WORLDCOIN

Prywatny z założenia

Spis treści

Ekosystem

Projekt Worldcoin składa się z wielu podmiotów i narzędzi, które łączą się, tworząc sieć tożsamości skoncentrowaną na człowieku, umożliwiającą zaufanie podczas transakcji lub komunikacji online.

Worldcoin to projekt obejmujący World ID- anonimowy paszport cyfrowy, oraz sieć umożliwiającą korzystanie z zasobów cyfrowych, zapewniającą miliardom ludzi dostęp do globalnej gospodarki cyfrowej.

World ID to zdecentralizowany protokół tożsamości, potwierdzający, że jesteś unikalną osobą. Możesz użyć World ID, aby dowieść, że jesteś człowiekiem w dowolnej aktywności online, takiej jak weryfikacja filmów czy ochrona przed deepfake'ami. Możesz go również używać do logowania się na stronach internetowych i w aplikacjach, podobnie jak funkcję Zaloguj się przez Google, potwierdzając, że jesteś unikalną osobą bez konieczności udostępniania danych osobowych, takich jak imię i nazwisko, adres e-mail czy numer telefonu.

World Chain to pakiet warstwy 2 w sieci Ethereum, którego uruchomienie planowane jest wkrótce, a który wykorzystuje World ID do priorytetyzowania transakcji ludzkocentrycznych przed botami.

WLD to token Worldcoin, który jest przyznawany osobom za bycie człowiekiem i jest częścią sieci Worldcoin.[1]

Fundacja Worldcoin to organizacja non-profit, która pełni funkcję zarządcy protokołu Worldcoin. Jest również właścicielem i zarządcą większości aktywów związanych z marką Worldcoin, w tym własności intelektualnej Orba i technologii open source protokołu.

Tools for Humanity (TFH) to firma technologiczna, która tworzy narzędzia dla Worldcoin, w tym Orba i aplikację World App.

Orb to specjalna kamera, która weryfikuje unikalną tożsamość osób i dostarcza danych potwierdzających Twoją tożsamość za pomocą World ID.

Aplikacja **World App** to portfel Worldcoin z własnym depozytem, w którym przechowywane jest Twoje World ID. Za pomocą aplikacji możesz również wysyłać i odbierać tokeny Worldcoin (WLD) i inne fundusze cyfrowe.

Po więcej informacji: Czym jest Worldcoin i jak działa?

[1] W odpowiednich jurysdykcjach

Ochrona prywatności w dobie sztucznej inteligencji

Raport z 2022 r. sporządzony przez unijną agencję egzekwowania prawa Europol sugeruje, że do 2026 r. aż 90% treści w internecie może być generowane syntetycznie.

Catfishing. Scamboty. Deepfake'i. Kradzież tożsamości. Dezinformacja. Internet może być niebezpiecznym miejscem. Rozwój sztucznej inteligencji sprawi, że internet będzie bardziej użyteczny niż kiedykolwiek, ale musimy mieć również świadomość jego potencjału do pogłębiania istniejących problemów. Widzieliśmy, co może pójść nie tak, gdy człowiek udaje kogoś innego. Co się dzieje, gdy myślimy, że mamy do czynienia z człowiekiem, podczas gdy w rzeczywistości jest on agentem sztucznej inteligencji?

Potrzebujemy sposobu na sprawdzenie, czy osoby, z którymi rozmawiamy, którym wysyłamy pieniądze i których treści oglądamy online (by wymienić tylko kilka przykładów), są rzeczywiście ludźmi. Worldcoin ma na celu zapewnienie Ci kontroli nad każdym z tych elementów w dobie sztucznej inteligencji.

Zapobieganie zalaniu internetu przez sztuczną inteligencję nieistniejącymi ludźmi wymaga nadzwyczajnych zabezpieczeń. Jednak wiele z przewidzianych podejść do radzenia sobie z tym problemem jest nieskuteczne. Istnieje pokusa sięgnięcia po te same stare narzędzia — usuwanie prywatności i poleganie na technikach identyfikacji lub weryfikacji, które można przejąć do nadzoru korporacyjnego i rządowego. Panoptykon może i zadziałać, ale jakim kosztem?

Wierzymy, że istnieje lepszy sposób: projekt Worldcoin polega na tworzeniu bezpiecznych technologii, które stawiają w centrum ludzi, pozwalając im lepiej kontrolować i ufać swoim doświadczeniom w internecie bez poświęcania swojej prywatności.

Worldcoin **prywatny z założenia**.

W jaki sposób sztuczna inteligencja stwarza zagrożenie dla prywatności

Widzieliśmy już krążące deepfake'i polityków i celebrytów — ludzi, dla których istnieje bogate źródło treści online.

