WORLDCOIN

Privado por Diseño

Contenido

Ecosistema 3

La privacidad en la era de la IA 4

Principios de privacidad de Worldcoin 5

Principio 1 Seguridad: Asegurado matemáticamente 7

Principio 2 Anonimato: Muévete libremente en línea 8

Computación multipartita segura (SMPC) 8

Pruebas de conocimiento cero (ZKPs) 10

Principio 3 Elección y control: tus datos, tus reglas 12

Datos mínimos 12

Custodia personal 13

Autenticación facial 13

Principio 4 Transparencia: Desarrollado de forma abierta 15

Auditado 15

Código abierto y sin permisos 15

Ecosistema

El proyecto Worldcoin consiste de múltiples factores y herramientas, las cuales se combinan para formar una red de identidad centrada en el ser humano que brinda confianza al completar una transacción o al comunicarse en línea.

Worldcoin es un proyecto que abarca el World ID, un pasaporte digital anonimo, y una red que habilita el uso de activos digitales, proporcionando acceso inclusivo a la economía global digital para miles de millones de personas.

World ID es un protocolo de identidad descentralizada para comprobar que eres una persona única. Puedes utilizar el World ID para comprobar que eres un ser humano en cualquier actividad en línea, cómo autenticar videos y protegerte contra deep fakes. También lo puedes utilizar para acceder a sitios web y aplicaciones, parecido al Inicio de sesión con Google, demostrando que eres un humano único sin tener que compartir nunca datos personales como tu nombre, correo electrónico o número de teléfono.

Worldcoin Chain es un rollup de capa 2 que se lanzará próximamente en la red Ethereum y que utiliza el World ID para dar prioridad a las transacciones centradas en humanos sobre los bots.

WLD es el token de Worldcoin, el cual se da gratuitamente a los individuos por ser humanos y formar parte de la red de Worldcoin.[1]

Worldcoin Foundation es una organización sin fines de lucro que actúa como administradora del protocolo de Worldcoin. También es propietaria y gestiona la mayoría de los bienes relacionados a la marca de Worldcoin, incluyendo la propiedad intelectual para el orb y la tecnología de fuente abierta del protocolo.

Tools for Humanity (TFH) es una empresa de tecnología que fabrica herramientas para Worldcoin, incluidos el Orb y la World App.

Un **orb** es una cámara especial que verifica la humanidad y singularidad y te proporciona los datos para confirmar tu humanidad y personalidad con el uso de un World ID.

World App es una billetera de autocustodia de Worldcoin que proporciona un hogar para el World ID. Con la aplicación, también puedes enviar y recibir Worldcoin (WLD) tokens y otros activos digitales.

Para más información: ¿Qué es Worldcoin y como funciona?

[1] En jurisdicciones elegibles

La privacidad en la era de la IA

Un informe de 2022 de Europol, la agencia policial de la Unión Europea, sugería que hasta el 90% del contenido de Internet podrían generarse sintéticamente en 2026.

Catfishing. Scambots. Deepfakes. Suplantación de identidad. Desinformación. El Internet puede ser un lugar peligroso. El avance de la inteligencia artificial hará que Internet sea más útil que nunca, pero debemos ser conscientes de su potencial para amplificar los problemas existentes. Ya hemos visto lo que puede salir mal cuando un ser humano se hace pasar por otro. ¿Qué ocurre cuando pensamos que estamos tratando con un humano que en realidad es un agente de IA?

Lo que necesitamos es una forma de verificar que las personas con las que hablamos, a las que enviamos dinero y de las que vemos contenido en Internet (por nombrar sólo algunos ejemplos) son realmente personas. El objetivo de Worldcoin es que puedas controlar cada uno de estos elementos en la era de la IA.

Evitar que la IA inunde el Internet de personas falsas requiere una seguridad extraordinaria. Sin embargo, muchos de los enfoques previstos para hacer frente a esto son de mano dura. Existe la tentación de recurrir a las mismas herramientas de siempre, eliminando la privacidad y confiando en técnicas de identificación o verificación que pueden ser cooptadas para la vigilancia corporativa y gubernamental. Un panóptico podría funcionar, pero ¿a qué precio?

