

Whitepaper [KR]

zkPass: Building the Verifiable Internet through zkTLS

— zkTLS를 통한 검증 가능한 인터넷 구축 —

발행 주체: **IFCONNECT TECHNOLOGY LIMITED**

업데이트: **2025년 11월**

Table of Contents

1. 요약(Executive Summary).....	2
2. 배경 및 동기(Background & Motivation).....	2
3. zkPass 프로토콜 아키텍처(Protocol Architecture).....	3
4. 기술 개요(Technology Overview).....	4
4.1 zkTLS.....	4
4.2 다자간 계산 (MPC, Multi-Party Computation).....	4
4.3 상호작용 제로 지식 증명 (IZK, Interactive Zero-Knowledge Proofs).....	5
4.4 회로 팩토리 및 모듈식 설계 (Circuit Factory & Modular Design).....	5
5. 개발자 생태계 및 활용 사례(Network Economy & Token Model).....	5
대표적 활용 사례 (Representative Applications).....	6
6. 네트워크 경제 및 토큰 모델(Network Economy & Token Model).....	6
6.1 토큰 개요 (Token Overview).....	7
6.2 토큰 유틸리티 (Token Utility).....	7
6.3 토큰 분배 및 베스팅 일정 (Token Allocation & Vesting Schedule).....	7
6.4 신뢰의 플라이휠 (The Credibility Flywheel).....	8
7. 거버넌스 및 보안 프레임워크(Governance & Security Framework).....	8
7.1 거버넌스 계층 구조 (Governance Layers).....	9
7.2 투표 규칙 (Voting Rules).....	9
7.3 보안 가정 (Security Assumptions).....	9
8. 로드맵 및 전망(Roadmap & Outlook).....	9
전략적 비전 (Strategic Vision).....	10
9. 법률 및 규제 준수 성명(Legal & Compliance Statement).....	10
10. 팀 및 프로젝트 연혁(Team & History).....	11
11. 보안 감사 및 위험 관리(Security Audits & Risk Management).....	12
11.1 프로토콜 수준의 보안 (Protocol-Level Security).....	13
11.2 스마트 컨트랙트 및 네트워크 감사 (Smart Contract & Network Audits).....	13
11.3 운영 보안 (Operational Security).....	13
11.4 위험 고지 (Risk Disclosure).....	14

법적 고지문 (Legal Disclaimer)

본 백서는 정보 제공을 목적으로 하며, 투자 권유 또는 증권 발행과 관련된 문서가 아닙니다. IFCONNECT TECHNOLOGY LIMITED는 이 문서의 내용과 관련하여 어떠한 법적 책임도 지지 않습니다. 본 문서는 사전 통보 없이 변경될 수 있으며, zkPass 프로토콜의 기술적 발전 및 거버넌스 결정에 따라 수정될 수 있습니다.

© 2025 IFCONNECT TECHNOLOGY LIMITED – All Rights Reserved

1. 요약(Executive Summary)

수십 년 동안 인터넷은 검증 가능성(**verifiability**) 보다 가시성(**visibility**)에 의존해 발전해 왔습니다.

네트워크를 통해 공유되는 데이터는 암호화될 수 있지만, 그 내용을 노출하지 않고 해당 데이터가 신뢰할 수 있는 출처에서 비롯되었음을 암호학적으로 증명(**cryptographic proof**) 할 수는 없었습니다.

이러한 구조적 한계로 인해, **Web2**는 본질적으로 비공개적이지만 검증이 불가능한 체계,

Web3는 검증은 가능하지만 모든 정보가 공개되는 체계로 자리 잡게 되었습니다.

zkPass는 이 문제를 해결하기 위해 새로운 암호화 원리인

zkTLS(Zero-Knowledge Transport Layer Security)를 도입했습니다.

zkTLS는 모든 HTTPS 세션을 프라이버시를 보호하면서도 검증 가능한 증명 소스로 변환합니다.

zkPass는 3자 **TLS(Three-Party TLS)**, **MPC(Multi-Party Computation)**, 그리고 **IZK(Interactive Zero-Knowledge Proofs)**를 결합하여 사용자가 자신의 Web2 데이터(예: 신원 정보, 평판 기록, 자산 내역, 학습 이력 등)에 대한 진술을 데이터를 노출하지 않고도 증명할 수 있도록 합니다.

