# A New Identity and Financial Network

## Introducing Worldcoin

Worldcoin was founded with the mission of creating a globally-inclusive identity and financial network, owned by the majority of humanity. If successful, Worldcoin could considerably increase economic opportunity, scale a reliable solution for distinguishing humans from AI online while preserving privacy, enable global democratic processes, and show a potential path to AI-funded UBI.

Worldcoin consists of a privacy-preserving digital identity network (World ID) built on proof of personhood and, where laws allow, a digital currency (WLD). Every human is eligible for a share of WLD simply for being human. World ID and WLD are currently complemented by World App, the first frontend to World ID and the Worldcoin Protocol, developed by the contributor team at Tools for Humanity (TFH).

"Proof of personhood" is one of the core ideas behind Worldcoin, and refers to establishing an individual is both human and unique. Once established, it gives the individual the ability to assert they are a real person and different from another real person, without having to reveal their real-world identity.

Today, proof of personhood is an unsolved problem on a global scale, making it difficult to vote online or distribute value on a large scale.The problem is even more pressing as increasingly powerful AI models will further amplify the difficulty of distinguishing humans from bots. If successful as part of Worldcoin, World ID could become a global proof of personhood standard.

Some of the core assumptions behind Worldcoin are:

1. Proof of personhood is a missing and necessary digital primitive. This primitive will become more important as increasingly powerful AI models become available.
2. Scalable and inclusive proof of personhood, for the first time, allows aligning the incentives of all network participants around adding real humans to the network. Bitcoin is issued to secure the Bitcoin network. Worldcoin is issued to grow the Worldcoin network, with security inherited from Ethereum.
3. In a time of increasingly powerful AI, the most reliable way to issue a global proof of personhood is through custom biometric hardware.

The following dynamic Whitepaper shares the reasoning behind the implementation of the project as well as the current state and roadmap.

### World ID

World ID is privacy preserving proof of personhood. It enables users to verify their humanness online while maintaining their privacy through zero-knowledge proofs, via a custom biometric device called the Orb. The Orb has been designed based on the realization that custom biometric hardware might be the only long term viable solution to issue AI-safe proof of personhood verifications. World IDs are issued on the Worldcoin protocol, which allows individuals to prove that they are human to any verifier (including web2 applications) while maintaining their privacy through zero-knowledge proofs. In the future, it should be possible to issue other credentials on the protocol as well.

World ID aspires to be personbound, meaning a World ID should only be used by the individual it was issued to. It should be very difficult to use by a fraudulent actor who stole or acquired World ID credentials. Further, it should always be possible for an individual to regain possession of a lost or stolen World ID.

### Worldcoin Token

While network effects will ultimately come from useful applications being built on top of the financial and identity infrastructure, the token is issued to all network participants to align their incentives around the growth of the network. This is especially important early on to bootstrap the network and bypass the "cold start problem". This could lead the Worldcoin token (WLD) to become the widest distributed digital asset.

### World App

World App is the first frontend to World ID: it guides individuals through the verification with the Orb and custodies an individual's World ID credentials and implements the cryptographic protocols to share those credentials with third parties in a privacy preserving manner. It is designed to provide frictionless access to global decentralized financial infrastructure. Eventually, there should be many different wallets integrating World ID.

### How does Worldcoin Work?

Worldcoin revolves around World ID, a privacy-preserving global identity network. Using World ID, individuals will be able to prove that they are a real, unique human to any platform that integrates with the protocol. This will enable fair airdrops, provide protection against bots/sybil attacks on social media, and enable the fairer distribution of limited resources. Furthermore, World ID can also enable global democratic processes and novel forms of governance (e.g., via quadratic voting), and it may eventually support a path to AI-funded UBI.

To engage with the Worldcoin protocol, individuals must first download World App, the first wallet app that supports the creation of a World ID. Individuals visit a physical imaging device called the Orb to get their World ID *Orb-verified*. Most Orbs are operated by a network of independent local businesses called Orb Operators. The Orb uses multispectral sensors to verify humanness and uniqueness to issue an Orb-verified World ID, with all images being promptly deleted on-device per default (absent explicit consent to Data Custody).

## Potential Applications

Worldcoin could significantly increase equality of opportunity globally by advancing a future where everyone, regardless of their location, can participate in the global digital economy through universally-accessible decentralized financial and identity infrastructure. As the network grows, so should its utility.

Today, many interactions in the digital realm are not possible globally. The way humans transact value, identify themselves, and interact on the internet is likely to change fundamentally. With universal access to finance and identity, the following future becomes possible:

### Finance

**Owning & Transferring Digital Money**: Sending money will be near instant and borderless, globally. Available to everyone. The world could be connected financially and everyone would be able to interact economically on the internet. The COVID relief fund for India, where over $400 million were raised in a short period of time by individuals around the world to support the country as a hint at what can be possible. Overall, this has the potential to connect people on a global scale unlike anything previously seen in human history.