Jednak zaawansowana sztuczna inteligencja oznacza, że deepfake'i — niezwykle realistyczne wideo i audio — mogą wkrótce zostać wykorzystane do imitowania zwykłych ludzi. Jesteśmy szczególnie zaniepokojeni tym, że internet i jego użytkownicy nie są przygotowani na wyzwania, jakie postawi przed nimi rozwój sztucznej inteligencji. Wyobraź sobie rozmowę na Zoomie ze współpracownikami, którzy tak naprawdę nimi nie są, lub bliskimi, którzy wcale nie są ludźmi. Ludzi można łatwo oszukać, aby wysłali pieniądze, ujawnili sekrety lub zrobili rzeczy, których jeszcze sobie nawet nie wyobrażamy.

Aby zwalczać szkodliwe zastosowanie sztucznej inteligencji, platformy muszą być w stanie rozpoznać, czy ktoś jest unikalnym człowiekiem. Narzędzia takie jak „CAPTCHA” nie są już skuteczne i opierają się na danych powiązanych ze śladem cyfrowym danej osoby. World ID to chroniąca prywatność alternatywa dla interakcji cyfrowych, takich jak CAPTCHA. Służy również jako alternatywa dla systemów PSK (Poznaj Swojego Klienta) oraz identyfikatorów cyfrowych, które albo ujawniają tożsamość osoby, albo łączą ją z jej działalnością cyfrową.

Zasady ochrony prywatności Worldcoin

Społeczność Worldcoin buduje coś bezprecedensowego: cieszącą się globalnym zaufaniem, maksymalnie inkluzywną, chroniącą prywatność sieć do udowadniania bycia człowiekiem. Jednak podejście projektu do ochrony prywatności jest sprzeczne z intuicją i nowatorskie, prezentując fundamentalnie nową drogę, której nie obrała dotychczas żadna firma, organizacja ani instytucja rządowa:

Worldcoin nie chce wiedzieć, kim jesteś. Chce wiedzieć jedynie to, że jesteś unikalnym człowiekiem.

Boty oparte na sztucznej inteligencji stają się coraz bardziej powszechne i wyrafinowane, podważają zaufanie w sieci i podszywają się pod ludzi. Dlatego coraz ważniejsze jest , aby wiedzieć, czy wchodzisz w interakcję z człowiekiem, czy botem. Gdyby udowodnienie bycia człowiekiem w internecie było naszym jedynym zmartwieniem, rozwiązanie mogłoby wydawać się dość proste: używanie wydanych przez organ rządowy dowodów osobistych, żeby zweryfikować naszą tożsamość i poruszać się po Internecie. W końcu często jesteśmy proszeni o okazanie dowodu osobistego w banku. Czy transakcje internetowe w dobie sztucznej inteligencji nie są potencjalnie równie wrażliwe?

Pomijając fakt, że około 850 milionów ludzi nie posiada żadnej formy oficjalnego dowodu tożsamości, a same rządy wdrożyły wyrafinowane internetowe kampanie dezinformacyjne, weryfikacja w internecie za pomocą wydanych przez organy rządowe dowodów osobistych nie jest rozwiązaniem. Ujawnia ona o wiele więcej informacji o Tobie, niż jest to konieczne, na przykład Twój adres, i naraża Cię na ryzyko kradzieży Twojej tożsamości lub wykorzystania jej do niegodziwych celów, również takich, których nie możemy sobie jeszcze wyobrazić ze względu na sztuczną inteligencję.

Potrzebujemy dowodu bycia człowiekiem i ochrony prywatności w jednym (z możliwie jak najmniejszą liczbą barier wejścia).

Jest to wyzwanie, które Worldcoin stara się rozwiązać, i robi to przede wszystkim za pomocą World ID. World ID to globalny cyfrowy paszport, umiejscowiony lokalnie w smartfonie swojego posiadacza i pozwalający na udowodnienie bycia unikalnym człowiekiem bez udostępniania komukolwiek danych osobowych.

To system weryfikacji ludzkiej tożsamości w internecie, który pozwala ludziom zachować anonimowość, gdziekolwiek się znajdują. Zweryfikowane World ID nie zbiera ani nie łączy się z takimi identyfikatorami, jak imię i nazwisko lub adres e-mail, nie łączy się z danymi transakcji portfela, ani nie ujawnia, czyje World ID jest używane. Z założenia Worldcoin opiera się na praktyce minimalizacji danych. Nie przechowuje informacji identyfikacyjnych.

"Do tej pory każdy, kto chciał udowodnić w sieci, że jest człowiekiem, korzystał z takich środków jak urzędowe dokumenty tożsamości, które są obciążone wadą identyfikacji użytkownika i ujawnienia dużej ilości innych danych osobowych bez konieczności. W przeciwieństwie do nich, World ID pozwala na anonimowy „dowód bycia unikalnym człowiekiem" i w ten sposób przeciwstawia modelowi „kapitalizmu inwigilacyjnego" model promujący ochronę danych. World ID wzmacnia tym samym możliwość działań w internecie zgodnych z ochroną danych".

Dr. Stefan Brink, były niemiecki komisarz ds. ochrony danych i wolności informacji w Badenii-Wirtembergii od stycznia 2017 r. do grudnia 2022 r.