이러한 아키텍처를 통해 zkPass는 인터넷의 ‘검증 계층(**Verifiability Layer**)’으로 자리 잡습니다.

zkPass는 Web2의 신뢰 경계를 Web3로 확장하여, 인증된 현실 데이터(**authenticated real-world data**)에 기반한 새로운 세대의 탈중앙화 애플리케이션(**dApp**)을 가능하게 합니다.

2. 배경 및 동기(Background & Motivation)

오늘날의 인터넷은 **TLS(Transport Layer Security)** 프로토콜을 기반으로 구축되어 있으며,

전 세계 웹사이트의 95% 이상이 종단 간 암호화(**end-to-end encryption**)를 통해 데이터를 보호하고 있습니다.

TLS는 데이터의 기밀성(**confidentiality**)과 무결성(**integrity**)을 보장하지만, 데이터가 특정 **HTTPS** 도메인에서 실제로 생성되었음을 제3자가 암호학적으로 검증(**verifiable authenticity**)하는 기능은 제공하지 않습니다.

한편, 탈중앙화 시스템(**decentralized systems**)의 부상은

체인 외부 데이터(**off-chain data**)에 대한 신뢰 불필요 검증(**trustless verification**)의 수요를 급격히 증가시켰습니다.

그러나 Web3 프로토콜은 설계상 투명성을 지니고 있음에도 불구하고,

금융 기록, 자격 증명, 행동 데이터 등 검증된 **Web2** 정보(**verified Web2 information**)에

접근할 수 없습니다.

이러한 데이터는 모두 중앙화된 서버(**private servers**) 안에 갇혀 있습니다.

이로 인해 **Web2-Web3** 간 신뢰 격차(**trust gap**)가 발생합니다:

- **Web2** 데이터는 비공개적이지만 검증이 불가능하고,
- **Web3** 데이터는 검증이 가능하지만 모든 정보가 공개됩니다.

zkPass는 이 모순을 해결합니다.

zkPass는 기존의 표준 **TLS** 세션을 제로 지식 증명(**Zero-Knowledge Proof, ZKP**)으로 변환하여,

사용자가 개인적이고 인증된 **Web2** 데이터를 프라이버시를 침해하지 않고도 온체인 검증 가능한 증명(**on-chain proof**)으로 변환할 수 있도록 합니다.

그 결과 **zkPass**는 프라이버시와 검증 가능성이 공존하는 새로운 인터넷 패러다임, 즉 **Verifiable Internet**을 구현합니다.

3. **zkPass** 프로토콜 아키텍처(**Protocol Architecture**)

kPass 프로토콜은 기존의 표준 **TLS** 통신 모델을 재정의하여,

여기에 세 번째 암호학적 참여자(**third cryptographic participant**)인 노드(**Node**)를 추가합니다.

이 시스템은 총 네 가지 논리적 구성 요소(**logical entities**)로 이루어집니다.

역할(Role)	기능(Function)
Prover (사용자)	Web2 데이터 소스로부터 개인 데이터를 수집하고, 해당 데이터를 기반으로 제로 지식 증명(Zero-Knowledge Proof, ZKP)을 생성합니다.
Verifier (애플리케이션)	사용자 데이터의 내용을 직접 보지 않고, 제출된 증명을 검증하여 진술의 진위성을 확인합니다.
Node (zkPass 네트워크)	3자 핸드셰이크(3-Party Handshake) 과정에 참여하여 TLS 세션의 진위성(authenticity)과 무결성(integrity)을 검증합니다.

Data Source (서버)	원본 데이터를 호스팅하는 HTTPS 엔드포인트(HTTPS endpoint) 역할을 수행합니다.
----------------------------	--

이 구조를 통해 설계된 **3자 TLS(3P-TLS, Three-Party TLS)** 프로토콜은,

사용자와 서버 간의 통신을 제3자가 암호학적으로 검증(**cryptographic verification**) 할 수 있는

프라이버시 보호형 채널(**privacy-preserving channel**)로 확장합니다.

4. 기술 개요(Technology Overview)

4.1 zkTLS

zkTLS(Zero-Knowledge Transport Layer Security)는 기존의 **2자 TLS(two-party TLS)** 구조를 확장하여,

Prover(사용자), **Node**(노드), **Data Source**(데이터 소스) 간의 **3자 핸드셰이크(three-party handshake)**를 수행합니다.