Digital money is safer than cash, which can be more easily stolen or forged. This is especially important in crisis situations where instant cross-border financial transactions need to be possible, such as during the Ukrainian refugee crisis, where USDC was used to distribute direct aid. Additionally, digital money is an asset that individuals can own and control directly without having to trust third parties.

### Identity

**Keep the Bots Out:** Bots on Twitter, spam messages, and robocalls are all symptoms of the lack of sound and frictionless digital identity. These issues are exacerbated by rapidly advancing AI models, which can solve CAPTCHAs and produce content that is convincingly "human". As services ramp up defenses against such content, it becomes essential that an inclusive and privacy-preserving solution for proof of personhood is available as public infrastructure. If every message or transaction included a "verified human" property, a lot of noise could be filtered from the digital world.

**Governance:** Currently, collective decision making in web3 largely relies on token-based governance (one token, one vote), which excludes some people from participating and heavily favors those with more economic power. A reliable sybil-resistant proof of personhood like World ID opens up the design space for global democratic governance mechanisms not just in web3 but for the internet. Additionally, for AI to maximally benefit all humans, rather than just a select group, it will become increasingly important to include everyone in its governance.

### Intersection of Finance and Identity

**Incentive Alignment:** Coupons, loyalty programs, referral programs and more generally sharing value with customers is traditionally prone to fraud as the incentives for fraudulent actors are high. Frictionless and fraud resistant digital identity helps to align incentives and benefit both consumers and companies. This could even incept a new wave of companies owned in part by its users.

**Equal Distribution of Scarce Resources:** Crucial elements of modern society, including subsidies and social welfare, can be rendered more equitably by employing proof of personhood. This is particularly pertinent in developing economies, where social benefit programs confront the issue of resource capture—fake identities employed to acquire more than a person's fair share of resources. In 2021, India saved $5 billion in subsidy programs by implementing a biometric-based system that reduced fraud. A decentralized proof of personhood protocol can extend similar benefits to any project or organization globally. As AI advances, fairly distributing access and some of the created value through UBI will play an increasingly vital role in counteracting the concentration of economic power. World ID could ensure that each individual registers only once and to guarantee equitable distribution.

# Proof of Personhood (PoP)

Different approaches have different requirements for PoP. For high-value uses, it is important that the identity system is robust against attacks. Some identity systems are more robust than others. For example, a government-issued passport is harder. Therefore, the Worldcoin ecosystem, centered around the Worldcoin Foundation, is trying the foundation for a high-assurance PoP mechanism with World ID. World ID is an open-source, zero-knowledge through biometric verification system. It is designed to be robust against Sybil attacks, while also being private. The Worldcoin Foundation believes forms of PoP are less than ideal implementations of World ID.

## Building Blocks

For a high-level, does not cover-and-building blocks are responsible for an effective PoP mechanism. These include:

**Uniqueness**: A mechanism that ensures that each person can only participate once in the system, preventing multiple accounts or identities from being used to gain an unfair advantage or to manipulate outcomes. This is crucial for maintaining fairness and the integrity of the system.

**Sybil resistance**: Sybil attacks involving a given specific (value-based-based) in order to cross certain resources or issue certain rewards multiple times. Within the context of a PoP protocol these claims are related to preventing multiple identities from being created.

**Liveness**: A collection of data that serves as proof for particular attributes of that user that indicate the user is a human being. This data can include biometrics or things from the presence of a certain government-issued ID, or other forms of human-specific data.

**Sybil**: An inactivity that affects certain information that has not yet gone from PoP validated. (also called "Sybil-resistant" or "Sybil-proof").

**Verifiable**: An data that includes a proof. PoP validated and that is authenticity as part of a verifiable process to prove the user access to some actions.

**Privacy**: Protecting sensitive personal information, like biometrics, ensures, and authentication are important. Techniques like zero-knowledge proofs, ensure that users can prove legal-level existence of the building blocks, as a proof PoP mechanism. Detailed explanations on how these are implemented into World ID follow in later sections.

Fig. 1 Proof of Personhood Mechanisms. Deduplication, Authentication, Recovery, Revocation, Expiry.

