WORLDCOIN

Privada por Definição

Conteúdo

Ecossistema

O projeto Worldcoin consiste em vários atores e ferramentas que se combinam para formar uma rede de identidade que prioriza o ser humano e que proporciona confiança ao realizar transações ou se comunicar online.

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

O **World ID** é um protocolo de identidade descentralizado que comprova que você é uma pessoa única. Ele pode ser utilizado para provar sua humanidade em várias atividades online, como autenticação de vídeos e proteção contra deepfakes. Também pode ser usado para fazer login em sites e aplicativos, de maneira similar ao "Entrar com o Google", comprovando que você é um ser humano único, mas sem compartilhar dados pessoais como nome, e-mail ou número de telefone.

O **World Chain** é uma solução de segunda camada na rede Ethereum, que será lançado em breve, que usa o World ID para priorizar as transações feitas por humanos em relação aos robôs..

O **WLD** é o token da Worldcoin, distribuído gratuitamente para indivíduos que comprovam sua humanidade e fazem parte da rede Worldcoin.[1]

A **Worldcoin Foundation** é uma organização sem fins lucrativos que atua como administradora do protocolo Worldcoin. Ela também é proprietária e governa a maioria dos ativos relacionados à marca Worldcoin, incluindo propriedade intelectual para a orb e a tecnologia de código aberto do protocolo.

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

Uma **orb** é uma câmera especial que verifica as características únicas de um humano e fornece a você os dados para confirmar seu status de pessoa com o uso do World ID.

O **World App** é uma carteira de autocustódia da Worldcoin que fornece um lugar para o World ID. Com o app, você também pode enviar e receber tokens Worldcoin (WLD) 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 agência de aplicação da lei da União Europeia, Europol, sugeriu que até 90% do conteúdo da Internet poderia ser gerado sinteticamente até 2026.

Catfishing. Bots. Deepfakes. Roubo de identidade. Desinformação. A internet pode ser um lugar perigoso. O avanço da IA aumentará a eficiência digital, mas precisamos ter clareza sobre seu potencial de amplificar problemas existentes. Já vimos o que pode dar errado quando um humano finge ser outra pessoa. O que acontece quando achamos que estamos lidando com um humano que na verdade é um agente da IA?

O que precisamos é de uma maneira de verificar se as pessoas com quem falamos, enviamos dinheiro e de quem visualizamos conteúdo online (para citar apenas alguns exemplos) são realmente pessoas. A Worldcoin visa dar a você controle sobre cada um desses elementos na era da IA.

Evitar que a IA inunde a internet com pessoas falsas requer uma segurança extraordinária. No entanto, muitas das abordagens previstas para lidar com isso são autoritárias. Há uma tentação de recorrer às mesmas ferramentas antigas — remover a privacidade e confiar em técnicas de identificação ou verificação que podem ser aproveitadas para vigilância corporativa e governamental. Um panóptico pode funcionar, mas a que custo?

Acreditamos que há uma maneira melhor: o projeto Worldcoin é sobre criar tecnologias seguras que colocam os humanos no centro, permitindo que eles vivam suas experiências online sem abrir mão de sua privacidade.

A Worldcoin é **privada por definição**.

Como a IA representa riscos à privacidade

Já vimos deepfakes de políticos e celebridades circulando — pessoas para as quais há uma grande quantidade de conteúdo online disponível.

Mas a IA avançada significa que os deepfakes — vídeos e áudios extremamente realistas — em breve poderão ser usados para imitar pessoas comuns. Estamos especialmente preocupados com o fato de que a internet e seus usuários não estão preparados para os desafios que a IA avançada trará. Imagine estar em uma chamada no Zoom com colegas que na verdade não são seus colegas ou com pessoas queridas que não são pessoas reais. As pessoas podem ser facilmente enganadas para enviar dinheiro, divulgar segredos ou fazer coisas que ainda nem conseguimos imaginar.

Para combater o uso malicioso da IA, as plataformas precisam ser capazes de reconhecer se uma pessoa é um ser humano único. Ferramentas como o "CAPTCHA" não são mais eficazes e dependem de dados atrelados à pegada digital de alguém. O World ID é uma alternativa que preserva a privacidade nas interações digitais, como o CAPTCHA. Ele também serve como alternativa ao KYC e aos sistemas de identificação digital que revelam a identidade de um indivíduo ou vinculam a identidade de uma pessoa à sua atividade digital.