이 과정에서 **Prover**와 **Node**는 공동으로 클라이언트(**client**) 역할을 수행하고, **Data Source**는 서버(**server**)로 동작합니다.

양측은 타원 곡선 디피-헬만(**Elliptic-Curve Diffie-Hellman, ECDH**) 키 교환과 보안 메시지 인증(**MAC, Message Authentication Code**) 공유를 통해 개인 정보를 노출하지 않은 상태에서 공동으로 세션 키(**session key**)를 도출합니다.

이 설계는 다음 세 가지 보안 속성을 보장합니다:

- **진위성 (Authenticity):** 합법적인 **HTTPS** 세션에서만 증명이 생성될 수 있습니다.
- **무결성 (Integrity):** 사용자가 데이터를 위조하거나 수정할 수 없습니다.
- **프라이버시 (Privacy):** **Node**나 **Verifier**는 어떤 평문 데이터도 접근할 수 없습니다.

4.2 다자간 계산 (MPC, Multi-Party Computation)

MPC는 어떤 단일 참여자도 민감한 정보를 단독으로 변경하거나 재구성할 수 없도록 보장합니다.

증명 생성 과정에서 **Prover**와 **Node**는 각각 세션 키의 일부(**partial key**)를 보유하며, 서로 협력하여 메시지 인증 코드(**MAC**)를 계산합니다.

이를 통해 서버의 진짜 응답(**genuine server response**)만이 증명에 포함될 수 있으며, 위조를 원천적으로 차단하고 참여자 간 암호학적 신뢰(**cryptographic trust**)를 확립합니다.

4.3 상호작용 제로 지식 증명 (IZK, Interactive Zero-Knowledge Proofs)

데이터 무결성이 확인된 후, zkPass는 **VOLE(Verifiable Oblivious Linear Evaluation)** 기반의

IZK(Interactive Zero-Knowledge Proof) 를 활용하여 브라우저 환경에서도 신뢰 설정(**trusted setup**) 없이 직접 증명을 생성할 수 있습니다.

사용자는 다음과 같은 형태의 진술을 로컬 환경에서 증명할 수 있습니다:

- “이 계정은 인증된 거래소(licensed exchange)에 의해 검증되었습니다.”
- “내 Duolingo 연속 학습 기록은 30일 이상입니다.”
- “내 은행 계좌 잔액은 10,000달러 이상입니다.”

이러한 진술은 온체인(**on-chain**) 또는 탈중앙화 시스템(**decentralized systems**) 내에서 검증 가능하며, 동시에 기초 데이터 값(**underlying data values**) 은 전혀 노출되지 않습니다.

4.4 회로 팩토리 및 모듈식 설계 (Circuit Factory & Modular Design)

zkPass는 **Bristol** 스타일 논리 게이트(**AND / XOR / INV**) 를 기반으로 한 모듈형 회로(**modular circuit**) 구조를 채택합니다.

각 증명 회로(proof circuit)는 스키마(**schema**) 라는 형태로 정의되며, 이는 특정 검증 유형(type of verification)을 위한 표준화된 논리 구조입니다.

이러한 스키마는 재사용(**reusable**), 조합(**composable**) 이 가능하며 **Schema Market** 을 통해 배포됩니다.

5. 개발자 생태계 및 활용 사례(Network Economy & Token Model)

zkPass는 누구나 애플리케이션에 프라이버시 보호형 검증(**private verification**) 기능을 통합할 수 있도록 완전한 개발자 스택(full development stack)을 제공합니다.

레이어(Layer)	구성 요소(Component)	설명(Description)
Protocol Layer	zkTLS	Web2와 Web3를 연결하는 암호학적 기반층(cryptographic foundation)
Developer Layer	DevHub	스키마(schema) 생성 및 증명(proof) 생성을 위한 툴킷, API, SDK

Gateway Layer	TransGate SDK	최소한의 통합 노력으로 dApp이 사용자 증명을 검증할 수 있는 통합 게이트웨이
Application Layer	Schema Market	재사용 가능한 검증 스키마를 거래·배포하는 탈중앙화 마켓플레이스

대표적 활용 사례 (Representative Applications)

