or undertakings to any entity or person (including without limitation warranties as to the accuracy, completeness, timeliness or reliability of the contents of the Whitepaper or the Website, or any other materials published by the Foundation or the Distributor). To the maximum extent permitted by law, the Foundation, the Distributor, their respective affiliates and service providers shall not be liable for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including, without limitation, any liability arising from default or negligence on the part of any of them, or any loss of revenue, income or profits, and loss of use or data) arising from the use of the Whitepaper or the Website, or any other materials published, or its contents (including without limitation any errors or omissions) or otherwise arising in connection with the same. Prospective purchasers of the WLD Token should carefully consider and evaluate all risks and uncertainties (including financial and legal risks and uncertainties) associated with the WLD Token sale, the Foundation, the Distributor and World Network.

5.5. Disclaimers Relating to the WLD Token

It is expressly highlighted that WLD Token:

- does not have any tangible or physical manifestation, and does not have any intrinsic value (nor does any person make any representation or give any commitment as to its value), and may lose its value in part or in full;
- is non-refundable and cannot be exchanged for cash (or its equivalent value in any other virtual currency) or any payment obligation by the Foundation, the Distributor or any of their respective affiliates, and may not always be transferrable or liquid;
- does not represent or confer on the token holder any right of any form with respect to the Foundation, the Distributor (or any of their respective affiliates), or its revenues or assets, including without limitation any right to receive future dividends, revenue, shares, ownership right or stake, share or security, any voting, distribution, redemption, liquidation, proprietary (including all forms of intellectual property or license rights), right to receive accounts, financial statements or other financial data, the right to requisition or participate in shareholder meetings, the right to nominate a director, or other financial or legal rights or equivalent rights, or intellectual property rights or any other form of participation in or relating to World Network, the Foundation, the Distributor and/or their service providers;
- does not entitle token holders to any promise of fees, dividends, revenue, profits or investment returns, and are not intended to constitute securities in any relevant jurisdiction;
- is not intended to represent any rights under a contract for differences or under any other contract the purpose or pretended purpose of which is to secure a profit or avoid a loss;
- may not be exchangeable against the good or service described herein, especially in case of failure or discontinuation of World;
- is not intended to be a representation of money (including electronic money), security, commodity, bond, debt instrument, unit in a collective investment scheme or any other kind of financial instrument or investment;
- is not a loan to the Foundation, the Distributor or any of their respective affiliates, is not intended to represent a debt owed by the Foundation, the Distributor or any of their respective affiliates, and there is no expectation of profit; and
- does not provide the token holder with any ownership or other interest in the Foundation, the Distributor or any of their respective affiliates.

5.6. Informational Purposes Only

The project roadmap in the Whitepaper is being shared in order to outline the current status of World as well as some of the plans of World Network and is provided solely for informational purposes and does not constitute any binding commitment. Please do not rely on this information in making purchasing decisions because ultimately, further development, release, and timing of any products, features or functionality remains at the sole discretion of the Foundation, the Distributor or their respective affiliates, and is subject to change. Further, the Whitepaper or the Website may be amended or replaced from time to time. There are no obligations to update the Whitepaper or the Website, or to provide recipients with access to any information beyond what is provided herein.

5.7. Regulatory Approval

No regulatory authority has examined or approved, whether formally or informally, of any of the information set out in the Whitepaper or the Website. No such action or assurance has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction. The publication, distribution or dissemination of the Whitepaper or the Website does not imply that the applicable laws, regulatory requirements or rules have been complied with. World is solely responsible for the content of this Whitepaper. This Whitepaper has not been reviewed or approved by any competent authority in any Member State of the European Union.

5.8. Cautionary Note on Forward-Looking Statements

All statements contained herein, statements made in press releases or in any place accessible by the public and oral statements that may be made by the Foundation, the Distributor and/or World Network, may constitute forward-looking statements (including statements regarding intent, belief or current expectations with respect to market conditions, business strategy and plans, financial condition, specific provisions and risk management practices). You are cautioned not to place undue reliance on these forward-looking statements given that these statements involve known and unknown risks, uncertainties and other factors that may cause the actual future results to be materially different from that described by such forward-looking statements, and no independent third party has reviewed the reasonableness of any such statements or assumptions. These forward-looking statements are applicable only as of the date indicated in the Whitepaper, and the Foundation, the Distributor as well as World Network expressly disclaim any responsibility (whether express or implied) to release any revisions to these forward-looking statements to reflect events after such date.

5.9. English Language

The Whitepaper and the Website may be translated into a language other than English for reference purpose only and in the event of conflict or ambiguity between the English language version and translated versions of the Whitepaper or the Website, the English language versions shall prevail. You acknowledge that you have read and understood the English language version of the Whitepaper and the Website.