Princípios de Privacidade da Worldcoin

A comunidade Worldcoin está construindo algo sem precedentes: uma rede globalmente confiável, maximamente inclusiva e que preserva a privacidade com prova de humanidade. Mas a abordagem do projeto em relação à privacidade é contraintuitiva e inovadora, apresentando um caminho fundamentalmente novo que nenhuma empresa, organização ou governo seguiu:

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

Bots alimentados por IA estão se tornando mais comuns, aumentando sua sofisticação, minando a confiança online e se passando por pessoas. Portanto, saber se você está interagindo com um humano ou um bot está se tornando cada vez mais importante. Se comprovar a condição de pessoa online fosse nossa única preocupação, a solução pareceria relativamente simples: usar documentos de identidade emitidos pelo governo para verificar nossa identidade e navegar online. Afinal, muitas vezes somos solicitados a mostrar um documento de identidade no banco. As transações online na era da IA não são potencialmente tão sensíveis quanto?

Deixando de lado o fato de que cerca de 850 milhões de pessoas não têm nenhuma forma de documento oficial e que os próprios governos já implementaram campanhas sofisticadas de desinformação online, a verificação via documentos de identidade emitidos pelo governo não é a solução. Isso revela muito mais sobre você do que o necessário, como o seu endereço, e coloca você em risco de ter sua identidade roubada ou usada para fins perversos, incluindo maneiras que ainda não conseguimos imaginar por causa da IA.

Precisamos de comprovação de humanidade e privacidade no mesmo pacote (com o menor número de barreiras de entrada possível).

Esse é o desafio que a Worldcoin busca resolver, e o faz principalmente por meio do World ID. O World ID é um passaporte digital global que fica localmente no smartphone de seu portador e permite que alguém prove que é uma pessoa única sem compartilhar dados pessoais com ninguém.

É um sistema de verificação de humanidade para a internet que permite que as pessoas fiquem anônimas onde quer que estejam. Um World ID verificado não coleta nem vincula a identificadores como nome ou e-mail, não se liga a dados de transações de carteiras digitais, nem revela de quem é o World ID sendo usado. Por design, a Worldcoin é baseada no princípio da minimização de dados. Ela não armazena informações identificáveis.

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

Dr. Stefan Brink, ex-Comissário de 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 foi construído de forma que as pessoas possam usá-lo em diferentes aplicativos sem que esses apps rastreiem suas atividades de um para o outro. Não há um repositório central de histórico de uso. Você pode usar o World ID em centenas de aplicativos diferentes sem que um saiba sobre os outros — nem que o World ID saiba sobre esses aplicativos.

A Worldcoin é privada por definição e incorpora quatro princípios de privacidade interligados:

Princípio 1

Segurança: Protegido matematicamente

Princípio 2

Anonimato: Navegue livremente online

Princípio 3

Escolha e Controle: Seus dados, suas regras

Princípio 4

Transparência: Construído de forma aberta

Princípio 1

Segurança: Protegido matematicamente

Sem segurança, não há privacidade.

A Worldcoin tem como objetivo permitir que as pessoas estejam online sem que suas identidades sejam expostas e empoderá-las a distinguir entre as interações baseadas em bots e interações com humanos. A segurança ajuda a garantir que esse nível de privacidade seja alcançado — sempre, sem falhas.

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

O conjunto envolve ferramentas humanas, como código aberto e auditorias (veja: Transparência), que ajudam a validar e testar as medidas de segurança que foram criadas e implementadas como parte do projeto Worldcoin.

O outro conjunto inclui ferramentas criptográficas, como ZKPs e SMPC (veja: Anonimato), que usam matemática avançada para proteger dados, criptografá-los e mantê-los privados ou torná-los anônimos.

A SMPC é um dos poucos resultados em criptografia que pode fornecer sigilo perfeito. Os ZKPs, por sua vez, usam hashes anuladores, ou valores exclusivos, para cada aplicativo, para que o histórico de uso das pessoas não possa ser rastreado.

Você pode chamar isso de **protegido pela matemática**.

Princípio 2

?