- **Proof of Humanity:** 신원, 사회적 자격, 정부 인증 정보를 검증
- **Proof of Learning:** 학업 또는 기술 기반 성취를 검증
- **Proof of Assets:** 자산 보유 또는 잔액을 노출 없이 증명
- **Proof of Participation:** 이벤트 또는 캠페인 참여 여부를 증명
- **Proof of Behavior:** 오프체인 행동(이용 내역, 주문, 멤버십 등)을 검증

2025년 2분기 기준, **zkPass**는

100개 이상의 검증된 데이터 소스(verified data sources),

300개 이상의 스키마(schemas),

80개 통합 파트너(integration partners)를 통해

누적 **2억 건(200M)** 이상의 검증 연산(Total Verifiable Computation, TVC)을 처리했습니다.

6. 네트워크 경제 및 토큰 모델(Network Economy & Token Model)

인터넷은 언제나 정보(information) 위에 구축되어 왔지만, 검증 가능한 진실(verifiable truth) 위에 세워지지는 않았습니다.

수십 년 동안 온라인 데이터는 “보이는(visible)” 형태로 존재했을 뿐, “검증 가능한(verifiable)” 형태로 존재하지 못했습니다.

스크린샷은 위조될 수 있고, 자격 증명은 조작될 수 있으며, 신뢰(trust)는 언제나 증명(proof)이 아닌 가정(assumption)에 의존해 왔습니다.

zkPass와 그 핵심 기술인 **zkTLS(Zero-Knowledge Transport Layer Security)**는 이 근본을 새롭게 정의합니다.

이제 처음으로, 개인의 **Web2** 데이터(예: 금융 기록, 신원 인증, 학습 이력, 여행 내역 등)가

이동 가능하고(portable), 프라이버시를 보호하며(privacy-preserving), 네트워크 간 검증 가능한(cryptographically verifiable) 형태의 암호학적 증명(cryptographic proof)으로 변환될 수 있습니다.

이 검증 가능한 데이터 경제(verifiable data economy)의 중심에는

zkPass 생태계의 정산(settlement), 검증(validation), 조정(coordination)을 가능하게 하는 기능형 유틸리티 토큰 **\$ZKP**가 자리하고 있습니다.

6.1 토큰 개요 (Token Overview)

항목	내용
토큰 티커 (Ticker)	\$ZKP
토큰 표준 (Token Standard)	ERC-20
총 공급량 (Total Supply)	1,000,000,000
공급 유형 (Supply Type)	고정형 (Fixed), 인플레이션 없음
디플레이션 모델 (Deflationary Model)	일부 정산 수수료(settlement fee)의 소각(burn) 메커니즘 적용
바이백 메커니즘 (Buyback Mechanism)	DAO 주도로 프로토콜 수익을 활용한 주기적 매입 (periodic buyback)

6.2 토큰 유틸리티 (Token Utility)

- **정산 매개체 (Settlement Medium):**
\$ZKP는 zkPass 생태계 내에서 증명 정산(proof settlement) 및 검증자 실행(verifier execution)에 필요한 기본 기능 단위입니다.
- **검증자 담보 (Validator Collateral):**
검증자는 네트워크의 정확성, 가용성, 안정성을 보장하기 위해 \$ZKP를 운영 담보로 스테이킹합니다.
- **네트워크 크레딧 (Network Credits):**
\$ZKP는 검증 연산(verifiable computation), 통합(integration) 등 네트워크 기여도를 기록·정산하기 위한 온체인 크레딧(on-chain credit) 역할을 수행합니다.
- **서비스 접근 (Service Access):**
기업 및 개발자는 \$ZKP를 사용하여 zk-native 검증 API 및 프라이버시 보호 데이터 인프라에 접근할 수 있습니다.
- **상호 검증성과 거버넌스 (Cross-System Verifiability & Governance):**
\$ZKP는 탈중앙화된 조정 메커니즘(decentralized coordination)을 지원하며, 검증 가능한 시스템 간의 신뢰 계층(trust layer)으로 기능합니다.
또한 감사(audit) 및 비영리적 유지 관리 활동을 위한 자금 흐름을 지원합니다.

