WORLDCOIN

Privada por Design

Conteúdo

Ecossistema 3

Privacidade na Era da IA 4

Princípios de Privacidade da Worldcoin 5

Princípio 1 Segurança: Protegido pela matemática 7

Princípio 2 Anonimato: Navega livremente online 8

Computação Multipartidária Segura (SMPC) 8

Provas de Conhecimento Zero (ZKPs) 10

Princípio 3 Escolha & Controlo: Os teus dados, as tuas regras 12

Quantidade mínima de dados 12

Custódia Pessoal 13

Autenticação Facial 13

Princípio 4 Transparência: Construída de forma aberta 15

Auditado 15

Código Aberto e Sem Permissões 15

Ecossistema

O projeto Worldcoin consiste em vários intervenientes e ferramentas, que combinados formam uma rede de identidade centrada do ser humano, permitindo confiança durante transações ou comunicações online.

A **Worldcoin** é um projeto que engloba o World ID, um passaporte digital anónimo, e uma rede que possibilita o uso de ativos digitais, providenciando acesso inclusivo à economia digital global para bilhões de pessoas.

O **World ID** é um protocolo de identidade descentralizado, para provar que és uma pessoa única. Podes usar o World ID para provar que és humano em qualquer atividade online, como autenticar vídeos e proteger contra *deepfakes*. Também podes usar para iniciar sessão em websites e aplicações, de forma semelhante ao início de sessão feito com a conta Google, provando que és um ser humano único, sem teres de partilhar dados pessoais, tais como o nome, o email ou o número de telemóvel.

A **World Chain** será uma camada de nível 2 da rede Ethereum, ainda a ser lançada, que utiliza o World ID para priorizar transações centradas em humanos em vez de bots.

O **WLD** é o token da Worldcoin, que é dado gratuitamente às pessoas por serem seres humanos e fazerem parte da rede Worldcoin.[1]

A **Worldcoin Foundation** é uma organização sem fins lucrativos que atua como responsável do protocolo Worldcoin. Também detém e governa a maior parte dos ativos relacionados com a marca Worldcoin, incluindo a propriedade intelectual da Orb e a tecnologia de código aberto relativa ao protocolo.

A **Tools for Humanity (TFH)** é uma empresa de tecnologia que cria ferramentas para a Worldcoin, incluindo a Orb e a World App.

A **Orb** é uma câmera especial que verifica a unicidade da pessoa e lhe fornece dados para confirmar a sua identidade utilizando um World ID.

A **World App** é uma carteira digital de autocustódia da Worldcoin, onde se encontra o teu World ID. Com a aplicação, também podes enviar e receber tokens Worldcoin e outros fundos digitais.

Para mais informações: O que é a Worldcoin, e como funciona?

[1] Em jurisdições elegíveis

Privacidade na Era da IA

Um relatório de 2022, da Europol, agência de aplicação da lei da União Europeia, sugeriu que até 90% do conteúdo da Internet podia ser gerado sinteticamente até 2026.

Catfishing. Scambots. Deepfakes. Roubo de identidade. Desinformação. A internet pode ser um lugar perigoso. O avanço da IA irá tornar a internet mais útil do que nunca, no entanto, devemos estar conscientes do seu potencial para amplificar problemas existentes. Já vimos o que pode dar errado quando uma pessoa finge ser outra. O que acontece quando achamos que estamos a lidar com um humano que, na verdade, é um agente de IA?

O que precisamos é de uma forma de verificar se as pessoas com quem conversamos, para quem enviamos dinheiro e de quem consumimos conteúdo online (para referir apenas alguns exemplos) são realmente pessoas. A Worldcoin tem como objetivo dar-te o controlo sobre cada um destes elementos na era da IA.

Impedir que a IA inunde a internet com pessoas falsas exige uma segurança extraordinária. No entanto, muitas das abordagens imaginadas para se lidar com isto são autoritárias. Há uma tentação de recorrer às mesmas ferramentas de sempre—eliminando a privacidade e confiando em técnicas de identificação ou verificação que podem ser usadas por corporações e governos para fins de vigilância. Uma vigilância total pode funcionar, mas a que custo?