Ponadto World ID jest zbudowane w taki sposób, aby ludzie mogli go używać w różnych aplikacjach, bez śledzenia przez te aplikacje ich aktywności. Nie ma centralnego repozytorium historii użytkowania. Możesz używać World ID w setkach różnych aplikacji tak, aby żadna z nich nigdy nie wiedziała o innych, i aby nie wiedział o nich World ID.

Worldcoin jest prywatny z założenia, z czterema powiązanymi zasadami ochrony prywatności:

Zasada nr 1

Bezpieczeństwo: Zabezpieczony przez matematykę

Zasada nr 2

Anonimowość: Poruszaj się swobodnie w sieci

Zasada nr 3

Wybór i Kontrola: Twoje dane, Twoje zasady

Zasada nr 4

Transparentność: Tworzony w sposób otwarty

Zasada nr 1

Bezpieczeństwo:
Zabezpieczony przez matematykę

Bez bezpieczeństwa nie ma ochrony prywatności.

W Worldcoin chodzi o umożliwienie ludziom korzystania z Internetu bez ujawniania ich tożsamości oraz rozróżnienia interakcji opartych na botach od tych z ludźmi. Zabezpieczenia pomagają zapewnić osiągnięcie tego poziomu prywatności — za każdym razem, niezawodnie.

World ID wykorzystuje wiele technik bezpieczeństwa, aby zapewnić posiadaczom World ID bezpieczeństwo danych.

Jeden zestaw obejmuje narzędzia ludzkie, takie jak open-source i audyty (patrz: Transparentność), które pomagają weryfikować i testować środki bezpieczeństwa, które zostały utworzone i wdrożone w ramach projektu Worldcoin.

Drugi zestaw obejmuje narzędzia kryptograficzne, takie jak Dowód Zerowej Wiedzy oraz Bezpieczne Obliczenia Wielostronne (patrz: Anonimowość), które wykorzystują zaawansowaną matematykę do zabezpieczania danych, szyfrowania ich i trzymania ich w tajemnicy lub anonimowego udostępniania.

Bezpieczne Obliczenia Wielostronne to jeden z niewielu wyników kryptografii, który może zapewnić doskonałe utajnienie. Z kolei Dowody Zerowej Wiedzy używają tzw. nullifier hashes lub unikalnych wartości dla każdej aplikacji, dzięki czemu nie można śledzić historii aktywności użytkowników.

Nazwijmy to **zabezpieczeniem przez matematykę**.

Zasada nr 2

?

Anonimowość:
Poruszaj się swobodnie w sieci

Przez większość czasu nie potrzebujemy identyfikacji, aby po prostu być. Gotowanie obiadu, czytanie książki, spanie-wykonywanie tych czynności rzadko wymaga od nas udowodnienia, kim jesteśmy. Przez większość naszego życia nasze działania pozostają niezauważone, niezaobserwowane i niezarejestrowane. Jesteśmy anonimowi.

Anonimowość jest trudniejsza do osiągnięcia w internecie. Strony internetowe widzą naszą aktywność, a przeglądarki mogą śledzić nasze ruchy i zachowania w sieci. Ta inwigilacja staje się potencjalnie bardziej szkodliwa, gdy jesteśmy proszeni o udowodnienie, kim jesteśmy, począwszy od monitorowania naszego adresu IP, aż po przedstawianie urzędowego dowodu tożsamości w skrajnych przypadkach.

Ale korzystanie ze stron internetowych i aplikacji nie powinno wiązać się z udostępnianiem naszych danych w większym stopniu niż gotowanie obiadu. Ludzie powinni móc **swobodnie poruszać się w internecie**. Logowanie się na stronach internetowych za pomocą World ID na to pozwala.

Ale korzystanie ze stron internetowych i aplikacji nie powinno wiązać się z udostępnianiem naszych danych w większym stopniu niż gotowanie obiadu. Ludzie powinni móc swobodnie poruszać się w internecie.

Aby zachować anonimowość w świecie online, Worldcoin wykorzystuje wiele technologii chroniących prywatność, w tym Bezpieczne Obliczenia Wielostronne (SMPC) i Dowody Zerowej Wiedzy (ZKP).

Bezpieczne Obliczenia Wielostronne (SMPC)

Do utworzenia World ID wystarczy smartfon, ale udowodnienie, że posiadacz jest unikalną osobą, która nie utworzyła wielu World ID, przy jednoczesnym zachowaniu prywatności jego danych, jest skomplikowanym wyzwaniem.

Rozwiązaniem są odpowiednio zanonimizowane dane biometryczne. Użyteczność danych biometrycznych oznacza, że powinny być one gromadzone i wykorzystywane w minimalnym stopniu, a kiedy nie można tego uniknąć, należy obchodzić się z nimi ostrożnie.

Worldcoin robi to za pośrednictwem SMPC.