Mas usar sites e aplicativos não deveria envolver fornecer nossos dados mais do que ao preparar o jantar. As pessoas deveriam poder navegar livremente online.

Anonimato: Navegue livremente online

Na maioria das vezes, não precisamos de identificação para apenas existir. Preparar o jantar, ler um livro, dormir. Realizar essas atividades raramente exige provar quem somos nós. Na maior parte de nossas vidas, nossas ações passam despercebidas, não observadas e não registradas. Somos anônimos.

O anonimato é mais difícil de se obter online. Os sites podem visualizar nossas atividades, e os navegadores podem rastrear nossos movimentos e comportamentos na internet. Essa vigilância se torna potencialmente mais prejudicial quando somos solicitados a provar quem somos, indo desde o monitoramento do nosso endereço de IP em um nível básico até a autenticação com documento de identidade emitido pelo governo em casos extremos.

Mas usar sites e aplicativos não deveria implicar em ceder nossos dados mais do que fazemos ao preparar o jantar. As pessoas deveriam poder **navegar livremente pela internet**. Fazer login em um site com um World ID permite que isso aconteça.

Para manter o anonimato no mundo digital, a Worldcoin utiliza várias tecnologias que preservam a privacidade, incluindo a 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 humano único, que não criou vários World IDs, mantendo sua identidade privada, é um desafio complexo.

Dados biométricos, quando devidamente anonimizados, oferecem a solução. A própria utilidade dos dados biométricos significa que eles devem ser coletados e usados minimamente, e, quando for o único caminho viável, devem ser tratados com cuidado.

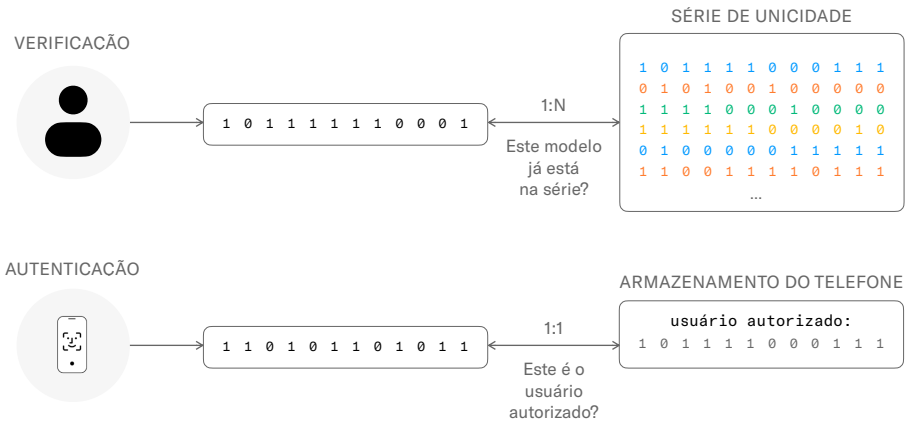
A Worldcoin faz isso por meio da SMPC.

Quando uma pessoa verifica seu World ID por meio de uma orb, a orb tira fotos da íris e do rosto. Ela usa essas fotos para criar um código de íris, que é essencialmente uma série de 1s e 0s. Nenhum código de íris é igual ao outro, nem revela identificadores diretos como nome, gênero, idade, etc.

Esse código de íris é dividido em diferentes partes e permanentemente criptografado usando SMPC, que torna os dados anônimos dividindo-os em vários valores abstratos (porções da SMPC) e armazenando-os em locais separados, geridos por duas entidades legalmente distintas. Em breve, serão adicionados parceiros de armazenamento adicionais (incluindo universidades e ONGs), o que significa que os códigos de íris serão divididos em ainda mais valores abstratos armazenados e geridos por mais entidades independentes. Nenhuma parte tem acesso a um código de íris completo. Elas têm apenas acesso à porção da SMPC sob seu controle e gerenciamento.

Embora armazenar os dados em vários locais aparentemente aumente a probabilidade de esses dados serem roubados, o oposto é verdadeiro. As porções da SMPC são armazenadas de forma que, se um ator mal-intencionado conseguisse acesso a uma única porção da SMPC, ela seria indecifrável; elas só fazem sentido quando todas as suas partes são reunidas.