## Deduplication

The UIDs for each user's iris codes is a basic-level of uniqueness. Or PoP, an be in proof-multiple-time and multinodes-a-time-based-based-based

# Decentralization and Open-Sourcing

Decentralization and Open Sourcing Roadmap

Decentralization is key to Worldcoin. The Worldcoin protocol is powerful and could be misused, especially if under centralized control. There have been countless occasions where people's trust in digital services has been abused. Therefore, to ensure that the Worldcoin protocol maximally benefits humanity, it is imperative that the protocol, ecosystem, technical computation, development, and governance are transparent, verifiable, and most importantly, decentralized. Decentralized community governance, in particular, is imperative to maintain the protocol's alignment with the people it serves—which is to say, everyone. This section focuses on all non-governance dimensions of decentralization that contribute to the overall integrity of the Worldcoin ecosystem.

## Worldcoin Protocol

The Worldcoin protocol is designed to be decentralized in order to make it resilient, remove single points of failure, and place control over the proof of personhood primitive in the hands of the people who use it. The decentralization goals of the protocol include:

- **Permissionless operation**, enabling anyone to issue and use credentials without central approval;
- **Decentralized operation**, allowing use without needing to trust or rely on a centralized party, including the ability to independently run off-chain infrastructure components;
- **Support for credentials on custom wallets**, offering flexibility and interoperability i.e. users should be able to choose their wallet and not be tied to a specific platform; and ultimately the
- **Ability to build on open standards** with independent implementations and interpretations (e.g., DIDs and verifiable credentials) to increase interoperability.

To use the protocol, certain open source, community-mainted components are or will be required:

- World ID requires a **sequencer,** similar to the L2 architecture for roll-ups, for increased scalability. It handles interaction with the on-chain contracts, both for issuance of credentials and proof generation (e.g., generating the World ID proof requires fetching the on-chain state of the contract to generate an inclusion proof).
- **Software development kits (SDKs) make** integration easy for wallets and verifiers will continue to be open source and community maintained. Other parties are able to develop and share their SDKs as well since they are based on open standards.
- **Crowd-curated lists of applications and issuers**, similar to the ERC-20 token lists of the Uniswap Protocol, helps prevent scams, spam and other forms of abuse.

Today, all protocol components are already open source. The protocol already supports privacy by enabling verification through zero-knowledge proofs, which lets a person prove ownership of a credential without revealing any details about it (e.g., one can prove today they have been verified at an Orb without revealing which verification belongs to them or when and where they were verified).

Community members may continue to contribute to, and develop new functionalities for the Worldcoin Protocol, like:

- An open source Wallet SDK so other wallets can easily support the Worldcoin protocol
- Specifications for future development of the Worldcoin protocol
- Sequencer decentralization (e.g., rotation of sequencers)
- Alternative credentials issued on the protocol
- A Decentralized metadata service
- A process for protocol improvement proposals to be submitted, so that any upgrades can be considered and authorized by the community prior to implementation

## The Orb

Anyone should be able to issue credentials on the Worldcoin protocol. While different applications have different requirements, high-stakes use cases such as social program support, global and equitable allocation of finite resources including AI-funded Universal Basic Income, as well as democratic governance of AI14 likely require a singular, highly secure and inclusive proof of personhood credential to prevent multiple registrations.

Decentralizing the issuance of this credential comes down to four parts:

- the uniqueness verification service,
- the development and production of biometric verification devices,
- the deployment of devices all over the world; and
- fraud prevention mechanisms.

### Uniqueness Service

World ID relies on iris biometrics to verify uniqueness among a global set. Several ideas for how the uniqueness service could be decentralized can be found here.

### Verification Devices

Design and manufacturing of biometric verification devices will be gradually decentralized to increase the resilience of the verification process against censorship and minimize the trust requirements in the manufacturing entity:

- **Decentralized Development** may be incentivized with grants from the Worldcoin Foundation, or later, by a token-based reward mechanism for each successful verification, analogous to validation rewards on Layer-1 chains. To enable the development of devices similar to the Orb, the Orb hardware is available under a shared source license, with the firmware expected to follow when it can be made available securely. Organizations who choose only to develop firmware to build their own devices can purchase Orb hardware from TFH, under a license granted from the Foundation. This is one step in the direction to reduce the dependence on TFH for firmware development, increase censorship resistance, and empower people to decide which organization they trust to perform the development process.
- **Development Standards:** The Worldcoin Foundation will develop an initial set of hardware and software standards related to biometric uniqueness verification devices, so that other organizations can then develop their biometric verification devices. Any device that meets the standards can then be whitelisted by the Worldcoin Foundation for use on the protocol, where compliance with the standards could be ensured through third party audits. Any organization could also issue their own proof of personhood credential on the Worldcoin protocol without any involvement from the Worldcoin Foundation. All verifications from whitelisted devices will pass through the same biometric uniqueness check ensuring there are no duplicate verifications across different issuing organizations, enabling individuals verified by any whitelisted device to be eligible to claim World ID. These standards will evolve based on community input, to reflect changes in technology and other factors.
- **Verifiability:** It is important to be able to verify the legitimacy of a biometric verification device (i.e., it's not counterfeit) and to validate that it runs a certain firmware (e.g., it doesn't store biometric data when it claims not to). One approach to verification is integrating a validation mechanism in TFH's World App or other protocol-compatible apps, where the device has to sign a challenge generated by the app and validated against a known set of public keys.

