WORLDCOIN

Dirancang bersifat Privat

Daftar Isi

Ekosistem

Proyek Worldcoin terdiri dari beberapa aktor dan alat bantu, yang digabungkan untuk membentuk jaringan identitas yang mengedepankan manusia, yang memungkinkan adanya kepercayaan saat bertransaksi atau melakukan komunikasi *online*.

Worldcoin adalah proyek yang mencakup World ID, paspor digital anonim, dan jaringan yang memungkinkan penggunaan aset digital, menyediakan akses inklusif ke ekonomi digital global bagi miliaran orang.

World ID adalah protokol identitas terdesentralisasi untuk membuktikan bahwa Anda adalah orang yang unik. Anda dapat menggunakan World ID untuk membuktikan bahwa Anda adalah manusia dalam aktivitas *online* apa pun, seperti mengotentikasi video dan melindungi dari *deepfake.* Anda juga dapat menggunakannya untuk masuk ke situs web dan aplikasi, mirip dengan Sign-in dengan Google, membuktikan bahwa Anda adalah manusia yang unik tanpa harus membagikan data pribadi seperti nama, email atau nomor telepon Anda.

World Chain adalah *layer 2 rollup* yang akan segera diluncurkan di jaringan Ethereum yang memanfaatkan World ID untuk memprioritaskan transaksi yang berpusat pada manusia daripada bot.

WLD adalah token Worldcoin, yang diberikan secara gratis kepada individu karena dia adalah seorang manusia dan menjadi bagian dari jaringan Worldcoin.[1]

Worldcoin Foundation adalah organisasi nirlaba yang berfungsi sebagai pengurus protokol Worldcoin. Worldcoin Founda juga memiliki dan mengatur sebagian besar aset yang terkait dengan merek Worldcoin, termasuk kekayaan intelektual untuk *orb* dan teknologi protokol *open source*.

***Tools for Humanity* (TFH)** adalah perusahaan teknologi yang membuat alat bantu untuk Worldcoin, termasuk *orb* and *World App*.

Orb adalah kamera khusus yang memverifikasi kepribadian unik dan memberi Anda data untuk mengonfirmasi kepribadian Anda dengan menggunakan *World ID.*

World App adalah dompet *self-custody* Worldcoin yang menyediakan pangkalan untuk *World ID*. Dengan aplikasi ini, Anda juga dapat mengirim dan menerima token *Worldcoin* dan dana digital lainnya.

Untuk informasi lebih lanjut: Apa yang dimaksudkan dengan Worldcoin, dan bagaimana cara kerjanya?

[1] Pada yurisdiksi yang memenuhi syarat

Privasi dalam Era AI

Laporan tahun 2022 yang dikeluarkan oleh lembaga penegakan hukum Uni Eropa Europol menyatakan bahwa sebanyak 90 persen konten internet dapat secara sintetis dihasilkan selambat-lambatnya tahun 2026.

Catfishing Scambots. Deepfakes, Pencurian identitas. Disinformasi. Internet bisa menjadi tempat yang berbahaya. Kemajuan AI akan membuat internet lebih berguna dari sebelumnya, tetapi kita harus berpandangan tajam tentang potensinya yang dapat memperbesar masalah yang ada. Kita telah melihat hal apa yang bisa menjadi masalah, ketika manusia berpura-pura menjadi orang lain. Apa yang terjadi ketika kita berpikir kita sedang berurusan dengan manusia padahal sebenarnya itu adalah agen AI?

Yang kita butuhkan adalah cara untuk memverifikasi bahwa orang dengan siapa kita berbicara, yang kita kirimkan uang, dan yang melihat konten secara *online* (beberapa contoh saja) sebenarnya adalah orang. Worldcoin bertujuan untuk memberi Anda kekuatan bertindak atas setiap elemen ini di era AI.

Mencegah AI membanjiri internet dengan orang palsu membutuhkan keamanan yang luar biasa. Namun banyak pendekatan yang divisualisasikan untuk menangani hal ini terasa kurang tepat. Ada godaan untuk menjangkau alat bantu lama yang sama – menghapus privasi dan mengandalkan pada teknik identifikasi atau verifikasi yang dapat dipilih untuk pengawasan perusahaan dan pemerintah. Panopticon mungkin bisa dilakukan, tetapi berapa biayanya?

Kami percaya ada cara yang lebih baik: Proyek Worldcoin adalah tentang menciptakan teknologi aman yang menempatkan manusia sebagai pusat, memungkinkan mereka untuk mengontrol dengan lebih baik dan mempercayai pengalaman *online* mereka tanpa mengorbankan privasi mereka.

Worldcoin **dirancang bersifat privat**.

Bagaimana AI membawa risiko terhadap privasi

Kita telah melihat *deepfake* beredar dari politisi dan tokoh selebriti—orang-orang yang memiliki banyak konten *online* untuk diambil.

