

KOSCOM

STO

STABLECOIN

STO Payment Leg을 위한 프라이버시 인프라

토큰증권(STO) 결제 시 거래 정보 보호 및 규제 준수를 동시에 달성



STO 발행



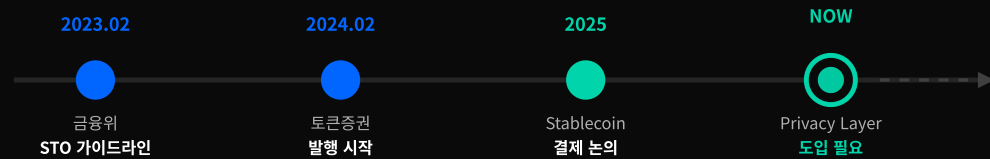
Stablecoin 결제



Privacy Layer

LatticA | ZK + FHE Infrastructure for KOSCOM

한국 STO 시장 동향



Source: 금융위원회, 코스콤

2024.02

토큰증권 발행 시작

11개

STO 발행 기업 (2025.01)

결제 인프라

Stablecoin 도입 논의 중

금융위원회

"토큰증권 발행·유통 규율체계 정비방안" 발표

2023.02

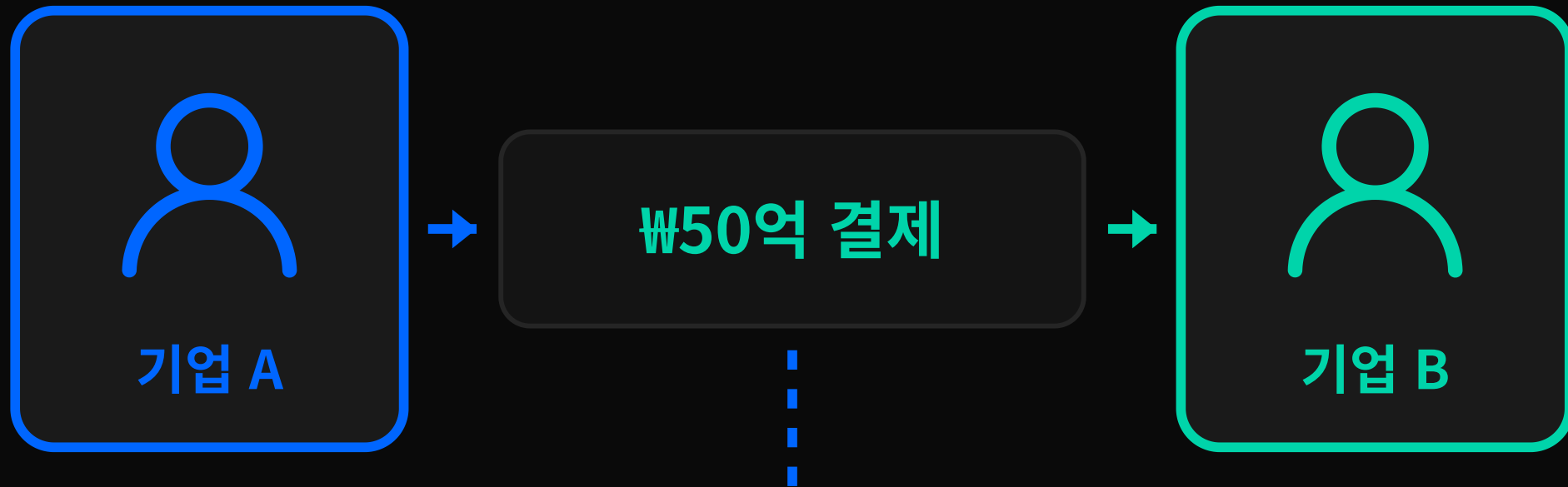
코스콤

STO 플랫폼 구축 및 스테이블코인 결제 검토

2024-2025

STO 결제 시 정보 노출 문제

STO 거래 금액 노출



기존 방식의 한계

기능	일반 블록체인	프라이빗 체인	LatticA
금액 비공개	×	제한적	✓
주소 비공개	×	내부만	✓
규제 준수 (AML/KYC)	✓	✓	✓
감독 기관 감사	✓	제한적	✓

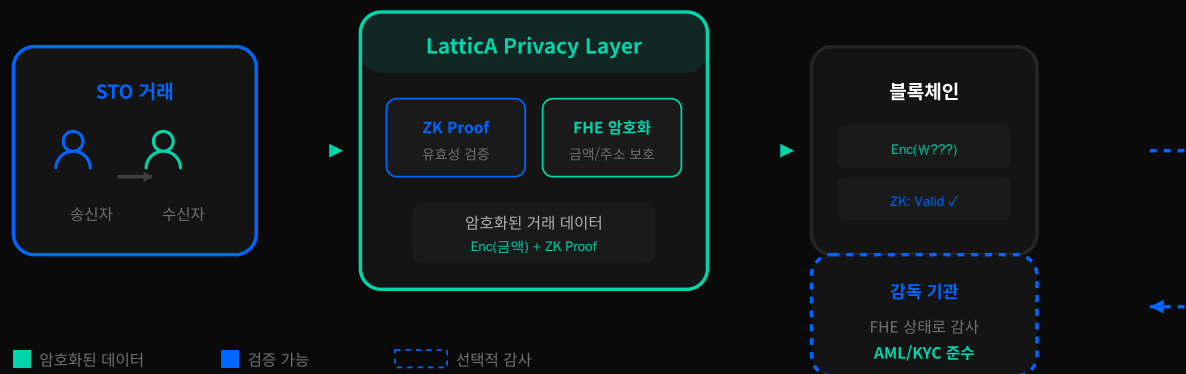


핵심 요구사항

프라이버시 + 규제준수 = 양립 가능해야 함

LatticA는 둘 다 제공

ZK + FHE 아키텍처



영지식 증명 (ZKP)

