

월드코인(Worldcoin)

해당 번역본은 이용자가 디지털자산 관련 정보를 편리하게 확인할 수 있도록
단순 참고용으로 번역된 것이며, 투자 권유를 목적으로 하지 않습니다.
그 내용이 정확하지 않을 수 있으므로 정확한 정보 습득을 위해서는
원문을 참고하시거나 원문 작성 주체 측에 문의하시기 바랍니다.
두나무는 해당 번역본 내용의 진실성 및 정확성을 보장하지 않고,
제공된 정보에 의한 투자 결과에 대하여 어떠한 책임도 지지 않으며,
투자 손실은 투자자에게 귀속됩니다.

새로운 정체성과 금융 네트워크

면책 고지 (Disclaimer)

이 암호자산 백서는 유럽연합의 어떤 회원국에서도 관할 당국의 승인을 받지 않았습니다. 거래 상장을 신청하는 자는 이 암호자산 백서의 내용에 대해 전적으로 책임을 집니다.

이 암호자산 백서는 (EU) 2023/1114 규정의 Title II를 준수하며, 경영진의 지식에 비추어 볼 때 본 백서에 제시된 정보는 공정하고 명확하며 오해의 소지가 없고, 본 암호자산 백서는 그 중요성에 영향을 미칠 만한 누락이 없습니다.

월드 네트워크 소개

월드 네트워크(World Network)는 인류 대다수가 소유하는 전 세계적으로 포용적인 정체성과 금융 네트워크를 만들겠다는 사명을 가지고 설립되었습니다. 성공할 경우, 월드 네트워크는 경제적 기회를 크게 확대하고, 개인정보 보호를 유지하면서 온라인에서 인간과 AI를 구별할 수 있는 신뢰할 수 있는 솔루션을 대규모로 제공하며, 전 세계적인 민주적 프로세스를 가능하게 하고, AI가 자금을 댄 UBI(기본소득)의 잠재적 경로를 제시할 수 있습니다.

월드 네트워크는 프라이버시를 보존하는 디지털 신원 네트워크인 **월드 아이디(World ID)** 와, 법률이 허용하는 경우 디지털 화폐 **WLD**로 구성됩니다. 모든 인간은 단지 인간이라는 이유만으로 WLD 토큰에 접근할 수 있습니다. 월드 아이디와 WLD 토큰은 현재 **월드 앱(World App)** 으로 보완되며, 이는 TFH(Tools for Humanity) 기여자 팀이 개발한 월드 아이디 및 월드 네트워크의 최초 프론트엔드입니다.

“인간 증명(Proof of Human)”은 월드의 핵심 아이디어 중 하나로, 개인이 인간이자 유일한 존재임을 확립하는 것을 의미합니다. 일단 확립되면, 개인은 자신의 실제 신원을 공개하지 않고도 자신이 실제 사람이며 다른 실제 사람과 다르다는 것을 주장할 수 있게 됩니다.

오늘날, 인간 증명은 전 세계적으로 해결되지 않은 문제로, 온라인 투표나 대규모 가치 분배를 어렵게 합니다. 점점 강력해지는 AI 모델은 인간과 봇을 구별하는 어려움을 더욱 증폭시킬 것이므로 이 문제는 더욱 시급합니다. 월드 네트워크의 일부로서 성공한다면, 월드 아이디어는 전 세계적인 인간 증명 표준이 될 수 있습니다.

월드의 핵심 전제는 다음과 같습니다:

- 인간 증명은 빠져 있는 필수 디지털 원시 요소입니다. 이 원시는 점점 더 강력해지는 AI 모델이 등장함에 따라 더욱 중요해질 것입니다.
- 확장 가능하고 포용적인 인간 증명은 처음으로 네트워크 참여자 모두의 인센티브를 진정한 인간을 네트워크에 추가하는 데 맞출 수 있게 합니다. 비트코인은 비트코인 네트워크 보안을 위해 발행됩니다. 월드코인은 이더리움에서 보안을 상속받으면서 월드 네트워크를 성장시키기 위해 발행됩니다.
- 점점 더 강력해지는 AI 시대에, 전 세계적인 인간 증명을 발행하는 가장 신뢰할 수 있는 방법은 맞춤형 생체인식 하드웨어를 통한 것입니다.

이 동적 백서는 프로젝트 구현 배경과 현재 상태, 그리고 로드맵을 공유합니다.

월드 아이디 (World ID)

월드 아이디는 프라이버시를 보존하는 인간 증명입니다. 사용자가 **오브(Orb)** 라는 맞춤형 생체인식 장치를 통해 제로 지식 증명(zero-knowledge proofs)으로 자신의 인간성을 온라인에서 검증하면서도 개인정보를 보호할 수 있도록 합니다. 오브는 맞춤형 생체인식 하드웨어만이 장기적으로 AI 안전성을 갖춘 인간 증명 검증을 발행할 수 있는 유일하게 실행 가능한 해결책일 수 있다는 인식에 따라 설계되었습니다. 월드 아이디는 월드 네트워크 상에서 발급되며, 이를 통해 개인은 웹2 애플리케이션을 포함한 모든 검증자에게 개인정보를 유지하면서 자신이 인간임을 증명할 수 있습니다. 향후 이 프로토콜에서 다른 자격 증명도 발급될 수 있을 것입니다.

월드 아이디는 **개인 귀속(personbound)** 을 목표로 하며, 이는 월드 아이디가 발급된 개인만 사용할 수 있어야 한다는 의미입니다. 월드 아이디 자격 증명을 도난당하거나 획득한 사기 행위자가 사용하기는 매우 어려워야 합니다.

월드코인 (WLD)

네트워크 효과는 궁극적으로 금융 및 신원 인프라 위에 구축되는 유용한 애플리케이션에서 비롯되겠지만, 토큰은 네트워크 성장에 대한 인센티브를 모든 참여자에게 맞추기 위해 발행됩니다. 이는 특히 네트워크를 초기 단계에서 부트스트랩하고 “콜드 스타트 문제(cold start problem)”를 우회하기 위해 중요합니다.

월드 앱 (World App)

월드 앱은 월드 아이디의 첫 번째 프론트엔드로, 개인이 오브를 통한 검증 과정을 안내하고, 개인의 월드 아이디 자격 증명을 보관하며, 해당 자격 증명을 제3자와 프라이버시 보존 방식으로 공유하기 위한 암호 프로토콜을 구현합니다. 월드 앱은 전 세계 탈중앙화 금융 인프라에 마찰 없는 접근을 제공하도록 설계되었습니다. 궁극적으로는 월드 아이디를 통합하는 다양한 지갑이 등장할 것입니다.

월드는 어떻게 작동하는가?

월드는 프라이버시를 보존하는 글로벌 신원 네트워크인 월드 아이디를 중심으로 운영됩니다. 월드 아이디를 사용하면 개인은 프로토콜과 통합된 어떤 플랫폼에서든 자신이 실제 존재하는 고유한 인간임을 증명할 수 있습니다. 이를 통해 공정한 에어드롭을 가능하게 하고, 소셜미디어에서의 봇/시빌 공격을 방지하며, 한정된 자원의 공정한 분배를 지원할 수 있습니다. 또한 월드 아이디는 전 세계적인 민주적 프로세스와 새로운 형태의 거버넌스(예: 제곱 투표(quadratic voting))를 가능하게 하며, 궁극적으로 AI가 자금을 대는 UBI로 가는 경로도 지원할 수 있습니다.

월드 네트워크 프로토콜에 참여하려면 개인은 먼저 월드 아이디 생성을 지원하는 최초의 지갑 앱인 월드 앱을 다운로드해야 합니다. 개인은 물리적 촬영 장치인 오브를 방문해 오브 검증을 거쳐 월드 아이디를 발급받습니다. 대부분의 오브는 **오브 운영자(Orb Operator)** 라는 독립적인 지역 사업자 네트워크에 의해 운영됩니다. 오브는 다중 스펙트럼 센서를 사용해 인간성과 유일성을 검증하고, 오브 검증된 월드 아이디를 발급하며, 모든 이미지는 기본적으로 기기 내에서 즉시 삭제됩니다(데이터 보관(Data Custody)에 대한 명시적 동의가 없는 경우).

잠재적 응용 (Potential Applications)

월드는 보편적으로 접근 가능한 탈중앙화 금융 및 신원 인프라를 통해, 위치에 관계없이 누구나 글로벌 디지털 경제에 참여할 수 있는 미래를 진전시켜 전 세계적으로 기회 평등을 크게 높일 수 있습니다. 네트워크가 성장함에 따라 그 효용도 커질 것입니다.

오늘날 디지털 영역에서 많은 상호작용은 전 세계적으로 불가능합니다. 인간이 가치를 거래하고, 자신을 식별하며, 인터넷에서 상호작용하는 방식은 근본적으로 변할 가능성이 큼니다. 금융과 신원에 대한 보편적 접근이 가능하다면, 다음과 같은 미래가 가능합니다:

금융 (Finance)

디지털 자산 소유 및 송금: 송금은 전 세계적으로 거의 즉각적이고 국경 없이 이뤄질 수 있습니다. 모든 사람에게 제공됩니다. 세계는 금융적으로 연결되고, 모두가 인터넷에서 경제적으로 상호작용할 수 있게 될 것입니다. 인도 COVID 구호 기금에서는 전 세계 사람들이 짧은 시간 안에 4억 달러 이상을 모아 지원했는데, 이는 가능성을 보여주는 사례입니다. 전반적으로 이는 인류 역사상 유례없는 규모로 사람들을 글로벌 차원에서 연결할 잠재력을 갖고 있습니다.

디지털 화폐는 현금보다 안전하며, 현금은 쉽게 도난당하거나 위조될 수 있습니다. 이는 특히 우크라이나 난민 위기와 같은 위기 상황에서 즉각적인 국경 간 금융 거래가 가능해야 할 때 중요합니다. 이때 USDC가 직접적인 지원을 배분하는 데 사용되었습니다. 또한 디지털 화폐는 개인이 제3자를 신뢰하지 않고도 직접 소유하고 통제할 수 있는 자산입니다.

신원 (Identity)

봇 차단: 트위터 봇, 스팸 메시지, 로보콜은 모두 건전하고 마찰 없는 디지털 신원의 부재로 발생하는 문제입니다. 고도화되는 AI 모델은 CAPTCHAs를 해결하고 그럴듯한 “인간” 콘텐츠를 생산할 수 있어 문제를 악화시킵니다. 서비스가 이런 콘텐츠에 대한 방어를 강화하면서, 포용적이고 프라이버시를 보존하는 인간 증명 솔루션이 공공 인프라로서 필수적이 됩니다. 모든 메시지나 거래가 “검증된 인간” 속성을 포함한다면, 디지털 세계에서 많은 잡음을 걸러낼 수 있습니다.

거버넌스: 현재 web3의 집단적 의사결정은 주로 토큰 기반 거버넌스(토큰 1개 = 1표)에 의존하며, 이는 일부 사람들을 배제하고 경제력이 더 큰 사람들에게 유리합니다. 월드 아이디와 같은 신뢰할 수 있는 시빌 저항 인간 증명은 web3뿐 아니라 인터넷 전반에 걸친 글로벌 민주적 거버넌스 메커니즘 설계 공간을 열어줍니다. 또한 AI가 일부 집단이 아닌 모든 인류에 최대한 이익이 되도록 하려면, 거버넌스에 모두가 포함되는 것이 점점 더 중요해질 것입니다.

금융과 신원의 교차 (Intersection of Finance and Identity)

인센티브 정렬: 쿠폰, 로열티 프로그램, 추천 프로그램 등 고객과 가치를 공유하는 메커니즘은 전통적으로 사기에 취약합니다. 마찰 없고 사기 저항적인 디지털 신원은 인센티브를 정렬하고 소비자와 기업 모두에게 이익을 줍니다. 이는 사용자가 부분적으로 소유하는 새로운 유형의 기업을 탄생시킬 수도 있습니다.

희소 자원의 공정한 분배: 보조금과 사회 복지 등 현대 사회의 핵심 요소는 인간 증명을 활용해 보다 공정하게 제공될 수 있습니다. 이는 특히 가짜 신원을 통해 한 사람이 받을 수 있는 자원보다 더 많이 확보하려는 문제가 발생하는 개발도상국에서 중요합니다. 2021년 인도는 생체인식 기반 시스템을 도입해 사기를 줄임으로써 보조금 프로그램에서 5억 달러 이상을 절감했습니다. 탈중앙화된 인간 증명 프로토콜은 전 세계의 어떤 프로젝트나 조직에도 유사한 혜택을 제공할 수 있습니다. AI가 발전함에 따라 접근성과 창출된 가치를 공정하게 분배하는 UBI는 경제 권력 집중을 억제하는 데 점점 더 중요한 역할을 하게 될 것입니다. 월드 아이디는 각 개인이 단 한 번만 등록되도록 하고, 공정한 분배를 보장할 수 있습니다.

인간 증명 (Proof of Human, PoH)

응용 분야에 따라 PoH에 대한 요구사항은 다릅니다. 글로벌 UBI, AI 및 월드 네트워크의 민주적 거버넌스와 같은 고위험 사용 사례에서는 다중 등록을 방지할 수 있는 고도의 보안성과 포용성을 갖춘 PoH 메커니즘이 필요합니다. 따라서 월드 재단(World Foundation)과 함께하는 월드 네트워크 개발자 커뮤니티는 월드 아이디(World ID)를 통해 고신뢰 PoH 메커니즘의 기초를 마련하고 있습니다. 월드 아이디는 생체인식 검증 장치(첫 번째 장치가 오브(Orb))를 통해 모든 고유한 인간에게 발급됩니다. 다음 섹션에서는 PoH의 근본적인 구성 요소와 그것들이 월드 아이디의 맥락에서 어떻게 구현되는지 살펴봅니다.

구성 요소 (Building Blocks)

높은 수준에서 효과적인 PoH 메커니즘에는 여러 구성 요소가 필요합니다. 여기에는 모든 사람이 단 한 번만 검증할 수 있도록 보장하는 **중복 제거(deduplication)**, PoH 자격 증명의 합법적인 소유자만 사용할 수 있도록 하는 **인증(authentication)**, 분실되거나 손상된 자격 증명을 복구하는 **복구(recovery)**가 포함됩니다. 이 섹션에서는 이러한 구성 요소를 높은 수준에서 논의합니다.

PoH 메커니즘은 세 가지 서로 다른 행위자와 그들이 교환하는 데이터로 구성됩니다.

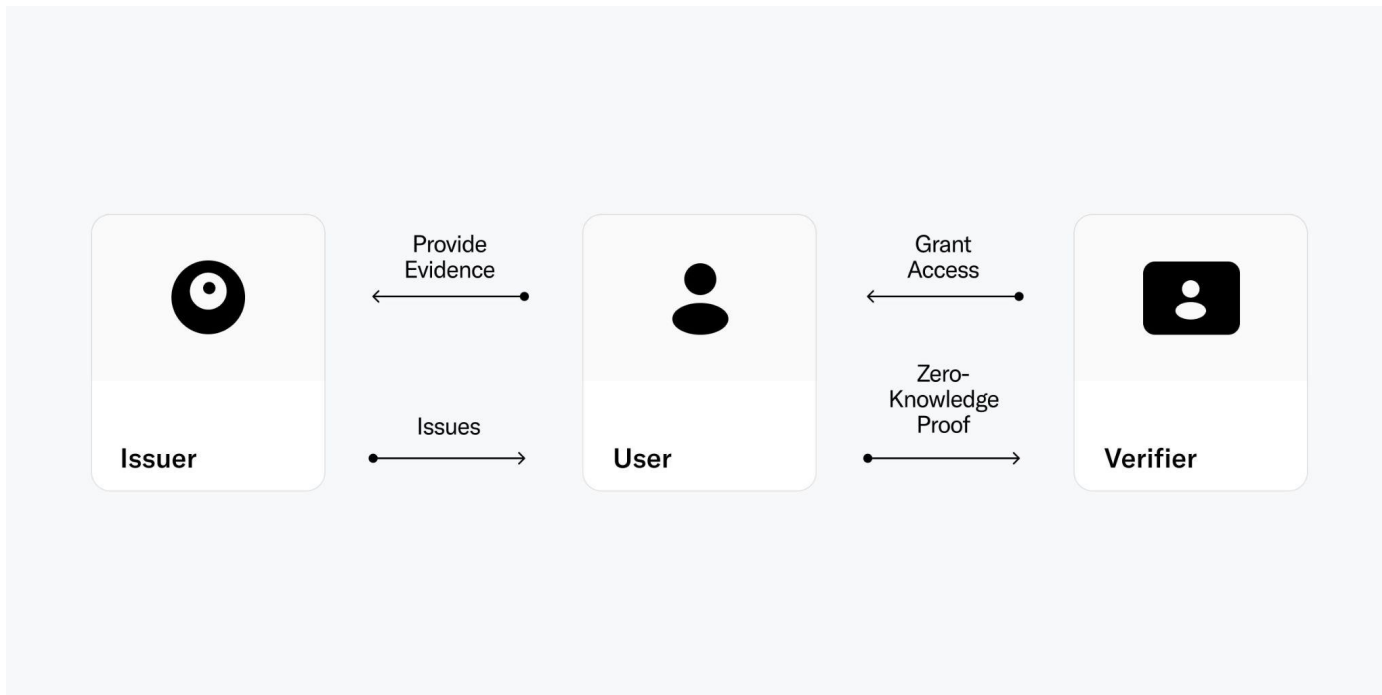


Figure 1: 사용자가 인간으로 인증되기 위해 필요한 인간 증명 생태계의 서로 다른 행위자 간 상호작용을 단순화하여 묘사한 다이어그램

이 섹션의 맥락에서, 용어는 다음과 같이 정의됩니다:

- **사용자(User):** 특정 자원에 접근하거나 특정 행동에 참여하기 위해 자신에 대한 특정 주장을 증명하려는 개인. PoH 프로토콜의 맥락에서 이러한 주장은 고유성과 인간성을 증명하는 것과 관련됩니다.
- **자격 증명(Credential):** 사용자가 인간임을 나타내는 특정 속성에 대한 증거 역할을 하는 데이터 집합. 이는 유효한 정부 발급 신분증 보유에서부터 생체인식을 통한 인간 및 고유성 검증까지 다양한 형태일 수 있습니다.
- **발급자(Issuer):** 사용자에 대한 특정 정보를 확인하고 PoH 자격 증명을 부여하는 신뢰할 수 있는 주체. 이를 통해 사용자는 자신의 주장을 타인에게 증명할 수 있습니다.
- **검증자(Verifier):** 사용자의 PoH 자격 증명을 검토하고 그 진위 여부를 확인하여 사용자가 특정 행동에 접근할 수 있도록 하는 주체.