Creemos que hay un camino mejor: El proyecto Worldcoin consiste en crear tecnologías seguras que sitúen a los seres humanos en el centro, permitiéndoles controlar mejor y confiar en sus experiencias en línea sin sacrificar su privacidad.

Worldcoin es **privado por diseño**.

Cómo la IA plantea reisgos para la privacidad

Ya hemos visto circular deepfakes de políticos y celebridades, personas para las que existe una gran fuente de contenido en línea.

Pero la IA avanzada significa que pronto podrían utilizarse imitaciones de vídeo y audio extremadamente realistas para imitar a la gente común y corriente. Nos preocupa especialmente que el Internet y sus usuarios no estén preparados para los retos que planteará la IA avanzada. Imagínese estar en una llamada de Zoom con colegas que en realidad no lo son o con seres queridos que no son personas en absoluto. Las personas pueden ser fácilmente estafadas para que envíen dinero, divulguen secretos o hagan cosas que aún no imaginamos.

Para combatir las aplicaciones maliciosas de la IA, las plataformas deben ser capaces de saber que alguien es un humano único. Herramientas como "CAPTCHA" ya no son eficaces y se basan en datos vinculados a la huella digital de una persona. World ID es una alternativa que preserva la privacidad de las interacciones digitales como los CAPTCHAs. También sirve como alternativa a KYC y sistemas de identificación digital que revelan la identidad de un individuo o vinculan la identidad de una persona a su actividad digital.

Principios de privacidad de Worldcoin

La comunidad Worldcoin está construyendo algo sin precedentes: una red de confianza global, de máxima inclusión y que preserva la privacidad para demostrar la identidad de las personas. Pero el enfoque del proyecto respecto a la privacidad es contraintuitivo y novedoso, presentando una ruta fundamentalmente nueva que ninguna empresa u organización, o gobiernos, han tomado:

Worldcoin no quiere saber quién eres, sólo que eres un ser humano único.

Bots propulsados por IA se vuelven cada vez más comunes, aumentando en sofisticación, socavando la confianza en línea y haciéndose pasar por otras personas. Por eso, saber si estás interactuando con un humano o con un bot es cada vez más importante. Si nuestra única preocupación fuera demostrar nuestra identidad en Internet, la solución podría parecer bastante sencilla: utilizar documentos de identidad proporcionados por el gobierno para verificar nuestras identidades y navegar en línea. Al fin y al cabo, a menudo nos piden enseñar nuestra identificación en el banco. ¿No son las transacciones en línea, en la era de la inteligencia artificial, potencialmente igual de delicadas?

Dejando a un lado el hecho de que un estimado de 850 millones de personas no tienen algún tipo de identificación oficial y que los propios gobiernos han desplegado campañas sofisticadas de desinformación en línea, la verificación en línea a través de las identificaciones proporcionadas por el gobierno no es la solución. Revela mucho más sobre ti de lo necesario, como tu dirección, y te pone en riesgo de que roben tu identidad o que la utilicen para fines malevolos, incluyendo formas que no podemos imaginar debido a la IA.

Necesitamos pruebas de identidad y de privacidad en el mismo paquete (con la menor cantidad de barreras de entrada posibles).

Este es el desafío que Worldcoin busca resolver, y lo hace principalmente a través de World ID. World ID es un pasaporte digital global que se ubica localmente en el teléfono inteligente de su poseedor y le permite a alguien probar que es una persona única sin tener que compartir datos personales a cualquiera.

Es un sistema de verificación de humanidad para Internet que permite a las personas ser anónimas dondequiera que vayan. Un World ID verificado no recopila ni vincula a los identificadores como nombre o correo, vincula a datos de transacción de billetera, ni revela de quién fue el World ID que se utiliza. Por su diseño, Worldcoin se basa en la práctica de la minimización de datos; no almacena información identificativa.