### Device Operators

Once manufactured, Orbs are operated by independent entrepreneurs and their organizations around the world. Those entities receive a reward for every successful verification, and, to some extent, the actual operation of Orbs is already decentralized. The Foundation will soon be responsible for issuing operator rewards, and has engaged TFH to help support and audit Orb operations. Eventually, operations will include a decentralized process for operators to qualify and receive an Orb, receive verification rewards, and audit operations that could potentially be enforce by on-chain smart contracts:

- **Orb Allocation:** Today, Orbs can only be borrowed but not rented, sold or auctioned off to operators. When an Operator joins the project, Orbs (and other equipment) are lent to Operators for a specified period of time. Short-term lending ensures that only Operators who use Orbs efficiently for verification purposes (i.e., not merely verifying a handful of people per week) get access to them, optimizing hardware production capacity and minimizing overhead. In a future-state with abundant Orb supply at low cost, Operators could simply buy biometric verification devices.
- **Signup Rewards:** Operators receive rewards for each successful verification. Eventually, governance could refine how the signup reward mechanism works or is calculated (e.g., to increase the likelihood of compliance with the Foundation's Operator Code of Conduct, a fraction of the signup reward could be locked-up. Governance could define the lock-up criteria, including any cap or other features).
- **Signup Quality:** 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 the Worldcoin project, Operator rewards are impacted by measures of sign-up quality. Governance could also refine the criteria for determining signup quality.

### World ID Integrity

Decentralizing the issuance and custody of World ID is challenging given the need to maintain high credential integrity (i.e., making it hard to illegitimately acquire and use the World ID of others). Different mechanisms across all participants—from hardware manufacturers to individual Orb operators to users—are required to prevent actions that undermine the integrity of the credential:

There are several scenarios that could result in the illegitimate creation or fraudulent ownership of proof of personhood credentials:

1. **Verification Device Compromise:** A third party submits fraudulent verifications by compromising the hardware or spoofing the verification process.
2. **Identity Theft:** The device operator or a third party manipulates individuals into verifying or compromising their phone to access their credentials.
3. **Identity Sale:** An individual decides to sell their credentials to a fraudulent actor.
4. **Issuer Fraud:** Organizations developing the firmware for verification devices secretly generate identities.

Each scenario decreases the utility of the proof of personhood credential issued by the Orb, so measures to make these attacks more costly are important. The following first five examples are integrity-strengthening measures on the Foundation's roadmap:

- **Biometric Verification Device Audits:** Audits that scope hardware, software and spoof security of the Orb, as well as investigate particular claims, such as "image data is not retained without explicit consent," increase the trust in the integrity of World ID. See here for the state of audits today.
- **Bug Bounty Program:** All organizations operating whitelisted verification hardware could be required to participate in a public bug bounty program covering hardware, software, and spoof security. The community is iterating on the design of a bug bounty program, which will launch soon.
- **Face Authentication:** As part of the verification process, a signed and encrypted face image could be transferred to the user's phone. The user could then authenticate against that image within the app, an approach similar to FaceID, making it hard to authenticate the credential of someone else. Beyond face recognition, the phone would also need to perform liveness detection to prevent spoofing attacks. The security guarantees that such a liveness check has actually been conducted and not spoofed are lower on consumer phones compared to custom hardware like the Orb (given consumer cameras are less advanced and that it is hard to create a trusted execution environment on a person's phone to ensure computational integrity). With improvements in mobile zero knowledge proof abilities, it may become possible to compute the authentication and liveness checks inside zero knowledge proofs on the user's phone, which would increase the security guarantees.
- **Iris Authentication**: Similar to face authentication, iris authentication performs a biometric authentication against a template as well as a liveness check. By requiring people to come back to a biometric verification device, the security guarantees that the liveness check has not been spoofed or bypassed are increased at the cost of convenience. If both face authentication and iris authentication were implemented, developers could choose which level of security is required for their application.
- **Recovery:** Victims of social fraud and identity theft should be able to recover their proof of personhood credential through an Orb using only their biometrics. This would also make the purchase of other individuals' proof of personhood unprofitable from a game-theoretic perspective.