사용자, 발급자, 검증자 간의 중복 제거, 복구, 인증과 같은 특정 상호작용은 기능적인 PoH 메커니즘의 중요한 구성 요소입니다. 이 섹션은 일반적인 PoH 메커니즘의 구성 요소를 높은 수준에서 개괄합니다. 이러한 요소들이 월드 아이디어에서 어떻게 구현되는지에 대한 상세 설명은 이후 섹션에서 이어집니다.

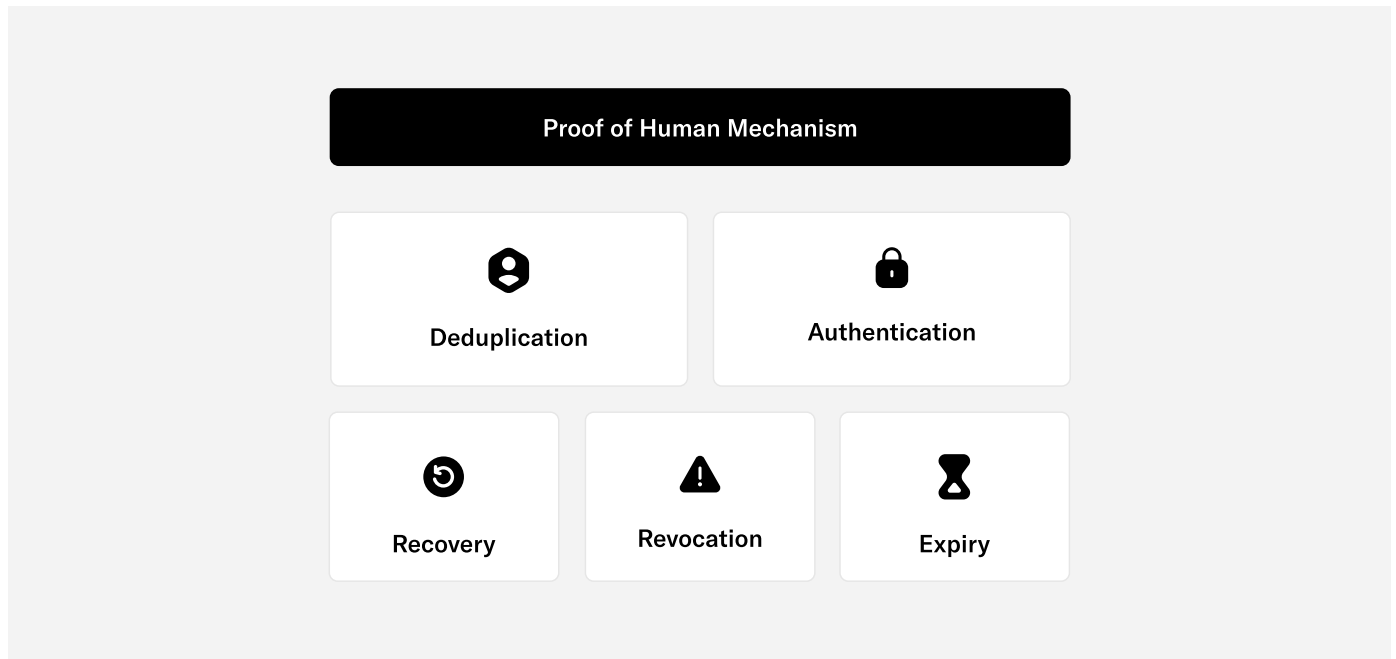


Figure 2: 효과적인 인간 증명 메커니즘을 구성하는 다양한 구성 요소를 시각화한 그림

중복 제거 (Deduplication)

PoH가 유용하려면 **고유성** 개념을 가져야 합니다. PoH를 여러 번 획득하거나 사기 행위자나 봇에게 이전할 수 있다면, 신뢰할 수 없으며 목적을 달성하지 못합니다. 따라서 PoH 메커니즘은 인간 증명 자격 증명을 발급받는 사용자 간의 **중복 제거**를 수행해야 합니다. 이는 모든 PoH 메커니즘에서 가장 어려운 과제입니다.

인증 (Authentication)

PoH 자격 증명에 유용하려면, 그것을 다른 사람(예: 봇)에게 이전하거나 사기 행위자가 사용하는 것이 어렵도록 만들어야 합니다. 이는 특히 자격 증명을 판매하는 행위의 결과를 알지 못하는 개인을 보호하는 데 중요합니다. 이러한 과제는 신원 시스템 전반에 내재된 문제입니다. 인증은 해당 사용자가 알지 못하거나 사기 행위자와 협력하려 하더라도 사기 행위자가 자격 증명을 사용하는 것을 막을 수 있습니다.

PoH 자격 증명을 발급할 때, 발급자는 단지 해당 인물이 실제로 고유한 사람임을 검증하기만 하면 됩니다. 그 외 추가적인 개인정보는 요구되지 않습니다. 그러나 각 PoH 자격 증명은 특정 개인에게 고유하게 연결되어야 합니다. 자격 증명에 양도 불가능하더라도, 지갑이나 휴대폰은 양도될 수 있습니다. 따라서 무결성이 중요한 사용 사례에서는 사용자가 해당 PoH 자격 증명의 정당한 소유자임을 인증하는 것이 필수적입니다. 이는 항공 탑승 시의 절차와 유사합니다. 예를 들어, 항공사 게이트 직원은 유효한 여행 서류 소지 여부와 개인의 신원이 문서와 일치하는지를 모두 확인합니다.

복구 (Recovery)

사용자가 자격 증명에 대한 접근 권한을 잃거나 자격 증명에 손상을 입은 경우, 효과적인 **복구 메커니즘**이 필요합니다. 그러나 사용자가 자체적으로 키를 관리하는 환경에서는 상당한 도전 과제가 됩니다. PoH 프로토콜 맥락에서는 다음과 같은 여러 복구 방법을 사용할 수 있습니다:

- **사용자 관리 백업 복원:** 가장 단순한 방법은 암호화된 사용자 관리 백업을 저장하는 것입니다. 이를 통해 사용자는 이전 기기를 잃어버렸을 때 새 기기에서 자격 증명을 복원할 수 있습니다.

- **소셜 복구:** 사용자 관리 백업이 없지만 사용자가 소셜 복구를 설정한 경우, 친구와 가족의 도움을 통해 자격 증명을 복구할 수 있습니다.
- **키 복구:** 백업이나 소셜 복구가 모두 불가능한 경우, 사용자는 발급자를 다시 방문해 원래 자격 증명에 대한 접근 권한을 되찾아야 합니다. 사용자는 특정 자격 증명의 정당한 소유자임을 발급자에게 입증해야 하며, 성공적으로 인증되면 발급자가 다시 접근 권한을 부여합니다. 이는 이전 신분증을 잃어버린 후 새로운 정부 발급 신분증을 받는 과정과 유사합니다. 다만, 사용자가 개인 키를 직접 생성하고 발급자가 공개 키만 기록한 경우(예: 월드 아이디), 이러한 방식은 불가능할 수 있습니다.
- **재발급(Re-Issuance):** 발급자를 통해 원래 자격 증명에 대한 접근을 회복할 수 없거나 바람직하지 않은 상황(예: 신원 도용)에서는 재발급을 통해 기존 자격 증명을 무효화하고 새 자격 증명을 발급할 수 있습니다. 이는 신용카드를 분실했을 때 카드를 정지시키고 새 카드를 발급받는 것과 유사합니다. 특히, 재발급 메커니즘을 통해 키를 교체할 수 있다는 점은 게임 이론적 관점에서 다른 사람의 PoH 자격 증명을 불법적으로 취득하는 것을 경제적으로 불가능하게 만듭니다. 진정한 자격 증명 소유자는 언제든지 자신의 자격 증명을 복구하고 도난/구매된 자격 증명을 무효화할 수 있기 때문입니다. 다만, 공모나 강압이 개입된 신원 이전의 경우는 여전히 방지할 수 없습니다.

해지 (Revocation)

모든 참여자가 성실하게 행동하기를 바라지만, 이를 전제로 할 수는 없습니다. 발급자가 손상되거나 악의적인 것으로 판명될 경우, 발급자나 개발자는 영향을 받은 PoH 자격 증명을 허용된 목록에서 제거함으로써 영향을 완화할 수 있습니다. 자격 증명에 여러 발급 위치에서 분산적으로 발급되고 일부만 손상된 경우, 해당 부분은 발급 기관에 의해 해지될 수 있습니다. 오늘날의 자격 증명에 비유하자면, 대학이 모든 요건을 충족하지 않은 사람에게 학위를 수여한 경우, 사기가 확인되면 학위가 취소될 수 있습니다.

만료 (Expiry)

보안 메커니즘의 효력은 시간이 지남에 따라 약화되며 새로운 메커니즘이 지속적으로 개발됩니다. 그 결과, 많은 신원 시스템은 발급 시점에 자격 증명에 **사전 정의된 만료일**을 포함합니다. 여권이 그 예입니다. PoH 메커니즘이 작동하는 데 만료일이 필수는 아니지만, 이를 포함하면 PoH의 무결성을 강화할 수 있습니다.

종합

앞서 언급된 구성 요소들의 조합은 기능적인 인간 증명 메커니즘을 형성합니다. 다음 그림은 예시 스마트폰 앱을 보여줍니다.

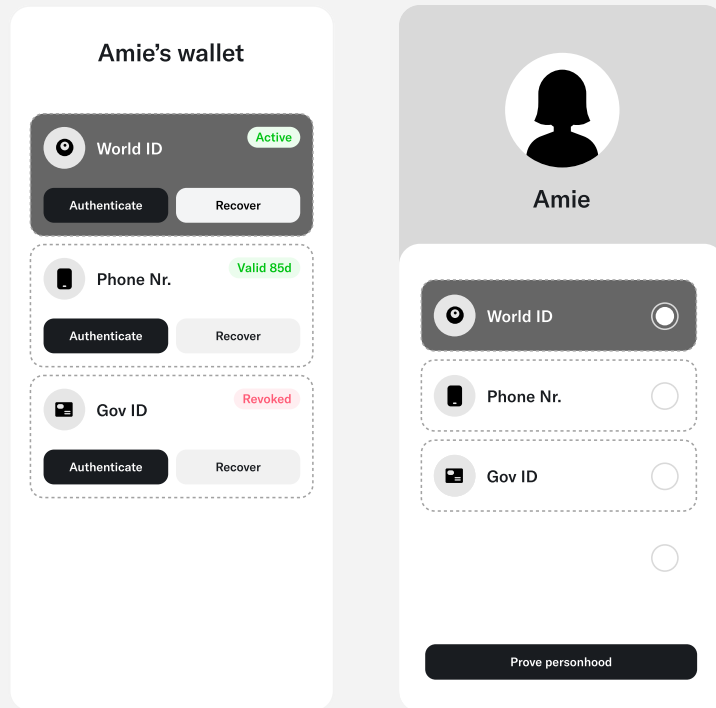


Figure 3: 다양한 발급자가 부여한 인간 증명 자격 증명을 보관하는 지갑을 묘사한 그림. 사용자는 해당 자격 증명을 활용해 자신이 실제 인간임을 검증자에게 보증할 수 있으며, 검증자는 이를 근거로 거래를 승인하고 수행할 수 있습니다.

대규모 PoH 해결 (Solving PoH at Scale)

앞서 언급한 높은 수준의 구성 요소에 기반하여, 전 세계적인 PoH 메커니즘을 평가하기 위해 도출할 수 있는 몇 가지 요구사항이 있습니다:

- **포용성과 확장성:** 글로벌 PoH는 최대한 포용적이어야 하며, 즉 모든 사람이 사용할 수 있어야 합니다. 이 말은 메커니즘이 수십억 명의 사람들을 구별할 수 있어야 함을 의미합니다. 전 세계적으로 구현할 수 있는 실행 가능한 경로가 있어야 하며, 사람들은 국적, 인종, 성별, 경제적 여건에 관계없이 참여할 수 있어야 합니다.
- **사기 저항성:** 글로벌 인간 증명에서 중요한 부분은 “식별(identification)” (즉, “누군가가 자신이 주장하는 사람인가?”)이 아니라 **부정 식별(negative identification)** (즉, “이 사람이 이미 등록한 적이 있는가?”)입니다. 따라서 중복 등록을 방지하는 사기 방지가 핵심입니다. 중복이 많이 발생하면 가능한 응용 프로그램의 설계 공간이 심각하게 제한되며, 모든 인간을 동등하게 대할 수 없게 됩니다. 이는 공정한 토큰 분배, 민주적 거버넌스, 신용 점수와 같은 평판 시스템, 복지(UBI 포함)와 같은 사용 사례에 심각한 영향을 미칩니다.
- **개인 귀속(Personbound):** PoH가 발급되면 개인 귀속적이어야 하며, 판매나 도난(즉, 이전)이 어렵고 분실하기도 어려워야 합니다. 올바르게 설계된 PoH 메커니즘은 가명성(pseudonymity)을 방해하지 않습니다. 따라서 PoH 메커니즘은 사기 행위자가 정당한 개인을 사칭하기 어렵도록 인증을 허용해야 합니다. 또한 개인이 모든 정보를 잃더라도 과거 행위와 무관하게 언제든지 복구할 수 있어야 합니다.

이러한 요구사항은 인간 증명 메커니즘의 필수 구성 요소에서 도출할 수 있는 것들입니다. 그러나 월드 (World)에 내재된 가치에서 도출할 수 있는 추가적인 중요한 요구사항이 있습니다:

- **탈중앙화:** 글로벌 인간 증명 자격 증명의 발급은 기본적인 인프라이며, 복원력과 무결성을 극대화하기 위해 단일 기관이 통제해서는 안 됩니다.
- **프라이버시:** 인간 증명 메커니즘은 개인의 프라이버시를 보존해야 합니다. 개인이 공유하는 데이터는 최소화되어야 하며, 사용자가 자신의 데이터를 통제해야 합니다.

수십억 명 중 고유성을 검증하는 메커니즘

위의 요구사항에 기반하여, 이 섹션에서는 월드 네트워크 맥락에서 글로벌 PoH 메커니즘을 확립하기 위한 다양한 접근 방식을 비교합니다.

Proof of Human Mechanisms					
	Online Accounts	KYC	Web of Trust	Social Graph Analysis	Biometrics
Privacy	Possible	Possible	Possible	Possible	Possible
Fraud Resistance	No	Possible	No	No	Possible
Inclusivity & Scalability	Possible	No	Possible	Possible	Possible
Decentralization	Possible	No	Possible	Possible	Possible
Personbound	No	Possible	Possible	Possible	Possible

Figure 4: 인간 증명 메커니즘 개요. 월드 네트워크 기여자들의 연구에 따르면, 적절히 구현되는 경우 생체인식이 모든 필수 요구사항을 충족할 수 있는 유일한 방법임이 결론지어졌다.

온라인 계정 (Online accounts)

PoH를 대규모로 확립하기 위한 가장 단순한 시도는 이메일, 전화번호, 소셜미디어와 같은 기존 계정을 사용하는 것입니다. 그러나 이 방법은 실패합니다. 한 사람이 각 플랫폼에서 여러 계정을 가질 수 있기 때문입니다. 또한 계정은 **개인 귀속(personbound)**이 아니므로 쉽게 다른 사람에게 이전될 수 있습니다. 흔히 봇 방지를 위해 사용되는 CAPTCHA도 여기서는 효과적이지 않습니다. 어떤 사람도 여러 CAPTCHA를 통과할 수 있기 때문입니다. 가장 최근의 구현 방식조차도 사실상 내부 평판 시스템에 의존하며, 한계가 있습니다.

일반적으로 기존 온라인 계정을 중복 제거(즉, 개인이 한 번만 등록할 수 있도록 보장)하는 현재의 방법, 예를 들어 계정 활동 분석은 상당한 인센티브를 견딜 만큼의 사기 저항성이 부족합니다. 이는 잘 확립된 금융 서비스 운영을 대상으로 한 대규모 공격에서도 입증되었습니다.