Por que armazenar as porções criptografadas da SMPC? Para que o protocolo Worldcoin possa continuar provando que uma pessoa é única. Sem isso, os usuários precisariam verificar novamente seu World ID toda vez que um aplicativo o solicitasse.



As fotos em si também não permanecem na orb. Em vez disso, a orb criptografa os dados de ponta a ponta com uma chave pública fornecida pelo smartphone do usuário (somente o usuário tem a chave privada para descriptografar) e, em seguida, a orb transmite as fotos criptografadas para o dispositivo do usuário antes de apagá-las da orb. Tudo isso acontece em questão de segundos durante o processo de verificação.

Por que a íris?

Orbs—câmeras avançadas—são os primeiros dispositivos de hardware a suportar o protocolo Worldcoin. Por enquanto, o único método para verificar se um World ID pertence a um ser humano único é visitar uma orb e tirar uma foto dos seus olhos.

A TFH estudou diversos tipos de biometria para verificar os World IDs, cada uma com seus prós e contras. Para atender aos critérios necessários de comprovação futura para garantir a humanidade de todos os indivíduos na Terra em um mundo tomado pela IA, qualquer método precisa ser: 1) preciso, 2) preservar a privacidade, 3) extremamente difícil de falsificar, 4) escalável e 5) muito fácil de usar.

Impressões digitais são muito úteis, mas fáceis de falsificar. Já as íris são precisas, úteis, escaláveis, amplamente inclusivas e extremamente difíceis de falsificar. Além disso, preservam a privacidade. Não existe um grande registro público de íris (como os rostos nas redes sociais), não é possível fotografar de perto a íris de alguém sem que essa pessoa perceba, e é necessário um equipamento especializado até mesmo para tentar fazer isso.

O protocolo Worldcoin é aberto e descentralizado, e mecanismos de verificação adicionais apenas fortalecerão o apelo e a segurança do projeto.

Provas de conhecimento zero (ZKPs)

Uma vez que uma pessoa tenha um World ID verificado, ela pode usá-la para fazer login e realizar transações com apps de terceiros que integram o protocolo World ID.

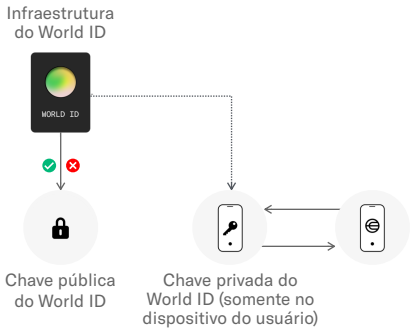
Mas isso não significa que as pessoas compartilham seu World ID com o app de terceiros.

Em vez disso, o World ID é usado para criar uma versão descartável de si mesma, semelhante ao Ocultar meu E-mail da Apple ou cartões de crédito virtuais. Imagine ter um cartão de crédito corporativo que só pode ser usado para uma compra. Para pagar outros fornecedores, seria necessário gerar cartões separados. Embora isso possa parecer trabalhoso, o protocolo faz isso de forma rápida e transparente nos bastidores, resultando em um sistema seguro para os aplicativos e que protege os usuários.

O método para fazer isso — de forma que nem a Worldcoin nem os aplicativos possam rastrear o histórico de uso entre apps ou as partes envolvidas em uma determinada transação — é um ZKP, uma ferramenta criptográfica que permite a alguém provar que algo é verdadeiro sem revelar qualquer informação usada para chegar a essa conclusão.

Sempre que você usa um aplicativo de terceiros, o aplicativo solicitará uma comprovação do seu dispositivo. Pense nisso como se estivesse fazendo uma pergunta ao seu dispositivo: este dispositivo controla este World ID? O World App no dispositivo do usuário envia de volta um ZKP que demonstra que o World ID está verificado.

Os ZKPs vão muito além dos requisitos regulatórios de qualquer jurisdição. A Worldcoin os implementou porque são a melhor forma de garantir que os usuários possam permanecer anônimos (a menos que forneçam informações adicionais diretamente ao serviço de terceiros que solicita a prova) e que os aplicativos não possam rastreá-los. Eles impedem que terceiros — e até mesmo a própria Worldcoin Foundation — saibam a World ID de um usuário ou quais serviços ele utiliza.



