WORLDCOIN

Private by Design

Inhalt

Das Projekt

Das Worldcoin-Projekt besteht aus mehreren Akteuren und Tools, die zusammen ein menschenzentriertes Identitätsnetzwerk bilden, das Vertrauen bei Online-Transaktionen oder -Kommunikation ermöglicht.

Worldcoin ist ein Projekt, das World ID, einen anonymen digitalen Ausweis sowie ein Netzwerk umfasst, das die Nutzung digitaler Vermögenswerte ermöglicht und Milliarden von Menschen einen inklusiven Zugang zur globalen digitalen Wirtschaft bietet.

World ID ist ein dezentrales Identitätsprotokoll, mit dem bewiesen werden kann, dass man eine echte, einzigartige Person ist. Mit World ID kannst du bei jeder Online-Aktivität, wie der Authentifizierung von Videos oder dem Schutz vor Deepfakes, nachweisen, dass du ein Mensch bist. Außerdem kannst du es zum Einloggen auf Websites und in Anwendungen verwenden, ähnlich wie bei „Mit Google anmelden“, wobei du beweisen kannst, dass du ein einzigartiger Mensch bist, ohne jemals persönliche Daten wie deinen Namen, deine E-Mail-Adresse oder Telefonnummer teilen zu müssen.

World Chain ist ein bald startender Layer-2-Rollup im Ethereum-Netzwerk, der World ID nutzt, um menschenzentrierte Transaktionen gegenüber Bots zu priorisieren.

WLD ist der Worldcoin Token, der Menschen kostenlos für ihre Teilnahme am Worldcoin-Netzwerk und den Nachweis ihrer Menschlichkeit gegeben wird.[1]

Die **Worldcoin Foundation** ist eine gemeinnützige Organisation, die als Verwalterin des Worldcoin Protokolls fungiert. Sie besitzt und verwaltet außerdem die meisten Vermögenswerte im Zusammenhang mit der Marke Worldcoin , einschließlich des geistigen Eigentums für die Orb-Technologie und die Open-Source-Technologie des Protokolls.

Tools for Humanity (TFH) ist ein Technologieunternehmen, das Tools für Worldcoin entwickelt, darunter der Orb und die World App.

Ein **Orb** ist eine spezielle Kamera, die die Einzigartigkeit einer Person überprüft und dir die Daten liefert, um deine Identität mithilfe einer World ID zu bestätigen.

Die **World App** ist ein selbstverwalteter Wallet von Worldcoin, der Aufebwahrungsort für die World ID ist. Mit der App kannst du außerdem Worldcoin Token und andere digitale Gelder senden und empfangen.

Für weitere Informationen: Was ist Worldcoin und wie funktioniert es?

[1] Wo es die Gesetzgebung zulässt

Datenschutz im Zeitalter der KI

Ein Bericht von Europol, der Polizeibehörde der Europäischen Union, aus dem Jahr 2022 deutete darauf hin, dass bis zu 90 % der Inhalte im Internet im Jahr 2026 synthetisch erzeugt werden könnten.

Catfishing. Scambots. Deepfakes. Identitätsdiebstahl. Desinformation. Das Internet kann ein gefährlicher Ort sein. Die Fortschritte im Bereich der KI werden das Internet nützlicher denn je machen, doch wir müssen uns bewusst sein, dass diese Technologie bestehende Probleme verstärken kann. Wir haben gesehen, was passieren kann, wenn ein Mensch vorgibt, jemand anderes zu sein. Was passiert, wenn wir glauben, mit einem Menschen zu interagieren, der in Wirklichkeit aber KI ist?

Wir brauchen eine Möglichkeit, um sicherzustellen, dass die Menschen, mit denen wir online sprechen, denen wir Geld senden oder deren Inhaltewir sehen (um nur ein paar Beispiele zu nennen), tatsächlich Menschen sind. Worldcoin möchte dir im Zeitalter der KI die Kontrolle über all diese Elemente geben.

Um zu verhindern, dass KI das Internet mit falschen Identitäten überschwemmt, ist außergewöhnliche Sicherheit erforderlich. Viele der vorgeschlagenen Lösungen sind jedoch oft übermäßig drastisch. Es besteht die Versuchung, auf alte und bekannte Werkzeuge zurückzugreifen – Datenschutz zurückfahren und Identifizierungs- oder Verifikationstechniken einsetzen, die für Überwachungszwecke durch Unternehmen und Regierungen missbraucht werden könnten. Ein Überwachungsstaat mag funktionieren, aber zu welchem Preis?

Wir glauben, dass es einen besseren Weg gibt: Das Worldcoin Projekt zielt darauf ab, sichere Technologien zu schaffen, die den Menschen ins Zentrum stellen und ihnen ermöglichen, ihre Online-Erfahrungen besser in der hand zu haben und zu vertrauen, ohne ihre privaten Daten zu opfern.

Worldcoin ist für diesen Zweck gemacht – **Private by Design**.