Tetapi AI canggih berarti bahwa *deepfakes*—video dan audio yang sangat realistis—dapat segera digunakan untuk menirukan orang biasa. Kami sangat prihatin bahwa internet dan penggunanya tidak siap menghadapi tantangan yang akan dihadirkan oleh AI canggih. Bayangkan berada dalam panggilan Zoom dengan rekan kerja yang sebenarnya bukan rekan kerja atau orang yang dicintai, yang sama sekali bukan manusia. Orang dapat dengan mudah ditipu untuk mengirim uang, membocorkan rahasia, atau hal-hal yang belum kita bayangkan.

Untuk memerangi aplikasi AI yang berbahaya, platform harus dapat mengetahui seseorang adalah manusia yang unik. Alat seperti "CAPTCHA" tidak lagi efektif dan mengandalkan data yang terkait dengan jejak digital seseorang. World ID adalah alternatif yang menjaga privasi untuk interaksi digital seperti CAPTCHA. Ini juga berfungsi sebagai alternatif untuk KYC dan sistem ID digital yang mengungkapkan identitas individu atau menghubungkan identitas seseorang dengan aktivitas digital mereka.

Prinsip-prinsip Privasi Worldcoin

Komunitas Worldcoin sedang membangun sesuatu yang belum pernah terjadi sebelumnya: jaringan yang tepercaya secara global, inklusif maksimal, dan yang menjaga privasi untuk membuktikan kepribadian. Tetapi pendekatan proyek terhadap privasi tidak diperkirakan sebelumnya dan terbilang baru, menghadirkan rute baru yang mendasar yang belum pernah diambil oleh perusahaan atau organisasi, atau pemerintah:

Worldcoin tidak ingin tahu siapa Anda, hanya bahwa Anda adalah manusia yang unik.

Bot bertenaga AI menjadi lebih banyak di mana-mana, semakin canggih, mengurangi kepercayaan dalam melakukan kegiatan secara *online,* dan meniru identitas orang. Jadi, mengetahui apakah Anda berinteraksi dengan manusia atau bot menjadi semakin penting. Jika membuktikan kepribadian dalam *online* adalah satu-satunya hal yang kami khawatirkan, maka solusinya mungkin tampak cukup mudah: gunakan ID yang dikeluarkan pemerintah untuk memverifikasi identitas kami dan menavigasi dalam *online*. Lagi pula, kita sering diminta untuk menunjukkan ID di bank. Bukankah transaksi *online* di era AI berpotensi sama sensitifnya?

Mengesampingkan fakta bahwa diperkirakan 850 juta orang tidak memiliki bentuk ID resmi apa pun dan bahwa pemerintah sendiri telah mengadakan kampanye disinformasi yang canggih secara *online,* verifikasi melalui ID yang dikeluarkan pemerintah secara *online* bukanlah solusi. Ini mengungkapkan lebih banyak tentang Anda daripada yang dibutuhkan, seperti alamat Anda, dan memaparkan Anda pada risiko identitas Anda bisa dicuri atau digunakan untuk tujuan jahat, termasuk melalui cara yang tidak dapat kita bayangkan karena adanya AI.

Kami membutuhkan bukti kepribadian dan privasi dalam paket yang sama (dengan sesedikit mungkin hambatan untuk masuk).

Ini adalah tantangan yang ingin dipecahkan oleh Worldcoin, dan mereka melakukannya terutama melalui World ID. World ID adalah paspor digital global yang berada secara lokal di ponsel cerdas pemegangnya dan memungkinkan seseorang untuk membuktikan bahwa mereka adalah orang yang unik tanpa membagikan data pribadi dengan siapa pun.

Ini adalah sistem verifikasi manusia untuk internet yang memungkinkan orang untuk menjadi anonim ke mana pun mereka pergi. World ID yang telah diverifikasi tidak mengumpulkan atau menautkan ke pengidentifikasi seperti nama atau email, menautkan ke data transaksi dompet, atau mengungkapkan World ID siapa yang digunakan. Secara desain, Worldcoin dibentuk berdasarkan praktik minimalisasi data. Worldcoin tidak menyimpan informasi pengidentifikasi.

“Sampai sekarang, siapa pun yang ingin membuktikan bahwa mereka manusia secara *online* telah menggunakan sarana seperti ID pemerintah, yang dibebani oleh ketidaknyamanan dalam mengidentifikasi pengguna dan mengungkapkan sejumlah besar data pribadi lainnya, meskipun ini tidak perlu dilakukan. Sebaliknya, World ID memungkinkan bukti keunikan manusia yang anonim dan dengan demikian melawan model 'kapitalisme pengawasan' dengan model yang mengedepankan perlindungan data. World ID dengan ini memperkuat peluang untuk aktivitas *online* yang mematuhi perlindungan data.”

Dr. Stefan Brink, mantan Komisaris Negara Jerman untuk Perlindungan Data dan Kebebasan Informasi di Baden-Württemberg dari Januari 2017 hingga Desember 2022.