6.3 토큰 분배 및 베스팅 일정 (Token Allocation & Vesting Schedule)

구분	비율	베스팅 조건	용도
커뮤니티 (Community)	48.5 %	TGE 시 12.5% 언락 + 3개월간 6% 선형 베스팅, 이후 5년간 매월 30% 베스팅	생태계 확장, 검증형 에어드롭, 커뮤니티

			세일, 마케팅 및 파트너십
초기 투자자 (Early Investors)	22.5 %	12개월 클리프 + 18개월 선형 베스팅	프로토콜 초기 개발을 지원한 전략적·기관 투자자
핵심 기여자 (Core Contributors)	14%	24개월 클리프 + 24개월 선형 베스팅	창립자, 엔지니어, 연구자, 핵심 운영 기여자
DAO 재무부 (DAO Treasury)	10%	5년간 선형 베스팅	거버넌스, 생태계 보조금, 비상 예비금 등 장기 지속 가능성 확보
유동성 (Liquidity)	5%	TGE 시 100% 언락	시장 유동성 공급 및 네트워크 부트스트래핑

초기 유통량 (**Initial Circulating Supply**):

TGE 기준 약 **20.167%**, 커뮤니티 및 유동성 풀만 유통되며 팀 및 투자자 물량은 **0%** 잠금 해제 상태로 시작합니다.

6.4 신뢰의 플라이휠 (**The Credibility Flywheel**)

- **Web2와 Web3의 융합**: 방대한 데이터 영역이 개방됨
- 프라이버시 보호형 검증: 데이터가 안전하게 이동하며 신뢰가 전이됨
- 검증된 상호작용: 실제 효용(utility)과 새로운 애플리케이션 창출
- 유틸리티 확대: 사용자와 기업의 채택(adoption) 가속화
- 참여 증가: 검증자 수와 네트워크 인센티브 확장
- 가치 성장: 더 많은 통합과 데이터 온보딩 촉진
- 반복되는 순환: 데이터 소스가 추가될 때마다 플라이휠의 속도·강도·범위 확대

이 순환은 매번 유틸리티(utility), 유동성(liquidity), 신뢰도(credibility)를 축적하며, 신뢰(trust)를 에너지(energy)로, 다시 에너지를 신뢰로 전환시킵니다.

zkPass는 단순히 하나의 제품을 만드는 것이 아닙니다.

zkPass는 디지털 세상을 위한 자가 지속형 신뢰 경제(self-sustaining trust economy), 즉 “모든 행동 이전에 증명해야 하는 시스템들의 조정 계층(coordination layer)”을 설계하고 있습니다.

7. 거버넌스 및 보안 프레임워크(**Governance & Security Framework**)

zkPass는 초기의 개발 주도형 조정 모델(development-led coordination model)에서

점진적으로 완전한 **DAO(Decentralized Autonomous Organization)** 거버넌스 체계로 전환하고 있습니다.

7.1 거버넌스 계층 구조 (Governance Layers)

- **zkPass DAO:**
프로토콜 매개변수, 재무(Treasury), 보조금(Grant) 프로그램을 총괄하는 최고 의사결정 기관(**ultimate decision-making entity**) 으로 기능합니다.
- **핵심 기여자 위원회(Core Contributor Committees):**
DAO가 승인한 권한 범위 내에서 운영되는 비집행(**non-executive**) 팀으로, 다음과 같은 하위 위원회로 구성됩니다:
 - 기술(Technology)
 - 생태계(Ecosystem)
 - 운영(Operations)
 - 법률 및 컴플라이언스(Legal & Compliance)
 - 재무(Treasury)
- **재무 멀티시그 위원회(Treasury Multisig Committee):**
DAO의 감독 하에 **3-of-5** 멀티시그(**Safe wallet**) 구조로 운영되며, 프로토콜 자금 집행 및 운영비 지출을 관리합니다.

7.2 투표 규칙 (Voting Rules)

- **최소 정족수 (Minimum Quorum):**
전체 유통 중인 \$ZKP의 **8%** 이상 참여해야 의결이 유효합니다.
- **일반 제안 (Standard Proposals):**
투표 참여자의 **50%** 이상 찬성으로 통과됩니다.
- **중대한 제안 (High-Impact Proposals):**
구조적 변경(Structural Change) 또는 재무 재배분(Treasury Reallocation)과 같은 고위험 제안의 경우, **66%** 이상의 초과 다수(**supermajority**) 가 필요합니다.