KI als Risko für den Datenschutz

Deepfakes von Politikern und prominenten Persönlichkeiten kennen wir – Menschen, über die es eine Fülle von Online-Inhalten gibt, die als Vorlage dienen können. Doch fortschrittliche KI bedeutet, dass Deepfakes – extrem realistische Videos und Audiodateien – bald genutzt werden könnten, um alltägliche Menschen zu imitieren. Uns geht es besonders um den Punkt, dass das Internet und seine Nutzer nicht auf die Herausforderungen vorbereitet sind, die fortschrittliche KI mit sich bringen wird. Stell dir vor, du bist in einem Zoom-Call mit Kollegen, die gar keine Kollegen sind, oder mit geliebten Menschen, die gar keine echten Personen sind. Menschen könnten leicht dazu verleitet werden, Geld zu senden, Geheimnisse preiszugeben oder Dinge zu tun, die wir uns noch gar nicht vorstellen können.

Um böswillige Anwendungen von KI zu bekämpfen, müssen Plattformen sicherstellen können, dass eine Person ein einzigartiger Mensch ist. Werkzeuge wie CAPTCHA sind nicht mehr effektiv und basieren auf Daten, die mit dem digitalen Fußabdruck einer Person verknüpft sind. World ID ist eine datenschutzfreundliche Alternative für digitale Interaktionen wie CAPTCHAs und dient als Ersatz für KYC (Know Your Customer), ein Verfahren, das die Identität einer Person offenlegt, sowie für digitale ID-Systeme, die die Identität einer Person mit ihrer digitalen Aktivität verknüpfen.

Datenschutzprinzipien von Worldcoin

Die Worldcoin-Community baut etwas völlig neues: ein weltweit vertrauenswürdiges, maximal inklusives, datenschutzfreundliches Netzwerk zum Nachweis der Identität. Doch der Ansatz des Projekts in Bezug auf Datenschutz ist gegen intuitive Erwartungen und neuartig, und stellt einen grundlegend neuen Weg dar, den bisher weder Unternehmen, Organisationen noch Regierungen eingeschlagen haben.

Worldcoin will nicht wissen, wer du bist, sondern nur, dass du ein einzigartiger Mensch bist.

KI-gesteuerte Bots werden immer allgegenwärtiger, immer ausgefeilter, untergraben das Vertrauen im Internet und imitieren Menschen. Daher wird es zunehmend wichtiger zu wissen, ob man mit einem Menschen oder einem Bot interagiert. Wäre der Proof of Humanness online unser einziges Anliegen, könnte die Lösung recht einfach aussehen: Wir verwenden die von der Regierung ausgestellten Ausweise, um unsere Identität zu verifizieren und uns im Internet zu bewegen. Schließlich werden wir oft gebeten, unseren Ausweis bei der Bank zu zeigen. Sind Online-Transaktionen im Zeitalter der KI nicht potenziell ebenso sensibel?

Abgesehen davon, dass schätzungsweise 850 Millionen Menschen keinen offiziellen Ausweis haben und Regierungen selbst ausgeklügelte Desinformationskampagnen online durchgeführt haben, ist die Verifizierung mittels amtlicher Ausweise online nicht die Lösung. Sie offenbart viel mehr Informationen als nötig, wie zum Beispiel deine Adresse, und setzt dich dem Risiko aus, dass deine Identität gestohlen oder für böswillige Zwecke verwendet wird, einschließlich Szenarien, die wir uns aufgrund von KI noch nicht vorstellen können.

Wir brauchen einen Proof of Humanness und Datenschutz in einem Paket (so barrierefrei wie möglich).

Dies ist die Herausforderung, die Worldcoin zu lösen versucht, und dies geschieht hauptsächlich durch World ID. World ID ist ein globaler digitaler Pass, der lokal auf dem Smartphone seines Inhabers gespeichert ist und es einer Person ermöglicht, nachzuweisen, dass sie einzigartig ist, ohne persönliche Daten mit jemandem zu teilen.

Es ist ein System zur Verifizierung der Humanness für das Internet, das es den Menschen ermöglicht, anonym zu bleiben, wohin sie auch gehen. Eine verifizierte World ID sammelt oder verknüpft keine Daten wie Namen oder E-Mail-Adressen, verknüpft keine Wallet-Transaktionsdaten und gibt nicht preis, wessen World ID verwendet wird. Worldcoin basiert von Grund auf auf dem Prinzip der Datenminimierung. Es speichert keine identifizierenden Informationen.

„Bis jetzt mussten Personen, die sich online als Mensch ausweisen wollten, auf Mittel wie staatliche Ausweise zurückgreifen, die den Nachteil haben, dass sie Benutzer identifizieren und gleichzeitig eine Vielzahl anderer persönlicher Daten preisgeben, obwohl dies nicht notwendig ist. Im Gegensatz dazu ermöglicht World ID einen anonymen 'Proof of Humanness' und stellt so dem Modell des 'Überwachungskapitalismus' ein Modell gegenüber, das den Datenschutz fördert. World ID stärkt damit die Möglichkeiten für datenschutzkonforme Online-Aktivitäten.“

Dr. Stefan Brink, ehemaliger Landesbeauftragter für Datenschutz und Informationsfreiheit in Baden-Württemberg von Januar 2017 bis Dezember 2022.