Acreditamos que existe uma forma melhor: o projeto Worldcoin está focado em criar tecnologias seguras que colocam os humanos no centro, permitindo que estes controlem e confiem nas suas experiências online, sem sacrificar a sua privacidade.

A Worldcoin é **privada por design.**

Como a IA apresenta riscos para a privacidade?

Já vimos coisas falsas a circular, sobre políticos e celebridades - pessoas para as quais há uma enorme quantidade de conteúdo online disponível para ser utilizado.

No entanto, com o avanço da IA, *deepfakes* - vídeos e áudios extremamente realistas - poderão em breve ser usados para imitar pessoas comuns. Estamos especialmente preocupados com o facto de a internet e os seus utilizadores não estão preparados para os desafios que a IA avançada irá trazer. Imagina estares numa chamada de Zoom com colegas que, na verdade, não são os teus colegas, ou entes queridos que nem sequer são pessoas reais. As pessoas podem ser facilmente enganadas para enviar dinheiro, revelar segredos ou coisas que ainda nem conseguimos imaginar.

Para combater o uso indevido da IA, as plataformas devem ser capazes de verificar se alguém é um humano único. Algumas ferramentas, como o “CAPTCHA”, já não são eficazes e dependem de dados vinculados à pegada digital de cada pessoa. O World ID é uma alternativa a interações digitais como os CAPTACHAs, mas que preserva a privacidade. Também serve como uma alternativa ao KYC e aos sistemas de identidade digital que revelam a identidade de um indivíduo ou ligam a sua identidade à sua atividade digital.

Princípios de Privacidade da Worldcoin

A comunidade da Worldcoin está a construir algo sem precedentes: uma rede globalmente confiável, totalmente inclusiva e que preserva a privacidade ao verificar a identidade humana. No entanto, a abordagem do projeto em relação à privacidade é contraintuitiva e inovadora, apresentando um caminho totalmente novo que nenhuma empresa, organização ou governo adotou:

A Worldcoin não quer saber quem és, apenas que és um ser humano único.

Bots alimentados por IA estão-se a tornar omnipresentes, com maior sofisticação, reduzindo a confiança online e imitando as pessoas. Ou seja, saber se estás a interagir com um humano ou com um bot é cada vez mais importante. Se a preocupação fosse unicamente comprovar a identidade online, a solução poderia parecer bastante simples: usar IDs emitidos pelo governo para verificar as nossas identidades e navegar online. Afinal de contas, frequentemente somos solicitados a mostrar um documento de identidade num banco. Não serão as transações online na era da IA potencialmente tão vulneráveis?

Deixando de lado o facto de que cerca de 850 milhões de pessoas não têm nenhum tipo de documento oficial e que os próprios governos têm realizado campanhas sofisticadas de desinformação online, a verificação por meio de identificações emitidas online pelo governo não é a solução. Isto revela muito mais informação sobre ti do que o necessário, como o teu endereço, e coloca-te em risco de teres a tua identidade roubada ou usada para fins nefastos, incluindo formas que nem conseguimos imaginar devido à IA.

Precisamos que a prova de identidade e a privacidade estejam no mesmo pacote (com o menor número possível de barreiras de entrada).

Este é o desafio que a Worldcoin procura resolver, e faz isto principalmente através do World ID. O World ID é um passaporte digital global que está armazenado localmente no smartphone do seu portador e permite que alguém prove que é uma pessoa única sem ter de compartilhar dados pessoais com ninguém.

É um sistema de verificação de humanidade para a internet, que permite às pessoas manterem o seu anonimato onde quer que estejam. Um World ID verificado não recolhe nem associa identificadores como o nome ou o e-mail, não está relacionado com dados de transações da carteira, nem revela a identidade de quem está a usar o World ID. Por design, a Worldcoin baseia-se no princípio da minimização de dados. Não armazena informações de identificação.

“Até agora, qualquer pessoa que desejasse provar a sua humanidade online usava meios como IDs emitidos pelo governo, que têm a desvantagem de identificar o utilizador e revelar uma grande quantidade de outros dados pessoais, mesmo que isso não seja necessário. Em contraste, o World ID permite uma ‘prova anónima de humanidade única’ e, assim, contrapõe o modelo de ‘capitalismo de vigilância’ com um modelo que promove a proteção de dados. O World ID fortalece as oportunidades para atividades online em conformidade com a proteção de dados.”