7.3 보안 가정 (Security Assumptions)

- 모든 네트워크 노드는 **MPC 검증(MPC-verified)** 된 연산만 수행하며, 단일 노드가 증명을 위조하거나 변경할 수 없습니다.
- **TLS 키(TLS Keys)** 는 브라우저 메모리 외부에서 복원(reconstruct)되지 않으며, 사용자 단말 내에서만 안전하게 관리됩니다.
- 증명 검증 컨트랙트(**Proof Verification Contracts**) 는 결정적(**deterministic**) 으로 설계되어 있으며, 완전한 오픈소스(**auditable open-source**) 형태로 공개되어 외부 감사를 통한 투명성을 보장합니다.

8. 로드맵 및 전망(Roadmap & Outlook)

단계 (Phase)	주요 마일스톤 (Milestone)	설명 (Description)
Phase I (2022–2023)	프로토콜 기반 구축 (Protocol Foundation)	zkTLS 연구 및 프로토타입 구현. 3P-TLS, MPC, IZK 통합 구조 설계 완료.
Phase II (2024)	개발자 생태계 조성 (Developer Ecosystem)	Schema Market 및 TransGate SDK 출시. 80개 이상의 파트너사 통합 달성.
Phase III (2025)	탈중앙화 노드 네트워크 (Decentralized Node Network)	zkPass Node Network 메인넷 출시. 증명 가중치(proof-weighted)에 기반한 스테이킹 경제 활성화.
Phase IV (2026+)	거버넌스 및 엔터프라이즈 확장 (Governance & Enterprise Expansion)	완전한 DAO 거버넌스 전환. 기관용 데이터 인증을 위한 zkTLS Enterprise Suite 출시 및 멀티체인 zkTLS 호환성 확보.

전략적 비전 (Strategic Vision)

zkPass는 검증 가능한 진실(verifiable truth) 과 프라이버시 보호(privacy) 가 공존하는 새로운 인터넷을 지향합니다.

Web2의 인증 체계를 제로 지식 암호학(zero-knowledge cryptography) 위에 정립함으로써,
zkPass는 개인 데이터를 공개 검증 가능한 데이터(publicly verifiable data) 로 전환합니다.

이로써 zkPass는 탈중앙 신원(decentralized identity), 검증 가능한 평판(verifiable reputation),
그리고 프라이버시 보호형 온체인 인텔리전스(privacy-preserving on-chain intelligence) 의 기반을 구축합니다.

9. 법률 및 규제 준수 성명(Legal & Compliance Statement)

zkPass 재단(zkPass Foundation) 은 스위스 민법(Swiss Civil Law) 에 따라 설립된 비영리 협회(Non-Profit Association) 로,
기술 중심 재단에 적용되는 거버넌스 및 투명성 요건(governance and transparency requirements) 을 준수하며 운영됩니다.

재단의 설립 목적(Mandate)은 zkPass 프로토콜(zkPass Protocol),
zkTLS(Zero-Knowledge Transport Layer Security) 기술 및 관련 인프라의
오픈 개발(open development) 과 유지보수(maintenance) 를 지원하는 데 있습니다.

\$ZKP 토큰은 zkPass 생태계 내에서 사용되는 기능형 유틸리티 토큰(**functional utility token**) 으로 설계되었습니다.

이는 다음의 역할을 수행합니다:

- 증명 정산(**proof settlement**) 의 매개체
- 검증자 스테이킹(**validator staking**) 담보 자산
- 계산량 측정(**computation metering**) 단위
- 탈중앙 거버넌스(**decentralized governance**) 참여 수단

\$ZKP는 채단이나 기여자의 지분(**equity**), 소유권(**ownership**), 이익 배분권(**profit-sharing rights**) 또는 향후 수익에 대한 청구권(**claim on future revenue**) 을 나타내지 않습니다.

\$ZKP 보유자는 어떠한 법인(**entity**)에 대한 의결권(**voting right**), 배당(**dividend**), 가치 상승에 대한 보장(**guaranteed appreciation**) 도 갖지 않습니다. 모든 사용은 온체인 로직(**on-chain logic**) 과 **DAO** 거버넌스 절차(**governance procedures**) 에 따라 관리됩니다.

zkPass 채단 및 그 산하 기관들은 국제 **AML**(자금세탁방지) 및 **CFT**(테러자금조달방지) 기준을 준수하며, 토큰 배분(**token distribution**) 및 거래소 통합(**exchange integration**) 시 엄격한 컴플라이언스(**compliance**) 절차를 적용합니다.