Darüber hinaus ist World ID so aufgebaut, dass Menschen sie in verschiedenen Anwendungen verwenden können, ohne dass diese Apps ihre Aktivitäten von einer zur anderen verfolgen. Es gibt kein zentrales Verzeichnis der Nutzungshistorie. Sie können World ID in Hunderten verschiedener Apps verwenden, ohne dass eine von der anderen weiß – oder dass World ID von diesen Apps erfährt.

Worldcoin ist von Grund auf datenschutzfreundlich gestaltet, basierend auf vier ineinandergreifenden Datenschutzprinzipien:

Prinzip 1

Sicherheit: Sicherheit durch Mathematik

Prinzip 2

Anonymität: Frei im Internet bewegen

Prinzip 3

freie Wahl & Kontrolle: Deine Daten, deine Regeln

Prinzip 4

Transparenz: Offen entwickelt

Prinzip 1

Sicherheit: Sicherheit durch Mathematik

Ohne Sicherheit gibt es keinen Datenschutz.

Bei Worldcoin geht es darum, Menschen die Möglichkeit zu geben, online zu sein, ohne ihre Identität preiszugeben, und sie dabei zu befähigen, zwischen bot-basierten und menschlichen Interaktionen zu unterscheiden. Sicherheit stellt sicher, dass dieses Datenschutzniveau jedes Mal zuverlässig erreicht wird.

World ID nutzt zahlreiche Sicherheitstechniken, um die Datensicherheit der World ID-Inhaber zu gewährleisten.

Ein Teil davon umfasst menschliche Werkzeuge wie Open-Source und Audits (siehe: Transparenz), die dabei helfen, die Sicherheitsmaßnahmen, die im Rahmen des Worldcoin-Projekts entwickelt und implementiert wurden, zu validieren und auf Herz und Nieren zu prüfen.

Der andere Teil beinhaltet kryptografische Werkzeuge wie Zero-Knowledge-Proofs (ZKPs) und Secure Multi-Party Computation (SMPC) (siehe: Anonymität), die fortgeschrittene mathematische Verfahren nutzen, um Daten zu sichern, zu verschlüsseln und privat zu halten oder anonym zu machen.

SMPC ist eine der wenigen kryptografischen Techniken, die perfekte Geheimhaltung bieten kann. ZKPs verwenden sogenannte Nullifier-Hashes oder einzigartige Werte für jede Anwendung, sodass die Nutzungshistorie von Personen nicht nachverfolgt werden kann.

Man könnte es als '**durch Mathematik gesichert**' bezeichnen.

Prinzip 2

?

Aber die Nutzung von Websites und Apps sollte nicht bedeuten, dass wir mehr Daten preisgeben müssen als wenn wir zuhause beim Abendessen sitzen. Die Menschen sollten sich frei im Internet bewegen können.

Anonymität: Frei im Internet bewegen

Im Alltag brauchen wir meist keine Identifizierung. Abendessen kochen, ein Buch lesen, schlafen – diese Aktivitäten erfordern selten einen Nachweis darüber, wer wir sind. Für den Großteil unseres Lebens bleiben unsere Handlungen unbemerkt, unbeobachtet und unaufgezeichnet. Wir sind anonym.

Anonymität ist online schwerer zu erreichen. Webseiten können unsere Aktivitäten einsehen, und Browser können unsere Bewegungen und unser Verhalten im Netz verfolgen. Diese Überwachung kann potenziell gefährlicher werden, wenn wir aufgefordert werden, unsere Identität nachzuweisen – sei es durch die Überwachung unserer IP-Adresse oder im Extremfall durch die Authentifizierung mit einem amtlichen Ausweis.

Aber die Nutzung von Websites und Apps sollte nicht mehr Daten preisgeben als das Kochen eines Abendessens. Menschen sollten sich **frei im Internet bewegen** können. Das Einloggen auf einer Website mit World ID ermöglicht dies.

Um Anonymität in einer digitalen Welt zu gewährleisten, verwendet Worldcoin zahlreiche datenschutzfreundliche Technologien, darunter Secure Multi-Party Computation (SMPC) und Zero-Knowledge-Proofs (ZKPs).

Secure Multiparty Computation (SMPC)

Es braucht lediglich ein Smartphone, um eine World ID zu erstellen. Der Beweis, dass der Inhaber ein einzigartiger Mensch ist, der nicht mehrere World IDs erstellt hat, während seine Identität privat bleibt, ist jedoch eine komplexe Herausforderung.

Biometrische Daten, wenn sie angemessen anonymisiert werden, bieten die Lösung. Gerade wegen ihrer Nützlichkeit sollten biometrische Daten minimal gesammelt und verwendet werden. Wenn dies der einzige gangbare Weg ist, müssen sie sorgfältig behandelt werden.