공식 신분증 검증 (KYC)

온라인 서비스는 종종 KYC(Know your Customer) 규정을 준수하기 위해 신분증(대개 여권이나 운전면허증)을 요구합니다. 이론적으로는 이를 사용해 전 세계적으로 개인을 중복 제거할 수 있지만, 실제로는 여러 가지 이유로 실패합니다.

KYC 서비스는 전 세계적으로 단순히 포용적이지 않습니다. 전 세계 인구의 50% 이상이 디지털로 검증할 수 있는 신분증을 가지고 있지 않습니다. 또한 프라이버시를 보존하는 방식으로 KYC 검증을 구축하는 것은 어렵습니다. KYC 공급자를 사용할 때, 민감한 데이터를 그들과 공유해야 합니다. 이는 zkKYC와 NFC 판독 가능한 신분증을 사용함으로써 해결할 수 있습니다. 관련 데이터는 사용자의 휴대폰으로 읽을 수 있으며, 발급 기관이 서명했기 때문에 로컬에서 검증될 수 있습니다. 고유한 인간성을 증명하는 것은 사용자의 신분증 정보에 기반한 해시를 제출함으로써 이루어질 수 있으며, 이 과정에서 어떤 개인정보도 공개되지 않습니다. 이 접근 방식의 주요 단점은 이러한 NFC 판독 가능한 신분증의 보급률이 일반 신분증에 비해 상당히 낮다는 점입니다.

NFC 판독 가능한 신분증이 사용 불가능한 곳에서는, 신분증 검증이 사기에 취약할 수 있으며—특히 신흥 시장에서 그러합니다. 신분증은 국가와 정부에 의해 발급되며, 이를 검증하거나 책임지는 전 세계적 시스템은 존재하지 않습니다. 많은 검증 서비스(KYC 공급자)는 시간이 지나면서 축적된 신용기관의 데이터에 의존하며, 이 데이터는 낡아 있으며 발급 기관(즉, 정부)과의 진위를 검증할 수단이 없습니다. 이는 종종 사용할 수 있는 API가 없기 때문입니다. 가짜 신분증뿐만 아니라 그것을 만드는 데 사용되는 실제 데이터도 암시장에서 쉽게 구할 수 있습니다. 또한 중앙집중적인 특성 때문에 발급 및 검증 기관 수준의 부패를 제거할 수 없습니다.

제공된 데이터의 진위가 검증 가능하더라도, 서로 다른 유형의 신분증 간 전 세계적인 고유성을 확립하는 것은 단순하지 않습니다. 같은 사람의 문서 간 퍼지 매칭은 오류가 많습니다. 이는 개인정보의 변화(예: 주소)와 개인정보가 담고 있는 낮은 엔트로피 때문입니다. 사람들이 시간이 지나면서 새로운 신분증을 발급받아 새로운 문서 번호와 (가능한) 개인정보를 가지게 되는 경우에도 유사한 문제가 발생합니다. 이러한 문제는 사용자들을 잘못 승인하거나 잘못 거부하는 높은 오류율을 초래합니다. 결국, 현재의 인프라에서는 포용성과 사기 저항성이 부족하기 때문에 KYC 검증을 통해 글로벌 인간 증명을 부트스트랩하는 것은 불가능합니다.

신뢰의 그물망 (Web of Trust)

“신뢰의 그물망(Web of Trust)”의 기본 아이디어는 탈중앙화 방식으로 신원 주장을 검증하는 것입니다.

예를 들어, PGP에서 사용되는 고전적인 신뢰의 그물망에서는 사용자가 대면 “키 서명 파티”에 참석하여 신원 문서를 통해 키가 실제 소유자에 의해 제어되고 있음을 증명합니다. 최근에는 Proof of Humanity 같은 프로젝트가 Web3를 위한 신뢰의 그물망을 구축하고 있습니다. 이는 얼굴 사진과 화상 채팅을 사용해 대면 요건을 피하면서 탈중앙화된 검증을 허용합니다.

그러나 이러한 시스템은 개인에게 크게 의존하기 때문에 사람의 실수에 취약하고 시빌 공격에 노출됩니다. 사용자에게 스테이킹을 요구하면 보안을 강화할 수 있습니다. 하지만 이는 실수에 대한 벌칙으로 인해 사용자들이 다른 사람을 검증하려는 동기를 약화시키며, 모든 사람이 자금을 묶을 의향이나 능력이 있는 것으로 포용성도 저하됩니다. 또한 얼굴 이미지나 영상 공개와 같은 프라이버시 문제와 딥페이크를 통한 사기 위험 때문에 위에서 언급한 설계 요구사항을 충족하지 못합니다.

소셜 그래프 분석 (Social graph analysis)

소셜 그래프 분석의 아이디어는 사람들 간의 관계(또는 관계의 부재)에 대한 정보를 사용하여 어떤 사용자가 실제 사람인지 추론하는 것입니다.

예를 들어, 관계 네트워크에서 친구가 5명 이상인 사용자는 실제 사용자일 가능성이 높다고 추론할 수 있습니다. 물론 이는 지나치게 단순화된 규칙이며, EigenTrust, Bright ID, 소울바운드 토큰(SBT)과 같은 프로젝트와 개념들은 더 정교한 규칙을 제안합니다. 참고로 SBT는 인간 증명 메커니즘으로 설계된 것이 아니며, 고유성보다는 관계 증명이 필요한 응용 프로그램에 보완적으로 사용됩니다. 그러나 때로는 이 맥락에서 언급되기도 하므로 관련 논의가 필요합니다.

이러한 메커니즘의 근본적 관찰은, 다른 프로필을 충분히 다양한 관계로 생성하기 어렵다면 사회적 관계가 고유한 인간 식별자로 기능한다는 것입니다. 충분히 어려운 경우, 각 사용자는 풍부한 사회적 관계를 가진 단일 프로필만 유지할 수 있으며, 이는 사용자의 인간 증명으로 활용될 수 있습니다. 그러나 이 접근 방식의 주요 과제는 전 세계적으로 필요한 관계를 구축하는 데 시간이 오래 걸린다는 점입니다. 특히 고용주나 대학과 같은 기관에 의존할 때 그렇습니다. 초기에는 이 시스템의 가치가 작기 때문에 기관들을 참여시키는 것이 얼마나 쉬운지도 불확실합니다. 게다가 가까운 미래에는 AI가(또는 사람들이 여러 “실세계” 자격 증명을 획득해 보조하는 경우) 이러한 프로필을 대규모로 생성할 수 있을 것이 불가피해 보입니다.

결국, 이러한 접근 방식은 많은 응용 프로그램에서 가치가 있지만, 앞서 언급된 인간 증명의 **사기 저항성 요구사항**을 충족하지 못합니다.

생체인식 (Biometrics)

위에서 설명한 각 시스템은 전 세계적인 규모에서 고유성을 효과적으로 검증하는 데 실패합니다. 신뢰할 수 없는 환경에서 사람들을 구별할 수 있는 유일한 메커니즘은 **생체인식(biometrics)**입니다. 생체인식은 인간성과 고유성을 모두 검증할 수 있는 가장 근본적인 수단입니다. 가장 중요한 점은, 생체인식은 **보편적**이어서 국적, 인종, 성별, 경제적 여건과 관계없이 접근을 가능하게 한다는 것입니다. 또한 올바르게 구현될 경우, 생체인식 시스템은 매우 프라이버시를 보존할 수 있습니다. 더 나아가, 생체인식은 앞서 언급된 구성 요소들을 가능하게 하는데, 예를 들어 복구 메커니즘(사람이 모든 것을 잊더라도 작동하는)을 제공하고 인증에 사용할 수 있습니다. 따라서 생체인식은 인간 증명 자격 증명을 **개인 귀속(personbound)**으로 만드는 것도 가능하게 합니다.

시스템마다 요구사항은 다릅니다. FaceID를 통해 사용자가 휴대폰의 정당한 소유자인지를 인증하는 것은 수십억 명의 사람을 고유하게 검증하는 것과는 매우 다릅니다. 요구사항의 주요 차이는 정확성과 사기 저항성과 관련됩니다. FaceID의 경우, 생체인식은 본질적으로 비밀번호처럼 사용되며, 휴대폰이 저장된 신원 템플릿과 단일 1:1 비교를 수행하여 사용자가 자신이 주장하는 사람인지 여부를 판단합니다. 글로벌 고유성을 확

립하는 것은 훨씬 더 어렵습니다. 생체인식은 (궁극적으로) 수십억 명의 기 등록 사용자와의 1:N 비교를 수행해야 합니다. 시스템의 정확도가 충분히 높지 않다면, 잘못 거부되는 사용자가 점점 늘어나게 됩니다.

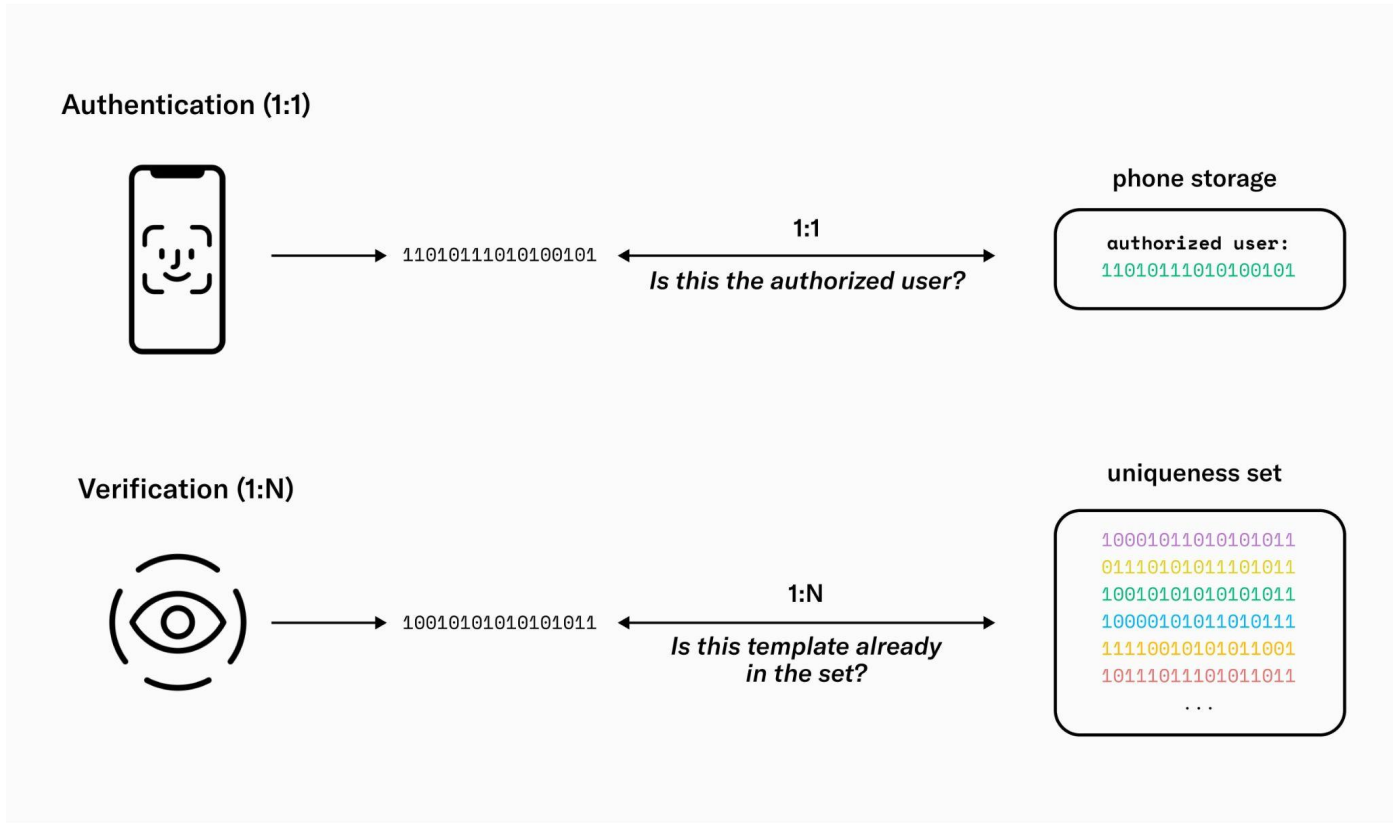


Figure 5: 생체인식과 관련해 고려해야 할 두 가지 모드가 있다. 더 단순한 모드는 1:1 인증으로, 사용자의 템플릿을 이전에 등록된 단일 템플릿(예: Face ID)과 비교한다. 글로벌 인간 증명을 위해서는 1:N 검증이 필요하며, 이는 중복 등록을 방지하기 위해 사용자의 템플릿을 대규모 템플릿 집합과 비교하는 것이다. 오류율, 그리고 따라서 시스템의 포용성은 사용되는 생체인식 특징의 통계적 특성에 의해 크게 영향을 받는다. 홍채 생체인식은 다른 생체인식 방식보다 성능이 뛰어나며, 2.5×10^{-14} (즉, 40조 번 중 1번의 오탐) 이상의 거짓 일치율을 달성할 수 있다. 이는 현재 최첨단 얼굴 인식 기술보다 몇 자릿수 더 정확하다. 게다가 홍채 구조는 시간이 지나도 놀라울 정도의 안정성을 보인다.

오류율, 그리고 따라서 시스템의 포용성은 사용되는 생체인식 특징의 통계적 특성에 의해 크게 영향을 받습니 다. 홍채 생체인식은 다른 생체인식 방식보다 성능이 뛰어나며, 2.5×10^{-14} (즉, 40조 번 중 1번의 오탐) 이상의 거짓 일치율을 달성할 수 있습니다. 이는 현재 최첨단 얼굴 인식 기술보다 몇 자릿수 더 정확합니다. 또 한 홍채 구조는 시간이 지나도 놀라울 정도의 안정성을 보입니다.

Biometric Modalities

	Fingerprint	Face	DNA	Iris
Privacy	Possible	Possible	Hard	Possible
Accuracy for global scale	Not enough	Not enough	Sufficient	Sufficient
Scalability	High	High	Low	High
Modification	Easy	Medium	Hard	Hard
Liveness detection	Hard	Good	Hard	Good

Figure 6: 다양한 생체인식 방식의 개요는, 홍채 생체인식만이 모든 필수 요구사항을 충족할 수 있는 유일한 방식임을 보여준다. 각 방식은 장단점이 있지만, 홍채 생체인식은 전 세계적 규모에서 인간성과 고유성을 검증하는 데 있어 가장 신뢰할 수 있고 정확한 방법으로 돋보인다.

또한 홍채는 변형하기 어렵습니다. 상처를 내어 지문을 변형하는 것은 쉽지만, 지문을 정확하게 이미지화하는 것은 어렵습니다. 지문의 윤기와 골은 시간이 지나면서 마모될 수 있기 때문입니다. 게다가 10개의 지문 모두를 중복 제거에 사용하거나 서로 다른 생체인식 방식을 결합하는 것은 조합 공격(예: 서로 다른 사람들의 지문을 결합하는 공격)에 취약합니다. DNA 시퀀싱은 이론적으로 충분한 정확도를 제공할 수 있지만, DNA는 사용자에게 대한 많은 추가 개인정보를 드러냅니다(최소한 시퀀싱을 수행하는 당사자에게는). 또한 비용 측면에서 확장하기 어렵고 신뢰할 수 있는 생체 감지(liveness detection) 조치를 구현하기도 어렵습니다. 얼굴 생체인식은 DNA 시퀀싱보다 훨씬 나은 생체 감지를 제공하지만, 홍채 생체인식에 비해 정확도가 훨씬 낮습니다. 이는 등록된 사용자의 수가 증가함에 따라 오류 충돌이 증가하는 결과를 낳습니다. 최적의 조건에서도 전 세계 수십억 명 규모에서는 10% 이상의 정당한 신규 사용자가 거부되어 시스템의 포용성이 손상될 수 있습니다.

따라서, 다양한 생체인식 방식의 상충 관계를 고려할 때, 월드 네트워크의 맥락에서 전 세계적인 고유성 검증에 적합한 유일한 방식은 **홍채 인식(iris recognition)**입니다.

월드 아이디: 대규모 인간 증명 구현 (World ID: Implementing Proof of Human at Scale)

전 세계적인 규모에서 고유성을 검증할 수 있는 유일한 방법이 **홍채 생체인식**이라는 결론에 따라, Tools for Humanity는 **오브(Orb)** 라는 맞춤형 생체인식 장치를 개발했습니다. 이 장치는 AI 안전성을 갖춘 인간 증명 자격 증명인 **월드 아이디(World ID)** 를 발급합니다. 오브는 인간성과 고유성을 공정하고 포용적인 방식으로 검증하기 위해 처음부터 새롭게 구축되었습니다.



Figure 7: 개인의 인간성과 고유성을 검증하여 월드 아이디를 발급하는 오브(Orb).

월드 아이디 발급은 프라이버시를 보존합니다. 인간성 검증은 로컬에서 이루어지며, 발급자가 이미지를 저장하거나 업로드할 필요가 없습니다. 월드 아이디를 사용할 때 개인에 대한 최소한의 정보만 공개되며, 프로토콜은 **제로 지식 증명(zero-knowledge proofs)** 을 활용합니다. 장치의 비전은 개발, 생산 및 운영이 시간이 지남에 따라 탈중앙화되어 단일 기관이 월드 아이디 발급을 통제하지 않도록 하는 것입니다.