토큰 판매(**Token Sale**)가 진행될 경우, 이는 해당 관할권의 디지털 자산 및 증권 규제(**digital asset and securities regulations**) 를 준수하는 적격 투자자(**eligible jurisdiction**) 에 한정됩니다.

zkPass 채단은 스위스, 싱가포르, 대한민국 등 주요 법률 시장에서 공인 법률 자문(**licensed counsel**) 과 지속적으로 협력하여, **\$ZKP**가 관련 법률 체계 내에서 비증권(**non-security**) 유틸리티 토큰(**utility token**) 으로서의 분류를 유지하도록 할 것입니다.

10. 팀 및 프로젝트 연혁(**Team & History**)

zkPass의 개발은 여러 단계의 진화를 거치며 진행되어 왔으며, 각 단계는 프라이버시를 보호하면서도 검증 가능한 인터넷(**Verifiable & Privacy-Preserving Internet**) 을 실현하기 위한 중요한 이정표로 기록되었습니다.

프로젝트는 **2022년 2분기(Q2)** 에 시작되었습니다.

핵심 창립팀은 **NTT 도코모(NTT Docomo)**, 텐센트(**Tencent**), **IBM** 출신의 엔지니어들로 구성되어 있으며,

이들은 응용 암호학(**applied cryptography**), 네트워크 보안(**network security**), 분산 시스템(**distributed systems**) 분야에서 깊은 전문성을 보유하고 있습니다.

2022년 말, 팀은 **zkTLS** 프로토타입의 초기 연구 및 구현을 완료했습니다.
이는 업계 최초로 **3자 TLS(Three-Party TLS, 3P-TLS)**, **MPC(Multi-Party Computation)**,
그리고 **IZK(Interactive Zero-Knowledge Proofs)** 를 통합한 혁신적 구조였습니다.

2023년 동안 **zkPass**는 프로토콜 알파(**Protocol Alpha**) 단계로 진입했습니다.
이 시기에는 개발자 테스트넷(**Developer Testnet**) 을 출시하고,
외부 애플리케이션과의 초기 생태계 통합(**Ecosystem Integration**)을 검증했습니다.
이를 통해 **TLS 기반 암호학적 인증(TLS-based Cryptographic Attestation)** 이
현실 세계 데이터 검증(**real-world data verification**)에 적용 가능성을 입증했습니다.

2024년에는 프로젝트가 연구 중심 단계(**research initiative**) 에서
성장하는 생태계(**growing ecosystem**) 로 전환했습니다.
Schema Market 과 **TransGate SDK** 의 출시를 통해
개발자들이 다양한 활용 사례(**use cases**)에 맞춰 재사용 가능한 검증 스키마(**reusable verification schema**) 를
생성 및 배포할 수 있게 되었습니다.
연말 기준으로 zkPass는 **80개** 이상의 통합 파트너 와 **300개** 이상의 스키마 템플릿 을
지원했습니다.

2025년 중반, zkPass 네트워크는 누적 **2억 건(200M)** 이상의 **TVC (Total Verifiable Computation)** 를 달성하였으며,
검증자 인센티브 모델(**Validator Incentive Design**) 과
초기 **DAO** 거버넌스 프레임워크(**Initial DAO Governance Framework**) 를
완성했습니다.
이로써 탈중앙 노드 참여(**Decentralized Node Participation**) 의 기반을 마련했습니다.

앞으로 **2026년** 및 그 이후, zkPass는 완전한 **DAO** 거버넌스 체계 로 전환하며,
엔터프라이즈급(**Enterprise-Grade**) 채택을 확대할 예정입니다.
곧 출시될 **zkTLS Enterprise Suite** 는
기관용 데이터 인증(**Institutional Data Attestation**)과 멀티체인 호환(**Multi-Chain Compatibility**) 을 지원하여,
zkPass를 인터넷의 기초 검증 계층(**Foundational Verification Layer**) 으로 확립할
것입니다.