“AHasta ahora, quien deseaba probar su humanidad en línea utilizaba medios como las identificaciones de gobierno, que tienen el inconveniente de identificar al usuario y de revelar una gran cantidad de otros datos personales, aunque no sea necesario. En cambio, World ID permite una ‘prueba de humanidad única’ anónima y así desafía el modelo de ‘capitalismo de vigilancia’ con un modelo que promueve la protección de datos. World ID refuerza así las posibilidades de realizar actividades en línea que respeten la protección de datos.”

Dr. Stefan Brink, excomisario estatal alemán de Protección de Datos y Libertad de Información en Baden-Württemberg de enero de 2017 a diciembre de 2022.

Además, World ID esta diseñado para que las personas lo puedan utilizar en todas las aplicaciones sin que éstas rastreen su actividad de una a otra. No hay un repositorio central del historial de uso. Puedes usar World ID en cientos de aplicaciones diferentes sin que una sepa de las otras, ni World ID de esas aplicaciones.

Worldcoin es privado por diseño con cuatro principios de privacidad entrelazados:

Principio 1

Seguridad: Asegurado matemáticamente

Principio 2

Anonimato: Muévete libremente en línea

Principio 3

Elección & Control: Tus datos, tus reglas

Principio 4

Transparencia: Desarrollado de forma abierta

Principio 1

Seguridad: Asegurado matemáticamente

Sin seguridad, no hay privacidad.

El objetivo de Worldcoin es que las personas puedan estar en línea sin que sus identidades queden expuestas y que puedan distinguir entre las interacciones basadas en bots y las humanas. La seguridad ayuda a garantizar ese nivel de privacidad, siempre y sin fallos.

World ID utiliza muchas técnicas de seguridad para garantizar la seguridad de los datos de los titulares de World ID.

Un conjunto incluye herramientas humanas, como el open-sourcing y las auditorías (véase: Transparencia), que ayudan a validar y someter a pruebas de presión las medidas de seguridad que se han creado e implantado como parte del proyecto Worldcoin.

El otro conjunto incluye herramientas criptográficas, como ZKPs y SMPC (véase: Anonimato), que utilizan matemáticas avanzadas para asegurar los datos, cifrarlos y mantenerlos privados o hacerlos anónimos.

La SMPC es uno de los pocos resultados en criptografía que puede proporcionar una confidencialidad perfecta. Las ZKP, por su parte, utilizan hashes anuladores, o valores únicos, para cada aplicación, de modo que no se pueda rastrear el historial de uso de las personas.

Es lo que se llama **asegurado por las matemáticas.**

Principio 2

?

Anonimato: Muévete libremente en línea

La mayor parte del tiempo no necesitamos identificación para estar en el mundo. Preparar la cena, leer un libro, dormir. Realizar estas actividades rara vez requiere que demostremos quiénes somos. Durante la mayor parte de nuestras vidas, nuestras acciones pasan desapercibidas, no son observadas ni registradas. Somos anónimos.

El anonimato es más difícil de conseguir en línea. Los sitios web pueden ver nuestra actividad y los navegadores pueden rastrear nuestros movimientos y comportamiento en línea. Esta vigilancia se vuelve potencialmente más dañina cuando se nos pide que demostremos quiénes somos, desde la monitorización de nuestra dirección IP en el extremo inferior hasta la autenticación mediante un documento de identidad emitido por el gobierno en el extremo superior.

Pero utilizar sitios web y aplicaciones no debería implicar ceder nuestros datos más que para hacer la cena. La gente debe poder moverse libremente por internet.

Pero utilizar sitios web y aplicaciones no debería implicar ceder nuestros datos más de lo que lo hace cocinar la cena. La gente debería poder **moverse libremente en internet**. Iniciar sesión en un sitio con una World ID lo permite.

Para mantener el anonimato en un mundo en línea, Worldcoin utiliza muchas tecnologías que preservan la privacidad, como la computación multipartita segura (SMPC) y las pruebas de conocimiento cero (ZKP).

Computación multipartita segura (SMPC)

Sólo hace falta un teléfono inteligente para crear un World ID, pero demostrar que el titular es un ser humano único que no ha creado múltiples World IDs, manteniendo la privacidad de su identidad, es un reto complicado.