다음 섹션에서는 효과적인 인간 증명 메커니즘을 위한 앞서 언급된 구성 요소들이 월드 아이디 맥락에서 어떻게 구현되는지를 설명합니다:

- Deduplication
- Authentication
- Recovery
- Revocation
- Expiry

중복 제거 (Deduplication)

포용적이면서도 고도의 보안을 갖춘 인간 증명 메커니즘에서 가장 어려운 부분은 모든 사용자가 정확히 하나의 인간 증명을 받을 수 있도록 보장하는 것입니다. 앞선 평가에 따르면, 홍채 생체인식은 전 세계적 규모에서 고유성을 정확하게 검증할 수 있는 최선의 수단입니다(제한점 참조).

생체인식 알고리즘에 내재된 또 다른 잠재적 오류는 사용자의 잘못된 승인(false acceptance)입니다. 잘못된 승인율은 주로 **프레젠테이션 공격(presentation attacks)**— 즉, 검증 과정을 속이거나 위조하려는 시도 —을 탐지하는 시스템의 능력에 달려 있습니다. 어떠한 생체인식 시스템도 이러한 공격에 완전히 무적이지는 않지만, 중요한 지표는 성공적인 공격에 필요한 **노력의 크기**입니다. 이러한 고려는 오브를 구상하는 데 있어 근본적이었습니다. 오브 개발은 결코 가벼이 내려진 결정이 아니었습니다. 이는 높은 비용이 드는 사업을 의미했습니다. 그러나 근본적인 원리에서 보면, 인간성과 고유성을 가장 포용적이면서도 안전하게 검증할 수 있는 시스템을 구축해야 했습니다.

오브는 악의적인 행위자의 존재를 배제할 수 없는 적대적 환경에서도 높은 정확도로 고유성을 검증하도록 설계되었습니다. 이를 달성하기 위해, 오브는 전자기 스펙트럼 전반에 걸친 모든 유효한 카메라 센서와 적절한 다중 스펙트럼 조명을 갖추고 있습니다. 이를 통해 장치는 사기적 위조 시도와 실제 인간 상호작용을 높은 정확도로 구별할 수 있습니다. 또한 오브는 여러 신경망을 실시간으로 동시에 실행할 수 있는 강력한 컴퓨팅 장치가 탑재되어 있습니다. 이러한 알고리즘은 사용자 프라이버시를 보호하면서 로컬에서 인간성을 검증합니다. 물리적 세계와 상호작용하는 어떤 하드웨어 시스템도 완벽한 보안을 달성할 수는 없지만, 오브는 특히 **대 규모 공격**에 대한 방어에서 높은 기준을 세우도록 설계되었습니다. 오브에 통합된 **사기 방지 조치**는 지속적으로 개선되고 있습니다.

Deduplication Roadmap Status	
Problem	Status
False rejections	0.001% false rejection rate of the biometric algorithm on a 1B people scale ✓ Done
	Zero false rejections on 8B people scale 🔥 Hard problem Ongoing research
	Seperate verification for people with eye diseases that make iris recognition unviable 🕒 Hard operational challenge Future Implementation
False acceptance	Orb is hard to spoof on scale ✓ Done
	Orb is impossible to spoof 🔥 Hard problem No system with a real world interface can become perfect but active research, red teaming & a bug bounty program make it harder everyday

Figure 8: 10억 명 규모의 인간 증명 메커니즘을 전개하기 위해 필요한 최소한의 중복 제거 기능이 달성되었다. 그러나 인간 증명 메커니즘의 포용성과 보안을 강화하기 위한 연구는 지속되고 있다.

인증 (Authentication)

인증은 오브(Orb)에 의해 발급된 월드 아이디의 정당한 소유자만이, 단순히 키를 소유한다는 것을 증명하는 것 이상으로, 스스로를 인증할 수 있도록 보장하는 것을 목표로 합니다. 이는 월드 아이디의 판매나 도난을 방지하는 데 중요한 역할을 합니다. 월드 아이디 범위 내에서는 두 가지 주요 메커니즘이 있으며, 어떤 메커니즘을 선택할지는 검증자(verifier)에게 달려 있습니다. 각 메커니즘은 보장 수준과 마찰의 정도가 다릅니다.

얼굴 인증 (Face Authentication)

얼굴 기반 인증은 애플의 Face ID와 유사합니다. 인증은 사용자의 휴대폰에 저장된 기존 템플릿과의 1:1 비교를 포함하며, 이는 오브가 수행하는 전 세계 고유성의 1:N 검증에 비해 훨씬 낮은 수준의 정확도가 요구됩니다. 따라서 얼굴 특징에 내재된 엔트로피는 충분합니다. 이 기능을 가능하게 하기 위해, 사용자의 얼굴을 오브가 서명한 암호화된 임베딩이 종단 간 암호화되어 사용자의 모바일 기기 내 월드 아이디 지갑으로 전송됩니다. 이후 Face ID와 유사한 방식으로 사용자의 기기에서 로컬로 수행되는 얼굴 인식을 통해 사용자를 인증할 수 있으며, 이를 통해 월드 아이디가 원래 발급된 사람만 인증 목적으로 사용할 수 있도록 합니다.

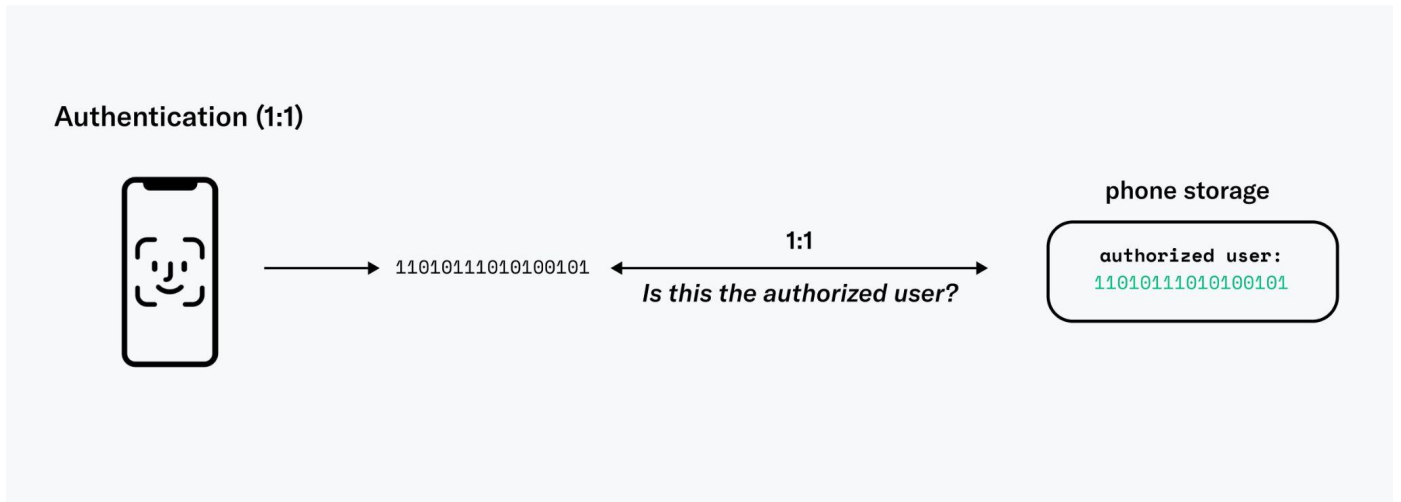


Figure 9: 사용자의 휴대폰에서 셀피를 오브가 촬영한 얼굴 이미지와 비교하여 얼굴 인증을 시각화한 그림. 이는 다른 사람의 월드 아이디를 사용하기 어렵게 만드는 데 도움이 된다.

이 메커니즘은 오브의 보안 하드웨어 보장을 사용자의 모바일 기기로 확장하는 역할을 합니다. 그러나 사용자의 기기는 본질적으로 신뢰할 수 없으므로, 적절한 코드가 실행되고 있는지 혹은 카메라 입력이 신뢰할 수 있는지에 대해 절대적인 보장은 없습니다. 보안을 강화하기 위해, 모바일 기기에서 **영지식 머신러닝(Zero Knowledge Machine Learning, ZKML)**을 연구 중입니다. 그러나 맞춤형 하드웨어가 없는 상황에서는 이 접근 방식이 오브와 동일한 보안 보장을 제공할 수 없습니다. 따라서 사용자 기기에서의 얼굴 인증은 위험이 낮은 애플리케이션에 한정해 사용해야 합니다.

이 기능은 아직 구현되지 않았지만, 올해 말 출시될 것으로 예상됩니다. 구현의 첫 단계는 오브가 종단 간 암호화된 얼굴 임베딩을 사용자의 휴대폰으로 전송하는 것입니다. 이후 이 임베딩은 셀피와 비교될 수 있습니다. 얼굴 이미지의 자가 보관(self-custody)은 얼굴 인증의 필수 조건이며, 따라서 누가 나중에 얼굴 인증에 참여할 수 있는지를 결정합니다. 따라서 이 기능은 로드맵에서 높은 우선순위를 가집니다.

홍채 인증 (Iris Authentication)

이는 개념적으로 얼굴 인증과 유사하지만, 사용자가 자신의 월드 아이디 지갑에서 생성된 특정 QR 코드를 제시하며 다시 오브를 방문해야 한다는 차이가 있습니다. 이 과정은 개인이 자신의 월드 아이디의 정당한 소유자임을 검증합니다. 오브를 통한 홍채 인증은 보안을 강화합니다.

이 인증 메커니즘은 예를 들어, 은행이나 공증인을 직접 방문해 특정 거래를 인증하는 것과 비교할 수 있습니다. 불편하기 때문에 자주 요구되지는 않지만, 더 높은 수준의 보안 보장을 제공합니다. 이 기능은 현재 활발히 개발 중이며 앞으로 몇 달 내 출시될 예정입니다.

Authentication Roadmap Status	
Problem	Status
Self-custody of images for face authentication	 In progress ETA 2-3 months
Face authentication implementation	 In progress ETA 6 months
Iris authentication implementation	 In progress ETA 2-3 months

Figure 10: 인증은 월드 아이디의 거래를 어렵게 만들어 오브 기반 인간 증명의 무결성을 높이는 데 중요한 우선순위를 가진다. 얼굴 인증의 사후 롤아웃을 위해서는 이전에 검증된 사용자들의 이미지 자가 보관이 필요하다.

복구 (Recovery)

월드 아이디를 복원하는 가장 간단한 방법은 백업을 통한 것입니다. 소셜 복구는 현재 구현되어 있지 않지만, 향후 탐구될 가능성이 큼니다. 오브 기반 인간 증명을 위한 가장 중요한 복구 메커니즘은 **재발급 (reissuance)**입니다. 사용자가 접근 권한을 잃었거나 월드 아이디가 사기 행위자에 의해 손상된 경우, 사용자는 비밀번호나 유사한 정보를 기억할 필요 없이 오브로 돌아가 월드 아이디를 재발급받을 수 있습니다.

그러나 중요한 점은, 생체인식을 통해 이루어지는 복구는 오직 월드 아이디에만 적용된다는 것입니다. 사용자의 지갑에 보관된 다른 자격 증명이나 지갑 자체는 보안상의 이유로 복구할 수 없습니다.

초기 구현은 곧 출시될 **키 회전(key rotation)**을 통해 실현될 예정입니다. 특히, 평판이나 단일 청구 보상 (single-claim rewards)과 같이 장기간 지속되는 널리파이어(nullifier)를 필요로 하는 사용 사례는, 복구 과정에서 널리파이어가 초기화될 수 있기 때문에 제한될 것입니다. 이는 제한 사항 섹션에서 논의됩니다. 그러나 이 제한은 ‘인간성(humanness)’ 증명에는 영향을 미치지 않습니다. 예를 들어, 계정을 지속적으로 세션을 통해 검증하거나, 투표 시작 시점 이전에 가장 최근 복구가 완료된 참가자만 허용하는 시간 제한 투표에서는 문제가 되지 않습니다. 키 복구를 가능하게 하려면 프라이버시를 보존하는 방식으로 어려운 연구 과제를 해결해야 합니다.

Recovery Roadmap Status	
Problem	Status
Backup & Restore	 Done
Social Recovery	 Future Evaluation
Re-Issuance	 In progress ETA 2-3 months
Recover Keys	 Hard problem Ongoing research

Figure 11: 월드 아이디를 복구하는 여러 가지 방법이 있다. 가장 쉬운 방법은 백업을 생성하고 복원하는 것이다. 백업이 없는 경우, 월드 아이디는 재발급을 통해 복원될 수 있으며, 이는 향후 2~3개월 안에 로드맵에 포함되어 있다. 안전하고 프라이버시 보존적인 방식으로 생체인식 키 복구를 구현하려면 여러 개방형 연구 과제가 해결되어야 하며, 따라서 현재로서는 생체인식 키 복구가 가능할지 불확실하다.

해지 (Revocation)

오브(Orb)가 손상된 경우, 악의적인 행위자가 이론적으로 위조된 월드 아이디를 생성할 수 있습니다.[^6] 발급자가 부적절하게 행동하거나 장치가 손상되었다고 커뮤니티가 판단할 경우, 월드 재단(World Foundation)은 기존 거버넌스 구조에 따라 특정 발급자나 장치에 연결된 월드 아이디를 자체 목적으로 “거부 목록(deny list)”에 올릴 수 있으며, 다른 애플리케이션 개발자들은 자체적인 조치를 구현할 수 있습니다. 본의 아니게 영향을 받는 사용자는 다른 어떤 오브를 통해서든 단순히 월드 아이디를 재발급받을 수 있습니다. 이 메커니즘에 대한 더 많은 세부 사항은 탈중앙화(decentralization) 부분에서 확인할 수 있습니다.

Revocation Roadmap Status	
Problem	Status
Remove from set	 In progress Blocked on Iris Authentication or Face Authentication
Field or credential level	 Future Evaluation Ongoing research

Figure 12: 해지는 처음에는 아직 해지되지 않은 활성 자격 증명 전체를 포함하는 온체인 집합을 생성하는 방식으로 구현된다. 이후에는 자격 증명 수준의 필드로 전환될 가능성이 높다.

만료 (Expiry)

실질적인 사기 행위가 없는 경우에도, 장치는 커뮤니티에 의해 취약한 것으로 판명되거나 단순히 구식의 보안 표준을 가지고 있다고 판정될 수 있습니다. 이러한 경우, 재단의 거버넌스 원칙에 따라 월드 아이디는 만료 기한이 설정될 수 있습니다. 이는 본질적으로 해지 과정과 동일하지만, 미리 정의된 만료 기간이 있어 개인에게 재검증을 위한 충분한 시간을 제공합니다(예: 1년). 또한 거버넌스에 따라 재단은 모든 참여자의 이익을 위해 인간 증명 메커니즘의 무결성을 더욱 강화하기 위해 일정 기간이 지난 후 검증을 만료시키기로 결정할 수도 있습니다.

Expiry Roadmap Status	
Problem	Status
Remove from set	 Future Evaluation
Field or credential level	 Per Default Never Expires Could be subject to change

Figure 13: 사후적 만료는 필요할 가능성이 높지만 다른 기능에 비해 우선순위가 낮으며 향후 평가될 것이다. 월드 아이디에 기본 만료 기간(즉, 특정 유효 기간 이후 사용자가 오브로 돌아가야 하는 조건)을 설정할지 여부는 아직 결정되지 않았다. 오늘날 기준으로 월드 아이디는 해지되지 않는 한 영구적으로 유효하다. 그러나 향후 몇 년간의 경험을 바탕으로 이는 변경될 수 있다.

추가 연구 (Further Research)

이 섹션에서 설명된 방어 조치들은 사기 행위의 기준선을 크게 높이며, 기존의 확장 가능한 인간 증명 검증 메커니즘을 넘어 그 영향을 제한할 수 있을 것으로 보입니다. 그러나 매수(bribery) 등 다른 방법을 통해 “한 사람당 하나의 증명(one-person-one-proof)” 원칙을 우회하려는 시도나 공모(collusion)와 같은 모든 위협으로부터 완전히 보호할 수는 없다는 점을 인식하는 것이 중요합니다. 기준선을 더욱 높이기 위해서는 메커니즘 설계 분야의 혁신적인 아이디어와 연구가 필요할 것입니다.

Footnotes

1. Possibly except for the validity date (유효 기간은 예외일 수 있음)
2. In recent implementations virtually all major providers switched from “labeling traffic lights” to the so-called silent CAPTCHAs (e.g. reCaptcha v3) (최근 구현에서 거의 모든 주요 공급자가 “신호등 고르기”에서 이른바 무음 CAPTCHA(reCaptcha v3)로 전환했다)
3. In this context, AI-safe refers to a process that’s hard for AI models. It’s assumed, for example, that spoofing the Orb is significantly harder for AI than performing a CAPTCHA. (이 맥락에서 AI-safe란 AI 모델에게 어려운 과정을 의미한다. 예를 들어, 오브를 속이는 것은 AI가 CAPTCHA를 푸는 것보다 훨씬 어렵다고 가정한다)
4. where N is the total number of previously verified users (여기서 N은 이전에 검증된 사용자 전체 수를 의미한다)
5. In the context of World ID, each holder has a unique nullifier for themselves in each application. This nullifier is what enables sybil resistance while preserving privacy as verifiers can use such nullifiers to prevent multiple registrations. (월

드 아이디 맥락에서, 각 소유자는 각 애플리케이션마다 자신에게 고유한 nullifier를 가진다. 이 nullifier는 프라이버시를 보존하면서 시빌 저항성을 가능하게 하며, 검증자는 이를 통해 다중 등록을 방지할 수 있다)

6. the Orb's secure computing environment was designed to make such compromises extremely difficult (오브의 보안 컴퓨팅 환경은 이러한 손상을 극도로 어렵게 만들도록 설계되었다)

월드코인 토크노믹스 (Worldcoin Tokenomics)

버전: 2025-08-04

사명(Mission): 글로벌 신원 및 금융 네트워크 구축

월드(World)의 사명은 전 세계에서 가장 큰 신원 및 금융 네트워크를 공공재로 구축하고, 모든 사람에게 소유권을 제공하는 것입니다. 월드코인 토큰(WLD)에 관한 프로젝트의 목표는 다음과 같습니다:

- WLD 토큰의 대다수는 단순히 고유한 인간으로 검증받은 개인들에 의해 청구될 것입니다.
- 오늘날 살아 있는 인류의 대다수가 WLD 토큰을 청구하게 될 것이며, 이는 WLD가 가장 널리 분배된 디지털 화폐가 될 수 있음을 의미합니다.
- WLD 토큰은 월드 아이디(World ID)와 함께 프로토콜 거버넌스에 사용될 것입니다.
- WLD 토큰은 가장 큰 익명 신원 및 금융 네트워크의 기반을 형성할 것입니다.