The following four measures are not on the Foundation's immediate roadmap but still ideas being considered:

- **In-Person Audits:** To ensure compliance with the Operator Code of Conduct and to prevent any organization from secretly generating fake identities, operations should be audited. Today, third-party organizations audit on-the-ground signup operations. A potential path to decentralize this process could be publishing a list of all verification devices, their locations, and verification counts. This would enable decentralized and in-person verification of all devices. Auditors could balance the published verification numbers against a count of real people verifying live, and thereby discover illegitimate identity generation. Such a process would require careful mechanism design to avoid unintended side effects.
- **Anomaly Detection:** Metadata from Orbs could be made public to be utilized for decentralized anomaly detection, informing decisions on which Orbs to audit in person. However, what data to publish would require careful consideration to preserve the privacy of individuals who verify. Community input would likely be necessary to strike that balance.
- **Revocation:** If a particular firmware version of a verification device is deemed insecure or an operating organization is found to be fraudulent, the verification credentials can be retrospectively revoked in line with the Foundation's governance, to eliminate potential fraudulent identities. Eventually, there might be the need for a separate adjudication body. If there were any real and legitimate individuals affected, they could re-verify at an Orb.
- **Expiry:** As biometric verification devices and their security standards evolve, it might become useful to version World IDs. Over time, older World IDs might be deprecated to increase security, similar to passport expiration.

## World App and Other Clients

TFH launched World App as the first client to support the Worldcoin protocol. Currently, World App is the only way for people to get their World ID verified at an Orb and claim their share of WLD tokens.

Eventually, users will be able to either easily export their accounts into other wallets or use a third-party wallet at the time of verification with an Orb. Additionally, a World ID WalletKit could incorporate all the required capabilities, so that other wallets could easily integrate World ID, allowing the use of World ID various wallets of choice.

On the frontend, World ID is already available to any developer that wants to use sybil protection in their application through the IDkit and developer portal. Users are able to use any third-party application through World App.

## Progressive Decentralization

Some parts of the Worldcoin ecosystem are already decentralized and open source. However, decentralization is an ongoing process that requires significant community contributions and participation. A gradual transition towards a decentralized ecosystem allows for careful assessment and refinement at each stage, ensuring that the transition is sustainable in the long term. Decentralization is core to the mission of Worldcoin and requires active participation of the broader community.

# Foundation and Governance

Worldcoin aims to create universal access to the global economy regardless of country or background, accelerating the transition to an economic future that welcomes and benefits everyone. This vision requires that the protocol and ecosystem become decentralized. Only decentralization can ensure its resilience and its alignment with the people it serves—which is to say, everyone. An important step on the path towards decentralization was the establishment of the Worldcoin Foundation. This section describes the Foundation and sketches its thinking around governance, which will ultimately be shaped through community participation.

## Initial Contributors

A global community of developers, individuals, economists and technologists conceived and made early contributions to build the Worldcoin protocol. The original idea started with co-founders Sam Altman, Alex Blania and Max Novendstern, who assembled a team to take the initial steps toward development of Worldcoin via their company Tools for Humanity (TFH).

TFH's mission is, unsurprisingly, to build tools for humanity. It is a Delaware (U.S.) corporation headquartered in San Francisco, California, with a wholly-owned subsidiary, Tools for Humanity GmbH based in Germany. TFH supported Worldcoin's multi-year beta testing phase, during which it developed the Orb and the World App.

To date, TFH and other early contributors have been united by their commitment to providing every person on the planet access to the global economy, regardless of country or background.

## Enabling Decentralization

On October 31st, 2022 the Worldcoin Foundation ("Foundation") was established as the non-profit steward of the Worldcoin protocol, supporting and growing the ecosystem until it becomes self-sufficient. Its main objective is to scale an inclusive identity and financial network as a public utility and to decentralize governance thereof. This infrastructure empowers everyone to participate in the global economy in the age of AI and lays the foundations for universal basic income.

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 the most common structure currently in use by protocol decentralized autonomous organizations (DAOs), according to the DAO Research Collective. To learn more about this entity arrangement, check out this Guide to the Cayman Islands Foundation Company and this Insight on DeFi, DAOs, and VASPs in the Cayman Islands from the Foundation's outside counsel at the law firm Ogier.

This entity setup was a good fit for Worldcoin due to its 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 a DAO. The DAO can therefore gradually steer matters such as running a grant program, open sourcing protocol intellectual property (IP), entering into service agreements, and managing a treasury. In the case of Worldcoin, 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 is able to safeguard protocol IP that cannot be technologically decentralized. In most legal systems today, a DAO itself could not protect IP such as trademarks, open-source copyrights and domains. TFH 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 accounts. And the Foundation has open sourced several core tech repositories and made the Orb's hardware available under its Responsible Use License.