Los datos biométricos, apropiadamente anonimizados, ofrecen la solución. La propia utilidad de los datos biométricos significa que deben recopilarse y utilizarse mínimamente y, cuando sea la única vía viable, debe manejarse con cuidado.

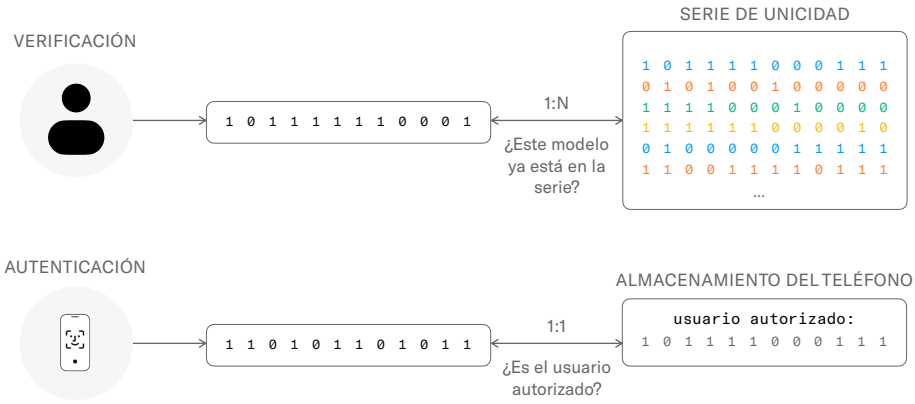
Worldcoin lo hace a través de la SMPC.

Cuando una persona verifica su World ID a través de un Orb, éste toma imágenes de su iris y de su cara. Utiliza estas imágenes para hacer un código de iris, que es esencialmente una serie de 1s y 0s. No hay dos códigos de iris iguales ni revelan identificadores directos como el nombre, el sexo, la edad, etc.

Este código de iris se divide en diferentes piezas y se cifra permanentemente mediante SMPC, que hace anónimos los datos al dividirlos en múltiples valores abstraídos (partes de SMPC) y almacenarlos en ubicaciones separadas gestionadas por dos entidades legalmente distintas. En un futuro próximo se añadirán socios de almacenamiento adicionales (incluidas universidades y organizaciones sin fines de lucro), lo que significa que los códigos del iris se dividirán en aún más valores abstraídos almacenados y gestionados por entidades aún más independientes. Ninguna sola parte tiene acceso a una parte del código del iris. Sólo tienen acceso a la parte de la SMPC almacenada bajo su control y gestión.

Aunque pueda parecer que almacenar los datos en varios lugares aumentaría la probabilidad de que esos datos fueran robados, en realidad ocurre todo lo contrario. Las partes de SMPC se almacenan de tal forma que, si un actor malintencionado consiguiera acceder de algún modo a una de ellas, ésta sería indescifrable; sólo tienen sentido cuando se juntan todas las piezas.

¿Por qué almacenar las acciones SMPC cifradas? Para que el protocolo Worldcoin pueda seguir demostrando que una persona es única. Sin él, los usuarios tendrían que volver a verificar su World ID cada vez que una aplicación lo solicitara.



Las fotos tampoco se quedan en el orb. En lugar de eso, el orb encripta los datos de extremo a extremo con una clave pública proporcionada por el teléfono inteligente del usuario (nadie más que el usuario tiene la clave privada para desencriptar) y luego el orb transmite las fotos encriptadas al dispositivo del usuario antes de borrarlas del orb. Todo esto ocurre en cuestión de segundos durante el proceso de verificación.

¿Por qué los iris?

Los Orbs–cámaras avanzadas–son los primeros dispositivos de hardware compatibles con el protocolo Worldcoin. Por ahora, el único método para verificar que los World IDs pertenecen a un ser humano único es visitar un Orb y tomarse una foto de los ojos.

TFH ha estudiado muchos tipos diferentes de biometría para verificar los World IDs, cada uno con sus pros y sus contras. Para cumplir los criterios del futuro necesarios para probar la humanidad de todos los individuos de la Tierra en un mundo de IA, cualquier método debe ser 1) preciso, 2) preservar la privacidad, 3) extremadamente difícil de falsificar, 4) escalable y 5) muy fácil de usar.