WLD 소개 (Introducing WLD)

WLD는 거버넌스 속성을 가진 암호화폐로 설계되었으며, 궁극적으로 사용자에게 프로토콜의 미래에 대한 발언권을 부여하는 것을 목표로 합니다. 기존의 “1토큰-1표(one-token-one-vote)” 거버넌스 메커니즘을 넘어, 월드 아이디의 도입은 “1인-1표(one-person-one-vote)” 메커니즘을 가능하게 합니다. 이 두 메커니즘은 다양한 방식으로 결합될 수 있으며, 이를 통해 새로운 형태의 거버넌스를 가능하게 합니다. 현재 월드 재단(World Foundation)이 프로토콜의 관리자로 활동하고 있지만, 월드 아이디와 WLD 토큰이 월드의 미래 거버넌스 모델에서 어떻게 상호작용해야 하는지에 대한 제안을 받고 커뮤니티 거버넌스 프로젝트와 협력할 계획입니다.

사용자 커뮤니티는 토큰의 거버넌스 활용도를 결정할 수 있으며, 그 외에도 몇 가지 다른 사용 사례가 등장할 수 있습니다. 예를 들어, 사용자는 WLD를 월드 네트워크 생태계 내에서 사용하여, 월드 앱(World App) 또는 다른 지갑 앱에서 팁을 주거나, 상품을 사고팔거나, 특정 원인이나 이니셔티브에 대한 지지를 표시하는 기능에 접근할 수 있도록 결정할 수 있습니다.

현재 월드 재단은 프로젝트를 운영하고 있으며, 거버넌스와 생태계를 점진적으로 탈중앙화하기 위해 노력하고 있습니다. 탈중앙화의 목표는, 대다수의 WLD 토큰 공급을 단순히 인간이라는 이유만으로 월드 네트워크 참여자들에게 제공하는 월드 재단의 독특한 접근 방식에 의해 촉진될 것입니다.

WLD 토큰 (The WLD Token)

항목	내용
출시일 (Launch Date)	2023년 7월 24일
네트워크 정보 (Network Information)	월드코인(Worldcoin, WLD)은 이더리움 메인넷(Ethereum Mainnet) 상의 ERC-20 토큰입니다. 사용자가 청구하는 토큰은 월드 체인 메인넷(World Chain Mainnet) 에서 브릿징된 WLD 토큰으로 수령됩니다. 월드 체인은 이더리움 위의 OP Stack 레이어-2 네트워크입니다. 따라서 대부분의 WLD 거래는 월드 체인에서 이루어질 것으로 보입니다. 필요할 경우, 토큰은 OP Stack 슈퍼브리지(Superbridge) 를 통해 이더리움으로 다시 브릿징될 수 있습니다.
주소: Ethereum	0x163f8C2467924be0ae7B5347228CABF260318753
주소: World Chain (주요 접근 및 사용 venue)	0x2cFc85d8E48F8EAB294be644d9E25C3030863003
주소: Optimism	0xdC6fF44d5d932Cbd77B52E5612Ba0529DC6226F1 2023년 7월 24일부터 2024년 10월 17일까지 Optimism은 WLD의 주요 접근 및 사용 venue였습니다. 현재도 WLD는 Optimism에서 사용 가능하지만, 주요 접근 및 사용 venue는 월드 체인입니다.
업그레이드 가능성 (Upgradability)	없음. (None) 토큰 출시 후 15년이 지난 시점부터 인플레이션이 시작될 수 있다는 점을 제외하면, 어떤 통제도 없습니다. (인플레이션 관련 내용은 아래 참조)
토큰 할당 주체 (Token allocation entity)	영국령 버진아일랜드(British Virgin Islands)에 설립된 World Assets, Ltd. 월드 재단(World Foundation)이 해당 법인의 유일한 멤버이자 이사입니다.
초기 공급 한도 (Initial supply cap)	100억(10B) WLD 토큰 (인플레이션 관련 내용은 아래 참조)
인플레이션 (Inflation)	초기 100억 개의 토큰을 초과하는 WLD 공급의 인플레이션은 토큰 출시 후 최소 15년 이후(구체적으로 2038년 7월 24일, 04:00 UTC)부터 시작될 수 있습니다. 인플레이션율은 프로토콜 거버넌스에 의해 결정됩니다. 새로 발행된 토큰의 할당 역시 거버넌스에 의해 결정됩니다. WLD 토큰 스마트 컨트랙트에 의해 강제되는 인플레이션 상한은 연 1.5%입니다. 기본 인플레이션율(default inflation rate) = 0%

이용 가능성 (Availability)

월드코인 토큰은 뉴욕주(State of New York) 또는 특정 제한 지역(restricted territories)에 거주하거나, 위치하거나, 법인 설립 또는 등록 대리인을 두고 있는 개인이나 회사에는 제공되지 않습니다. 이용 약관(Terms of Use)에서 자격에 대한 추가 제한을 포함한 더 많은 세부 정보를 확인할 수 있습니다.

안전 유의사항 (Safety reminder)

월드와 연관되어 있다고 주장하는 가짜 앱이나, 가짜 WLD 토큰을 판매하거나 제공하려는 플랫폼 또는 제3자에 주의하십시오! WLD를 거래할 때는 반드시 위에 명시된 올바른 토큰 주소를 사용하고 있는지 확인해야 합니다. WLD가 이더리움(Ethereum), 월드 체인(World Chain), Optimism이 아닌 다른 체인으로 “브릿징”되었다면, 이 브릿징된 버전이 안전하며 언제든지 이더리움, 월드 체인, Optimism 상의 WLD로 교환(redeem)되거나 다시 브릿징될 수 있는지 반드시 확인하십시오. 월드 재단(World Foundation)과 그 계열사는 제3자가 배포한 어떤 브리지의 생성, 운영, 보안에 대해서도 책임을 지지 않으며, 그러한 브리지를 통해 브릿징된 WLD에 대해서도 책임을 지지 않습니다.

중요한 사용자 정보 (Important User Information)

암호화폐, 토큰, 블록체인 애플리케이션은 매우 높은 위험을 내포하고 있습니다. 이들은 새로운 동시에 빠르게 진화하는 기술이며, 그 가용성, 사용, 효용, 가치, 기능성은 제3자의 행위, 시장 요인, 규제 환경, 그리고 새롭게 등장하거나 변화하는 기술과 행태에 따라 좌우되고 영향을 받습니다. 이러한 요인들은 상당한 복잡성을 만들어내며 새로운 예기치 못한 위험이나 결과를 초래합니다. WLD는 가치나 효용이 결코 증가하지 않을 수도 있으며, 가치와 효용을 모두 잃을 수도 있습니다.

더 많은 정보는 www.world.org/risks 에서 확인할 수 있습니다.

WLD 토큰 분배 (WLD Token Allocation)

아래 그림은 WLD 전체 공급량이 네 가지 주요 이해관계자 그룹에 어떻게 배분되는지를 보여줍니다. 주목할 점은, 출시 이후 토큰 분배는 TFH 투자자 + 팀 + TFH 준비금 분배(25%) 내에서만 변경되었으며, 월드 커뮤니티(World Community) 토큰 75%는 이에 영향을 받지 않는다는 것입니다.

WLD Token Allocation

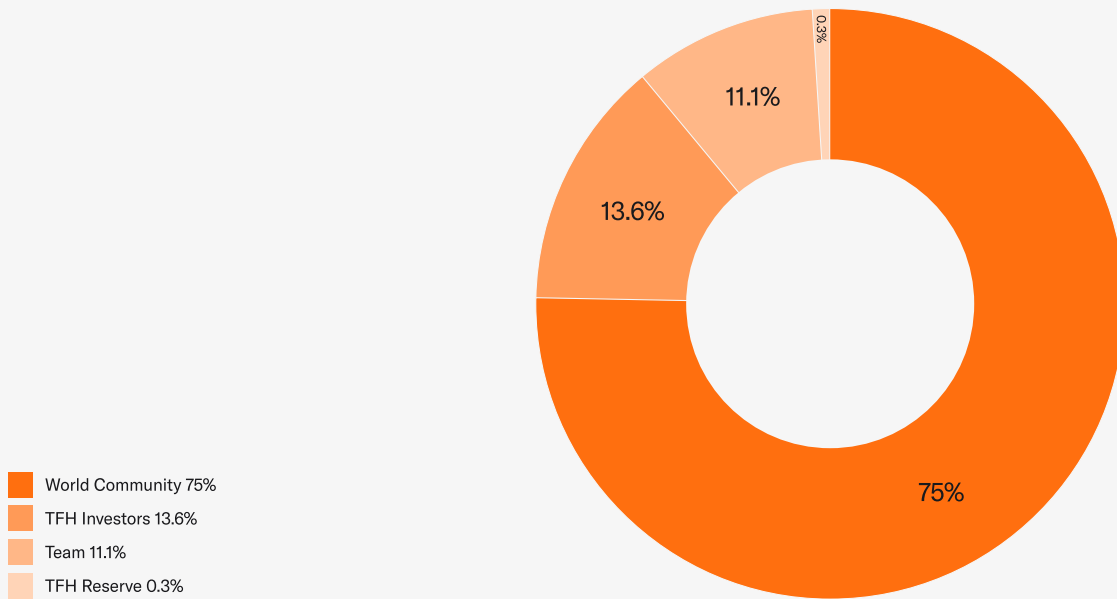


Figure 4.1: 2025년 4월 28일 기준 WLD 토큰 분배 현황 (전체 초기 100억 토큰 공급량의 백분율)

토큰 분배 세부 내용

비율 (Percentage)	카테고리 (Category)	설명(Description)
75%	월드 커뮤니티 (World Community)	월드 재단(World Foundation)은 정관(Articles of Association)에 따라 이 토큰의 분배를 관리하며, 토큰 관리 의사결정의 탈중앙화를 지속적으로 추진할 임무를 가지고 있습니다. 이러한 토큰 대부분은 사용자에게 할당되며, 일부는 생태계 펀드와 네트워크 운영에 사용됩니다 (자세한 내용은 아래).
11.1%	팀 (Team)	이 토큰은 TFH 팀 및 월드 개발을 위한 단계를 수행한 기타 서비스 제공자들에게 할당됩니다.
13.6%	TFH 투자자 (TFH Investors)	TFH 투자자들은 다년간의 사전 출시(pre-launch) 단계에서 TFH가 월드를 지원할 수 있도록 자금을 제공했습니다.
0.3%	TFH 준비금 (TFH Reserve)	TFH는 향후 필요를 충족하기 위해 WLD 토큰 준비금을 유지합니다.

언락 공급량(Unlocked Supply)과 유통 공급량(Circulating Supply)

이 섹션에서는 토큰 락업(lock-up)과 WLD가 어떻게 유통되는지를 다룹니다. 이해해야 할 두 가지 용어는 다음과 같습니다:

- **유통 공급량(Circulating supply):** 자유롭게 유통되는 WLD 토큰의 총량을 의미합니다. 이는 특정한 전송 제한이 부과되지 않았으며, 프로토콜의 거버넌스 재량에 따라 통제되지 않는 토큰을 뜻합니다. 여기에는 외부 참여자가 언제든지 획득할 수 있는 토큰(예: 유동성 포지션)도 포함됩니다.
- **언락 공급량(Unlocked supply):** 유통 공급량에 속하거나, 유통 공급량으로의 출시 속도(rate of release)가 프로토콜 거버넌스의 재량에 달려 있는 언락된 토큰의 총량을 의미합니다.

언락 공급 스케줄 (Unlocked Supply Schedule)

언락 공급 스케줄의 중요한 특징은 (a) 팀과 투자자 토큰은 락업의 대상이 되는 반면, (b) 사용자가 청구한 토큰은 락업되지 않는다는 점입니다. 아래 그림은 15년 동안의 WLD 토큰 언락 스케줄을 보여줍니다. 중요한 점은, 거버넌스가 월드 커뮤니티 카테고리의 WLD 토큰이 유통 공급량에 도입되는 속도를 결정한다는 것입니다. 이는 여러 요인, 특히 월드 사용자 수가 증가하는 속도에 따라 달라집니다. 따라서, 언락 공급량은 최대 유통 공급량의 상한선을 나타냅니다.

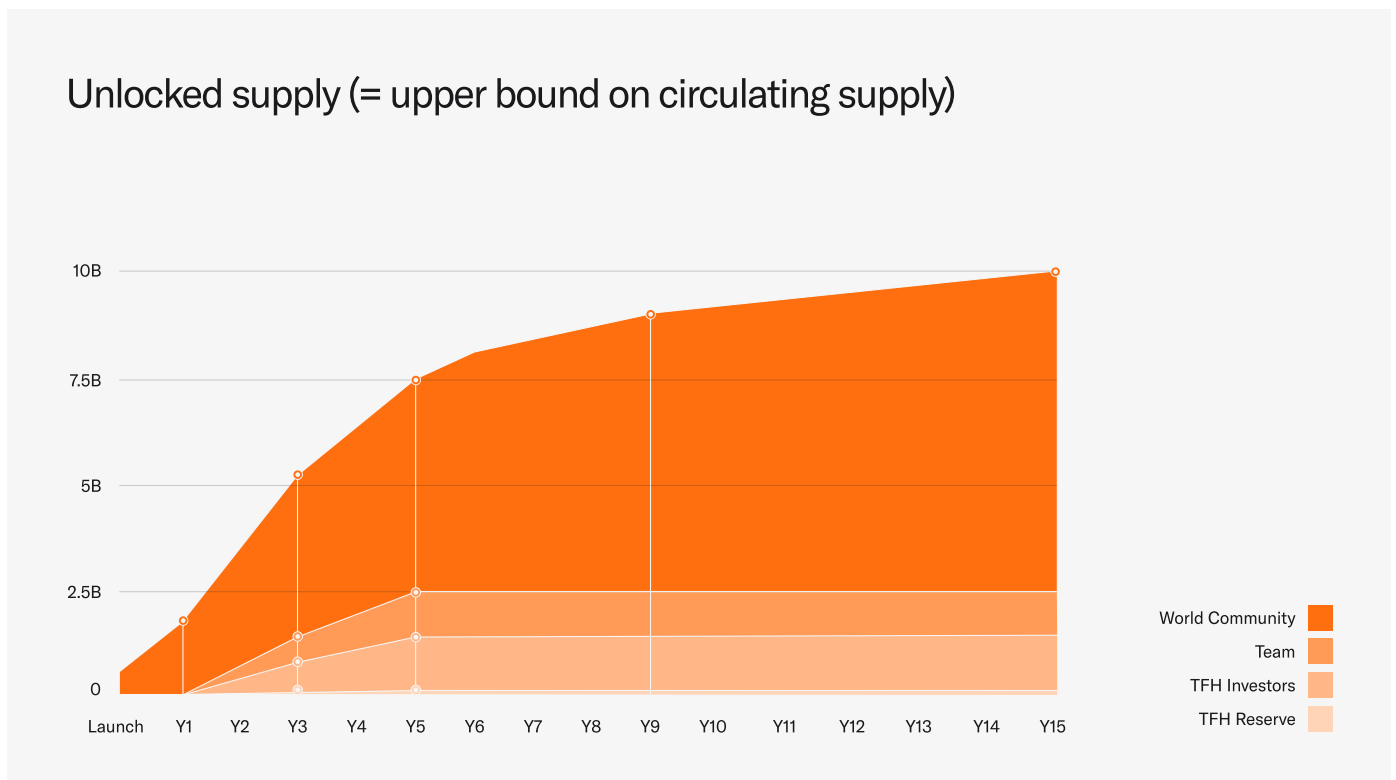


Figure 4.2: 15년간의 WLD 토큰 언락 공급 스케줄(유통 공급량의 상한선을 나타냄). 거버넌스는 언락된 월드 커뮤니티 토큰이 유통 공급량에 도입되는 속도를 통제한다. 15년 이후에는 거버넌스가 연간 최대 1.5%의 인플레이션율을 시행할 수 있다.