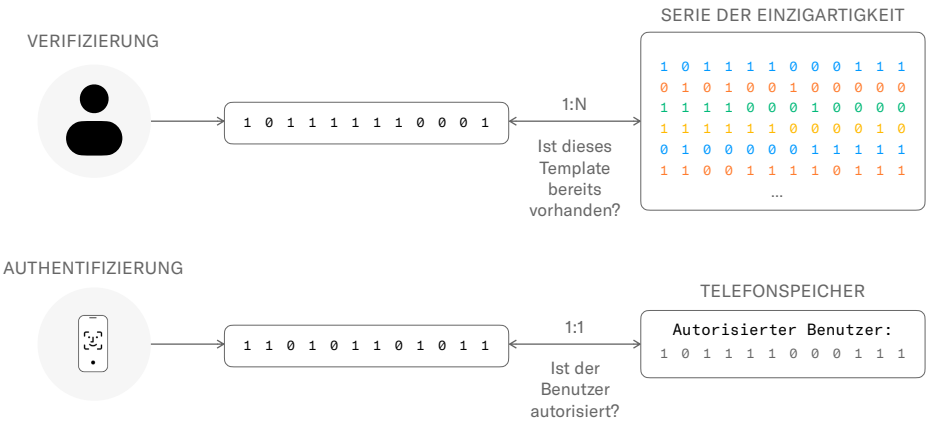
Worldcoin erreicht dies über SMPC.

Wenn eine Person ihre World ID über einen Orb verifiziert, macht der Orb Fotos von der Iris und dem Gesicht der Person. Diese Bilder werden verwendet, um einen Iriscode zu erstellen, der im Wesentlichen eine Reihe von Einsen und Nullen ist. Kein Iriscode gleicht einem anderen, und keiner offenbart direkte Identifikatoren wie Name, Geschlecht, Alter usw.

Dieser Iriscode wird in verschiedene Teile aufgeteilt und dauerhaft mit SMPC verschlüsselt. SMPC macht Daten anonym, indem es sie in mehrere abstrahierte Werte (SMPC-Anteile) aufteilt und diese an verschiedenen Standorten speichert, die von zwei rechtlich getrennten Einheiten verwaltet werden. In naher Zukunft werden zusätzliche Speicherpartner (einschließlich Universitäten und gemeinnütziger Organisationen) hinzugefügt, wodurch die Iriscodes in noch mehr abstrahierte Werte aufgeteilt und von noch mehr unabhängigen Entitäten verwaltet werden. Keine einzelne Partei hat Zugriff auf einen Teil eines Iriscodes. Sie haben nur Zugriff auf den SMPC-Anteil, der unter ihrer Kontrolle und Verwaltung gespeichert ist.

Obwohl die Speicherung der Daten an mehreren Orten scheinbar das Risiko eines Datendiebstahls erhöhen könnte, ist das Gegenteil der Fall. Die SMPC-Anteile werden so gespeichert, dass, falls ein böswilliger Akteur Zugriff auf einen SMPC-Anteil erlangen würde, dieser unentzifferbar wäre; die Daten ergeben nur dann Sinn, wenn alle Teile zusammengefügt werden.

Warum die verschlüsselten SMPC-Teile überhaupt speichern? Damit das Worldcoin-Protokoll weiterhin nachweisen kann, dass eine Person einzigartig ist. Ohne diese Speicherung müssten die Benutzer ihre World ID jedes Mal erneut verifizieren, wenn eine App sie anfordert.



Die Fotos selbst bleiben ebenfalls nicht auf dem Orb. Stattdessen verschlüsselt der Orb die Daten Ende-zu-Ende mit einem öffentlichen Schlüssel, der vom Smartphone des Benutzers bereitgestellt wird (nur der Benutzer hat den privaten Schlüssel zum Entschlüsseln). Anschließend überträgt der Orb die verschlüsselten Bilder an das Gerät des Benutzers, bevor sie vom Orb gelöscht werden. All dies geschieht innerhalb weniger Sekunden während des Verifizierungsprozesses.

Warum die Iris?

Orbs – fortschrittliche Kameras – sind die ersten Hardwaregeräte, die das Worldcoin-Protokoll unterstützen. Derzeit ist der einzige Weg, um eine World ID als zu einem einzigartigen Menschen gehörend zu verifizieren, direkt an einem Orb deine Iris fotografieren zu lassen.

TFH hat viele verschiedene Arten von Biometrie untersucht, um World IDs zu verifizieren, wobei jede ihre eigenen Vor- und Nachteile hat. Um den Kriterien der Zukunftssicherheit zu entsprechen, die erforderlich sind, um im Zeitalter der KI zu gewährleisten, dass Menschen miteinander interagieren, muss jede Methode 1) genau, 2) datenschutzfreundlich, 3) extrem schwer zu fälschen, 4) skalierbar und 5) sehr einfach zu verwenden sein.

Fingerabdrücke sind zwar sehr benutzerfreundlich, aber leicht zu fälschen. Irisbilder hingegen sind genau, benutzerfreundlich, skalierbar, weitgehend inklusiv und extrem schwer zu fälschen. Es gibt keine umfangreiche öffentliche Datenbank von Iriden (wie bei Gesichtern auf Social Media), man kann nicht unbemerkt eine Nahaufnahme der Iris einer Person machen, und es ist spezielle Kameraausrüstung erforderlich, um dies überhaupt zu versuchen.