Selain itu, World ID dibuat agar orang dapat menggunakannya di seluruh aplikasi tanpa aplikasi tersebut melacak aktivitas mereka dari satu ke yang lain. Tidak ada repositori pusat tentang riwayat penggunaan. Anda dapat menggunakan World ID di berbagai ratusan aplikasi tanpa mengetahui satu dengan lainnya—atau World ID mengetahui tentang aplikasi tersebut.

Worldcoin dirancang bersifat privat dengan empat fondasi privasi yang saling terkait:

Prinsip 1

Keamanan: Diamankan oleh matematika

Prinsip 2

Anonimitas: Bergerak secara bebas dalam *online*

Prinsip 3

Pilihan & Kendali: Data Anda, aturan Anda

Prinsip 4

Transparansi: Dibangun secara terbuka

Prinsip 1

Keamanan: Diamankan oleh matematika

Tanpa keamanan, tidak ada privasi.

Worldcoin adalah tentang memungkinkan orang untuk *online* tanpa memaparkan identitas mereka dan memberdayakan mereka untuk membedakan antara interaksi berbasis bot dan interaksi manusia. Keamanan membantu memastikan tingkat privasi tercapai—setiap saat, dipastikan berhasil.

World ID menggunakan banyak teknik keamanan untuk memastikan keamanan data pemegang World ID.

Satu set melibatkan alat bantu manusia, seperti *open-source* dan audit (lihat: Transparansi), yang membantu memvalidasi dan menguji tekanan langkah-langkah keamanan yang telah dibuat dan diimplementasikan sebagai bagian dari proyek Worldcoin.

Set lainnya termasuk alat bantu kriptografi, seperti ZKPs dan SMPC (lihat: Anonimitas), yang menggunakan matematika tingkat lanjut untuk mengamankan data, mengenkripsinya, dan menjaganya tetap bersifat pribadi atau membuatnya anonim.

SMPC adalah salah satu dari beberapa hasil dalam kriptografi yang dapat memberikan kerahasiaan yang sempurna. Sementara itu, ZKP menggunakan hash nullifier, atau nilai unik, untuk setiap aplikasi sehingga riwayat penggunaan orang tidak dapat dilacak.

Sebut saja **diamankan oleh matematika.**

Prinsip 2

?

Tetapi menggunakan situs web dan apps sebaiknya tidak melibatkan memberikan data lebih dari data di luar keinginan kita. Orang harus dapat bergerak secara bebas secara online

Anonimitas:
Bergerak secara bebas dalam *online*

Seringkali, kita tidak membutuhkan identifikasi hanya untuk berada di dunia. Memasak makan malam, membaca buku, tidur. Melakukan kegiatan ini jarang mengharuskan kita untuk membuktikan siapa kita. Dalam sebagian besar hidup kita, tindakan kita berjalan tanpa diperhatikan, tidak diamati, dan tidak dicatat. Kita anonim.

Anonimitas lebih sulit dicapai secara *online*. Situs dapat melihat aktivitas kami, dan perambah dapat melacak pergerakan dan perilaku *online* kami. Pengawasan ini berpotensi menjadi lebih berbahaya ketika kita diminta untuk membuktikan siapa kita, mulai dari paling dasar pemantauan alamat IP kita hingga yang paling canggih dengan menampilkan otentikasi ID yang dikeluarkan pemerintah.

Tetapi menggunakan situs web dan aplikasi seharusnya tidak melibatkan pemberian data kita lebih dari data di luar keinginan kita. Orang-orang harus dapat **bergerak bebas secara *online***. Masuk ke situs dengan World ID memungkinkan hal ini.

Untuk menjaga anonimitas di dunia *online,* Worldcoin menggunakan banyak teknologi yang menjaga privasi termasuk komputasi multipihak yang aman (SMPC) dan bukti pengetahuan nol (ZKP).

Komputasi multipihak yang aman (SMPC)

Hanya memerlukan ponsel cerdas untuk membuat World ID, tetapi membuktikan pemiliknya adalah manusia yang unik yang belum membuat beberapa World ID – sementara menjaga identitas mereka tetap bersifat pribadi merupakan tantangan yang rumit.

Data biometrik, jika dianonimkan dengan tepat, memberikan solusi. Kegunaan data biometrik berarti data tersebut harus dikumpulkan dan digunakan secara minimal dan ketika itu adalah satu-satunya jalur yang layak, maka itu harus ditangani dengan hati-hati.

Worldcoin melakukan ini melalui SMPC.

Ketika seseorang memverifikasi World ID mereka melalui *orb, orb* tersebut mengambil gambar iris dan wajah mereka. Ini menggunakan gambar-gambar ini untuk membuat kode iris, yang pada dasarnya adalah serangkaian 1 dan 0. Tidak ada dua kode iris yang sama dan kode iris ini juga tidak mengungkapkan secara langsung pengidentifikasi seperti nama, jenis kelamin, usia, dll.