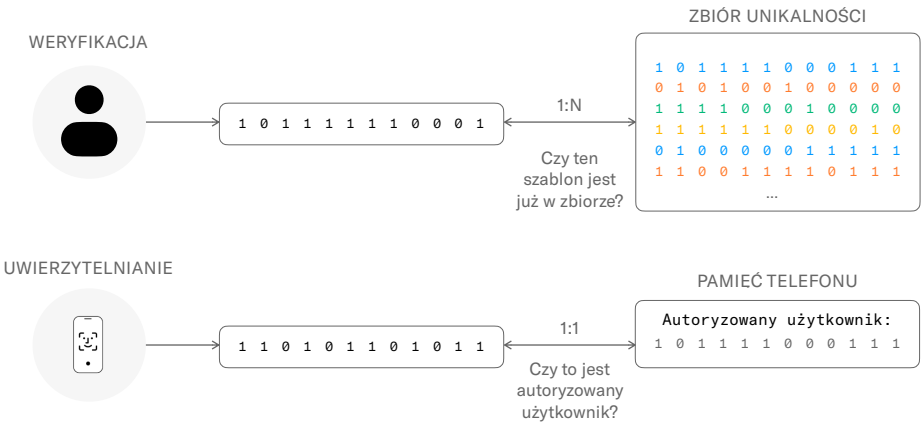
Gdy osoba weryfikuje swoje World ID za pomocą Orba, Orb robi zdjęcia tęczówki jej oka oraz twarzy. Wykorzystuje te zdjęcia do utworzenia kodu tęczówki oka, który jest zasadniczo serią jedynek i zer. Nie ma dwóch takich samych kodów tęczówki. Kody tęczówki nie ujawniają bezpośrednich identyfikatorów, takich jak imię i nazwisko, płeć, wiek itp.

Kod tęczówki jest dzielony na różne części i trwale szyfrowany za pomocą SMPC, co sprawia, że dane stają się anonimowe poprzez podzielenie ich na wiele abstrakcyjnych wartości (udziały SMPC) i przechowywanie ich w oddzielnych lokalizacjach zarządzanych przez dwa prawnie odrębne podmioty. W niedalekiej przyszłości zostaną dodani dodatkowi partnerzy ds. przechowywania (w tym uniwersytety i organizacje non-profit), co oznacza, że kody tęczówki zostaną podzielone na jeszcze bardziej abstrakcyjne wartości, przechowywane i zarządzane przez jeszcze bardziej niezależne podmioty. Żadna pojedyńcza strona nie ma dostępu do części kodu tęczówki. Mają dostęp tylko do udziału SMPC przechowywanego pod ich kontrolą i zarządzaniem.

Podczas gdy przechowywanie danych w wielu lokalizacjach pozornie zwiększa prawdopodobieństwo kradzieży danych, w rzeczywistości jest odwrotnie. Części SMPC są

przechowywane w taki sposób, że gdyby złośliwy podmiot w jakiś sposób uzyskał dostęp do jednej części SMPC, byłaby ona nieczytelna; mają one sens tylko wtedy, gdy wszystkie elementy zostaną ułożone w całość.

Po co w ogóle przechowywać zaszyfrowane części SMPC? Po to, żeby protokół Worldcoin mógł stale udowadniać, że dana osoba jest unikalna. Bez tego użytkownicy musieliby ponownie weryfikować swoje World ID za każdym razem, gdy zażąda tego aplikacja.



Same zdjęcia również nie zostają w Orbie. Zamiast tego Orb szyfruje dane od początku do końca za pomocą klucza publicznego dostarczonego przez smartfon użytkownika (nikt poza użytkownikiem nie ma prywatnego klucza do jego odszyfrowania), a następnie Orb przesyła zaszyfrowane zdjęcia na urządzenie użytkownika, zanim zostaną usunięte z Orba. Wszystko to dzieje się w ciągu kilku sekund podczas procesu weryfikacji.

Dlaczego tęczówki?

Orby — zaawansowane kamery — to pierwsze urządzenia sprzętowe obsługujące protokół Worldcoin. Na razie jedyną metodą zweryfikowania World ID jako należącego do unikalnego człowieka jest odwiedzenie Orba i zrobienie zdjęcia swoich oczu.

TFH badało wiele różnych typów biometrii do weryfikacji World ID, z których każda ma swoje wady i zalety. Aby spełnić przyszłe kryteria niezbędne do zapewnienia potwierdzenia bycia człowiekiem wszystkim jednostkom na Ziemi w świecie sztucznej inteligencji, każda metoda musi być 1) dokładna, 2) chroniąca prywatność, 3) maksymalnie trudna do podrobienia, 4) skalowalna i 5) bardzo łatwa w użyciu.

Odciski palców są bardzo użyteczne, ale łatwe do podrobienia. Tęczówki natomiast są dokładne, użyteczne, skalowalne, szeroko inkluzywne i maksymalnie trudne do podrobienia. Do tego chronią prywatność. Nie ma dużego publicznego rejestru tęczówek (jak rejestr twarzy w mediach społecznościowych), nie można sfotografować z bliska czyjejś tęczówki bez bycia przez nią zauważonym , a żeby choć spróbować to zrobić, wymagany jest specjalistyczny sprzęt fotograficzny.