Das Worldcoin-Protokoll ist offen und dezentral, und zusätzliche Verifikationsmechanismen werden die Attraktivität und Sicherheit des Projekts weiter stärken.

Zero-Knowledge Proofs (ZKPs)

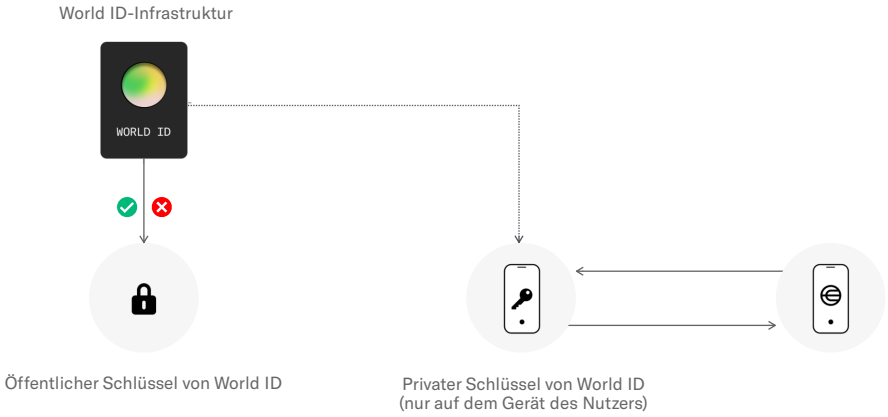
Sobald eine Person eine verifizierte World ID besitzt, kann sie diese verwenden, um sich bei Drittanbieter-Apps anzumelden und Transaktionen durchzuführen, die mit dem World ID-Protokoll integriert sind. Das bedeutet jedoch nicht, dass Menschen ihre World ID mit der Drittanbieter-App teilen.

Die World ID wird verwendet, um eine temporäre Version von sich selbst zu erstellen, ähnlich wie Apples „Meine Email verbergen“ oder virtuelle Kreditkarten. Stell' dir vor, du hättest eine Firmenkreditkarte, die nur für einen Kauf verwendet werden kann. Um bei anderen Anbietern zu bezahlen, müsstest du separate Karten erstellen. Auch wenn dies umständlich klingt, erledigt das Protokoll dies schnell und nahtlos im Hintergrund, wodurch ein sicheres System für Apps entsteht, das die Nutzer schützt.

Die Methode ist ein Zero-Knowledge Proof (ZKP), ein kryptografisches Werkzeug, das es ermöglicht, etwas zu beweisen, ohne Informationen preiszugeben, die zur Schlussfolgerung geführt haben.

Jedes Mal, wenn du eine Drittanbieter-App verwendest, wird die App eine Bestätigung von deinem Gerät anfordern. Stell dir vor, die App in deinem Gerät stellt die Frage: „Kontrolliert dieses Gerät diese World ID?“ Die World App auf dem Gerät des Benutzers sendet dann einen ZKP zurück, der nachweist, dass die World ID verifiziert ist.

ZKPs gehen weit über die regulatorischen Anforderungen irgendeiner Gerichtsbarkeit hinaus. Worldcoin hat sie implementiert, weil sie die beste Möglichkeit sind, sicherzustellen, dass Benutzer anonym bleiben können (es sei denn, der Benutzer gibt direkt zusätzliche Informationen an den Drittanbieterdienst, der die Bestätigung anfordert), und Apps sie nicht verfolgen können. Sie verhindern, dass Drittanbieter – und sogar die Worldcoin Foundation selbst – jemals die World ID eines Benutzers oder die Dienste, mit denen sie interagieren, erfahren.



Eine praktische Analogie für ZKPs

ZKPs sind fortschrittliche Kryptographie, daher sind perfekte Analogien schwierig. Um das Grundprinzip zu verstehen, kannst du dir ein Rätsel vorstellen, bei dem du einen bestimmten Gegenstand oder eine Person in einer Szene finden musst.[2]

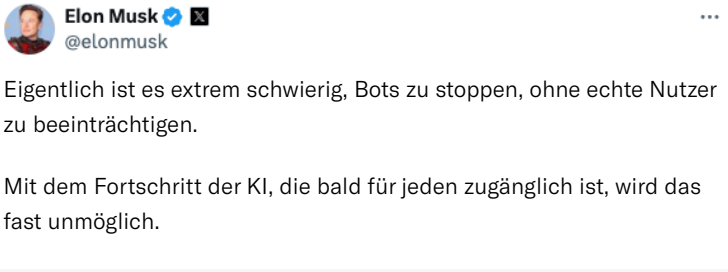
Nach ein paar Minuten Suche sagt eine Person zur anderen, dass sie weiß, wo sich der Gegenstand befindet. Die zweite Person, die es nicht weiß, ist sich unsicher, ob sie das glauben soll.