Kode iris ini dibagi menjadi beberapa bagian dan dienkripsi secara permanen menggunakan SMPC, yang membuat data anonim dengan membaginya menjadi beberapa nilai abstrak (bagian SMPC) dan menyimpannya di lokasi terpisah yang dikelola oleh dua entitas yang berbeda secara hukum. Dalam waktu dekat mitra untuk penyimpanan tambahan (termasuk universitas dan nirlaba) akan ditambahkan, yang berarti bahwa kode iris akan dibagi menjadi nilai yang lebih abstrak yang disimpan dan dikelola oleh entitas yang bahkan lebih independen. Tidak ada satu pihak pun yang memiliki akses ke bagian dari kode iris. Mereka hanya memiliki akses ke bagian SMPC yang disimpan di bawah kendali dan manajemen mereka.

Meskipun menyimpan data di beberapa lokasi tampaknya akan meningkatkan kemungkinan data itu dicuri, yang terjadi justru sebaliknya. Bagian SMPC disimpan sedemikian rupa sehingga, jika aktor jahat entah dengan cara apa mendapatkan akses ke satu bagian SMPC,

itu tidak akan dapat dibaca/dipahami, semua itu baru dapat dimengerti ketika semua bagian disatukan.

Mengapa sampai harus menyimpan bagian SMPC yang terenkripsi? Supaya protokol Worldcoin dapat terus membuktikan orang itu unik. Tanpa itu, pengguna perlu memverifikasi ulang World ID mereka setiap kali aplikasi memintanya.

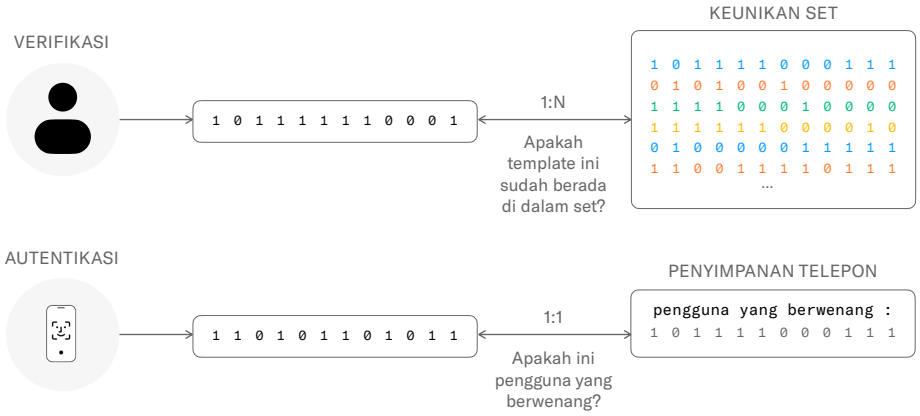


Foto-foto itu sendiri tidak tetap berada di *orb*, alih-alih, *orb* mengenkripsi data dari awal hingga akhir dengan kunci publik yang disediakan ponsel cerdas pengguna (tidak seorang pun kecuali pengguna yang memiliki kunci pribadi untuk mendekripsi) dan kemudian *orb* mengirimkan gambar terenkripsi ke perangkat pengguna sebelum menghapusnya dari *orb*. Semua ini terjadi dalam hitungan detik selama proses verifikasi.

Mengapa iris?

Orbs—kamera canggih—adalah perangkat keras pertama yang mendukung protokol Worldcoin. Untuk saat ini, adalah satu-satunya metode untuk memverifikasi World ID dimiliki manusia unik adalah dengan mengunjungi *orb* dan mengambil foto mata Anda.

TFH mempelajari berbagai jenis biometrik untuk memverifikasi World ID, masing-masing dengan pro dan kontranya sendiri. Untuk memenuhi kriteria bukti masa depan yang diperlukan untuk memberikan sifat manusia bagi semua individu di bumi dalam dunia AI, metode apa pun harus 1) akurat, 2) menjaga privasi, 3) sangat sulit untuk dipalsukan, 4) terukur, dan 5) sangat mudah digunakan.

Sidik jari sangat berguna tetapi mudah dipalsukan. Namun, Iris, akurat, dapat digunakan, terukur, inklusif secara luas, dan sangat sulit untuk dipalsukan. Dan, mereka menjaga privasi. Tidak terdapat banyak catatan publik tentang iris (seperti wajah di media sosial), seseorang tidak dapat memotret iris seseorang dengan jarak dekat, tanpa orang tersebut menyadarinya, dan peralatan kamera khusus diperlukan untuk mencoba melakukannya.

Protokol Worldcoin terbuka dan terdesentralisasi, dan mekanisme verifikasi tambahan hanya akan memperkuat daya tarik dan keamanan proyek.