Protokół Worldcoin jest otwarty i zdecentralizowany, a dodatkowe mechanizmy weryfikacji jedynie zwiększą atrakcyjność i bezpieczeństwo projektu.

Dowody Zerowej Wiedzy (ZKP)

Gdy dana osoba posiada zweryfikowane World ID, może używać go do logowania się i dokonywania transakcji za pomocą aplikacji innych firm, które integrują się z protokołem World ID.

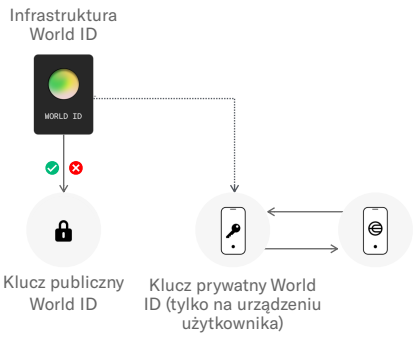
Nie oznacza to jednak, że ludzie udostępniają swoje World ID aplikacji innej firmy.

Zamiast tego World ID jest używane do tworzenia jednorazowej wersji samego siebie, podobnie jak funkcja Ukryj mój adres e-mail firmy Apple lub wirtualne karty kredytowe. Wyobraź sobie posiadanie firmowej karty kredytowej, której można użyć tylko do jednego zakupu. Aby zapłacić za rzeczy u innych sprzedawców, trzeba by wygenerować osobne karty. Choć może to brzmieć uciążliwie, protokół robi to w tle szybko i bezproblemowo, czego skutkiem jest system, który jest bezpieczny dla aplikacji i chroni użytkowników.

Metoda robienia tego w taki sposób, żeby ani Worldcoin, ani aplikacje nie mogły śledzić historii użytkowania, aplikacji ani stron zaangażowanych w daną transakcję to Dowody Zerowej Wiedzy (ZKP) - narzędzie kryptograficzne, które pozwala komuś udowodnić, że coś jest prawdą, bez ujawniania jakichkolwiek informacji, które doprowadziły do tego wniosku.

Za każdym razem, gdy korzystasz z aplikacji innej firmy, aplikacja poprosi o dowód z Twojego urządzenia. Można to porównać do zadawania urządzeniu pytania. Aplikacja chce wiedzieć: czy to urządzenie kontroluje to World ID? Aplikacja World na urządzeniu użytkownika odsyła ZKP, który potwierdza, że World ID jest zweryfikowane.

Dowody Zerowej Wiedzy wykraczają daleko poza wymogi regulacyjne jakiejkolwiek jurysdykcji. Worldcoin wdrożył je, ponieważ są najlepszym sposobem zapewnienia, że użytkownicy mogą pozostać anonimowi (chyba, że użytkownik poda dodatkowe informacje bezpośrednio do usługi zewnętrznej, która zażąda dowodu), a aplikacje nie mogą ich śledzić. Zapobiegają one poznaniu przez strony trzecie, i samą Fundację Worldcoin, World ID użytkownika lub tego, z jakimi usługami wchodzi on w interakcję.



Praktyczna analogia dla Dowodów Zerowej Wiedzy

ZKP to zaawansowana kryptografia, dlatego trudno o idealną analogię. Ale żeby zrozumieć podstawową ideę, wyobraź sobie łamigłówkę, w której musisz znaleźć na obrazku konkretny przedmiot lub osobę.[2]

Po kilku minutach poszukiwań jedna osoba mówi do drugiej, że wie, gdzie jest szukany przedmiot. Druga osoba, która nie wie, gdzie jest przedmiot, nie jest pewna, czy ma w to wierzyć.

Wtedy pierwsza osoba mówi, że może to udowodnić — tylko bez ujawniania, gdzie jest przedmiot.

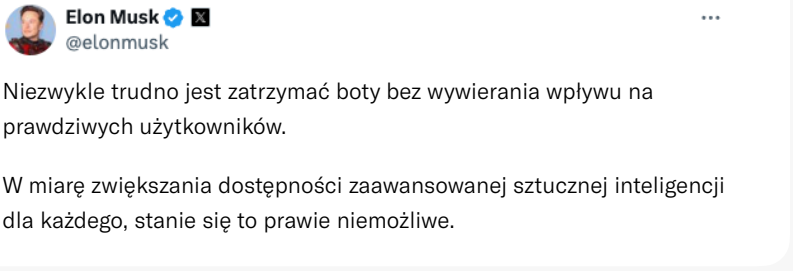
Kseruje całą łamigłówkę, wycina przedmiot i pokazuje go drugiej osobie, która teraz ma pewność, że przedmiot znajduje się w łamigłówce i że pierwsza osoba wie, gdzie on jest.

[2] Np. „Gdzie jest Waldo/Wally?"