Dr. Stefan Brink, ex-Comissário da Proteção de Dados e Liberdade de Informação do Estado da Alemanha em Baden-Württemberg de janeiro de 2017 a dezembro de 2022.

Além disso, o World ID é construído para que as pessoas possam usá-lo em diferentes aplicações, sem que estas rastreiem a sua atividade. Não há um repositório central do histórico de utilização de uma para outra. Podes usar o World ID em centenas de aplicações diferentes sem nenhuma saiba sobre as restantes — ou o World ID saiba sobre essas aplicações.

A Worldcoin é privada por design e incorpora quatro princípios de privacidade, que estão interligados:

Princípio 1

Segurança: Protegida pela matemática

Princípio 2

Anonimato: Navega livremente online

Princípio 3

Escolha & Controlo: Os teus dados, as tuas regras

Princípio 4

Transparência: Construída de forma aberta

Princípio 1

Segurança: Protegido pela matemática

Sem segurança não há privacidade.

A Worldcoin visa permitir que as pessoas estejam online sem que as suas identidades sejam expostas e sobre capacitá-las a distinguir entre interações baseadas em bots e interações humanas. A segurança ajuda a garantir que esse nível de privacidade é alcançado — sempre, sem falhas.

O World ID usa muitas técnicas de segurança para garantir a segurança dos dados dos titulares do World ID.

Um conjunto engloba ferramentas humanas, como o código aberto e as auditorias (vê: Transparência), que ajudam a validar e a testar a robustez das medidas de segurança que foram criadas e implementadas como parte do projeto Worldcoin.

O outro conjunto inclui ferramentas criptográficas, como ZKPs e SMPC (vê: Anonimato), que utilizam matemática avançada para proteger dados, encriptá-los e mantê-los privados ou torná-los anónimos.

O SMPC é um dos poucos resultados na criptografia que pode fornecer um sigilo perfeito. Os ZKPs, por sua vez, utilizam hashes anuladores ("nullifier"), ou valores exclusivos, para cada aplicação, de modo a que o histórico de utilização das pessoas não possa ser rastreado.

Podes chamar-lhe **de segurança através da matemática**.

Princípio 2

?

Mas usar websites e apps não deveria envolver dar os nossos dados mais do que cozinhar o jantar envolve. As pessoas deveriam ser capazes de navegar livremente online.

Anonimato: Navega livremente online

Frequentemente, não precisamos de identificação apenas para existir no mundo. Cozinhar o jantar, ler um livro, dormir. Realizar estas atividades raramente requer que provemos quem somos. Na maior parte do tempo das nossas vidas as nossas ações passam despercebidas, não são observadas nem registadas. Somos anónimos.

A anonimidade é mais difícil de alcançar online. Os sites podem ver a nossa atividade, e os navegadores podem rastrear os nossos movimentos e comportamentos online. Esta vigilância torna-se potencialmente mais prejudicial quando nos é pedido que provemos quem somos, desde a monitorização do nosso endereço IP, numa escala mínima, até à autenticação com um documento de identificação emitido pelo governo, numa escala mais extrema.

Mas usar websites e aplicações não deveria implicar entregarmos os nossos dados, tal como cozinhar o jantar não o implica. As pessoas deveriam ser capazes de se **movimentar livremente online**. Iniciar sessão num site com um World ID permite isso.

Para manter o anonimato no mundo online, a Worldcoin utiliza várias tecnologias que preservam a privacidade, incluindo computação multipartidária segura (SMPC) e provas de conhecimento zero (ZKPs).

Computação Multipartidária Segura (SMPC)

Basta um smartphone para criar um World ID, mas provar que o titular é um ser humano único que não criou múltiplos World IDs — enquanto mantém a sua identidade privada — é um desafio complicado.

Os dados biométricos, quando devidamente anonimizados, fornecem a solução. A utilidade dos dados biométricos significa que devem ser recolhidos e utilizados de forma mínima e, quando é o único caminho viável, devem ser tratados com cuidado.