참고: 단순화를 위해 위 그림은 TFH 준비금(TFH Reserve)에 포함된 토큰이 **2025-04-27부터 시작되는 1년 전체 락업** 이후 **2년의 선형 언락**을 따른다고 가정합니다(아래 참조). 이 토큰들은 현재 배정되지 않았기 때문에, 추가적인 락업 기간의 대상이 될 수 있으며, 그림에 표시된 것보다 더 늦게 언락될 수 있습니다. 언락 스케줄의 라이브 버전은 Dune에서 확인할 수 있습니다.

아래는 각 수령자 카테고리별 언락 공급 스케줄의 세부 사항입니다:

월드 커뮤니티 토큰 (World Community Tokens)

출시 전에, 월드 커뮤니티에 할당된 75억(7.5B) WLD 토큰은 모두 발행되었습니다. 그러나 이들 대부분은 15년에 걸쳐 언락됩니다 (세부사항은 아래 참조). 이 언락 스케줄은 생태계 참여자들에게 이 토큰이 제공되는 속도를 제한합니다. 토큰의 언락 스케줄은 네 개의 스마트 컨트랙트(1, 2, 3, 4)에 의해 집행됩니다. 중요한 점은, 사용자와 운영자에게 할당된 토큰은 락업되지 않는다는 것입니다.

아래 표에 나타난 WLD 토큰 수량은 지정된 기간 동안 언락됩니다. 각 기간 동안 매일 동일한 수량의 토큰이 언락됩니다.

기간 (Time Period)	기간 중 언락된 WLD 수량 (Amount of WLD Unlocked During Period)	기간 종료 시점 누적 언락 WLD (Cumulative WLD Unlocked at End of Period)
출시 시 (At Launch)	0.5B WLD	0.5B WLD
출시 ~ 3년차 종료 (Launch – End of Year 3)	3.5B WLD	4B WLD
4년차 시작 ~ 6년차 종료 (Start of Year 4 – End of Year 6)	1.75B WLD	5.75B WLD
7년차 시작 ~ 9년차 종료 (Start of Year 7 – End of Year 9)	0.875B WLD	6.625B WLD
10년차 시작 ~ 15년차 종료 (Start of Year 10 – End of Year 15)	0.875B WLD	7.5B WLD

참고: 월드는 네트워크를 모든 인류에게 확장하는 것을 목표로 합니다. 프로젝트가 성장함에 따라, 커뮤니티에 속하지 않은 사람들의 수는 필연적으로 줄어듭니다. 이러한 역학을 고려할 때, 출시 직후 몇 년 동안은 월드 커뮤니티를 위해 상당한 양의 토큰이 제공됩니다. 이 시기가 가장 많은 사람들이 합류할 수 있고 성장 속도가 가장 빠르기 때문입니다. 이 때문에 40억(4B) 개의 월드 커뮤니티 토큰이 최초 3년 동안 언락됩니다. 그러나 이 토큰들이 유통 공급량으로 진입하는 속도는 네트워크 성장 속도에 달려 있습니다.

TFH 팀 및 투자자 토큰 (TFH Team and Investor Tokens)

TFH 투자자에게 할당된 토큰은 투자자가 각자의 토큰 워런트(token warrants)를 행사한 후(출시 시 가능) 12개월 동안 전면 락업(contractually fully locked up)되었습니다. 팀 토큰도 동일하게 12개월의 전면 락업이 적용되었습니다. 전체 락업 기간이 끝난 후, 약 80%의 TFH 팀 및 투자자 토큰은 48개월 동안 선형적으로 언락되기 시작했으며, 약 20%는 24개월 동안 선형적으로 언락되었습니다. 따라서 대부분의 토큰은 프로토콜 출시 5년 후인 2028년 7월 말까지 언락이 완료됩니다.

원래는 모든 언락 스케줄이 24개월이었으나, 2024년 7월에 대다수 토큰의 언락 기간이 48개월로 연장되었습니다. 월드 재단은 이전에 이러한 언락에 대한 정보를 공유한 바 있습니다 ([링크 참조](#)). 이처럼 매우 점진적인 언락 스케줄은 다른 많은 프로젝트보다 길며, 월드의 장기적 성격과 일치합니다. 또한 팀 멤버의 토큰은 일반적으로 TFH 근속 기간(tenure)에 연동된 자체 베스팅 스케줄(vesting schedules)에 의해 추가적으로 제한될 수 있습니다.

TFH 준비금 (TFH Reserve)

TFH 준비금에 포함된 토큰은 할당 시점부터 최소 1년간 전면 락업(contractually locked up)되며, 이후 2년에 걸친 선형 언락을 거칩니다. 정확한 락업 기간은 이 토큰들이 언제 할당되는지에 따라 달라집니다.

출시 시점의 유통 공급량 (Circulating Supply at Launch)

Figure 4.2는 시간에 따른 언락된 WLD 토큰의 양을 보여줍니다. 이는 유통 공급량과는 다릅니다. 유통 공급량에는 재단의 금고에 보관되어 있으나 특정 용도로 할당되지 않은 언락된 WLD 토큰은 포함되지 않습니다.

WLD의 유통 공급량은 주로 네트워크 규모와 사용량에 따라 증가합니다. 출시 시점에 약 200만 명의 인간이 검증되었으며, 이들에게 사전 출시 단계에서 총 4,300만(43M) 베타 WLD 토큰이 할당되었습니다. 월드의 목표가 가능한 많은 인간으로 네트워크를 구축하는 것이므로, 출시 시점의 WLD 유통 공급량은 총 공급량의 1%인 1억 70만(100.7M) WLD로 매우 낮았습니다. 이 공급량은 다음과 같은 부분으로 구성되었습니다:

- 출시 시점에 사용자들이 사전 출시 단계에서 70만(700k) WLD 토큰을 마이그레이션했습니다. 나머지 4,230만(42.3M) WLD는 출시 이후 일정 기간 동안 마이그레이션 가능 상태로 남아 있었습니다.
- 1억(100M) WLD 토큰이 미국 외에서 활동하는 트레이딩 회사들에 대출되었습니다.

출시 이후 WLD의 유통 공급량은 꾸준히 증가했습니다. 2025년 4월 28일 기준으로 약 13억(1.3B) WLD(즉, 총 공급량의 13%)에 달합니다. 실시간 수치는 Dune 대시보드에서 확인할 수 있습니다.

재단의 토큰 할당 목표 (Foundation's Token Allocation Goal)

프로토콜이 자급자족할 수 있을 때까지, 월드 재단(World Foundation)은 월드 커뮤니티 토큰의 관리자로 활동합니다. 그 역할의 일환으로, 재단은 이 토큰들을 세 가지 목적으로 할당했습니다:

1. 사용자 토큰(User tokens)
2. 네트워크 운영(Network operations)
3. 생태계 펀드(Ecosystem fund)

시간에 따른 월드의 진화는 여러 요인에 의해 영향을 받을 수 있으며, 각각은 중요한 의미를 가질 수 있습니다. 이러한 요인에는 현장에 배치된 오브(Orb)의 수, 주당 신규 검증 수, 월드 사용자들의 활동, 월드 기능을 활용하려는 상인·플랫폼·개발자 및 기타 주체의 수와 위치, 향후 거버넌스 결정, 그리고 수많은 알려진/알려지지 않은 요인들이 포함됩니다. 따라서 월드 커뮤니티 토큰의 최종 할당은 아직 확정될 수 없습니다.

그럼에도 불구하고, 프로젝트의 목표와 현재 규모를 고려하여, 월드 재단은 아래 그림과 같이 **지향적 토큰 할당 목표**를 수립했습니다:

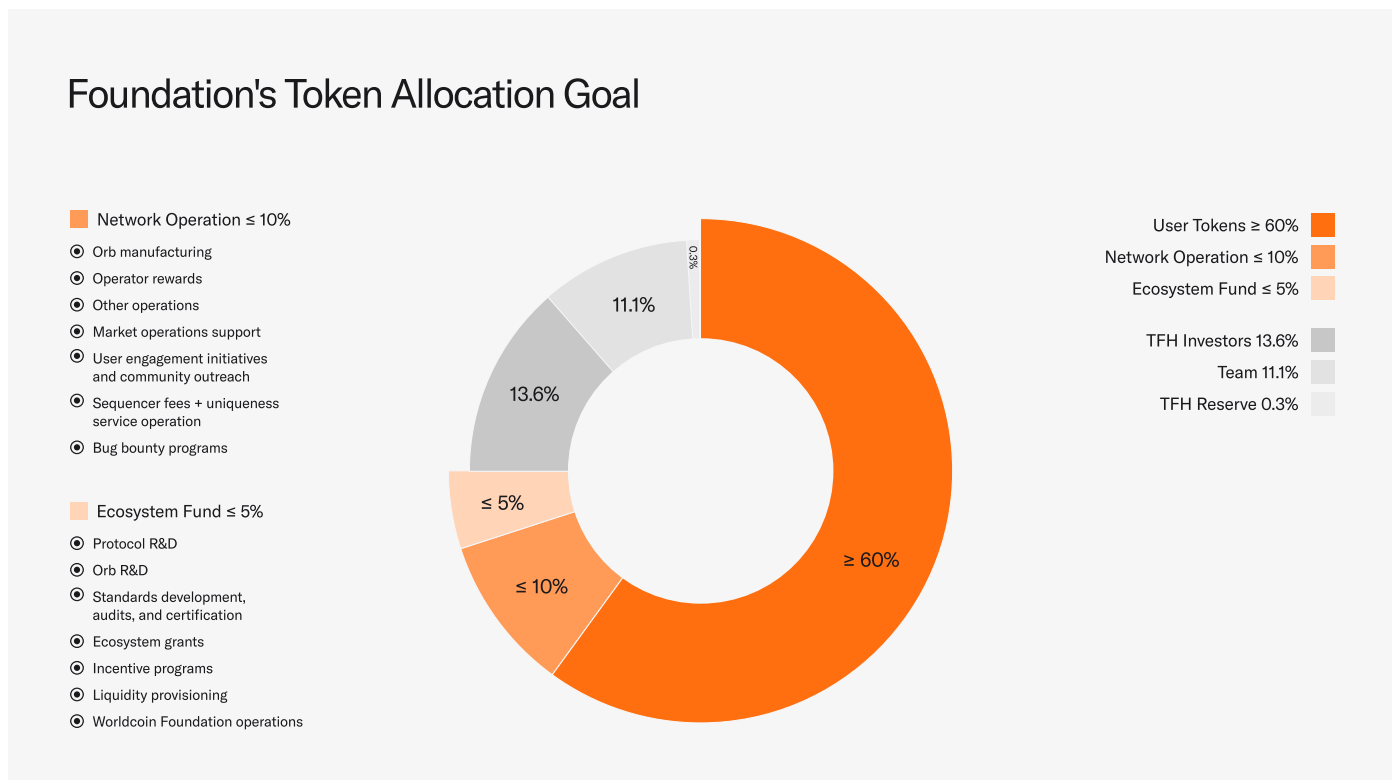


Figure 4.3: 재단의 토큰 할당 목표. 네트워크 운영 및 생태계 펀드 카테고리에서는 주요 비용 항목도 함께 표시된다.

월드 재단은 월드 네트워크의 성장을 좌우하는 다양한 요인에 맞추어, 최대한 많은 WLD 토큰이 사용자에게 할당되도록 하는 것을 목표로 합니다. 이는 시간이 지남에 따라 재단이 네트워크 운영 및 생태계 펀드에 할당하는 토큰의 양이 위 그림에 표시된 것보다 줄어든 수 있음을 의미합니다.

사용자 토큰 (User Tokens) (목표 할당: ≥ 60%)

월드코인의 토크노믹스는 WLD 토큰의 대다수가 시간이 지남에 따라 사용자 토큰(user tokens)의 형태로 개인에게 자유롭게 청구(claim) 가능하다는 점에서 독특합니다. (이전에는 “사용자 그랜트(user grants)” 또는 “WLD 에어드롭(airdrop)”이라고 불렸습니다.) 개인은 월드 네트워크에 참여하고 자신의 고유한 인간성(humanness)을 검증하는 것만으로 이 토큰을 청구할 수 있습니다. 이 때문에 WLD의 유통 공급량은 주로 네트워크 규모와 사용량에 따라 증가합니다.

평등성은 프로젝트의 핵심 가치 중 하나이므로, 출시 시점에 대규모 1회성 에어드롭은 이루어지지 않았습니다. 그러한 이벤트는 소수의 집단에게 토큰이 집중될 가능성이 있었기 때문입니다. 대신, WLD 토큰의 가용성은 다음 세 가지 원칙에 기반합니다:

1. **고유한 인간성(Unique humanness):** 고유하게 검증된 모든 인간은 사용자 토큰을 청구할 자격이 있습니다(상기된 가용성에 따름).
2. **공정성(Fairness):** 특정 시점에서, 적용 가능한 모든 국가의 검증된 개인은 동일한 수량의 토큰을 청구할 수 있습니다(가용성에 따름).
3. **인센티브(Incentives):** 사용자 토큰은 시간이 지남에 따라 분배되며, 청구 가능한 수량은 시간이 지남에 따라 감소합니다. 이는 사용자가 네트워크에 조기에 합류하고 프로토콜에 정기적으로 참여하도록 추가적인 동기를 부여하며, 새로운 네트워크 출시 시 내재된 콜드스타트 문제를 해결합니다.

사용자 토큰은 **투자 상품이 아닙니다**. 이미 자격을 갖춘 자격 증명(아래 참조)을 월드 아이디어에 연결한 경우, 어떠한 가치도 월드에 제공하지 않고 사용자 토큰을 청구할 수 있습니다. 청구 자체는 영지식 증명(zero-knowledge proofs)을 통해 자격을 확인하는 단순한 절차입니다. 가치 상승이나 보장의 약속은 존재하지 않으며, 월드 네트워크에 참여하기 위해 사용자 토큰을 반드시 청구할 필요도 없습니다.

사용자가 WLD 토큰을 청구하는 방법 (How users can claim WLD tokens)

사용자가 사용자 토큰을 청구하려면, 월드 아이디어에 프로토콜이 사용자 토큰 청구 자격으로 인정하는 자격 증명을 연결해야 합니다. 현재 두 가지 자격 증명이 인정됩니다:

1. **인간 증명 자격 증명(Proof of human credential):** 개인은 오브(Orb)에서 고유성을 검증함으로써 획득하며, 이는 자동으로 월드 아이디어에 연결됩니다.
2. **여권 자격 증명(Passport credential)** (일부 국가에서는 정부 신분증 자격 증명): 개인은 휴대폰을 사용하여 NFC를 지원하는 정부 발급 신분증(예: 여권)을 연결함으로써 이를 월드 아이디어에 연결할 수 있습니다. 단, 일부 관할권에서는 이러한 자격 증명이 제공되지 않을 수 있습니다.

자격을 갖춘 개인은 이후 호환 가능한 앱(예: 월드 앱(World App))을 통해 프로토콜에서 자격 증명이 등록되었는지를 확인한 뒤, 다음 두 가지 유형의 사용자 토큰 수량을 청구할 수 있습니다:

- **최초 사용자 토큰 수량 (First User Token Amount):** 자격 증명이 추가된 후 24시간이 지나면 첫 번째 사용자 토큰 수량을 청구할 수 있습니다. 2025년 8월 1일 기준으로, 인간 증명 자격 증명은 25 WLD, 여권 자격 증명은 12.5 WLD입니다. 이 수량은 시간이 지남에 따라 감소할 것으로 예상됩니다.
- **반복 사용자 토큰 수량 (Recurring User Token Amounts):** 자격 증명이 추가된 후 한 달이 지나면 첫 번째 반복 사용자 토큰 수량을 청구할 수 있습니다. 각 반복 사용자 토큰 수량은 한 달 동안 전

세계 모든 (자격을 갖춘) 개인에게 청구 가능하며, 특정 시점에서는 모두 동일한 수량이지만 시간이 지남에 따라 감소합니다. 2025년 8월 기준 반복 수량은 인간 증명 자격 증명의 경우 3.22 WLD, 여권 자격 증명의 경우 1.61 WLD입니다. 반복 사용자 토큰 수량 청구 권한은 현재로서는 만료되지 않지만, 거버넌스가 향후 변경할 수 있습니다.

같은 개인이 인간 증명 자격 증명과 여권 자격 증명을 모두 연결한 경우, 각 자격 증명에 해당하는 (최초 및 반복) 사용자 토큰 수량을 모두 청구할 수 있습니다. 예를 들어, 2025년 4월에 두 자격 증명을 모두 연결한 개인은 최초 사용자 토큰 수량으로 총 $25 + 12.5 = 37.5$ WLD를 청구할 수 있습니다.

오늘 자격을 갖춘 사용자가 있다면, 그가 향후 1년 동안 최대 몇 개의 WLD를 청구할 수 있는지 계산할 수 있습니다. 이를 위해, 최초 사용자 토큰 수량과 1년 동안 예정된 미래 반복 사용자 토큰 수량(기술 정보 참조)을 합산합니다. 월드 앱의 **월드코인 미니 앱(Worldcoin Mini App)**은 현재 이 결과를 사용자의 총 사용자 토큰 수량으로 표시하여 반복 수량 스케줄의 복잡성을 추상화합니다.

2025년 8월 1일 기준으로, 스마트 컨트랙트에 현재 설정된 미래 반복 사용자 토큰 수량은 다음과 같습니다. (거버넌스는 이 수량을 변경할 수 있습니다.)