Las huellas dactilares son muy fáciles de usar, pero también de falsificar. Los iris, sin embargo, son precisos, utilizables, escalables, ampliamente inclusivos y extremadamente difíciles de falsificar. Además, preservan la privacidad. No hay grandes registros públicos de iris (como ocurre con las caras en las redes sociales), no se puede fotografiar un primer plano del iris de alguien sin que esa persona se dé cuenta, y se necesita un equipo de cámara especializado incluso para intentarlo.

El protocolo Worldcoin es abierto y descentralizado, y los mecanismos de verificación adicionales no harán sino reforzar el atractivo y la seguridad del proyecto.

Pruebas de conocimiento cero (ZKPs)

Una vez que una persona tiene un World ID verificado, puede utilizarlo para iniciar sesión y realizar transacciones con aplicaciones de terceros que se integren con el protocolo World ID.

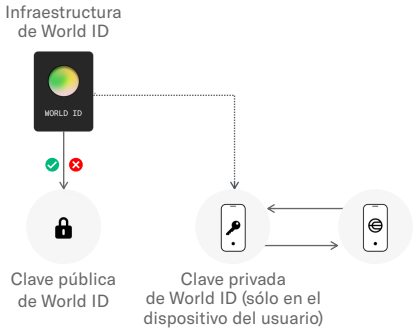
Pero eso no significa que la persona comparta su World ID con la aplicación de terceros.

En su lugar, el World ID se utiliza para crear una versión desechable de sí mismo, similar a Hide My Email de Apple o a las tarjetas de crédito virtuales. Imagina tener una tarjeta de crédito de empresa que sólo puede utilizarse para una compra. Para pagar cosas en otros proveedores, tendrías que generar tarjetas distintas. Aunque esto pueda parecer oneroso, el protocolo lo hace rápidamente y sin problemas tras bambalinas, lo que resulta en un sistema seguro para las aplicaciones y que protege a los usuarios.

El método para hacerlo—para que ni Worldcoin ni las aplicaciones puedan rastrear el historial de uso o entre aplicaciones o los grupos involucrados en una determinada transacción–es un ZKP, una herramienta criptográfica que permite demostrar que algo es cierto sin revelar la información utilizada para llegar a esa conclusión.

Cada vez que utilices una aplicación de terceros, la aplicación solicitará una prueba a tu dispositivo. Piensa en ello como si le hicieras una pregunta a tu dispositivo. Quiere saber si, ¿éste dispositivo controla este World ID? La World App del dispositivo del usuario devuelve un ZKP que demuestra que el World ID está verificado.

Los ZKP van mucho más allá de los requisitos normativos de cualquier jurisdicción. Worldcoin los implementó porque son la mejor manera de garantizar que los usuarios puedan permanecer anónimos (a menos que el usuario proporcione información adicional directamente al servicio de terceros que solicita la prueba) y que las aplicaciones no puedan rastrearlos. Evitan que terceros—y la propia Worldcoin Foundation—conozcan el World ID de un usuario o los servicios con los que interactúa.



Una analogía práctica para las ZKPs

Las ZKP son criptografía avanzada, por lo que no se prestan a analogías perfectas. Pero para hacerte una idea básica, imagina un juego en el que hay que encontrar un objeto o una persona en particular dentro de una imagen.[2]

Después de buscar durante unos minutos, una persona le dice a la otra que sabe dónde está el objeto. La segunda persona, que no sabe dónde está el objeto, no sabe si creérselo.

Así que la primera persona dice que puede demostrarlo sin revelar dónde está el objeto.

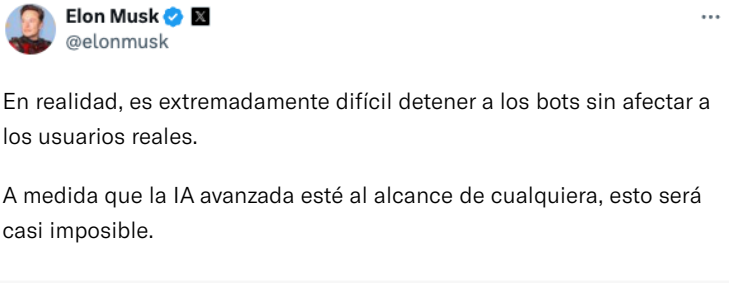
Fotocopia la imagen completo, recorta el objeto y se lo enseña a la segunda persona, que ahora está segura de que el objeto está en el rompecabezas y de que la primera persona sabe dónde está.