## Areas of Responsibility

**Decentralize Governance**: There are several assets that are governed by the Foundation:

- Orb IP: Tools for Humanity has transferred all Orb IP to the Worldcoin Foundation. The Orb hardware and software will be open source with a restricted use license, prohibiting the misuse of the technology. This allows the Foundation to onboard other organizations building Orbs or similar devices.
- Data: In the case of Worldcoin, the shared governance model is especially critical. The Foundation is the "data controller" for any personal data collected via Orb sign-ups after Network launch. Down the road, decisions about that data should reside with the community. As the Foundation is a non-profit, this demonstrates the commitment that user data will never be sold.
- Ability to Whitelist Orb Credential Issuers: The Foundation manages the permissions for adding Orbs to the network, balancing hardware decentralization, security, and growth.

**Decentralize Orb Development, Production and Operations**: Today, Orbs are developed and produced by Tools for Humanity. Orb operations are already semi-decentralized, managed by several organizations around the world. In cooperation with Tools for Humanity, the Foundation will work on standards and incentives for organizations to develop, produce and operate Orbs such that the ecosystem can be decentralized.

**Worldcoin Protocol Research**: The foundation is actively working on open research questions to advance the Worldcoin protocol.

**Develop a Grants Program to Evolve the Ecosystem**: To encourage individuals and organizations to contribute to the Worldcoin ecosystem through research, the development and production of Orbs (and similar devices) or auditing the system, the Worldcoin Foundation will set up a grants program.

## Governance Today

Today, the Worldcoin Foundation is "memberless"; it has no owners or shareholders. It is governed by a Board with three Directors: Chris "W" Waclawek, Phillip Sippl, and Glenn Kennedy of Leeward Management Ltd. Other Foundation advisors and contributors include Jacek Czarnecki, Remco Bloemen, and Sonja Prstec.

The Foundation currently uses a 4-of-6 multi-signature wallet to take any action related to Worldcoin's smart contracts.

## Decentralizing Governance

Decentralizing the governance of the Worldcoin protocol 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 DAO-based governance system for Worldcoin 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 DAO-driven governance. These provisions make it possible, through a prescribed process, for the DAO to make recommendations to the Foundation's Board of Directors. The Board is then bound to "observe, implement, carry out, action and execute with best efforts any and all DAO Recommendations," subject to directors' fiduciary duties and legal requirements. For further details, see the Foundation's Memorandum of Association and Articles of Association.

World ID provides a unique opportunity to harness input from a large and diverse set of individuals in DAO-driven governance. The reach of World ID is unprecedented: over two million World IDs have already been issued, and tens of thousands more are issued each week. As a proof of personhood, World ID naturally supports "one-person-one-vote" voting, in contrast to token-based voting commonly used by DAOs. Notably, this adds more democratic options to the design space of voting mechanisms for Worldcoin.

In keeping with its limited role, the Foundation will solicit proposals for how World ID should interact in Worldcoin's governance model. In general, the Foundation seeks input from contributors, the community and experts in the field as it decentralizes governance of the Worldcoin protocol.

This content is not available in your region.

# Limitations

This section outlines some limitations (without claiming exhaustiveness) based on laws, intrinsic limitations of the project as well as temporary limitations that can be mitigated by further open development.

## UBI

Worldcoin enables the fair distribution of UBI globally as it offers both globally-accessible digital financial rails while ensuring each participant cannot double-claim the same UBI distribution. The Worldcoin Protocol is not intended to generate profits to distribute UBI, and instead, it requires a separate funding source (e.g., a share of the profits generated by an AI Lab) to distribute global UBI.

## Orb Security

The Orb sets a high bar to defend against scalable attacks; however, no hardware system interacting with the physical world can achieve perfect security. The anti-fraud measures integrated into the Orb are continuously refined. Several contributor teams are continuously working on increasing the accuracy of the liveness algorithms as well as other security measures that are deployed via over-the-air updates. Even though significant effort has been spent on raising the security bar of the Orb, it is expected that the Orb may get spoofed or compromised by determined actors. The Orb has been designed with this threat model in mind: any World ID issued by a particular Orb can later on be revoked through the governance of the Worldcoin Protocol. To continuously discover potential vulnerabilities of the Orb, contributor red teams test various attack vectors. Several audits on the Orb and its infrastructure have been conducted and a bug bounty program will soon launch.

