PRIVACY-PRESERVING TRANSFER

zkTransfer — 프라이버시와 검증 가능성을 함께

발신자 · 금액은 감추고 , 거래의 유효성은 누구나 검증하며 , 인가된 기관만 필요할 때 열람하는 프라이버시 전송 인프라 .

지금의 딜레마 — 투명함과 익명 , 둘 다 문제

완전 공개 (투명)

누가 · 누구에게 · 얼마를 보냈는지 모두에게 공개 .
기관 전략 · 개인 자산 정보 노출로 이어지는 구조 .

완전 익명

자금세탁방지 (AML) 대응 · 감사 열람 불가 .
제도권 금융 · 규제 심사를 통과할 수 없는 구조 .

프라이버시와 검증 가능성 — 둘 다 필요

→

① 비공개 전송

발신자와 금액을 공개하지 않고 온체인으로 전송

② 공개 검증

영지식증명 (ZKP) 으로 거래 유효성을 누구나 수학적으로 검증

③ 감사키 열람

인가된 기관만 감사키 (Audit Key) 로 거래를 복호화해 열람

감사 대응을 전제로 한 익명 송금 — AML/CFT 규제 대응 가능 구조

모니터링 가능한 프라이버시 거래 — 프라이버시는 지키고 , 감사 · 규제 대응은 가능하게 . 둘 중 하나를 포기하지 않는 구조 .

PROVEN TECHNOLOGY & USE CASES

이미 검증된 기술 , 넓어지는 활용

중앙은행 실증으로 검증된 익명 전송 기술을 스테이블코인 · 금융 · 공공 영역으로 확장 .

레퍼런스

한국은행 CBDC 모의실험 영지식증명 (ZKP) 기술 공급 ('22)

- 익명 전송 2~3 초 내 처리 (모의실험 환경 측정 성능)
- 인가 기관만 검증 가능한 감사키 구조 — AML 기반 글로벌 익명 송금 구현
- 실증 레퍼런스 기반의 안정성 — 상용 환경 맞춤 성능 설계 지원

활용 분야

기관 간 프라이버시 송금 당사자 · 금액을 가린 기관 간 전송

스테이블코인 프라이버시 결제 결제 정보 노출 없는 온체인 결제

정책자금의 개인정보 없는 이전 개인정보 수집 없는 자금 집행 · 증빙

RWA 자산의 청산 · 소각 실물자산 토큰의 청산 · 소각 처리

제품 스택 내 위치 — Stablecoin Lifecycle

zkWallet Custody
발행 · 키 통제

→

zkPoRL
준비금 증명

→

zkTransfer
프라이버시 전송

→

Evidence Bundle
감사 · 공시

실제 데모 : demo.zkrypto.com (비공개 전송 · 감사키 복호화 체험) 제품 문의 : contact@zkrypto.com