Daraufhin sagt die erste Person, dass sie es beweisen kann, ohne direkt zu verraten, wo der Gegenstand ist. Sie kopiert das gesamte Rätsel, schneidet den Gegenstand aus und hält ihn der zweiten Person vor. Diese ist jetzt sicher, dass der Gegenstand im Rätsel ist und die erste Person weiß, wo er sich befindet.

In diesem Szenario entspricht die zweite Person jeder App, die bestätigen will, dass ein Benutzer ein Mensch ist; der ausgeschnittene Gegenstand ist der ZKP; und die erste Person ist das Worldcoin Protokoll, das beweist, dass der Benutzer ein Mensch ist, ohne dessen Identität preiszugeben.

Anwendungsfall: X-Bot oder Mensch

Elon Musk kaufte X (damals Twitter) und versprach, die Bots von der Plattform zu vertreiben. Doch der neue Eigentümer erkannte schnell, dass dies leichter gesagt als getan war. „Es ist extrem schwierig, Bots zu stoppen, ohne echte Nutzer zu beeinträchtigen“, schrieb Musk im Dezember 2023. „Da fortgeschrittene KI für jeden verfügbar wird, wird es nahezu unmöglich werden.



Musk hatte recht mit der Herausforderung, die Bots für die Social-Media-Plattform darstellten. Doch mittlerweile gibt es eine praktikable Lösung, um sie zu bekämpfen, ohne die Nutzer zu beeinträchtigen.

[2] Zum Beipiel: Wo ist Waldo?

X bietet drei Anmeldemöglichkeiten: "Mit Google anmelden", "Mit Apple-ID anmelden" oder die Anmeldung per Benutzername/Passwort. Bei der Erstellung eines Kontos müssen die Nutzer ihren Namen, ihre Telefonnummer oder E-Mail-Adresse und ihr Geburtsdatum angeben. Da es relativ einfach ist, mehrere E-Mail-Adressen zu erstellen, ist es auch sehr einfach, mehrere X-Konten zu eröffnen. Dadurch gibt es nur wenige Hürden für Bots, um online zu gehen und das Benutzererlebnis für echte Menschen zu beeinträchtigen.

World ID hingegen stützt sich weder auf E-Mail-Adressen, die einfach einzurichten sind, noch auf Telefonnummern, die leicht zu fälschen sind. Nur echte Menschen können eine verifizierte World ID erhalten – und im Gegensatz zu E-Mails ist sie auf eine pro Person beschränkt. Wenn X World ID als Mechanismus zur Verifizierung der Person nutzen würde, könnte der Dienst ein Abzeichen hinzufügen, das anzeigt, dass solche Konten von echten Menschen verifiziert wurden. Bots, die sich einloggen, könnten sich nicht verifizieren lassen.

Wichtig ist, dass dies die Anonymität der X-Nutzer sogar noch verbessern würde, da sie keine weiteren Informationen angeben müssten, außer denen, die sie bereits X zur Verfügung gestellt haben.

Dies ist nicht rein theoretisch. TFH hat eine World ID-Integration für Telegram entwickelt, um Spam-Bots im Netzwerk zu beseitigen. Administratoren öffentlicher Chats können festlegen, dass individuelle Konten sich zunächst mit World ID verifizieren müssen, bevor sie in einer Gruppe posten dürfen.

Prinzip 3

Freie Wahl und Kontrolle: Deine Daten, deine Regeln

Die Menschen haben sich zunehmend an ein Big-Tech-Paradigma gewöhnt, bei dem sie im Austausch für den Zugang zu Dienstleistungen ihre persönlichen Daten an Unternehmen weitergeben, damit diese an den Höchstbietenden verkauft werden können.[3]

Worldcoin agiert außerhalb dieses Paradigmas. Das ist nicht nur ein Versprechen. Worldcoin wird bewusst so gestaltet, dass es unmöglich ist, persönliche Daten auf diese Weise zu nutzen.

Der Worldcoin-Ansatz: **deine Daten, deine Regeln.**

Minimale Datenmenge

Der Ausgangspunkt, um die Kontrolle der Daten beim Menschen zu lassen, besteht darin, gar nicht erst viele Daten abzufragen. Da verifizierte World IDs anonym sind, müssen Menschen weder ihren Namen, Telefonnummern, Adresse noch andere Informationen angeben, die normalerweise von Technologieunternehmen erfasst werden. Um einen Bibliotheksausweis zu bekommen, muss man einen Wohnsitznachweis mit einer Adresse vorlegen. Um eine verifizierte World ID, einen globalen digitalen Ausweis, zu erhalten, benötigt man lediglich ein Smartphone und muss einen Orb aufsuchen.

Anwendungsfall
Shopify-Rabattcodes

Shopify ist eine E-Commerce-Plattform für Unternehmen, die ihren Umsatz steigern und Online-Zahlungen verwalten möchten. Händler auf der Plattform versuchen manchmal, neue Kunden durch einmalige Rabattaktionen zu aquirieren.