Bukti pengetahuan nol (ZKPs)

Setelah seseorang memiliki World ID yang sudah diverifikasi, mereka dapat menggunakannya untuk masuk dan bertransaksi dengan aplikasi pihak ketiga yang terintegrasi dengan protokol World ID.

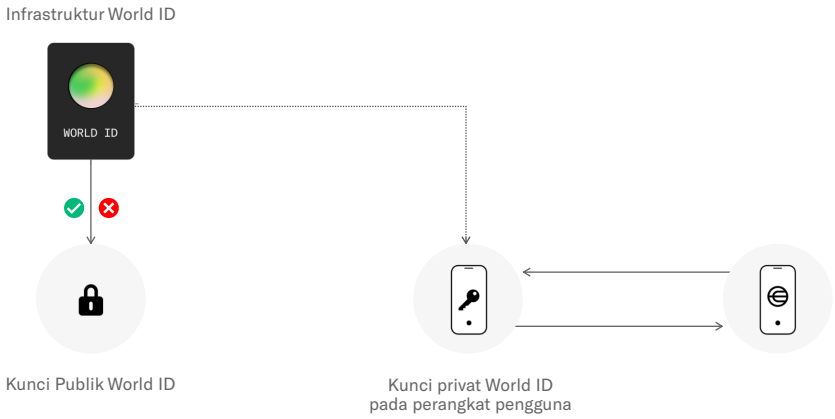
Tapi itu tidak berarti orang membagikan World ID mereka dengan aplikasi pihak ketiga.

Alih-alih, World ID digunakan untuk membuat versi sekali pakai itu sendiri, serupa dengan *Apple's Hide My Email* atau kartu kredit virtual. Bayangkan memiliki kartu kredit perusahaan yang hanya dapat digunakan untuk satu kali pembelian. Untuk membayar barang-barang di vendor lain, Anda harus membuat kartu terpisah. Meskipun ini mungkin terdengar sangat membebani, protokol melakukannya dengan cepat dan mulus di belakang layar, menghasilkan sistem yang aman untuk aplikasi dan melindungi pengguna.

Metode untuk melakukan ini—sehingga baik Worldcoin maupun aplikasi tidak dapat melacak riwayat penggunaan atau di seluruh aplikasi atau pihak yang terlibat dalam transaksi tertentu—adalah ZKP, alat bantu kriptografi yang memungkinkan seseorang untuk membuktikan sesuatu itu benar tanpa mengungkapkan informasi apa pun yang digunakan untuk sampai pada kesimpulan itu.

Setiap kali Anda menggunakan aplikasi pihak ketiga, aplikasi akan meminta bukti dari perangkat Anda. Anggap saja sebagai mengajukan pertanyaan kepada perangkat Anda. Ia ingin tahu, apakah perangkat ini mengontrol World ID ini? World App di perangkat pengguna mengirimkan kembali ZKP yang menunjukkan bahwa World ID telah diverifikasi.

ZKP melampaui persyaratan peraturan yurisdiksi mana pun. Worldcoin menerapkannya karena itu adalah cara terbaik untuk memastikan pengguna dapat tetap anonim (kecuali pengguna memberikan informasi tambahan secara langsung ke layanan pihak ketiga yang meminta bukti) dan aplikasi tidak dapat melacaknya. Ini mencegah pihak ketiga—dan Worldcoin Foundation itu sendiri—untuk mengetahui World ID pengguna, atau layanan apa yang berinteraksi dengan mereka.



Analogi praktis untuk ZKP

ZKP adalah kriptografi canggih, sehingga tidak sesuai untuk analogi yang sempurna. Tetapi untuk mendapatkan ide dasarnyya, bayangkan sebuah teka-teki di mana Anda harus menemukan obyek atau orang orang tertentu di dalam suatu adegan.[2]

Setelah mencari selama beberapa menit, satu orang mengatakan kepada yang lain bahwa dia tahu di mana barang itu berada. Orang kedua, yang tidak tahu di mana barang itu, tidak yakin apakah harus mempercayai ini.

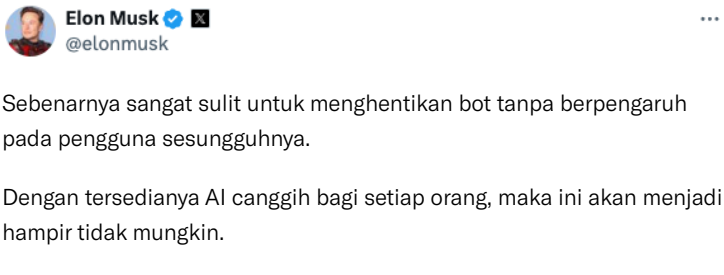
Jadi orang pertama mengatakan dia bisa membuktikannya—tanpa dengan hanya mengungkapkan di mana barang itu berada.

Dia memfotokopi teka-teki yang lengkap, memotong barang tersebut, dan memperlihatkan kepada orang kedua, yang sekarang yakin barang itu ada dalam teka-teki dan orang pertama tahu di mana itu.