Uma analogia prática para os ZKPs

Os ZKPs são uma criptografia avançada, portanto, analogias perfeitas são difíceis. Mas, para entender a ideia básica, imagine um quebra-cabeça em que você tem que encontrar um objeto ou pessoa específicos dentro de uma cena.[2]

Depois de procurar por alguns minutos, uma pessoa diz à outra que sabe onde está o item. A segunda pessoa, que não sabe onde está o item, não tem certeza se deve acreditar nisso.

Então, a primeira pessoa diz que pode provar isso—sem mesmo revelar onde está o item.

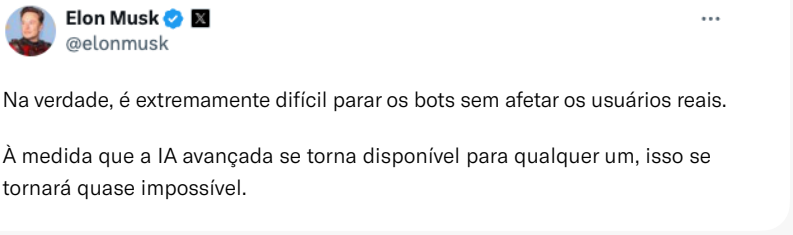
[2] Ex., "Onde está o Waldo/Wally?"

Ela faz uma fotocópia do quebra-cabeça completo, recorta o item e o mostra para a segunda pessoa, que agora tem certeza de que o item está no quebra-cabeça e que a primeira pessoa sabe onde ele está.

Nesse cenário, a segunda pessoa é qualquer aplicativo tentando confirmar que um usuário é humano; o item recortado é o ZKP; e a primeira pessoa é o protocolo Worldcoin provando que o usuário é humano sem revelar sua identidade.

Caso de uso:
X bot ou humano?

Elon Musk comprou o X (antigo Twitter) prometendo eliminar os bots da plataforma. Mas o novo proprietário rapidamente percebeu que era mais fácil de falar do que de fazer isso. “É extremamente difícil parar os bots sem afetar os usuários reais,” escreveu Musk em dezembro de 2023. “À medida que a IA avançada se torna disponível para qualquer pessoa, será quase impossível.”



Musk estava certo sobre o desafio que os bots apresentavam para a plataforma social. Mas agora há uma solução viável para combatê-los sem afetar os usuários.

O X permite três modos de login: Entrar com o Google, Entrar com a Apple ou usar um nome de usuário/senha. Para criar uma conta, os usuários são solicitados a fornecer seu nome, telefone ou e-mail e data de nascimento. Como é relativamente fácil criar vários endereços de e-mail, também é bastante simples criar várias contas no X. Assim, não há muita barreira para os bots entrarem, o que pode degradar a experiência do usuário para os humanos.

No entanto, o World ID não depende de endereços de e-mail, que são fáceis de criar, ou números de telefone, que são simples de falsificar. Apenas humanos podem obter um World ID verificado — e, ao contrário dos e-mails, eles são limitados a um único ID. Assim, se o X passasse a usar o World ID como seu mecanismo de verificação de status de pessoa, o serviço poderia adicionar um selo que denote que tais contas foram verificadas como humanas. Quaisquer bots que se conectassem não seriam capazes de se verificar.

Importante, fazer isso até aumentaria a anonimidade para os usuários do X, que não precisariam fornecer informações adicionais além das que já foram fornecidas ao X.

Isso não é inteiramente teórico. A TFH criou uma integração do World ID com o Telegram para se livrar dos bots de spam na rede. Os administradores de chats públicos podem exigir que contas individuais se verifiquem com o World ID antes de postar em um grupo.

Princípio 3

Escolha e Controle: Seus dados, suas regras

As pessoas estão cada vez mais acostumadas ao paradigma das Big Techs em que, em troca do acesso a serviços, elas entregam seus dados pessoais a corporações para que eles possam ser vendidos ao maior lance.[3]

A Worldcoin opera fora desse paradigma. Isso não é apenas uma promessa. A Worldcoin está sendo intencionalmente projetada para tornar essa prática impossível.