Das Problem ist allerdings, dass das System von Menschen manipuliert werden kann, indem sie falsche E-Mails erstellen und Rabatte mehrfach einfordern – oder Bots einsetzen, die dies für sie erledigen. Anstatt neue Kunden zu gewinnen, subventionieren die Händler so einen Betrug.

Durch die Integration von World ID in ihren Shop können Händler echten Kunden ermöglichen, einen QR-Code zu scannen, der ihre World ID verifiziert und einen Rabattcode anwendet. Diese Methode stellt sicher, dass pro Mensch nur ein Rabatt gewährt wird, wodurch das Problem der Händler gelöst wird, ohne dass der Benutzer zusätzliche Informationen angeben muss. (Allerdings müssen sie beim Bezahlen ihre Kreditkarten- und Versanddetails angeben!)

[3] Für mehr Infomationen dazu, klicke hier: https://en.wikipedia.org/wiki/Real-time_bidding

Personal Custody

Der Prozess zur Verifizierung einer World ID erfordert die Verwendung einiger Daten, nämlich biometrischer Bilder und Iriscodes. Die Iriscodes werden nach der Verarbeitung durch SMPC auf Servern gespeichert, wo sie in vollständig anonymisierter Form verbleiben. Die vom Benutzer bereitgestellten Daten zur Verifizierung der Identität über die Orb werden jedoch nicht gespeichert oder an Dritte weitergegeben. Stattdessen bleiben sie nur auf dem Smartphone der Person, wo sie mit dem öffentlichen Schlüssel des Benutzers verschlüsselt werden.

Mit Worldcoin Personal Custody haben die Menschen die Kontrolle über die während der Verifizierung gesammelten und generierten Daten – einschließlich der World ID und der Bilder – und entscheiden selbst, mit wem sie diese teilen möchten.

Face Auth

Durch die Einführung von World ID können Plattformen sich gegen Bots schützen, ohne die Datensicherheit ihrer Kunden zu verletzen. Eine verifizierte World ID gibt diesen Plattformen ein hohes Maß an Sicherheit, dass ein Nutzer tatsächlich eine echte Person ist.

In einigen risikoreichen Szenarien (z. B. bei Finanztransaktionen) müssen Plattformen oder Personen nicht nur wissen, dass sie es mit einem Menschen zu tun haben, sondern auch mit einer bestimmten Person. Sie möchten sicherstellen, dass die Person, die die World ID verwendet, derselbe einzigartige Mensch ist, der die World ID auf diesem Gerät verifiziert hat.

Dafür können Apps auf Worldcoin Face Auth verwenden.

Face Auth ist eine Methode, bei der das während der Verifizierung aufgenommene Bild mit einem Bild der Person verglichen wird, die die World ID nutzen möchte. Diese Methode ist geräteunabhängig.

Das erste Bild wird erstellt, wenn eine Person ihre World ID an einem Orb verifiziert. Das Mobiltelefon des Nutzers ist standardmäßig der einzige Ort, an dem diese Daten gespeichert werden. Diese hochauflösenden Fotos werden verschlüsselt und im Rahmen der Personal Custody sicher auf das Geräat des Nutzers übertragen und vollständig vom Orb gelöscht.

Das zweite Bild ist ein Selfie, das auf dem Gerät des Nutzers innerhalb der World App aufgenommen wird, wenn der Nutzer seine World ID nutzen oder darauf zugreifen möchte. Face Auth für die World ID vergleicht das vom Gerät des Nutzers aufgenommene Bild mit dem ursprünglichen Authentifizierungsbild, das während der Verifizierung am Orb erstellt wurde. Der Nutzer kann nur dann mit dem Login oder der Transaktion fortfahren, wenn die beiden Bilder übereinstimmen.

Dies verhindert Betrug, indem auch bei Diebstahl oder Verkauf des Telefons die World ID nicht verwendet werden kann. Mit Face Auth behält der rechtmäßige Nutzer stets die Kontrolle über seine Daten und seine World ID. **Der Vergleich erfolgt lokal auf dem Gerät des Nutzers.** Dadurch wird weder das Selfie noch das Bild vom Orb oder andere persönliche Daten mit Dritten, einschließlich Tools for Humanity oder der Worldcoin Foundation, geteilt.[4]

[4] In Zukunft wird das Projekt es ermöglichen, dass Menschen freiwillig zustimmen können, ihre Informationen mit Worldcoin zu teilen, um die Sicherheit und das Training von KI zu unterstützen. Dies ist zu 100 % optional, und die Erlaubnis kann jederzeit widerrufen werden.