Dalam skenario ini, orang kedua adalah aplikasi apa pun yang mencoba mengonfirmasi bahwa pengguna adalah manusia; barang yang dipotong adalah ZKP; dan orang pertama adalah protokol Worldcoin yang membuktikan bahwa penggunanya adalah manusia tanpa mengungkapkan identitas mereka.

Kasus penggunaan: X bot atau manusia?

Elon Musk membeli X (sebelumnya namanya Twitter) berjanji untuk membuang bot dari platform. Tetapi pemilik baru dengan cepat menyadari bahwa ini lebih mudah diucapkan daripada dilakukan. "Sangat sulit untuk menghentikan bot tanpa mempengaruhi pengguna nyata," tulis Musk pada Desember 2023. "Ketika AI canggih? tersedia untuk siapa saja, itu akan menjadi hampir tidak mungkin."



Musk benar tentang tantangan yang disajikan bot ke platform sosial. Tetapi sekarang ada solusi yang layak untuk memerangi mereka tanpa mempengaruhi pengguna.

[2] Misalnya, "Di mana Waldo/Wally?"

X mengizinkan tiga mode masuk: Masuk dengan Google, Masuk dengan Apple, atau nama pengguna/kata sandi. Untuk membuat akun, pengguna diminta untuk memberikan nama, nomor telepon atau email, dan tanggal lahir mereka. Karena relatif mudah untuk membuat beberapa alamat email, membuat beberapa akun X juga cukup mudah. Dengan demikian, tidak banyak penghalang bagi bot untuk *online*, di mana mereka dapat mengurangi pengalaman pengguna untuk manusia.

Namun, World ID tidak mengandalkan alamat email, yang mudah diatur, atau nomor telepon, yang mudah dipalsukan. Hanya manusia yang bisa mendapatkan World ID yang sudah diverifikasi—dan, tidak seperti email, ini terbatas hanya satu. Jadi, jika X akan menggunakan World ID sebagai mekanisme verifikasi kepribadiannya, maka layanan ini dapat menambahkan tanda yang menunjukkan akun tersebut adalah manusia yang telah diverifikasi. Setiap bot yang masuk tidak akan lolos verifikasi.

Yang penting, hal itu bahkan akan meningkatkan anonimitas bagi pengguna X, yang tidak perlu memberikan informasi tambahan apa pun di luar apa yang telah mereka berikan kepada X.

Ini bukan semata-mata bersifat teoritis. TFH membangun integrasi Telegram World ID untuk menyingkirkan *spam bots* di jaringan. Administrator obrolan publik dapat mewajibkan bahwa akun individu harus terlebih dahulu melakukan verifikasi dengan World ID sebelum memposting di grup.

Prinsip 3

Pilihan & Kendali:
Data Anda, aturan Anda

Orang-orang menjadi semakin terbiasa dengan paradigma *Big Tech* di mana, sebagai imbalan untuk mengakses layanan, mereka menyerahkan data pribadi mereka kepada perusahaan sehingga dapat dijual kepada penawar tertinggi.[3]

Worldcoin beroperasi di luar paradigma ini. Ini bukan hanya janji. Worldcoin sengaja dirancang untuk membuatnya tidak mungkin untuk melakukan hal itu.

Pendekatan Worldcoin adalah: **Data Anda, aturan Anda.**

Data minimal

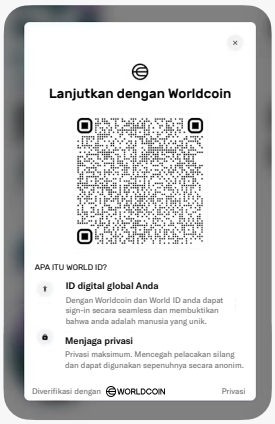
Titik awal untuk mengenali kontrol orang atas data mereka adalah tidak meminta banyak data untuk memulai. Karena World ID yang telah diverifikasi bersifat anonim, orang tidak memberikan nama, nomor telepon, alamat, atau informasi lain yang biasa ditangkap oleh perusahaan teknologi. Pikirkan tentang hal ini: Untuk mendapatkan kartu perpustakaan, orang memerlukan bukti tempat tinggal dengan alamat. Untuk mendapatkan ID Dunia yang telah diverifikasi, suatu paspor digital global, mereka hanya memerlukan ponsel cerdas dan mengunjungi *orb*.

Kasus penggunaan:
Kode diskon Shopify

Shopify adalah platform e-commerce untuk bisnis yang berusaha meningkatkan penjualan dan mengelola pembayaran *online*. Pedagang di platform terkadang berusaha menarik pelanggan baru dengan memberikan diskon satu kali.

Masalahnya adalah bahwa orang dapat mempermainkan sistem ini dengan membuat email palsu dan mengklaim diskon beberapa kali—atau menempatkan bot untuk melakukan ini untuk mereka. Alih-alih menarik pelanggan baru, vendor mensubsidi suatu penipuan.