## False Rejections

Biometrics are probabilistic and biometric verification has inherent error rates. Currently, the error rate of the Orb for confusing any two people to be the same, is approximately 1 in 40 trillion. On a billion people scale, this translates to a 99.999% true acceptance rate or 0.001% false rejection rate, which is significantly better than other known alternatives. However, the ultimate objective is enabling total inclusivity. Using the birthday problem approximation, a false rejection rate of $10 - 20$ is statistically required to prevent the false exclusion of a single individual at a global scale. Ongoing community research is focussed on improving iris biometrics beyond the current state-of-the-art by leveraging AI and advanced hardware capabilities of the Orb. In the event that iris biometrics turn out to be insufficient, combining several biometric signals (biometric fusion15) could be employed to further reduce the error rate, a functionality already supported by the current hardware version of the Orb.

It is important to note that many health conditions, like cataracts to a certain degree, do not impede iris biometrics. Already today, iris biometrics surpass the inclusivity of other PoP verification alternatives like official IDs since less than 50% of the global population has digitally verifiable identities. However, if the proof of personhood mechanism becomes essential for society, it is important that eventually every single person can verify if they want to. Although not currently established, there could be specialized verification centers to facilitate alternative means of verification for individuals with eye conditions, via e.g. facial biometrics. The introduction of alternative means of verification for World ID could potentially create loopholes.

## Decentralization and Open Sourcing

Today, large parts of the Worldcoin Protocol stack are open source. This includes the World ID protocol, the sequencer for the Orb credential, and the SDK to access it. Other parts, like the firmware of the Orb are not yet open source due to security considerations; however, eventually every part of the infrastructure supporting the Orb credential should be open source. Further, while operations are already spread across independent entities, Orbs are only available via Tools for Humanity. For more details, see decentralization.

## World ID Transferability

While deduplication, i.e. ensuring that everyone can only verify once, has been solved to a high degree of certainty with the Orb, the authentication of the legitimate owner of a proof of personhood credential is both an important as well as a difficult challenge. This challenge is the same for any digital identity or PoP mechanism. Today, if someone passes on their World ID keys to a fraudster (e.g., through being tricked to sell their keys), the fraudster can then use that World ID to authenticate. Therefore, fraudsters could bypass the “one-person one-X” principle by acquiring multiple World IDs. There are several preventative measures in the World App that make it harder to restore another user’s backup, however, those measures are only temporary, especially since access to World ID through other wallets will become increasingly important over time. Therefore, several additional measures should be implemented:

- **Face Authentication:** Facial recognition, performed locally on the user’s device in a fashion similar to Face ID, can be used to authenticate users against their Orb verification, thereby ensuring that only the person to whom the World ID was originally issued can use it to prove that they are human. Authentication involves a 1:1 comparison with a pre-existing template that is stored on the user's phone, which requires considerably lower levels of accuracy in contrast to the 1:N global verification of uniqueness that the Orb is performing. Therefore, the entropy inherent to facial features is sufficient.
- **Iris Authentication:** This is conceptually similar to face authentication with the difference that an individual needs to return to an Orb. This process validates the individual as the rightful owner of their PoP credential. Using iris authentication through the Orb instead of face authentication on the users phone increases security. This authentication mechanism can be compared with, for example, physically showing up to a bank or notary to authenticate certain transactions. Although inconvenient, and therefore rarely required, it provides increased security guarantees.
- **World ID Recovery and Re-Issuance of Keys**: If a proof of personhood credential has been lost or compromised by a fraudulent actor, individuals can get their Orb credential re-issued by returning to the Orb, without the need to remember a password or similar information.

## Key Recovery and Persistent Reputation

Today, keys can be recovered through restoring user-managed backups. If someone lost their keys, they can get a new World ID (and deactivate their previous one); however, the keys for the previous World ID cannot be recovered through biometrics. For privacy reasons, actions associated with a particular World ID cannot be recovered today. Consequently, humanness validation should be implemented today with time bounds to ensure sybil resistance. It also means that certain use cases like persistent reputation, as would be required for undercollateralized lending, are limited today. Enabling World ID recovery requires solving hard research challenges to preserve privacy as well as a careful consideration of societal implications of persistent reputation.

# Other Resources

## Community

The Worldcoin roadmap is a dynamic and evolving blueprint that is subject to change and refinement through input and decisions from the Worldcoin 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 Twitter or Discord
- Contribute to open source repositories on Github
- Visit the World ID Developer Docs and Portal
- Reach out directly to the World ID team
- View live on-chain data on Dune Dashboard
- View the Decentralization and Open Source Roadmap

## Security Audits

Over the course of several months beginning in April 2023, audit firms Nethermind and Least Authority conducted two separate security assessments on the off-chain and on-chain components of the Worldcoin Protocol.

Included in the audits were 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 during the Nethermind security assessment, which performed a comprehensive audit of Worldcoin's smart contracts, 92.6% were identified as fixed after the re-audit stage, while 3.7% were mitigated and an additional 3.7% were acknowledged.