W tym scenariuszu drugą osobą jest dowolna aplikacja próbująca potwierdzić, że użytkownik jest człowiekiem; wycięty przedmiot to ZKP; a pierwszą osobą jest protokół Worldcoin przedstawiający dowód, że użytkownik jest człowiekiem bez ujawniania jego tożsamości.

Przypadek użycia:
X-bot czy człowiek?

Elon Musk kupił X (wtedy nazywany Twitterem), obiecując wyparcie botów z platformy. Nowy właściciel szybko jednak przekonał się, że łatwiej powiedzieć, niż zrobić. „Niezwykle trudno jest zatrzymać boty bez wywierania wpływu na prawdziwych użytkowników" – napisał Musk w grudniu 2023 r. „W miarę zwiększania dostępności zaawansowanej sztucznej inteligencji dla każdego, stanie się to prawie niemożliwe".



Musk miał rację co do wyzwania, przed jakim stanęła platforma społecznościowa przez boty. Teraz jednak istnieje skuteczne rozwiązanie, które pozwala walczyć z nimi bez oddziaływania na użytkowników.

X umożliwia trzy tryby logowania: Logowanie przez Google, logowanie przez Apple lub przez podanie nazwy użytkownika/hasło. Aby utworzyć konto, użytkownicy są proszeni o podanie swojego imienia, numeru telefonu lub adresu e-mail oraz daty urodzenia. Ponieważ stosunkowo łatwo jest utworzyć wiele adresów e-mail, utworzenie wielu kont X jest również stosunkowo proste. Dlatego boty nie mają większych przeszkód w wejściu do sieci, gdzie mogą obniżyć komfort użytkowania dla ludzi.

Z kolei World ID nie opiera się na adresach e-mail, które są łatwe do utworzenia, ani na numerach telefonu, które można łatwo sfałszować. Tylko ludzie mogą uzyskać zweryfikowane World ID — i, w przeciwieństwie do adresów mailowych, są one ograniczone do jednego. Gdyby zatem X miał używać World ID jako mechanizmu weryfikacji tożsamości, usługa mogłaby dodać plakietkę oznaczającą, że takie konta zostały zweryfikowane jako ludzie. Żaden próbujący się zalogować bot nie byłby w stanie się zweryfikować.

Co ważne, takie działanie dodatkowo zwiększyłoby anonimowość użytkowników X, którzy nie musieliby podawać żadnych dodatkowych informacji poza tymi, które już przekazali platformie X.

To nie jest tylko teoria. TFH opracowało integrację z World ID dla Telegrama, aby pozbyć się botów spamujących w sieci. Administratorzy czatu publicznego mogą wymagać weryfikacji poszczególnych kont za pomocą World ID przed opublikowaniem postu w grupie.

Zasada nr 3

Wybór i Kontrola:
Twoje dane, Twoje zasady

Ludzie są coraz bardziej przyzwyczajeni do modelu Big Tech, w którym w zamian za dostęp do usług oddają swoje dane osobowe korporacjom, aby mogły zostać sprzedane temu, kto zaoferuje za nie najwyższą cenę.[3]

Worldcoin działa poza tym modelem. To nie jest tylko obietnica. Worldcoin jest celowo projektowany tak, aby uniemożliwić takie działanie.

Podejście Worldcoin jest takie: **Twoje dane, Twoje zasady.**

Minimalne dane

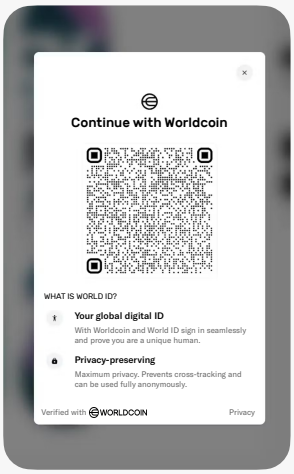
Punktem wyjścia do uznania kontroli ludzi nad ich danymi jest nie proszenie ich o dużą ilość danych. Ponieważ zweryfikowane World ID są anonimowe, ludzie nie podają swojego imienia, numeru telefonu, adresu ani innych danych powszechnie gromadzonych przez firmy technologiczne. Pomyśl tylko: aby dostać kartę biblioteczną, ludzie potrzebują potwierdzenia adresu zamieszkania. Aby uzyskać zweryfikowane World ID, globalny paszport cyfrowy, muszą jedynie posiadać smartfon i odwiedzić Orba.

Przypadek użycia:
Kody rabatowe Shopify

Shopify to platforma e-commerce dla firm, które chcą zwiększyć sprzedaż i zarządzać płatnościami online. Sprzedawcy platformy czasami próbują przyciągnąć nowych klientów, oferując jednorazowe rabaty.

Problem polega na tym, że ludzie mogą oszukać system, tworząc fikcyjne e-maile i wielokrotnie ubiegając się o zniżki lub używając botów, które robią to za nich. Zamiast przyciągać nowych klientów, sprzedawcy dofinansowują oszustwo.