Dengan mengintegrasikan World ID di toko mereka, pedagang dapat membiarkan pelanggan yang sebenarnya memindai kode QR yang memverifikasi World ID mereka dan menerapkan kode diskon. Metode ini memastikan satu diskon per manusia, menyelesaikan masalah pedagang tanpa meminta pengguna untuk memberikan informasi tambahan apa pun. (Meskipun mereka harus memberikan kartu kredit dan detail pengiriman mereka untuk menyelesaikan transaksi!)



[3] Untuk informasi lebih lanjut tentang hal ini kunjungi https://en.wikipedia.org/wiki/Real-time_bidding

Personal Custody

Proses untuk memverifikasi World ID memerlukan penggunaan beberapa data, yaitu, gambar biometrik dan kode iris. Kode iris, setelah melalui SMPC, menuju ke server tempat mereka berada dalam format yang sepenuhnya anonim. Tetapi data yang diberikan oleh pengguna untuk memverifikasi kepribadian melalui *orb* tidak disimpan atau diberikan kepada pihak ketiga mana pun. Alih-alih, data itu hanya berada di ponsel cerdas orang tersebut, di mana data itu dienkripsi dengan kunci publik individu.

Dengan *Worldcoin Personal Custody*, orang mengontrol data yang dikumpulkan dan dihasilkan selama verifikasi—termasuk World ID dan gambar—dan memutuskan dengan siapa akan membagikannya.

Otentikasi Wajah

Dengan memperkenalkan World ID, platform dapat memberi perlindungan dari bot tanpa mengganggu privasi pelanggan mereka. ID Dunia yang telah diverifikasi memberi platform ini tingkat kepercayaan yang tinggi bahwa pengguna sebenarnya adalah orang.

Tetapi dalam beberapa skenario berisiko tinggi (misalnya, transaksi keuangan) ketika platform atau orang harus tahu tidak hanya apakah mereka berurusan dengan orang tetapi juga bahwa mereka berurusan dengan orang tertentu. Mereka ingin tahu bahwa orang yang menggunakan World ID adalah manusia unik yang sama dengan yang memverifikasi World ID Dunia di perangkat itu.

Untuk mencapai ini, aplikasi di Worldcoin dapat menggunakan Otentikasi Wajah.

Otentikasi Wajah adalah metode untuk membandingkan gambar yang diambil selama verifikasi dengan gambar orang yang ingin menggunakan World ID dan agnostik perangkat.

Gambar pertama dihasilkan ketika seseorang memverifikasi World ID mereka di *orb*. Ponsel pengguna dengan setelan standar adalah satu-satunya tempat di mana data ini ada. Foto-foto dengan resolusi tinggi tersebut dienkripsi, dan dikirim dengan aman ke ponsel pengguna sebagai bagian dari *Personal Custody*, dan sepenuhnya dihapus dari *orb.*

Gambar kedua adalah *selfie* yang diambil di perangkat pengguna dalam *World App* saat pengguna berusaha mengakses atau menggunakan World ID mereka. Otentikasi Wajah untuk World ID membandingkan gambar yang diambil oleh perangkat pengguna dengan gambar otentikasi wajah asli yang diambil selama verifikasi di *orb*. Pengguna hanya dapat melanjutkan untuk masuk atau melanjutkan transaksi mereka jika kedua gambar cocok.

Ini mencegah penipuan dengan melakukan pertahanan diri dari aktor jahat yang mencuri (atau membeli) ponsel seseorang dan menggunakan World ID mereka. Dengan Otentikasi Wajah, pengguna yang dituju selalu memegang kendali atas data dan World ID mereka. **Perbandingan dilakukan secara lokal pada perangkat individu.** Akibatnya, baik *selfie*, gambar dari *orb,* atau data pribadi lainnya tidak dibagikan dengan pihak ketiga mana pun termasuk *Tools for Humanity* atau *Worldcoin Foundation.*[4]

[4] Di masa depan, proyek ini akan memungkinkan orang untuk memilih untuk secara sukarela berbagi informasi mereka dengan Worldcoin untuk membantu keamanan dan pelatihan AI. Ini adalah 100% opsional, dan izin dapat dicabut kapan saja.