A abordagem do projeto Worldcoin é: **Seus dados, suas regras.**

Mínimo de dados

O ponto de partida para reconhecer o controle das pessoas sobre seus dados é não pedir muitos dados desde o início. Como os World IDs verificados são anônimos, as pessoas não fornecem seu nome, número de telefone, endereço ou outras informações comumente capturadas por empresas de tecnologia. Pense nisso: para obter um cartão de biblioteca, as pessoas precisam de um comprovante de residência com um endereço. Para obter um World ID verificado, um passaporte digital global, elas só precisam de um smartphone e uma visita à uma orb.

Caso de uso:
Códigos de desconto do Shopify

A Shopify é uma plataforma de comércio eletrônico para empresas que buscam aumentar suas vendas e gerenciar pagamentos online. Os vendedores na plataforma às vezes buscam atrair novos clientes oferecendo descontos únicos.

O problema é que as pessoas podem manipular o sistema criando e-mails falsos e reivindicando descontos múltiplas vezes — ou usando bots para fazer isso por elas. Em vez de atrair novos clientes, os vendedores acabam subsidiando um golpe.

Ao integrar o World ID em suas lojas, os vendedores podem permitir que clientes reais leiam um código QR que verifica seu World ID e aplica um código de desconto. Esse método garante um desconto por pessoa, resolvendo o problema dos comerciantes sem exigir que o usuário forneça informações adicionais. (Embora eles precisem fornecer os dados do cartão de crédito e de envio para finalizar a compra!)

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

Custódia Pessoal

O processo de verificação de um World ID requer o uso de alguns dados, a saber, imagens biométricas e códigos de íris. Os códigos de íris, após passarem pela SMPC, vão para servidores onde residem em um formato totalmente anonimizado. Mas os dados fornecidos pelo usuário para verificar a identidade por meio da orb não são retidos nem fornecidos a terceiros. Em vez disso, eles permanecem apenas no smartphone da pessoa, onde são criptografados com a chave pública do indivíduo.

Com a Custódia Pessoal Worldcoin, as pessoas controlam os dados coletados e gerados durante a verificação — incluindo o World ID e as imagens — e decidem com quem compartilhá-los.

Autenticação Facial

Ao instituir o World ID, as plataformas podem se proteger contra bots sem invadir a privacidade de seus clientes. Um World ID verificado fornece a essas plataformas um alto nível de confiança de que um usuário é realmente uma pessoa.

Mas em alguns cenários de alto risco (por exemplo, transações financeiras), quando as plataformas ou pessoas precisam saber não apenas que estão lidando com uma pessoa, mas que estão lidando com uma pessoa específica. Eles querem ter certeza de que a pessoa usando o World ID é o mesmo ser humano único que verificou o World ID naquele dispositivo.

Para fazer isso, os aplicativos na Worldcoin podem usar a Autenticação Facial.

A Autenticação Facial é um método para comparar a imagem tirada durante a verificação com uma imagem da pessoa que deseja usar o World ID e é independente do dispositivo.

A primeira imagem é gerada quando uma pessoa verifica seu World ID em uma orb. O telefone do usuário é, por padrão, o único lugar onde esses dados existem. Essas fotos de alta resolução são criptografadas, enviadas com segurança para o telefone do usuário como parte da Custódia Pessoal e completamente deletadas da orb.

A segunda imagem é uma selfie tirada no dispositivo do usuário dentro do World App quando o usuário busca acessar ou usar seu World ID. A Autenticação Facial para o World ID compara a imagem tirada pelo dispositivo do usuário com a imagem original de autenticação facial tirada durante a verificação na orb. O usuário só pode continuar com o login ou a transação se as duas imagens corresponderem.

Isso previne fraudes ao proteger contra um agente mal-intencionado que rouba (ou compra) o telefone de alguém e tenta usar seu World ID. Com a Autenticação Facial, o usuário legítimo está sempre no controle de seus dados e de seu World ID. **A comparação é feita localmente no dispositivo da pessoa**. Como resultado, nem a selfie, nem a foto tirada na orb, nem qualquer outro dado pessoal são compartilhados com terceiros, incluindo a Tools for Humanity ou a Worldcoin Foundation.[4]

[4] No futuro, o projeto permitirá que as pessoas optem por compartilhar voluntariamente suas informações com a Worldcoin para auxiliar na segurança e no treinamento da IA. Isso é 100% opcional, e a permissão pode ser revogada a qualquer momento.