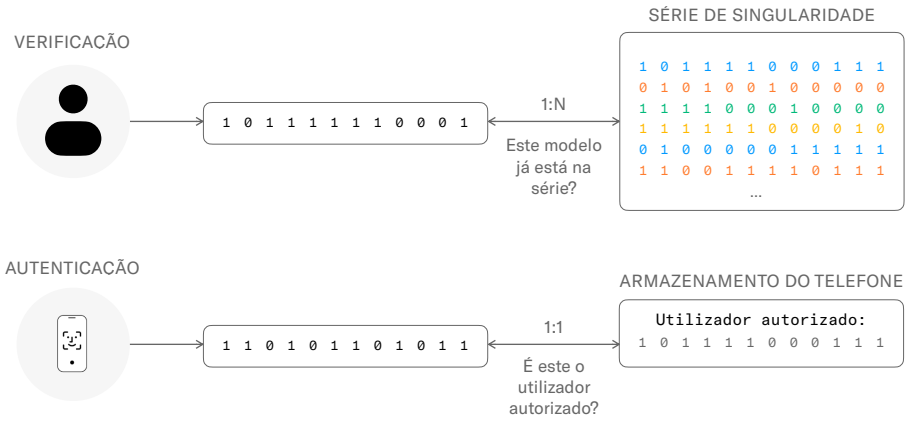
A Worldcoin faz isso através do SMPC.

Quando uma pessoa verifica o seu World ID através de uma orb, a orb tira fotografias da íris e do rosto. Utiliza estas imagens para criar um código de íris, que é essencialmente uma série de 1s e 0s. Nenhum código da íris é igual, nem revela identificadores diretos como o nome, o género, a idade, etc.

Este código da íris é dividido em diferentes partes e permanentemente encriptado usando SMPC, o que torna os dados anónimos ao dividi-los em múltiplos valores abstratos (partes SMPC) e armazená-los em locais separados, geridos por duas entidades juridicamente distintas. Num futuro próximo, serão adicionados parceiros de armazenamento adicionais (incluindo universidades e organizações sem fins lucrativos), o que significa que os códigos de íris serão divididos em ainda mais valores abstratos, armazenados e geridos por ainda mais entidades independentes. Nenhuma parte tem acesso a um código da íris completo. Cada uma só tem acesso à parte SMPC armazenada sob o seu controlo e gestão.

Embora armazenar os dados em múltiplos locais possa parecer que aumenta a probabilidade de esses dados serem roubados, na verdade o que acontece é o oposto. As partes SMPC são armazenadas de uma forma que, se um ator malicioso conseguisse, de alguma forma, aceder a uma parte SMPC, esta seria indecifrável; só fazem sentido quando todas as peças são reunidas.

Por que é que se armazena então as partes encriptadas do SMPC? Para que o protocolo Worldcoin possa continuar a provar que uma pessoa é única. Sem isso, os utilizadores precisariam de voltar a verificar o seu World ID sempre que uma aplicação o solicitasse.



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

Porquê a íris

As Orbs—câmaras especializadas—são os primeiros dispositivos de hardware a suportar o protocolo Worldcoin. Por agora, o único método para verificar um World ID como pertencente a um ser humano único é visitar uma Orb e tirar uma foto dos teus olhos.

A TFH estudou vários tipos de biometria para verificar os World IDs, cada uma com os seus próprios prós e contras. Para cumprir com os critérios a longo prazo, necessários para provar a humanidade de todos os indivíduos na Terra num mundo dominado pela IA, é necessário ser 1) preciso, 2) proteger a privacidade, 3) extremamente difícil de falsificar, 4) escalável, e 5) muito fácil de usar.

As impressões digitais são muito utilizadas, mas são fáceis de falsificar. A íris, por outro lado, é precisa, utilizável, escalável, amplamente inclusiva e extremamente difícil de falsificar. Além disso, protege a privacidade. Não existe um grande registo público da íris (como existe dos rostos nas redes sociais), não é possível fotografar de perto a íris de alguém sem que essa pessoa se aperceba, e é necessária uma câmara altamente especializada para sequer se tentar fazê-lo.