[2] Por ejemplo, «¿Dónde está Waldo/Wally?».

En este escenario, la segunda persona es cualquier aplicación que intente confirmar que un usuario es humano; el objeto recortado es la ZKP; y la primera persona es el protocolo Worldcoin que prueba que el usuario es humano sin revelar su identidad.

Caso de uso:
¿X bot o humano?

Elon Musk compró X (entonces llamada Twitter) prometiendo expulsar a los bots de la plataforma. Pero el nuevo propietario no tardó en darse cuenta de que era más fácil decirlo que hacerlo. “Es extremadamente difícil detener a los bots sin afectar a los usuarios reales,” escribió Musk en diciembre de 2023. “A medida que la IA avanzada esté al alcance de cualquiera, será casi imposible.”



Musk tenía razón sobre el reto que suponían los bots para la plataforma social. pero ahora existe una solución viable para combatirlos sin afectar a los usuarios.

X permite tres modos de inicio de sesión: Iniciar sesión con Google, Iniciar sesión con Apple o un nombre de usuario/contraseña. Para crear una cuenta, se pide a los usuarios que faciliten su nombre, número de teléfono o correo electrónico y fecha de nacimiento. Como es relativamente fácil crear varias direcciones de correo electrónico, también es bastante sencillo crear varias cuentas de X. Así, no hay mucha barrera para que los bots se conecten, debido a esto pueden degradar la experiencia de usuario para los humanos.

Sin embargo, World ID no se basa en direcciones de correo electrónico, que son fáciles de crear, ni en números de teléfono, que son fáciles de falsificar. Sólo los humanos pueden obtener un World ID verificado y, a diferencia de los correos electrónicos, están limitados a uno. Por lo tanto, si X utilizara World ID como mecanismo de verificación de la persona, el servicio podría añadir una insignia que indicara que esas cuentas tienen verificacion humana. Los bots que se conecten no podrían verificar esto nunca.

Y lo que es más importante, esto incluso aumentaría el anonimato de los usuarios de X, que no tendrían que facilitar más información de la que ya han proporcionado a X.

Esto no es totalmente teórico. TFH construyó una integración de World ID Telegram para deshacerse de los bots de spam en la red. Los administradores del chat público pueden ordenar que las cuentas individuales se verifiquen primero con World ID antes de publicar en un grupo.

Principio 3

Elección y control: tus datos, tus reglas

Las personas se ha acostumbrado cada vez más a un paradigma de Big Tech en el que, a cambio de acceder a servicios, cede sus datos personales a empresas para que los vendan al mejor postor.[3]

Worldcoin opera fuera de este paradigma. Esto no es sólo una promesa. Worldcoin se está diseñando intencionadamente para que sea imposible hacerlo.

El enfoque de Worldcoin es: **Tus datos, tus reglas.**

Datos mínimos

El punto de partida para reconocer el control de las personas sobre sus datos es no pedir muchos datos para empezar. Dado que los World IDs verificados son anónimos, las personas no proporcionan su nombre, números de teléfono, dirección u otra información comúnmente captada por las empresas tecnológicas. Piensa en esto: Para obtener un carné de biblioteca, la gente necesita una prueba de residencia con una dirección. Para obtener un World ID verificado, un pasaporte digital global, sólo necesitan un teléfono inteligente y visitar un Orb.

Caso de uso:
Códigos de descuento de Shopify

Shopify es una plataforma de comercio electrónico para empresas que buscan aumentar sus ventas y gestionar los pagos en línea. Los comerciantes de la plataforma a veces buscan atraer a nuevos clientes mediante descuentos únicos.