Integrując World ID w swoim sklepie, sprzedawcy mogą pozwolić prawdziwym klientom zeskanować kod QR, który zweryfikuje ich World ID i zastosuje kod rabatowy. Ta metoda zapewnia jeden rabat na osobę, rozwiązując problem sprzedawców bez konieczności proszenia użytkowników o podanie dodatkowych danych. (Chociaż będą musieli podać dane swojej karty kredytowej i dane do wysyłki, aby dokonać płatności!)



[3] Dosłownie! Więcej informacji na ten temat znajdziesz na stronie https://en.wikipedia.org/wiki/Real-time_bidding

Przechowywanie osobiste

Proces weryfikacji World ID wymaga użycia pewnych danych, a mianowicie obrazów biometrycznych i kodów tęczówki. Kody tęczówki, po przejściu przez SMPC, trafiają na serwery, gdzie znajdują się w całkowicie zanonimizowanym formacie. Jednak dane dostarczone przez użytkownika w celu weryfikacji tożsamości za pomocą Orba nie są przechowywane ani udostępniane żadnej stronie trzeciej. Znajdują się jedynie na smartfonie tej osoby, gdzie są szyfrowane za pomocą jej klucza publicznego.

Dzięki Przechowywaniu Osobistemu Worldcoin, ludzie kontrolują dane zebrane i wygenerowane podczas weryfikacji – w tym World ID oraz obrazy – i decydują, komu je udostępnić.

Uwierzytelnianie za pomocą twarzy

Dzięki wprowadzeniu World ID platformy mogą chronić się przed botami bez naruszania prywatności swoich klientów. Zweryfikowane World ID zapewnia tym platformom wysoki poziom pewności, że użytkownik jest faktyczną osobą.

Jednak w niektórych scenariuszach, w których w grę wchodzą wysokie stawki (np. transakcjach finansowych), platformy lub osoby muszą wiedzieć nie tylko to, że mają do czynienia z faktyczną osobą, ale także to, że mają do czynienia z konkretną osobą. Chcą wiedzieć, że osoba korzystająca z World ID to ta sama unikalna osoba, która zweryfikowała World ID na tym urządzeniu.

Aby to zrealizować, aplikacje na Worldcoin mogą korzystać z Uwierzytelniania za pomocą twarzy.

Uwierzytelnianie za pomocą twarzy to metoda porównywania zdjęcia wykonanego podczas weryfikacji ze zdjęciem osoby chcącej skorzystać z World ID. Jest niezależna od urządzenia.

Pierwsze zdjęcie jest generowane, gdy osoba weryfikuje swoje World ID w Orbie. Domyślnie jedynym miejscem, w którym znajdują się te dane, jest telefon użytkownika. Te zdjęcia o wysokiej rozdzielczości są szyfrowane i bezpiecznie wysyłane na telefon użytkownika w ramach Przechowywania osobistego, a następnie całkowicie usuwane z Orba.

Drugie zdjęcie to selfie zrobione na urządzeniu użytkownika w aplikacji World App, podczas próby użytkownika wejścia do lub skorzystania z World ID. Uwierzytelnianie za pomocą twarzy w World ID porównuje obraz zrobiony przez urządzenie użytkownika z oryginalnym zdjęciem uwierzytelniania twarzy zrobionym podczas weryfikacji z Orbem. Użytkownik może kontynuować logowanie lub transakcję tylko wtedy, gdy oba obrazy są zgodne.

Zapobiega to oszustwom poprzez ochronę przed złośliwym podmiotem, który kradnie (lub kupuje) czyjś telefon i używa jego World ID. Dzięki Uwierzytelnianiu za pomocą twarzy zamierzony użytkownik zawsze ma kontrolę nad swoimi danymi i swoim World ID. **Porównanie odbywa się lokalnie na urządzeniu danej osoby.** W rezultacie ani selfie, ani zdjęcie z Orba, ani żadne inne dane osobowe nie są udostępniane żadnym stronom trzecim, w tym Tools for Humanity ani Fundacji Worldcoin.[4]

[4] W przyszłości projekt umożliwi ludziom dobrowolne udostępnianie swoich informacji Worldcoin w celu pomocy w szkoleniu z zakresu bezpieczeństwa i AI. Jest to w 100% dobrowolne, a pozwolenie można cofnąć w dowolnym momencie.