O protocolo Worldcoin é aberto e descentralizado, e mecanismos de verificação adicionais apenas reforçarão a atratividade e a segurança do projeto.

Provas de Conhecimento Zero (ZKPs)

Assim que uma pessoa tenha um World ID verificado, pode usá-lo para iniciar sessão e interagir com aplicações terceiras que integrem o protocolo World ID.

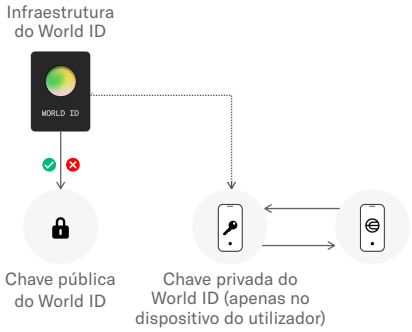
Mas isso não significa que as pessoas partilhem o seu World ID com essa outra aplicação.

Em vez disso, o World ID é usado para criar uma versão descartável de si mesmo, semelhante ao 'Ocultar o meu Email' da Apple ou a cartões de crédito virtuais. Imagina ter um cartão de crédito da empresa que só pode ser usado para uma única compra. Para pagar noutros fornecedores, seria necessário gerar cartões separados. Embora isso possa parecer oneroso, o protocolo faz isso de forma rápida e fluida nos bastidores, resultando num sistema seguro para as aplicações e que protege os utilizadores.

O método para fazer isso—de modo a que nem a Worldcoin nem as outras aplicações possam rastrear o histórico de utilização ou as partes envolvidas numa interação específica—é através de uma ZKP, uma ferramenta criptográfica que permite a alguém provar que algo é verdade sem revelar qualquer informação usada para chegar a essa conclusão.

Sempre que usares uma aplicação de terceiros, a aplicação pedirá uma prova ao teu dispositivo. Pensa nisto como fazer uma pergunta ao teu dispositivo. A aplicação quer saber: este dispositivo controla este World ID? A World App, no dispositivo do utilizador, envia uma ZKP que demonstra que o World ID está verificado.

As ZKPs vão muito além dos requisitos regulamentares de qualquer jurisdição. A Worldcoin implementou-as porque são a melhor forma de garantir que os utilizadores podem permanecer anónimos (a menos que o utilizador forneça informações adicionais diretamente à entidade terceira que solicitou a prova) e que as aplicações não podem rastreá-los. Elas impedem que terceiros—e até a própria Worldcoin Foundation—saibam o World ID de um utilizador, ou com que serviços eles interagem.



Uma analogia prática para ZKPs

As ZKPs são criptografia avançada, por isso não se prestam a analogias perfeitas. Mas, para entenderes o conceito básico, imagina um quebra-cabeças em que tens de encontrar um objeto ou pessoa específica numa cena.[2]

Depois de alguns minutos de procura, uma pessoa diz à outra que sabe onde está o objeto. A segunda pessoa, que não sabe onde está o objeto, não tem a certeza se deve acreditar.

Então, a primeira pessoa diz que o pode provar—sem simplesmente revelar onde o objeto está.

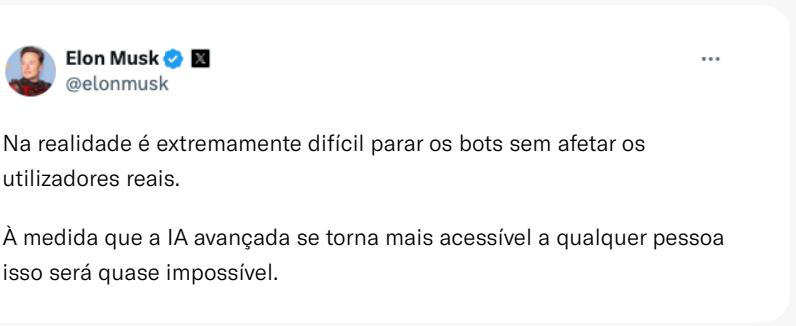
Ela fotocopia o quebra-cabeças completo, recorta o objeto e mostra-o à segunda pessoa, que agora está certa de que o objeto está no quebra-cabeças e que a primeira pessoa sabe onde ele está.