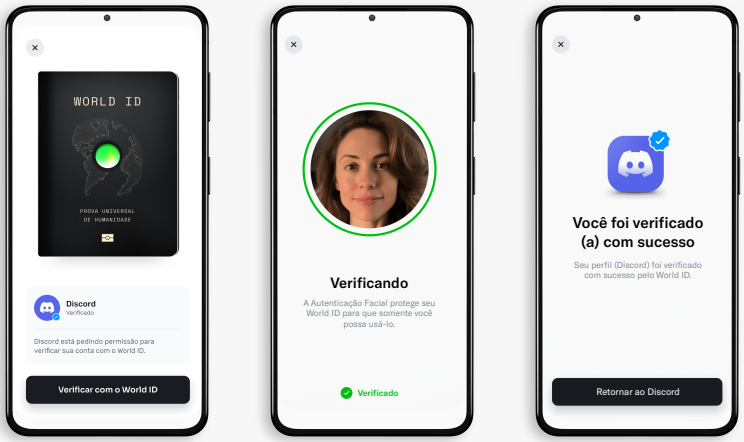
Autenticação Facial comparada ao Face ID

Para os usuários, a Autenticação Facial será tão reconhecível quanto o Face ID da Apple.

Então, por que não usar o Face ID?

A Autenticação Facial garante que a pessoa usando o World App é a mesma pessoa que criou o World ID associado na orb. O Face ID não tem essa capacidade.

O Face ID é uma combinação de hardware e software, portanto, está vinculado a um iPhone. Com o Face ID, os usuários poderiam ter um rosto diferente associado ao dispositivo daquele que usaram para verificar o World ID, o que aumenta o potencial para fraudes. Ao usar o World ID, que está no nível do aplicativo em vez do nível do dispositivo, a Autenticação Facial impede que qualquer pessoa além da pessoa que verificou o World ID tenha acesso a ele.



Princípio 4

Transparência: Construído em aberto

Especialistas em segurança são bastante céticos, procurando perigos em cada linha de código-fonte. E isso é uma coisa boa, é assim que eles nos mantêm seguros.

Seria inimaginável pensar que a TFH ou alguns desenvolvedores da Worldcoin poderiam prever todas as possíveis falhas no protocolo. Por isso, a Worldcoin é **desenvolvida de forma aberta**.

Auditado

A Worldcoin incorpora o maior número possível de opiniões externas e áreas de especialização. Criptógrafos e especialistas em biometria estão continuamente avaliando o código-fonte, enquanto auditores de segurança e consultores tentam encontrar a menor possibilidade de vulnerabilidade. A Worldcoin então publica os resultados — e o que fez para resolver até mesmo os menores problemas

Para identificar possíveis brechas, também precisamos entender como o protocolo pode ser usado no mundo real — agora e no futuro. Isso significa pensar em milhares de realidades culturais ao redor do globo e incorporar essas considerações em um modelo de segurança que proteja contra usos indevidos que nem existem ainda.

A partir de abril de 2023, as empresas de auditoria Nethermind e Least Authority conduziram duas auditorias de segurança separadas do protocolo Worldcoin. Especificamente, as auditorias cobriram as seguintes áreas:

- Correção da implementação, incluindo construções criptográficas e primitivas e uso apropriado de construções de contrato inteligente
- Erros de implementação comuns e específicos do caso
- Ações adversas e outros ataques ao código
- Armazenamento seguro de chaves e gerenciamento adequado de chaves de criptografia e assinatura
- Exposição de qualquer informação crítica durante as interações do usuário
- Resistência a DDoS (ataque distribuído de negação de 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 ou outros impactos potenciais no desempenho
- Privacidade de dados, vazamento de dados e integridade das informações
- Permissões inadequadas, escalonamento de privilégios e excesso de autoridade

De Código Aberto e Sem Permissão

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

Segundo, permite que os desenvolvedores se sintam confiantes ao construir sobre o protocolo Worldcoin. É possível que outras equipes criem um aplicativo de comprovação de humanidade baseado no World ID ou encontrem um método de verificação ainda mais utilizável do que a orb.

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


WORLDCOIN