반복 사용자 토큰 수량 (Recurring User Token Amounts)

연도 (Year)	월 (Month)	반복 사용자 토큰 수량, 인간 증명 자격 증명 (WLD)	반복 사용자 토큰 수량, 여권 자 격 증명 (WLD)
2025	8월 (August)	3.22	1.61
2025	9월 (September)	3.20	1.60
2025	10월 (October)	3.18	1.59
2025	11월 (November)	3.16	1.58
2025	12월 (December)	3.14	1.57
2026	1월 (January)	3.12	1.56
2026	2월 (February)	2.68	1.43
2026	3월 (March)	2.60	1.30
2026	4월 (April)	2.34	1.17
2026	5월 (May)	2.08	1.04
2026	6월 (June)	1.82	0.91
2026	7월 (July)	1.56	0.78
2026	8월 (August)	1.36	0.68

청구되지 않은 WLD 토큰은 월드 커뮤니티 풀에 남아 있습니다. 중요한 점은, “청구(claim)”라는 용어는 위에서 설명한 사용자 토큰 수량을 수령하는 과정을 의미하며, 개인과 월드 재단(World Foundation) 또는 다른 어떤 주체 간의 법적 관계를 창출하거나 암시하는 것이 아닙니다.

사용자 토큰 수량에 대한 거버넌스 (Governance over user token amounts)

사용자 토큰 수량은 프로토콜 거버넌스에 의해 설정됩니다. 현재는 월드 재단을 통해 거버넌스가 구현되고 있지만, 시간이 지남에 따라 점점 더 탈중앙화될 것으로 예상됩니다. 이는 거버넌스가 사용자 토큰의 발행 메커니즘을 변경할 수도 있음을 의미합니다. 예를 들어, 시스템이 안정화되면 거버넌스는 스마트 컨트랙트에 구현된 규칙에 따라 사용자 토큰 수량을 자동으로 업데이트하도록 결정할 수 있습니다.

사용자 토큰 발행의 장기적 지속 가능성 (Long-term sustainability of the user token emission)

모든 인간에게 WLD 토큰을 제공한다는 목표를 달성하기 위해(가용성 및 적격성에 따름), 거버넌스는 몇 년 후 반복 사용자 토큰 수량을 종료하고 최초 사용자 토큰 수량만 유지하기로 결정할 수도 있습니다. 이렇게 하면 나머지 토큰을 미래의 신규 사용자들을 위해 보존할 수 있습니다. 앞서 설명했듯, 거버넌스는 또한 향후 사용자 토큰 발행을 위한 미래 수수료 수익(World ID fees)의 일부를 사용자 토큰으로 할당하기로 결정할 수도 있습니다. 마지막으로, 출시 후 15년이 지나면 거버넌스는 사용자 토큰 메커니즘을 지속하기 위해 연 1.5%까지의 인플레이션율을 시행하기로 결정할 수도 있습니다.

역사적 참고: 검증되지 않은 개인을 위한 사용자 토큰 예약 (Historical note: user token reservations for unverified individuals)

출시 이후 일정 기간 동안, 개인은 검증 이전에 사용자 토큰 수량을 **예약(reserve)** 할 수 있었으며, 오브(Orb)에서 검증을 마친 후 예약된 수량을 받을 수 있었습니다. 예약은 이제 종료되었으며, 이러한 예약의 상환은 2025년 7월에 마감됩니다.

역사적 참고: 사전 출시 단계에서의 사용자 토큰 할당 (Historical note: User token allocations during the pre-launch phase)

월드의 사전 출시 단계(2021년 5월 ~ 2023년 7월) 동안, 베타 WLD 토큰은 다양한 단계에서 사용자들에게 할당되었습니다(가용성에 따름). 사용자는 출시 시점 또는 이후에 자신들의 베타 WLD를 WLD로 마이그레이션할 수 있었습니다.

이 섹션의 나머지 부분에서는 재단의 토큰 할당 목표 내 다른 카테고리에 대해 논의합니다.¹

네트워크 운영 (Network Operation) (목표 할당: ≤ 10%)

WLD 토큰 공급량의 일부는 월드 커뮤니티에 할당되며, 네트워크 운영을 지원하는 데 사용될 예정입니다. 이 섹션에서는 네트워크의 주요 운영 비용을 설명하지만, 이 목록은 포괄적인 것이 아닙니다. 필요할 경우, 이러한 비용은 월드 재단(World Foundation)이 네트워크 운영에 할당된 WLD 토큰의 일부를 법정화폐 또는 기타 통화로 전환하여 충당할 수 있습니다.

네트워크 운영의 영역과 책임

월드 재단은 월드 프로젝트의 관리자로서 커뮤니티를 지원하고 성장시키는 역할을 합니다. 월드 재단은 월드 아이디(World ID) 프로토콜, 오브(Orb), 월드 체인(World Chain), 월드코인 토큰 프로토콜에 대한 지식재산권(IP)을 보유하고 있습니다. 또한 월드 재단은 월드 커뮤니티에 할당된 전체 WLD 토큰의 75%를 관리합니다. 프로젝트 목표에 따라, 재단은 이 토큰의 일부를 네트워크 운영과 생태계 구축에 할당하고 있으며, 여기에는 월드 아이디 가입 시퀀서(sign-up sequencer) 및 고유성 서비스, 월드 체인을 지원하는 기관, 사용자 참여, 커뮤니티 아웃리치(outreach) 등이 포함됩니다.

네트워크 운영의 다른 영역은 생태계 기여자의 책임입니다. 여기에는 오브 제조 및 운영이 포함됩니다. 이러한 생태계 기여자 중 하나는 월드 네트워크를 출범시킨 초기 개발 회사인 TFH(Tools for Humanity)입니다.

월드 재단은 네트워크 운영을 추가적인 서비스 제공자와 탈중앙화된 구조를 통해 더욱 탈중앙화하여, 네트워크 운영의 장기적 지속 가능성을 보장할 계획입니다.

오브 제조 (Orb Manufacturing)

WLD 토큰 공급량의 일부는 지속적인 제조 비용을 충당하는 데 사용됩니다. 이를 위해, 월드 재단은 TFH와 협력하여 오브 제조를 감독합니다. 향후에는 다른 서비스 제공자가 오브 또는 유사한 장치를 제조하도록 참여할 수도 있습니다.

오브 운영 (Orb Operations)

오브 운영자(Orb Operators)는 독립적인 생태계 참여자로서 오브를 운영하며, 오브에서 개인을 검증해주는 대가로 운영자 보상(Operator rewards)을 받습니다. 운영자는 사용자가 프로젝트를 이해하고 검증 과정에서 지원을 받을 수 있도록 교육함으로써 고품질 경험을 제공하는 것이 중요합니다. 운영자의 재정적 이익을 월드의 목표와 일치시키기 위해, 운영자 보상은 가입 품질(sign-up quality) 측정에 의해 영향을 받습니다.

월드의 장기적 재정적 지속 가능성을 보장하기 위해(재단의 장기 목표는 50,000개의 오브 배치), 공정한 운영자 보상을 결정하기 위해 경쟁 메커니즘이 시험되었습니다. 이는 또한 운영자가 프로젝트의 변화하는 요구에 빠르게 적응하고 혁신하도록 장려합니다. 운영자 보상의 대부분은 WLD 토큰으로 지급되며(상기된 가용성에 따름), 소량은 USDC로 지급됩니다.

기타 운영 (Other Operations)

WLD 토큰 공급량의 일부는 월드 재단에 의해 기타 운영 비용을 충당하는 데 사용되며, 여기에는 오브 배치와 관련된 물류, 운영자에게 제공되는 장비 생산 등이 포함됩니다.

시장 운영 지원 (Market Operations Support)

WLD 토큰 공급량의 일부는 월드 재단에 의해 시장 운영 지원 자금으로 사용되며, 여기에는 전 세계 운영자 네트워크의 모집, 교육, 조정이 포함됩니다.

사용자 참여 이니셔티브 및 커뮤니티 아웃리치 (User Engagement Initiatives and Community Outreach)

새로운 국가나 지역에서 출시할 때, WLD 토큰 공급량의 일부는 월드 재단이 사용자 참여 이니셔티브 및 커뮤니티 아웃리치 프로그램(예: 지역 단체와의 파트너십)을 지원하는 데 사용될 수 있습니다.

시퀀서 및 고유성 서비스 운영 (Sequencer and Uniqueness Service Operation)

개인이 오브에서 검증을 받을 때, 생체 정보의 고유성을 확인하고 고유성 증명이 블록체인에 기록되어야 합니다. 해당 서비스는 월드 재단이 운영합니다. 월드 재단은 또한 월드 체인의 상태를 이더리움에 기록하는 월드 체인용 시퀀서 운영을 지원합니다. 토큰 공급량의 일부는 이러한 서비스의 비용을 충당하는 데 할당됩니다.

버그 바운티 프로그램 (Bug Bounty Programs)

하드웨어와 소프트웨어는 외부 보안 감사 회사에 의해 광범위하게 감사되었지만(오브 감사 및 프로토콜 감사 참조), 스마트 컨트랙트 및 기타 소프트웨어에 대한 추가적인 버그 바운티 프로그램이 마련되었습니다. 이러한 버그 바운티 프로그램은 프로젝트의 점진적 탈중앙화를 위한 도구로도 기능할 수 있습니다.

생태계 펀드 (Ecosystem Fund) (목표 할당: $\leq 5\%$)

생태계 펀드는 월드 재단(World Foundation)이 월드의 지속적인 개발과 탈중앙화를 지원하는 활동을 위해 사용하도록 의도되었습니다. 이러한 비용은 네트워크 규모나 현장 운영의 규모와는 크게 무관합니다.

프로토콜 연구개발 (Protocol R&D)

일부 자금은 월드와 관련 소프트웨어의 지속적인 개발을 위해 월드 재단이 사용합니다. 여기에는 예를 들어, 월드 아이디(World ID) 프로토콜, 월드 체인(World Chain)의 개발이 포함되며, 향후 클라이언트 앱 개발도 포함될 수 있습니다.

오브 연구개발 (Orb R&D)

생태계 펀드는 또한 오브 하드웨어 및 소프트웨어의 지속적인 연구개발, 보안 메커니즘과 새로운 기능을 위해 사용됩니다.

표준 개발, 감사, 인증 (Standards Development, Audits, and Certification)

일부 자금은 월드의 다양한 부분(여러 지갑 앱, 오브, 온체인 프로토콜 등)의 표준화를 촉진하기 위해 월드 재단이 사용합니다. 표준은 서로 다른 주체가 네트워크의 일부가 되는 것을 쉽게 만들어 탈중앙화를 돕습니다. 향후 일부 자금은 새로운 생체 장치나 새로운 지갑 앱의 감사, 새로운 서비스 제공자의 인증 등에 사용될 것으로 예상됩니다.

생태계 그랜트 (Ecosystem Grants)

일부 자금은 월드의 일부인 새로운 프로토콜, 시스템, 통합 개발 및 추가적인 연구개발을 위해 발급되는 생태계 그랜트에 사용됩니다.

인센티브 프로그램 (Incentive Programs)

일부 자금은 생태계의 성장을 촉진하는 개인, 기업, 프로토콜의 활동을 직접적으로 장려하는 프로그램에 사용됩니다.

유동성 공급 (Liquidity Provisioning)

World Assets, Ltd.는 미국 외에서 활동하는 여러 트레이딩 회사와 대출 계약을 체결했습니다. 이러한 대출은 트레이딩 회사가 독립적으로 WLD 토큰의 유동성을 평가하고 제공할 수 있도록 합니다.

2025년 4월 28일 기준, 이들 기관은 총 1,300만(13M) WLD에 해당하는 대출을 보유하고 있습니다. 이 중 1,000만(10M) WLD는 2025년 6월 14일 만기, 100만(1M) WLD는 2025년 9월 26일 만기이며, 200만(2M) WLD는 현재 만기가 지정되지 않았습니다. 이 대출은 반드시 WLD로 전액 상환되어야 하며, 특히 콜옵션(call option)은 존재하지 않습니다.

월드 재단 운영 (World Foundation Operations)

생태계 펀드의 일부는 월드 재단에서 근무하는 소규모 인력과 관련 운영 비용(법무, 행정 등)을 충당하는 데 사용됩니다.

월드 아이디 수수료 (World ID Fees)

월드 아이디는 글로벌, 프라이버시 보존형 신원 네트워크를 가능하게 하는 프로토콜입니다. 그 핵심은 오브가 제공하는 인간 증명 자격 증명입니다. 추가적으로, 월드 아이디 프로토콜은 기업이나 정부 기관 등 어떤 주체든 새로운 월드 아이디 자격 증명(예: 신용 보고서, 대학 증명서)을 생성할 수 있도록 하며, 개인은 이를 월드 아이디에 연결할 수 있습니다. 개인은 실제 신원을 공개하지 않고 자신에 대한 정보를 공유할 수 있습니다. 예를 들어, 오브에서 검증된 개인은 애플리케이션(신뢰 기관)에게 “나는 고유한 인간이다”라고 증명할 수 있으며, 여권 자격 증명을 추가한 개인은 “나는 18세 이상이다” 또는 “나는 미국 시민이다”라고 증명할 수 있습니다. 자격 증명은 결합되어 복합 증명(composite proofs)을 만들 수도 있습니다. 예를 들어, “나는 18

세 이상인 고유한 인간이다”라고 증명하면서 다른 정보를 공개하지 않을 수 있습니다. 특정 애플리케이션에서 자격 증명이 단 한 번만 사용되었는지를 아는 것이 중요하기 때문에, 대부분의 월드 아이디 증명은 이러한 방식으로 인간 증명 자격 증명을 포함할 것으로 예상됩니다.

월드 아이디를 통합하는 애플리케이션은 이러한 증명을 요청하고 사용할 수 있으며, 예를 들어 봇 계정을 방지하거나 AI 사칭 및 사기를 막거나 연령 제한을 구현하는 데 활용할 수 있습니다. 또한 가까운 미래에는 인간이 AI 에이전트에게 권한을 위임하기 위해 월드 아이디와 같은 기술이 필요할 수도 있습니다.

사명의 일환으로, 월드 재단은 점진적으로 생태계를 탈중앙화하고 프로젝트를 자급자족 가능한 상태로 만드는 것을 목표로 합니다. 월드 아이디 프로토콜 맥락에서, 이는 두 가지 주요 구성 요소를 가집니다:

- 1. **자격 증명 발급자에 대한 인센티브:** 발급자가 자격 증명을 발급하고 유지하도록 충분한 수익을 얻을 수 있게 함.
- 2. **프로토콜 지속 가능성:** 프로토콜을 지속 가능하게 만들 수익을 창출함.

이를 위해, 재단은 현재 월드 아이디 프로토콜에 변경을 설계하고 있으며, 이를 통해 월드 아이디 증명을 사용하는 애플리케이션에 대해 WLD로 지불되는 수수료를 부과할 수 있도록 할 예정입니다.

애플리케이션에 부과, 사용자에게는 아님 (Charging Applications, not Users)

월드 아이디 수수료는 최종 사용자가 아닌 애플리케이션에 부과됩니다. 그 이유는 가치 창출이 가장 직접적으로 측정되는 곳이 애플리케이션이기 때문입니다. 월드 아이디의 가치는 애플리케이션이 이를 통합해 기존 서비스를 향상시키거나 전혀 새로운 서비스를 가능하게 할 때 실현됩니다. 이는 이전에는 불가능했던 새로운 비즈니스 모델을 탄생시킬 수도 있습니다. 따라서 애플리케이션이 월드 아이디 서비스를 소비하는 데 대해 비용을 지불하는 것은 자연스러운 일입니다. 애플리케이션은 자신이 통합하는 구성 요소에 비용을 지불하는 것에 익숙하며, 월드 아이디가 제공하는 가치를 인식할 수 있을 것으로 기대됩니다. 이러한 접근 방식은 애플리케이션을 위해 창출된 가치의 일부가 자격 증명 발급자와 프로토콜로 되돌아가도록 보장합니다.

월드 아이디 수수료 세부 사항 (Details on World ID Fees)

월드 아이디 수수료는 두 가지 구성 요소로 이루어집니다:

- **자격 증명 수수료(Credential fee):** 각 자격 증명 발급자(예: 오브 자격 증명에 대한 월드 재단, 자체 자격 증명에 대한 기업이나 정부 기관)는 자신들의 자격 증명에 대한 수수료를 설정할 수 있으며, 해당 수수료 수익을 받게 됩니다. 이를 통해 자격 증명 발급자는 자격 증명을 생성하고 유지할 인센티브를 갖게 됩니다.
- **프로토콜 수수료(Protocol fee):** 프로토콜은 기본 수수료(base fee)를 설정하고, 자격 증명 수수료 위에 소액의 프리미엄을 추가로 부과합니다. 이를 통해 프로토콜이 자급자족할 수 있을 만큼 충분한 수익이 발생하도록 합니다.

애플리케이션 관점에서 보면, 월드 아이디 수수료는 단 하나—자격 증명 수수료와 프로토콜 수수료의 합계—입니다. 월드 아이디 수수료는 애플리케이션(고유 app id로 식별)이 월드 아이디 증명을 요청할 때 부과됩니다.

수수료 지불은 프로토콜 수준에서 강제됩니다. 이는 향후 월드 아이디 아키텍처에서 사용되는 프라이빗 스테이트 블록체인(private state blockchain)에 의해 가능해지는 기능 중 하나입니다(사용되는 암호화 기술의 기술적 배경은 [여기](#) 참조). 비공식적으로 말하면, 프라이빗 스테이트 블록체인은 누구도 관찰할 수 없는 상태에서 내부 상태를 업데이트할 수 있으며, 동시에 퍼미션리스(permissionless)입니다. 즉, 누구나 노드를 운영할 수 있지만, 특정 상태 변수는 프라이빗 스테이트 블록체인 내부 계산에서만 사용 가능하며 외부에서는 평문으로 관찰할 수 없습니다.