[2] Por exemplo, "Onde está o Wally?"

Neste cenário, a segunda pessoa é qualquer aplicação que tenta confirmar que um utilizador é humano; o objeto recortado é a ZKP; e a primeira pessoa é o protocolo Worldcoin, a provar que o utilizador é humano sem revelar a sua identidade.

Caso prático:
Bot ou humano na plataforma X?

O Elon Musk comprou o X (também conhecido como Twitter) prometendo eliminar bots da plataforma. No entanto, o novo proprietário rapidamente percebeu que isso era mais fácil dizer do que fazer. “É extremamente difícil parar os bots sem afetar os utilizadores reais,” escreveu Musk em dezembro de 2023. “À medida que a IA avançada se torna acessível a todos, será quase impossível.”



O Musk estava certo sobre o desafio que os bots representam para a plataforma social, mas agora existe uma solução viável para combatê-los sem afetar os utilizadores.

O X permite três modos de login: Entrar com o Google, Entrar com a Apple ou através de um nome de utilizador/palavra-passe. Para criar uma conta, os utilizadores são solicitados a fornecer o seu nome, o número de telemóvelou e-mail e a data de nascimento. Como é relativamente fácil criar vários endereços de e-mail, também é simples fazer várias contas no X. Assim, não há muitas barreiras para que bots entrem online, podendo degradar a experiência dos utilizadores humanos.

No entanto, o World ID não depende de endereços de e-mail, que são fáceis de criar, ou de números de telemóvel, que são simples de falsificar. Apenas humanos podem obter um World ID verificado e, ao contrário dos e-mails, são limitados a um único por pessoa. Portanto, se o X usasse o World ID como mecanismo de verificação de identidade, o serviço poderia adicionar um distintivo que indica que essas contas são de humanos verificados. Qualquer bot que tentasse entrar não conseguiria verificar-se.

O mais importante é que essa solução aumentaria até a anonimidade dos utilizadores do X, que não precisariam fornecer nenhuma informação adicional além da que já forneceram à plataforma.

Isso não é inteiramente teórico. A TFH criou uma integração do World ID com o Telegram para eliminar bots de spam na rede. Administradores de chats públicos podem exigir que contas individuais se verifiquem com o World ID antes de fazerem uma publicação num grupo.

Princípio 3

Escolha & Controlo:
Os teus dados, as tuas regras

As pessoas têm-se habituado cada vez mais ao paradigma das grande empresas de tecnologia, em que, em troca de acederem a um serviço, entregam os seus dados pessoais às empresas, para que estas os possam vender a quem pagar mais.[3]

A Worldcoin opera fora deste paradigma. Isto não é apenas uma promessa. A Worldcoin está a ser intencionalmente construida de uma forma que torna isso impossível de acontecer.

A abordagem da Worldcoin é: **Os teus dados, as tuas regras.**

Quantidade mínima de dados

O ponto de partida para garantir o controlo das pessoas sobre os seus dados é, desde logo, não pedir muitos dados. Como os World IDs verificadas são anónimos, as pessoas não fornecem o seu nome, número de telefone, endereço ou outras informações, que normalmente são capturadas por empresas de tecnologia. Pensa no seguinte: para obter um cartão da biblioteca, as pessoas precisam de uma prova de residência com um endereço. Para obter um World ID verificado, um passaporte digital global, só precisam de um smartphone e de visitar uma Orb.

Códigos de
desconto no Shopify

O Shopify é uma plataforma de comércio eletrónico para empresas que procuram aumentar as vendas e permitir pagamentos online. Os comerciantes na plataforma, por vezes, tentam atrair novos clientes emitindo descontos de utilização única.

O problema é que as pessoas podem manipular o sistema criando e-mails falsos e reivindicando o desconto várias vezes—ou utilizando bots para fazer isso por elas. Em vez de atrair novos clientes, os vendedores acabam por subsidiar uma fraude.