El problema es que la gente puede engañar al sistema enviando correos electrónicos falsos y solicitando descuentos varias veces, o utilizando bots para que lo hagan por ellos. En lugar de atraer a nuevos clientes, los vendedores están subsidiando una estafa.

Al integrar World ID en su tienda, los comerciantes pueden dejar que los clientes reales escaneen un código QR que verifica su World ID y aplica un código de descuento. Este método garantiza un descuento por humano, lo que resuelve el problema de los comerciantes sin pedir al usuario ninguna información adicional. (¡Aunque tendrán que dar los datos de su tarjeta de crédito y de envío para pasar por caja!)

[3] ¡Literalmente! Más información en https://en.wikipedia.org/wiki/Real-time_bidding

Custodia personal

El proceso de verificación de un World ID requiere el uso de algunos datos, específicamente, imágenes biométricas y códigos de iris. Los códigos de iris, tras pasar por la SMPC, van a unos servidores donde residen en un formato totalmente anonimizado. Pero los datos facilitados por el usuario para verificar su identidad a través del Orb no se conservan ni se facilitan a terceros. En su lugar, residen únicamente en el smartphone de la persona, donde se cifran con su clave pública.

Con la Custodia Personal de Worldcoin, las personas controlan los datos recolectados y generados durante la verificación—incluidos el World ID y las imágenes—y deciden con quién compartirlos.

Autenticación facial

Al instituir World ID, las plataformas pueden protegerse de los bots sin invadir la privacidad de sus clientes. Un World ID verificado proporciona a estas plataformas un alto nivel de confianza en que un usuario es realmente una persona.

Pero en algunos escenarios de alto riesgo (por ejemplo, las transacciones financieras), cuando las plataformas o las personas deben saber no sólo que están tratando con una persona, sino que están tratando con una persona específica. Quieren saber que la persona que utiliza el World ID es el mismo ser humano único que verificó el World ID en ese dispositivo.

Para conseguirlo, las aplicaciones de Worldcoin pueden utilizar la Autenticación Facial.

La autenticación facial es un método para comparar la imagen tomada durante la verificación con una imagen de la persona que desea utilizar el World ID y es independiente del dispositivo.

La primera imagen se genera cuando una persona verifica su World ID en un orb. El teléfono del usuario es, por defecto, el único lugar donde existen estos datos. Estas fotos de alta resolución se encriptan y se envían de forma segura al teléfono del usuario como parte de la Custodia Personal, y se eliminan completamente del orb.

La segunda imagen es una selfie tomada en el dispositivo del usuario dentro de la World App cuando el usuario intenta acceder o utilizar su World ID. La autenticación facial para World ID compara la imagen tomada por el dispositivo del usuario con la imagen original de autenticación facial tomada durante la verificación en el orb. El usuario solo puede continuar con su inicio de sesión o transacción si las dos imágenes coinciden.

De este modo, se previene el fraude al defenderse de un actor malintencionado que robe (o compre) el teléfono de alguien y utilice su World ID. Con la autenticación facial, el usuario destinado siempre tiene el control de sus datos y de su World ID. **La comparación se realiza localmente en el dispositivo del individuo.** Como resultado, ni la selfie, ni la foto del orb, ni ningún otro dato personal se comparte con terceros, incluidos Tools for Humanity o la Fundación Worldcoin.[4]

[4] En el futuro, el proyecto permitirá que las personas opten por compartir voluntariamente su información con Worldcoin para contribuir a la seguridad y al entrenamiento de la IA. Esto es 100% opcional, y el permiso puede ser revocado en cualquier momento.

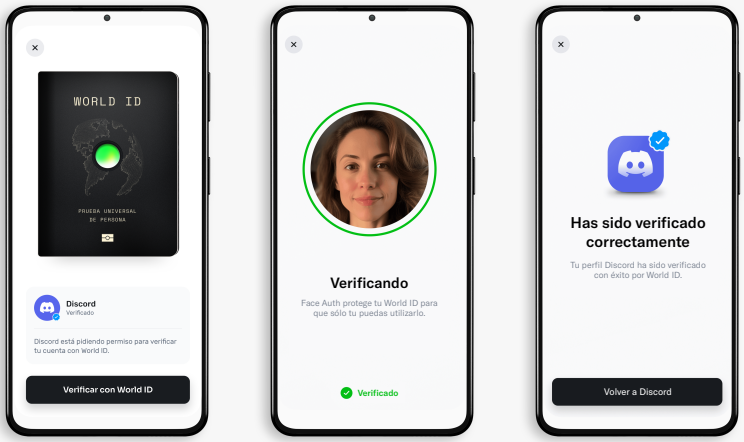
Autenticación Facial comparado con Face ID

Para los usuarios, Autenticación Facial será tan reconocible como el Face ID de Apple.