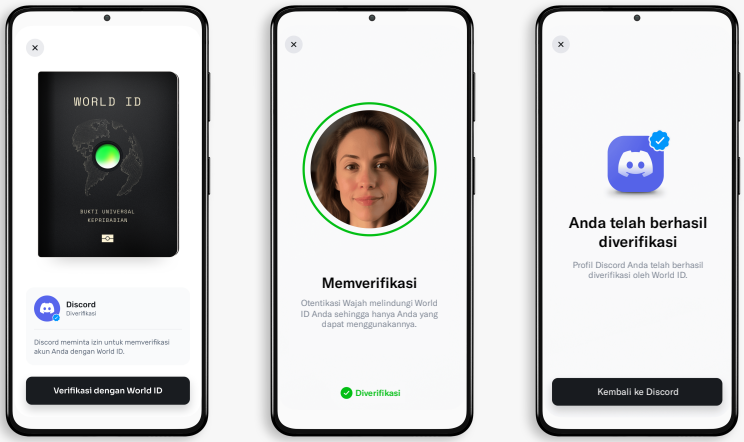
Otentikasi Wajah dibandingkan dengan Face ID

Bagi pengguna, Otentikasi Wajah akan terasa sama dapat dikenali seperti *Apple Face ID.*

Jadi, mengapa tidak menggunakan *Face ID* saja?

Otentikasi Wajah memastikan orang yang menggunakan World App adalah orang yang sama yang membuat World ID di *orb*. Face ID tidak memiliki kemampuan ini.

Face ID adalah kombinasi perangkat keras dan perangkat lunak, jadi pada akhirnya terkait dengan iPhone. Dengan Face ID, pengguna dapat memiliki wajah berbeda terkait dengan perangkat dengan yang mereka gunakan untuk memverifikasi World ID, yang meningkatkan potensi penipuan. Dengan menggunakan World ID, yang berada di tingkat aplikasi, dan bukan di tingkat perangkat, Otentikasi Wajah mencegah siapa pun selain orang yang memverifikasi World ID Dunia untuk mengaksesnya.



Prinsip 4

Transparansi: Dibangun secara transparan

Pakar keamanan sangat skeptis, mencari bahaya di balik setiap baris kode sumber. Dan itu hal yang baik, begitulah cara mereka menjaga kita tetap aman.

Sulit dipahami untuk berpikir bahwa TFH atau beberapa pengembang Worldcoin dapat membayangkan setiap kemungkinan adanya kesalahan dengan protokol. Itulah sebabnya Worldcoin dibangun **secara transparan.**

Diaudit

Worldcoin menggabungkan sebanyak mungkin pendapat dan bidang keahlian eksternal. Ahli kriptografer dan ahli biometrik terus mengevaluasi kode sumber saat auditor keamanan dan konsultan mencoba menemukan kemungkinan kerentanan sekecil apa pun. Worldcoin kemudian menerbitkan hasilnya—dan apa yang dilakukannya untuk mengatasi bahkan masalah terkecil sekalipun.

Untuk mengidentifikasi potensi pelanggaran, kita juga harus memahami bagaimana protokol dapat digunakan di dunia nyata—sekarang dan di masa depan. Itu berarti memikirkan ribuan realitas budaya di seluruh dunia dan memasukkan pertimbangan ini ke dalam model keamanan yang melindungi dari penyalahgunaan yang bahkan mungkin belum ada.

Mulai April 2023, perusahaan audit Nethermind dan Least Authority melakukan dua audit keamanan terpisah untuk protokol Worldcoin. Secara khusus audit mencakup bidang-bidang berikut ini :

- Implementasi yang benar, termasuk konstruksi kriptografik dan penggunaan primitif dan penggunaan yang sesuai dari konstruksi kontrak digital
- Kesalahan implementasi umum dan kasus khusus
- Tindakan adversarial dan serangan lain terhadap kode
- Penyimpanan kunci yang aman dan pengelolaan enkripsi dan kunci penandatanganan yang tepat
- Paparan informasi penting apa pun selama interaksi pengguna
- Resistensi terhadap DDoS (penolakan layanan terdistribusi) dan serangan serupa
- Kerentanan dalam kode yang mengarah ke tindakan adversarial dan serangan lainnya
- Perlindungan terhadap serangan berbahaya dan metode eksploitasi lainnya
- Masalah kinerja atau dampak potensial lainnya terhadap kinerja
- Privasi data, kebocoran data, dan integritas informasi
- Izin yang tidak tepat, eskalasi hak istimewa, dan otoritas yang berlebihan

Open-sourced dan *Permissionless* (tidak memerlukan izin)

Membuat kode Worldcoin *open-source* dan *permissionless* (tidak memerlukan izin) dapat membantunya memenuhi tiga tujuan. Pertama, hal ini memaparkan jaringan terhadap kritik yang dapat memperbaiki jaringan.

Kedua, ini memungkinkan pengembang untuk merasa percaya diri untuk menempatkan di atas protokol Worldcoin. Ada kemungkinan bahwa tim lain mungkin membuat aplikasi bukti kepribadian selain dari ID Dunia, atau menemukan metode verifikasi yang lebih berguna daripada *orb.*

Pada akhirnya, menjadi *open source* dan *permissionless* sangat penting untuk proyek terdesentralisasi: siapa pun dapat membuat versi protokol mereka sendiri (atau *"fork"*) kapan saja, untuk alasan apa pun—dan ini adalah hal yang baik.


WORLDCOIN