Ao integrarem o World ID na sua loja, os comerciantes podem permitir que clientes reais scaneiem um código QR que verifica o seu World ID e aplica um código de desconto. Este método garante um desconto por pessoa, resolvendo o problema dos comerciantes, sem pedir ao utilizador que forneça qualquer informação adicional. (Embora, para finalizar a compra, ainda tenham de fornecer os dados do cartão de crédito e de envio!)

[3] Literalmente! Para mais informações, consulta https://en.wikipedia.org/wiki/Real-time_bidding

Custódia Pessoal

O processo de verificação de um World ID requer o uso de alguns dados, como imagens biométricas e códigos da íris. Após passarem pelo SMPC, os códigos da íris são armazenados em servidores de forma totalmente anónima. No entanto, os dados fornecidos pelo utilizador para verificar a identidade através da Orb não são mantidos nem fornecidos a terceiros. Em vez disso, ficam únicamente no smartphone da pessoa, onde estão encriptados com a chave pública individual.

Com a Custódia Pessoal Worldcoin, as pessoas têm controlo sobre os dados recolhidos e gerados durante a verificação—incluindo o World ID e as imagens—e decidem com quem partilhar essas informações.

Autenticação Facial

Ao instituir o World ID, as plataformas podem proteger-se contra bots sem invadir a privacidade dos seus clientes. Um World ID verificado oferece a essas plataformas um elevado nível de confiança de que o utilizador é, de facto, uma pessoa.

Mas em alguns cenários de alto risco (por exemplo, transações financeiras), as plataformas ou as pessoas precisam de saber não apenas que estão a lidar com um ser humano, mas também que estão a lidar com uma pessoa específica. Querem garantir que a pessoa que está a usar o World ID é a mesma pessoa única que verificou o World ID nesse dispositivo.

Para alcançar isso, as aplicações na Worldcoin podem utilizar a Autenticação Facial.

A autenticação facial é um método que compara a imagem capturada durante a verificação com uma imagem da pessoa que procura usar o World ID, e é independente do dispositivo.

A primeira imagem é gerada quando uma pessoa verifica o seu World ID numa Orb. Por padrão, o telemóvel do utilizador é o único lugar onde esses dados existem. As fotos de alta resolução são encriptadas e enviadas com segurança para o telemóvel do utilizador, como parte da Custódia Pessoal, sendo completamente apagadas da Orb.

A segunda imagem é uma selfie tirada no dispositivo do utilizador dentro da World App, quando este tenta aceder ou usar o seu World ID. A Autenticação Facial para o World ID compara esta imagem com a imagem original de autenticação facial tirada durante a verificação na Orb. O utilizador só pode prosseguir com o login ou a transação se as duas imagens coincidirem.

Isto previne fraudes, ao defender contra um ator malicioso que rouba (ou compra) o telemóvel de alguém e tenta usar o World ID dessa pessoa. Com a Autenticação Facial, o utilizador legítimo está sempre no controlo dos seus dados e do seu World ID. **A comparação é feita localmente no dispositivo do utilizador.** Como resultado, nem a selfie, nem a foto tirada pela Orb, nem quaisquer outros dados pessoais são partilhados com terceiros, incluindo a Tools for Humanity ou a Worldcoin Foundation.[4]

[4] No futuro, o projeto permitirá que as pessoas optem por partilhar voluntariamente as suas informações com a Worldcoin, para ajudar na segurança e no treino da IA. Esta opção será 100% voluntária, e a permissão poderá ser revogada a qualquer momento.

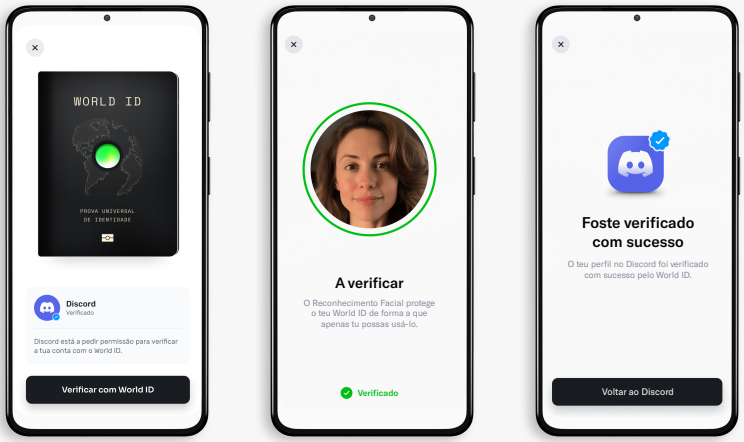
Autenticação Facial comparado com o Face ID

Para os utilizadores, a Autenticação Facial irá parecer o Face ID da Apple.