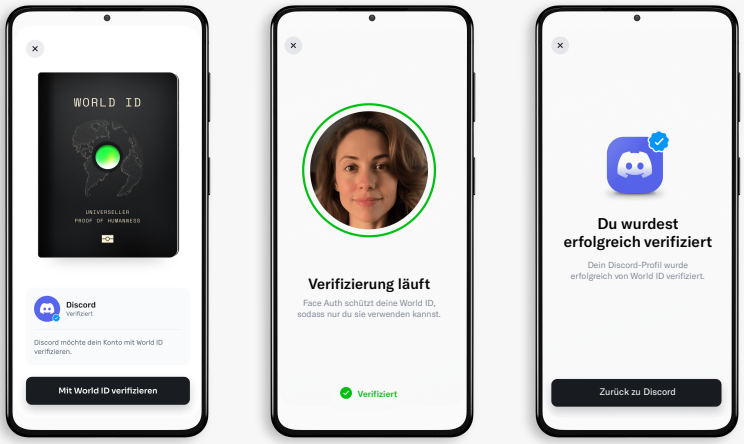
Face Auth und Face ID

Für die Nutzer ist Face Auth der Apple Face ID ähnlich.

Also warum nicht einfach Gesichtserkennung durch Face ID nutzen?

Face Auth stellt sicher, dass die Person, die die World App nutzt, dieselbe Person ist, die die zugehörige World ID an einem Orb erstellt hat. Face ID bietet diese Möglichkeit nicht.

Face ID ist eine Kombination aus Hardware und Software und daher letztlich an ein iPhone gebunden. Mit Face ID könnte ein anderes Gesicht mit dem Gerät verknüpft sein als das, welches zur Verifizierung der World ID verwendet wurde, was das Potenzial für Betrug erhöht. Durch die Verwendung von World ID, die auf App-Ebene statt auf Geräteebene funktioniert, stellt Face Auth sicher, dass niemand außer der Person, die die World ID verifiziert hat, darauf zugreifen kann.



Prinzip 4

Transparenz: Offen entwickelt

Sicherheitsexperten sind von Natur aus skeptisch und suchen hinter jeder Codezeile nach Gefahren. Und das ist auch gut so, denn so sorgen sie für unsere Sicherheit.

Für uns ist es unvorstellbar, dass TFH oder ein paar Worldcoin-Entwickler jeden möglichen Fehler im Protokoll vorhersehen könnten. Deshalb wird Worldcoin **offen entwickelt**.

Geprüft

Worldcoin bezieht so viele externe Meinungen und Fachgebiete wie möglich ein. Kryptografen und Biometrie-Experten evaluieren ständig den Quellcode, während Sicherheitsexperten und Berater versuchen, die kleinste mögliche Schwachstelle zu finden. Worldcoin veröffentlicht die Ergebnisse – und zeigt auf, was unternommen wurde, um selbst kleinste Probleme zu beheben.

Um potenzielle Sicherheitslücken zu identifizieren, müssen wir auch verstehen, wie das Protokoll in der realen Welt – sowohl jetzt als auch in der Zukunft – genutzt werden könnte. Das bedeutet, Tausende von kulturellen Realitäten auf der ganzen Welt zu durchdenken und diese Überlegungen in ein Sicherheitsmodell zu integrieren, das gegen Missbräuche schützt, die möglicherweise noch gar nicht existieren.

Ab April 2023 führten die Prüfungsunternehmen Nethermind und Least Authority zwei separate Sicherheitsprüfungen des Worldcoin-Protokolls durch. Die Audits deckten insbesondere die folgenden Bereiche ab:

- Korrektheit der Implementierung, einschließlich kryptografischer Konstruktionen und Primitiven sowie die angemessene Verwendung von Smart-Contract-Konstruktionen.
- Häufige und spezifische Implementierungsfehler.
- Schädliche Aktionen und andere Angriffe auf den Code.
- Sichere Schlüsselaufbewahrung und ordnungsgemäße Verwaltung von Verschlüsselungs- und Signaturschlüsseln.
- Aufdeckung kritischer Informationen während der Nutzerinteraktionen.
- Widerstandsfähigkeit gegen DDoS-Angriffe (Distributed Denial of Service) und ähnliche Angriffe.
- Schwachstellen im Code, die schädliche Aktionen und andere Angriffe ermöglichen.
- Schutz vor böswilligen Angriffen und anderen Ausnutzungsmethoden.
- Leistungsprobleme oder andere potenzielle Auswirkungen auf die Performance.
- Datenschutz, Datenlecks und Integrität der Informationen.
- Unzureichende Berechtigungen, Privilegieneskalation und übermäßige Autorität.

Open-Source und frei zugänglich

Die Veröffentlichung des Worldcoin-Codes als Open-Source und frei zugänglich verfolgt drei Ziele. Erstens kann das Netzwerk so kritisch geprüft werden. Diese Prüfung kann zur Verbesserung des Netzwerks beitragen.

Zweitens gibt es Entwicklern das Vertrauen, auf dem Worldcoin-Protokoll aufzubauen. Es ist möglich, dass andere Teams eine Proof-of-Humanness-Anwendung auf Basis von World ID entwickeln oder eine noch benutzerfreundlichere Verifizierungsmethode als den Orb finden.

Open-Source und freie Zugänglichkeit ist für ein dezentrales Projekt zudem unerlässlich: Jeder kann jederzeit aus beliebigen Gründen seine eigene Version (oder „Fork“) des Protokolls erstellen – und das ist positiv.


WORLDCOIN