데이터 공개 없이 유효성 검증



동형암호 (FHE)

암호화 상태로 연산 수행

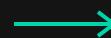


MPC Threshold

다자간 연산으로 복호화 분산

감독 기관 질의

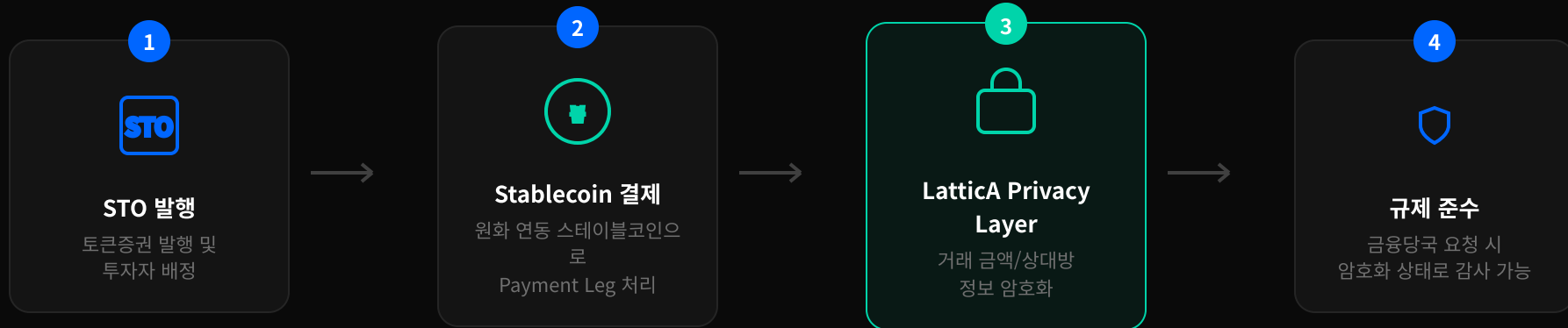
"X 기업의 월간 거래 총액 > 10억?"



FHE 응답

TRUE (암호화 상태로 계산됨)

코스콤 STO 적용 사례



기업 고객
경쟁사에 거래 정보 비공개
전략적 M&A, 투자 정보 보호

코스콤
차별화된 STO 인프라 제공
프라이버시 기능으로 경쟁력 확보

금융당국
필요시 암호화 상태로 감사
AML/KYC 규정 완전 준수

Why LatticA

FHE 부트스트래핑 성능 (64-bit)

Add/Sub 연산 벤치마크

ZAMA TFHE-rs

182ms

LatticA

95ms

1.9x
FASTER

Source: ePrint 2025/2150

1.9x

FHE 성능

ZAMA 대비 부트스트래핑 속도

Cross-Platform

결정론적 연산

CPU/GPU/FPGA 동일 결과



NTT 기반
FFT 오차 없는 정밀 연산

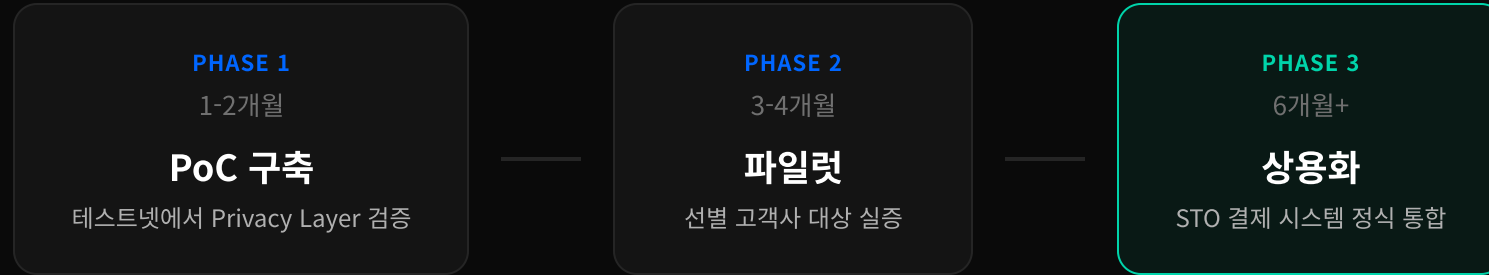


Threshold 복호화
다자간 키 분산으로 단일 장애점 제거



Production Ready
PoC 즉시 진행 가능

코스콤과 함께



코스콤 STO 플랫폼에 프라이버시 레이어 구축

[미팅 요청](#)

✉ contact@lattica.io

🔗 lattica.io