Assim sendo, porque não usar simplesmente o Face ID?

A Autenticação Facial garante que a pessoa a usar a World App é a mesma que criou o respetivo World ID numa Orb. O Face ID da Apple não permite esta capacidade, pois a Autenticação Facial foca-se na correspondência direta com a verificação original feita na Orb, garantindo que o utilizador é único e autenticado de forma anónima e segura.

O Face ID é uma combinação de hardware e software, o que o liga diretamente a um iPhone. Com o Face ID, os utilizadores podem ter um rosto diferente associado ao dispositivo em comparação com aquele utilizado para verificar o World ID, aumentando o risco de fraude. Ao utilizar o World ID, que funciona ao nível da aplicação, e não do dispositivo, a Autenticação Facial garante que apenas a pessoa que verificou o World ID pode aceder a ele, evitando assim o uso indevido.



Princípio 4

Transparência: Construída de forma aberta

Os especialistas em segurança são naturalmente céticos, procurando perigos em cada linha de código. E isso é algo positivo, pois é assim que nos mantêm seguros.

Seria impensável imaginar que apenas a TFH ou alguns programadores da Worldcoin pudessem antecipar todas as possíveis falhas do protocolo. Por isso, a Worldcoin é **construída de forma clara.**

Auditado

A Worldcoin incorpora o maior número possível de opiniões externas e áreas de especialização. Criptógrafos e especialistas em biometria estão continuamente a avaliar o código-fonte, assim como auditores de segurança e consultores procuram a menor possibilidade de vulnerabilidade. A Worldcoin publica, posteriormente, os resultados—e o que fez para resolver até os mais pequenos problemas.

Para identificar possíveis vulnerabilidades, também temos de compreender como o protocolo pode ser utilizado no mundo real—agora e no futuro. Isso implica pensar em milhares de realidades culturais em todo o mundo e incorporar essas considerações num modelo de segurança que proteja contra abusos que possam nem sequer existir ainda.

A partir de abril de 2023, as empresas de auditoria Nethermind e Least Authority irão conduzir duas auditorias de segurança do protocolo Worldcoin em separado. Especificamente, as auditorias irão cobrir as seguintes áreas:

- Correção da implementação, incluindo as construções criptográficas e primitivas e a utilização apropriada da construção de contratos inteligentes
- Erros de implementação comuns e específicos do caso
- Ações adversas e outros ataques ao código
- Armazenamento seguro e gestão adequada de chaves de criptografia e assinatura
- Exposição de qualquer informação crítifca durante as interações do utilizador
- Resistência a DDoS (ataque distribuído de negação do serviço) e ataques semelhantes
- Vulnerabilidades no código que levam a ações adversas e outros ataques
- Proteção contra ataques maliciosos e outros métodos de exploração
- Problemas de desempenho e outros potenciais impactos no desempenho
- Privacidade dos dados, fuga de dados e integridade da informação
- Permissões inapropriadas, aumento de privilégios e autoridade excessiva

Código Aberto e Sem Permissões

Tornar o código da Worldcoin um código aberto e sem permissões ajuda a cumprir três objetivos. Primeiro, expõe a rede a críticas que podem melhorar o seu funcionamento.

Em segundo lugar, permite que os programadores se sintam confiantes ao construir sobre o protocolo da Worldcoin. É possível que outras equipas criem uma aplicação de prova de identidade baseada no World ID, ou encontrem um método de verificação ainda mais prático do que a Orb.

Por fim, ser de código aberto e sem permissões é essencial para um projeto descentralizado: qualquer pessoa pode criar a sua própria versão (ou “fork”) do protocolo a qualquer momento, por qualquer motivo—e isso é uma coisa boa.


WORLDCOIN