Entonces, ¿por qué no utilizar simplemente Face ID?

La Autenticación Facial garantiza que la persona que utiliza la World App es la misma que creó el World ID asociada en un orb. Face ID no permite esta capacidad.

Face ID es una combinación de hardware y software, por lo que en última instancia está vinculado a un iPhone. Con Face ID, los usuarios podrían tener una cara asociada al dispositivo distinta de la que utilizaron para verificar el World ID, lo que aumenta las posibilidades de fraude. Al utilizar World ID, que se encuentra a nivel de aplicación y no de dispositivo, la autenticación facial impide que cualquier persona que no sea la que verificó el World ID pueda acceder a él.



Principio 4

Transparencia: Desarrollado de forma abierta

Los expertos en seguridad son escépticos y buscan peligros detrás de cada línea de código fuente. Y eso es bueno, así es como nos mantienen a salvo.

Sería inconcebible pensar que TFH o unos pocos desarrolladores de Worldcoin pudieran imaginar todos los fallos posibles del protocolo. Por eso Worldcoin se **desarrolla de forma abierta.**

Auditado

Worldcoin incorpora tantas opiniones y campos de experiencia externos como es posible. Criptógrafos y expertos en biometría evalúan continuamente el código fuente mientras auditores y consultores de seguridad ratan de encontrar la más mínima posibilidad de vulnerabilidad. A continuación, Worldcoin publica los resultados y lo que ha hecho para solucionar incluso los problemas más pequeños.

Para detectar posibles infracciones, también tenemos que entender cómo podría utilizarse el protocolo en el mundo real, ahora y en el futuro. Eso significa pensar en miles de realidades culturales de todo el mundo e incorporar estas consideraciones a un modelo de seguridad que proteja contra usos indebidos que quizá ni siquiera existan todavía.

A partir de abril de 2023, las empresas de auditoría Nethermind y Least Authority llevaron a cabo dos auditorías de seguridad separadas del protocolo Worldcoin. Especificamente, las auditorías cubrieron las siguientes áreas:

- Corrección de la implementación, incluyendo construcciones y primitivas criptográficas y el uso apropiado de construcciones de contratos inteligentes.
- Errores de implementación comunes y específicos de cada caso
- Acciones adversas y otros ataques al código
- Almacenamiento seguro de claves y gestión adecuada de las claves de cifrado y firma
- Exposición de cualquier información crítica durante las interacciones del usuario
- Resistencia a ataques DDoS (denegación de servicio distribuida) y similares
- Vulnerabilidades en el código que provoquen acciones adversas y otros ataques
- Protección contra ataques maliciosos y otros métodos de explotación
- Problemas de rendimiento u otras posibles repercusiones en el rendimiento
- Privacidad de los datos, fuga de datos e integridad de la información
- Permisos inadecuados, escalada de privilegios y autoridad excesiva

Código abierto y sin permisos

Hacer que el código de Worldcoin sea de código abierto y sin permisos ayuda a cumplir tres objetivos. En primer lugar, expone a la red a críticas que pueden mejorarla.

En segundo lugar, permite que los desarrolladores se sientan seguros a la hora de implementar el protocolo Worldcoin. Es posible que otros equipos creen una aplicación de prueba de persona sobre World ID, o que encuentren un método de verificación aún más útil que un orb.

Por último, ser de código abierto y sin permisos es esencial para un proyecto descentralizado: cualquiera puede crear su propia versión (o “fork”) del protocolo en cualquier momento, por cualquier motivo, y esto es algo bueno.


WORLDCOIN