Links to full details of both audits will be linked shortly.

# 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 WORLDCOIN FOUNDATION (THE **FOUNDATION**) AND ANY OF THE PROJECT PARTICIPANTS (TOGETHER WITH THE PROJECT PARTICIPANTS, THE **WORLDCOIN ECOSYSTEM**) WHO HAVE WORKED ON THE WORLDCOIN PLATFORM (AS DESCRIBED HEREIN) OR DEVELOPERS OF THE WORLDCOIN PLATFORM 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:// WORLDCOIN.ORG (THE **WEBSITE**) OR ANY OTHER WEBSITES OR MATERIALS PUBLISHED BY THE FOUNDATION.

## 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. Any value ascribed to WLD may change quickly and may be lost in its entirety. Further, the technologies comprising the Worldcoin Platform, including the WLD token, are experimental in nature. There is no guarantee that the network will operate as planned. For more information, visit www.worldcoin.org/risks. Holding, buying, or selling WLD 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 http://www.worldcoin.org/tos.

As described further below, this document contains forward-looking estimates and statements regarding the intended actions and objectives of the Worldcoin Foundation and the Worldcoin Ecosystem, 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.worldcoin.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.

## 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 the Worldcoin Platform. 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 the Worldcoin Platform. 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 the Worldcoin Ecosystem 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.worldcoin.org/tos. The Terms of Service must be read together with the Whitepaper and further information available at www.worldcoin.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.

## Token Features

The native digital cryptographically-secured utility token of the Worldcoin Platform (**WLD Token**) is a transferable representation of attributed functions specified in the protocol/code of the Worldcoin Platform, designed to play a major role in the functioning of the ecosystem on the Worldcoin Platform, 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 the Worldcoin Platform, 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 the Worldcoin Platform, 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 the Worldcoin Platform.

## 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 the Worldcoin Ecosystem 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 the Worldcoin Ecosystem 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 the Worldcoin Ecosystem.

## 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 the Worldcoin Platform, 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 the Worldcoin project;
- 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.

## Informational Purposes Only

The project roadmap in the Whitepaper is being shared in order to outline the current status of Worldcoin as well as some of the plans of the Worldcoin Ecosystem and is provided solely for informational purposes and does not constitute any binding commitment. Because 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.

## 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. Worldcoin 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.

## 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 the Worldcoin Ecosystem, 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 the Worldcoin Ecosystem expressly disclaim any responsibility (whether express or implied) to release any revisions to these forward-looking statements to reflect events after such date.

## 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.

1. Possibly except for the validity date.↩
2. In recent implementations virtually all major providers switched from “labeling traffic lights” to the so-called *silent* CAPTCHAs (e.g. reCaptcha v3).↩
3. In this context, AI-safe refers to a process that’s hard for AI models. It’s assumed, for example, that spoofing the Orb is significantly harder for AI than performing a CAPTCHA.↩
4. where N is the total number of previously verified users.↩
5. In the context of World ID, each holder has a unique nullifier for themselves in each application. This nullifier is what enables *sybil* resistance while preserving privacy as verifiers can use such nullifiers to prevent multiple registrations.↩
6. the Orb’s secure computing environment was designed to make such compromises extremely difficult.↩
7. Also evaluated were private information retrieval (PIR) protocols, but even with state-of-the-art protocols like OnionPIR and further optimizations, the services would need 10 seconds of multi-core compute per request. Multi-party computation (MPC)-based PIRs would perform much better, but they offer no anonymization advantage over using an MPC-based anonymization network.↩
8. Note there’s a trust assumption on obtaining the inclusion proof from an indexing service as the user needs to provide their identity commitment to obtain an inclusion proof. Further decentralization of the indexing service is being explored.↩
9. It is sufficient to check uniqueness on a per-context basis, but the nullifiers should be globally unique values.↩
10. In this context, *credential* is used as a generic term to refer to a set of data about a subject, and in this case attested by a third-party (called issuer).↩
11. ZKML would allow the iris code to be recalculated in the event of a model upgrade, without users needing to go back to an Orb.↩
12. In this, *issuer* is the party who attests to a set of data about a subject. For example, Tools for Humanity is the issuer of the Orb *credential*.↩
13. This is in addition to the decentralization introduced by the distribution of Orb manufacturing and operations across different entities.↩
14. Some AI models might become very powerful. In that case, it might be required to develop governance mechanisms that reach beyond the organization running the model to decide on the guardrails and actions of such models.↩
15. This requires the prevention of combinatorial attacks and therefore excludes *e.g.* fingerprints. Therefore, the only possible combination would be combining pictures of the iris and the face since they are imaged at the same point in time and in the same location (*i.e.* the face).↩