프라이빗 스테이트 블록체인을 사용하면 월드 아이디 프로토콜에서 다양한 기능(예: 월드 아이디 복구, 다중 지갑 사용)이 가능해집니다. 중요한 점은, 이는 검증된 사용자 각각의 애플리케이션 상태 일부를 저장하기도 한다는 것입니다. 월드 아이디 스마트 컨트랙트는 사용자가 증명을 생성할 수 있도록 프라이빗 스테이트 블록체인에서 상태 변경 영수증(receipt)을 제공하기 전에 수수료가 지불되었는지를 프로그래밍적으로 확인합니다. 이렇게 하면 애플리케이션이 블록체인의 상태를 관찰할 수 없기 때문에 월드 아이디 수수료를 회피할 수 없도록 보장합니다.

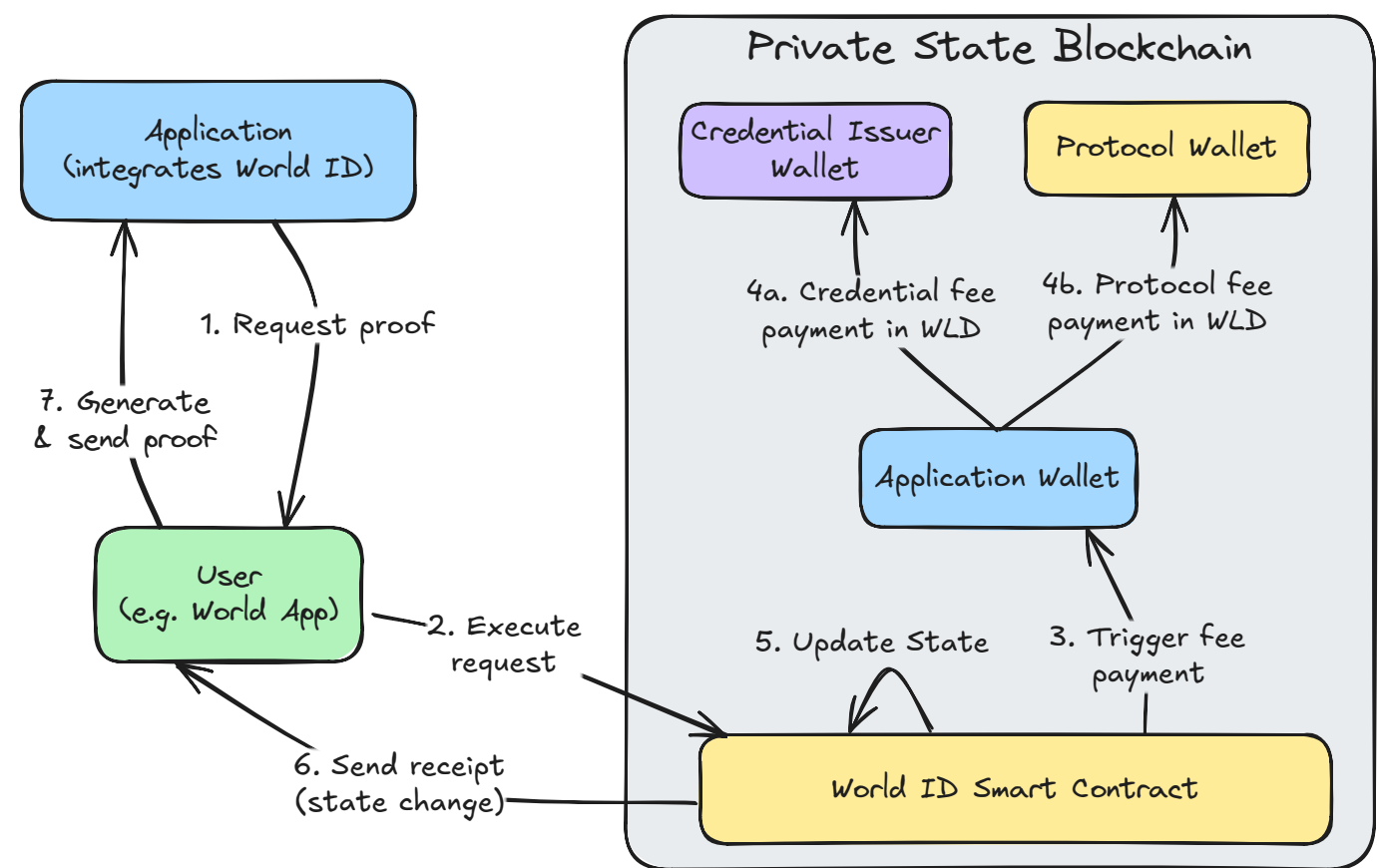


Figure 4.4: 계획된 월드 아이디 수수료 구현의 높은 수준 개요

Figure 4.4는 이미 자격 증명 발급자에게 등록된 자격 증명을 보유한 사용자의 예시를 사용하여, 계획된 월드 아이디 수수료 구현의 높은 수준 개요를 보여줍니다. 월드 아이디 수수료는 다음과 같이 작동합니다:

1. 월드 아이디와 통합된 애플리케이션이 사용자에게 증명(예: 고유한 인간성)을 요청합니다.
2. 사용자는 월드 앱(World App)과 같은 월드 아이디 앱을 통해 이 요청을 프라이빗 스테이트 블록체인의 월드 아이디 스마트 컨트랙트로 실행하기로 결정합니다.
3. 스마트 컨트랙트는 자동으로 요청 애플리케이션 지갑에서 WLD 수수료를 트리거합니다.
4. 해당 자격 증명 수수료는 자격 증명 발급자 지갑으로, 프로토콜 수수료는 프로토콜 지갑으로 지급됩니다.

5. 월드 아이디 스마트 컨트랙트는 자체 상태를 업데이트합니다.
6. 월드 아이디 스마트 컨트랙트는 상태 변경 영수증을 사용자에게 전송합니다.
7. 사용자의 앱은 월드 아이디 증명을 생성해 애플리케이션에 전송합니다.

월드 아이디 스마트 컨트랙트는 수수료를 WLD로 지불하도록 요구합니다. 이는 애플리케이션 지갑이 프라이빗 스테이트 블록체인에서 사전에 WLD로 자금이 조달되어야 함을 의미합니다. Web3 네이티브 애플리케이션은 블록체인에서 직접 지갑에 자금을 조달할 수 있습니다. 반대로 Web2 플랫폼과 같은 애플리케이션은 지갑 자금 조달을 대신 처리하고 애플리케이션에 법정화폐로 요금을 부과하는 제3자 사전 자금 조달 서비스를 사용할 수도 있습니다. 어느 쪽이든, 최종적으로 모든 수수료는 WLD 토큰으로 지불됩니다.

가격 메커니즘 (Pricing Mechanisms)

Figure 4.4는 모든 월드 아이디 증명에 대해 수수료가 지불되는 것으로 가정합니다. 실제로는 각 자격 증명 발급자가 Figure 4.4에 표시된 아키텍처와 호환되는 임의의 가격 메커니즘을 선택할 수 있습니다. 가격 메커니즘은 프라이빗 스테이트 블록체인 상의 스마트 컨트랙트로 구현되므로, 다양한 옵션이 가능합니다. 예를 들면:

- **증명별(per-proof):** 모든 월드 아이디 증명마다 수수료를 부과할 수 있습니다.
- **월간 활성 사용자별(per-monthly-active-user):** 매월 활성 사용자(앱 id별)마다 수수료를 부과할 수 있습니다. 각 사용자에 대해서는 특정 달의 첫 번째 증명 요청 시 수수료가 징수됩니다. 프라이빗 스테이트 블록체인 내부에서 계산이 이루어지므로, 사용자 신원을 공개하지 않고도 월간 활성 사용자별 과금 모델을 구현할 수 있습니다.
- **무료 티어(free tiers):** 처음 1,000명의 사용자 또는 처음 1,000개의 증명은 무료일 수 있습니다.
- **볼륨 할인(volume discounts):** 사용자 또는 증명 단위 수수료가 거래량에 따라 감소할 수 있습니다.
- **특정 애플리케이션에 대한 할인:** 자격 증명 발급자가 특정 애플리케이션(예: NGO)에 할인 또는 무료 자격 증명을 제공할 수 있습니다.
- **경제적 가치에 비례하는 수수료:** 자격 증명 발급자가 여러 수준의 증명을 서로 다른 수수료로 제공할 수 있으며, 일부 변형은 의도적으로 낮은 수준의 보증을 제공하여 애플리케이션이 필요에 가장 적합한 수준을 선택할 수 있도록 할 수 있습니다.

프로토콜 수수료의 기본 수수료(base fee)에 대해서도 거버넌스가 적절한 가격 메커니즘을 결정할 수 있습니다. 여러 다른 가격 메커니즘이 가능하지만, 대부분의 애플리케이션은 월간 활성 사용자별 요금을 선호할 가능성이 큼니다. 이는 애플리케이션이 월드 아이디가 사용자당 월별로 생성하는 가치(예: ARPU 증가)와 비교할 수 있기 때문입니다.

“나는 18세 이상의 고유한 인간이다”와 같은 복합 증명(composite proofs)의 경우, 필요한 자격 증명의 조합에 따라 수수료 금액이 달라질 수 있습니다. 예를 들어, “고유성” 증명의 수수료는 “고유성 + 나이” 증명의 수수료보다 낮을 수 있습니다.

수수료 사용 (Fee usage)

각 자격 증명 발급자는 자격 증명 수수료의 사용 방식에 대해 재량권을 가집니다. 프로토콜 수수료는 초기에는 월드 재단이 그 할당을 관리합니다. 시간이 지나 거버넌스가 더욱 탈중앙화되면, 월드 커뮤니티가 이 책임을 맡게 됩니다. 커뮤니티는 수수료의 일부를 네트워크 성장을 위해 사용하도록 결정할 수 있으며 —예를 들어 운영자를 지원하거나 사용자 토큰을 자금 지원— 심지어 수수료의 일부를 소각(burn)하기로 결정할 수도 있습니다. 월드 아이디 프로토콜이 성장함에 따라(더 많은 참여자, 더 많은 애플리케이션, 더 많은 증명 검증), 더 많은 수수료가 발생하고, 이는 다시 생태계로 흘러 들어가 추가적인 성장을 만들어내며, 자기 강화적 성장 메커니즘을 형성합니다.

월드 아이디 수수료의 다음 단계 (Next steps on World ID Fees)

월드 재단은 현재 월드 아이디 수수료를 가능하게 하기 위해 필요한 프로토콜 변경 작업을 진행 중입니다. 재단은 이 작업을 완료하고 2025년 3분기에 수수료 메커니즘을 테스트하기 위한 첫 번째 파일럿을 실행할 것으로 예상합니다. 재단은 월드 아이디 수수료로 가는 경로를 조기에 보여주는 것이, 생태계의 다른 주체들이 자격 증명을 발급하고 유지하도록 인센티브를 제공하고 프로토콜이 자급자족할 수 있음을 보여주는 데 중요하다고 믿습니다.

재단이 월드 아이디 수수료 도입을 준비하는 동안, 주요 초점은 월드 네트워크 성장을 계속 추진하는 데 있습니다. 재단은 또한 미니 앱 개발자, 자격 증명 발급자, 월드 아이디를 통합하는 애플리케이션 커뮤니티를 지원하기 위해 생태계 그랜트 제공을 지속할 것입니다.

기술 정보 (Technical Information)

계약 및 주소 (Contracts and Addresses)

스마트 컨트랙트 (Smart Contracts)

계약 (Contract)	네트워크 (Network)	주소 (Address)
WLD 토큰 컨트랙트 (WLD Token Contract)	Ethereum	0x163f8C2467924be0ae7B5347228CABF260318753
WLD 토큰 컨트랙트	World Chain	0x2cFc85d8E48F8EAB294be644d9E25C3030863003
WLD 토큰 컨트랙트	Optimism	0xdC6fF44d5d932Cbd77B52E5612Ba0529DC6226F1
커뮤니티 토큰 언락 컨트랙트 (Community Tokens Unlock Contracts)	Ethereum	0x1770bd8186AA27Df9B050D565f86CF2cdC92C960xaEE0360b73B5D01dad134F234d3a933adc1680e570x938cD21eE4AFB220929F96ce2B754C053C77F70x5B5442C5fcEaE3b40C230C32a3f5e924BcBe7D93
반복 사용자 토큰 수량 할당 컨트랙트, 오브 (Recurring User Token Amounts Allocation Contract, Orb) (폐기됨, deprecated)	Optimism	0xe773335550b63eed23a6e60dcc4709160a1f653c
반복 사용자 토큰 수량 할당 컨트랙트, 여권 (Recurring User Token Amounts Allocation Contract, Passport Credential)	World Chain	0x85C0BEb46E91D18dFeA0294E6FC46A8c8AF2BeaD
최초 사용자 토큰 수량 할당 컨트랙트, 오브 (First User Token Amounts Allocation Contract, Orb)	World Chain	0xf4d26620B6d9AE0F7F2495757C8Bd00090cE2A172
최초 사용자 토큰 수량 할당 컨트랙트, 여권 (First User Token Amounts Allocation Contract, Passport Credential)	World Chain	0x008177c4F0C0c64334D7CC2702b783387fCe6d62
베타 WLD 토큰 컨트랙트 (Beta WLD Token Contract) (폐기됨, deprecated)	Optimism	0x0346c32E5d7e98bD57100b6F7002a0Ae17188048

사용자 토큰 수량은 다음과 같이 가져올 수 있습니다: 현재 활성 그랜트 ID와 미래 반복 사용자 토큰 수량은 **WLDGrant** 컨트랙트에서 가져올 수 있으며, 이는 (Recurring User Token Amounts Allocation Contract).grant() 함수를 통해 가능합니다. 여기서 인간 증명(Orb) 또는 여권 (Passport)에 해당하는 **반복 사용자 토큰 수량 할당 컨트랙트**를 선택하면 됩니다.

현재 최초 사용자 토큰 수량은 다음 API 엔드포인트에서 가져올 수 있습니다:

주요 지갑 (Main Wallets)

지갑 (Wallet)	네트워크 (Network)	주소 (Address)
월드 재단 콜드 월렛 (World Foundation Cold Wallets)	Ethereum	0xc534a745bFfaF9466Ed7B47fA23B0177b99A3e77

	Optimism	0xc534a745bFfaF9466Ed7B47fA23B0177b99A3e77
	World Chain	0xc534a745bFfaF9466Ed7B47fA23B0177b99A3e77
월드 애셋, Ltd. 콜드 월렛 (World Assets, Ltd. Cold Wallets)	Ethereum	0x59a0f98345f54bAB245A0343488CEC7FCecD7B596
	Optimism	0x59a0f98345f54bAB245A0343488CEC7FCecD7B596
	World Chain	0x59a0f98345f54bAB245A0343488CEC7FCecD7B596
월드 애셋, Ltd. 핫 월렛 (World Assets, Ltd. Hot Wallets)	Ethereum	0xc4151Dd19A38E7224793F5aD8fBDD912750e3565
	World Chain	0x8C00371AfE2482477c15c878D58044d64A7FCcA3
월드 애셋, Ltd. 핫 월렛: 반복 사용자 토큰 수량 (Recurring User Token Amounts)	World Chain	0x30672EbB8D3c3b62C261a23B4a225712FF2CaDBC
	Optimism (폐기됨, deprecated)	0x7f26A7572E8B877654eeDcBc4E573657619FA3CE
월드 애셋, Ltd. 핫 월렛: 최초 사용자 토큰 수량 (First User Token Amount)	World Chain	0x1c288c748F368E8dcD87dB0d29888666842502aA
월드 애셋, Ltd. 핫 월렛: 예약 (Reservations)	World Chain	0xDAA7BbAD496c4D4431423bE64d878a769FbDEBc8
WLD 금고 (WLD Vault)	World Chain	0x14a028cC500108307947dca4a1Aa35029FB66CE0
	Optimism (폐기됨, deprecated)	0x21c4928109acB0659A88AE5329b5374A3024694C
옵티미즘 – 월드 체인 마이그레이션 (Optimism – World Chain Migration)	Optimism	0x6CE3A5478232F0DfAE37D7178C24F984cCa696a8
	World Chain	0xC6968c6DF1a2C31Ac66B42945BbaD91635a0095B
월드 애셋, Ltd. 핫 월렛: 웰컴 그랜트 및 베타 토큰 마이그레이션 (Welcome Grants and Beta Token Migration) (폐기됨)	Optimism	0x074a9ed58d11e3f0f589072c99de86f80971a844
월드 애셋, Ltd. 핫 월렛: 임시 보관 지갑 (Temporary holding wallet)	Optimism	0xF8Cf291d92e52B722C31af1FDE9F0D7E8900EE0A
월드 애셋, Ltd. 핫 월렛: 베타 토큰 마이그레이션 2 (Beta Token Migration 2) (폐기됨)	Optimism	0x46DcEC50647abFb2905Af8Da4e670051653A5FBC
폴리곤 브리지 (Polygon Bridge, 베타 사용자 마이그레이션, 폐기됨)	Optimism	0xe710657bEbBD75fBDaCA07D57c2A5aE04085507