11. 보안 감사 및 위험 관리(**Security Audits & Risk Management**)

보안(**Security**), 프라이버시(**Privacy**), 그리고 검증 가능성(**Verifiability**) 은 zkPass
프로토콜의 핵심 기반입니다.
zkPass는 장기적인 안정성(**resilience**)과 무결성(**integrity**)을 확보하기 위해,
공식 암호학적 검증(**Formal Cryptographic Verification**), 스마트 컨트랙트 감사(**Smart Contract Audit**),

운영 리스크 관리(**Operational Risk Control**) 를 결합한 다계층 보안 프레임워크(**Multi-Layer Security Framework**) 를 유지하고 있습니다.

11.1 프로토콜 수준의 보안 (Protocol-Level Security)

- **zkTLS** 프로토콜은 **MPC(Multi-Party Computation)** 와 **IZK(Interactive Zero-Knowledge Proofs)** 의 공식 검증된 암호학적 기본 구성요소(**formally verified cryptographic primitives**) 를 기반으로 합니다.
- 세션 키(**Session Key**)와 **MAC(Message Authentication Code)** 공유값 은 임계값 암호화(**Threshold Cryptography**) 를 통해 생성되며, 그 어떤 단일 참여자도 평문 데이터를 복원(reconstruct)할 수 없습니다.
- **TLS 핸드셰이크 증명(TLS Handshake Proofs)** 은 엔드투엔드(**End-to-End**) 로 검증 가능하며, 데이터 출처의 진위성(**authenticity**) 과 부인 방지(**non-repudiation**) 를 보장합니다.
- 모든 온체인 컨트랙트와 zkTLS 프로토콜 모듈에 대한 종합 보안 감사 보고서(**Comprehensive Security Audit Report**) 는 완료 후 아래 링크를 통해 공개될 예정입니다.
👉 [Halborn 공식 감사 보고서 링크 참조](#)

11.2 스마트 컨트랙트 및 네트워크 감사 (Smart Contract & Network Audits)

- 모든 온체인 스마트 컨트랙트(**On-Chain Smart Contracts**) 와 검증자 모듈(**Validator Modules**) 은 **SlowMist, PeckShield, Trail of Bits** 등 업계 공인 보안 감사 기관(industry-recognized security firms)에 의해 독립적 보안 감사(**Independent Audit**)를 거칩니다.
- zkPass는 프로토콜 업데이트 전, 지속적 통합(**Continuous Integration**) 및 형식 검증(**Formal Verification**) 절차를 거치는 내부 테스트 환경(**Internal Testing Environment**) 을 운영하고 있습니다.
- 네트워크는 지속적인 버그 바운티 프로그램(**Ongoing Bug Bounty Program**) 을 운영하여, 책임 있는 취약점 공개(responsible disclosure)와 개방형 보안 협력(open security collaboration)을 장려합니다.

11.3 운영 보안 (Operational Security)

- **DAO 재무부(Treasury)** 및 멀티시그 지갑(**Multisig Wallets**) 은 **3-of-5 서명 구조(3-of-5 Multi-Signature Control)** 로 운영되며, 서명자(Signer)는 주기적으로 교체(rotation)됩니다.

- 검증자 등록(**Validator Registration**) 은 일정량의 \$ZKP 스테이킹(staking)과 가동 시간(**uptime**) 및 신뢰성(**reliability**) 지표를 충족해야 합니다.
- 노드 운영에 사용되는 키(Key)와 자격 증명(Credentials)은 **HSM 기반 인프라(Hardware Security Module-backed Infrastructure)** 에 안전하게 보관되며, 재해 복구 프로토콜(**Disaster Recovery Protocol**) 은 분기별 감사(**Quarterly Audit**) 를 통해 검증됩니다.

11.4 위험 고지 (**Risk Disclosure**)

zkPass 프로토콜은 광범위한 내부 테스트를 거쳤지만, 모든 분산형 암호 시스템(distributed cryptographic system)은 소프트웨어 버그(**Software Bugs**), 네트워크 지연(**Network Latency**), 또는 외부 종속성(**Third-Party Dependencies**) 과 관련된 잔존 위험(residual risk)을 내포할 수 있습니다.

zkPass 재단은 취약점(Vulnerability)이 발견될 경우 이를 투명하게 공개(**public transparency**) 하고, 커뮤니티 주도형 복구 절차(**Community-Driven Remediation Process**) 를 통해 신속히 대응할 것을 약속합니다.