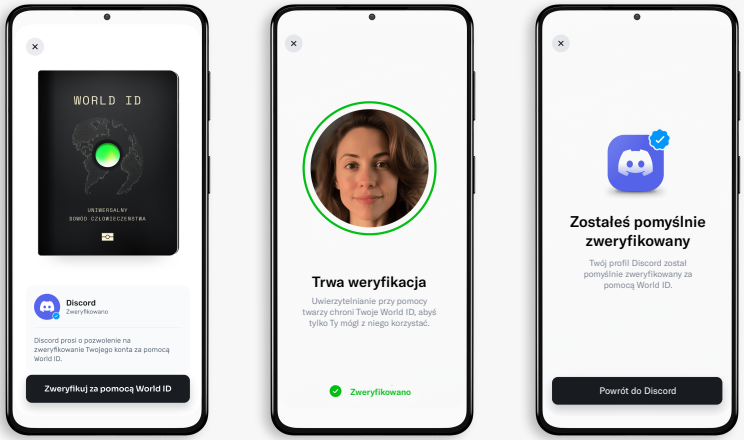
Uwierzytelnianie za pomocą twarzy, a Face ID

Dla użytkowników funkcja uwierzytelniania za pomocą twarzy będzie równie rozpoznawalna jak Apple Face ID.

Dlaczego więc nie używać po prostu Face ID?

Uwierzytelnianie za pomocą twarzy zapewnia, że osoba korzystająca z aplikacji World App jest tą samą osobą, która utworzyła powiązane World ID przy Orbie. Face ID nie umożliwia tej funkcji.

Face ID jest połączeniem hardware'u i software'u, więc jest finalnie powiązane z iPhonem. W Face ID użytkownicy mogą mieć inną twarz powiązaną z urządzeniem niż ta, której użyli do weryfikacji World ID, co zwiększa ryzyko oszustwa. Dzięki użyciu World ID, które jest dostępne na poziomie aplikacji, a nie urządzenia, Uwierzytelnianie za pomocą twarzy uniemożliwia dostęp do niego komukolwiek innemu niż osoba, która zweryfikowała World ID.



Zasada nr 4

Transparentność:
Tworzony w sposób otwarty

Eksperci ds. bezpieczeństwa są sceptyczni, szukają zagrożeń za każdą linijką kodu źródłowego. I dobrze, bo w ten sposób dbają o nasze bezpieczeństwo.

Byłoby nie do pomyślenia, aby TFH lub kilku programistów Worldcoin mogło przewidzieć każdą możliwą wadę protokołu. Dlatego właśnie Worldcoin jest **tworzony w sposób otwarty.**

Sprawdzony

Worldcoin uwzględnia możliwie najwięcej zewnętrznych opinii i specjalizacji. Kryptografowie i eksperci biometryczni nieustannie oceniają kod źródłowy, podczas gdy audytorzy i konsultanci ds. bezpieczeństwa próbują znaleźć choćby najmniejszą możliwość wystąpienia słabych punktów. Następnie Worldcoin publikuje wyniki oraz co zrobiono, aby rozwiązać choćby najmniejsze problemy.

Aby zidentyfikować potencjalne naruszenia, musimy także zrozumieć, w jaki sposób protokół może być używany w prawdziwym świecie – teraz i w przyszłości. Oznacza to przemyślenie tysięcy realiów kulturowych na całym świecie i włączenie tych czynników do modelu bezpieczeństwa, chroniącego przed nadużyciami, które mogą jeszcze nawet nie istnieć.

Od kwietnia 2023 r. firmy audytorskie Nethermind i Least Authority przeprowadziły dwa oddzielne audyty bezpieczeństwa protokołu Worldcoin. Audyty objęły w szczególności następujące obszary:

- Poprawność implementacji, w tym konstrukcji i prymitywów kryptograficznych oraz odpowiednie wykorzystanie konstrukcji inteligentnych kontraktów
- Typowe i konkretne błędy wdrożeniowe
- Złośliwe działania i inne ataki na kod
- Bezpieczne przechowywanie kluczy i właściwe zarządzanie kluczami szyfrującymi i podpisu
- Ujawnienie jakichkolwiek kluczowych informacji podczas interakcji z użytkownikiem
- Odporność na ataki Rozproszonej Odmowy Usługi (ang. Distributed Denial of Service lub DDoS) i podobne ataki
- Luki w kodzie umożliwiające złośliwe działania i inne ataki
- Ochrona przed złośliwymi atakami i innymi metodami wykorzystania
- Problemy z wydajnością lub inny możliwy wpływ na wydajność
- Prywatność danych, wyciek danych oraz integralność informacji
- Niewłaściwe uprawnienia, eskalacja uprawnień i nadmierne uprawnienia

Otwarty i Ogólnodostępny

Fakt, że kod Worldcoin jest otwarty (Open source) i ogólnodostępny, pomaga mu spełnić trzy cele. Po pierwsze, sieć może byc wtedy poddana ocenie, co może prowadzić do jej udoskonalenia.

Po drugie, daje programistom pewność, że mogą opierać się na protokole Worldcoin. Możliwe, że inne zespoły utworzą dodatkową aplikację potwierdzającą tożsamość lub znajdą jeszcze bardziej użyteczną metodę weryfikacji niż Orb.

Po trzecie, otwarty i ogólnodostępny charakter oprogramowania jest też niezbędny dla zdecentralizowanego projektu: każdy może utworzyć własną wersję (lub „fork") protokołu w dowolnym momencie i z dowolnego powodu — i dobrze!


WORLDCOIN