

# STO PAYMENT LEG을 위한 프라이버시 인프라

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

KOSCOM

STO

STABLECOIN

LatticA | ZK + FHE Infrastructure

# 한국 STO 시장 현황

**2023.02**

금융위 STO 가이드라인

**2024.02**

토큰증권 발행 시작

**2025**

Stablecoin 결제 논의

**11개** 기업이 STO 발행 완료 (2025.01 기준)

출처: 금융위원회 | 한국경제


# 문제: STO 결제 시 정보 노출

## 거래 금액 노출

- 블록체인 상 모든 결제 내역 공개
- 경쟁사가 거래 규모 파악 가능

## 거래 관계 노출

- 누가 누구와 거래하는지 추적 가능
- 기업 전략 및 파트너십 유출 우려

 **현재 상황:** Stablecoin 결제가 시작되면 모든 거래 내역이 체인에 기록 → 경쟁사/제3자가 분석 가능

# 기존 방식의 한계

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

핵심: 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

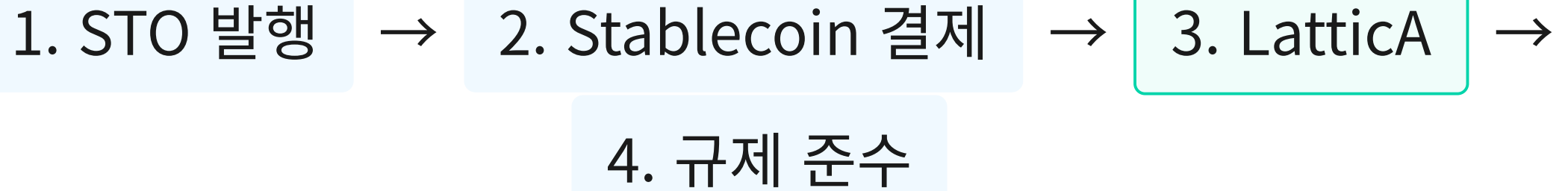
## MPC THRESHOLD

다자간 연산으로 복호화  
분산

감독 기관 질의: "X 기업의 월간 거래 총액 > 10억?"

**FHE 응답:** TRUE (암호화 상태로 계산됨)

# 코스콤 STO 적용 시나리오



## 기업 고객

경쟁사에 거래 정보 비공개



## 코스콤

차별화된 STO 인프라 제공



## 금융당국

암호화 상태로 감사 가능

# WHY LATTICA

**1.9x**

**FHE 성능**

ZAMA 대비 부트스트래핑  
속도

**Cross-  
Platform**

**결정론적 연산**

CPU/GPU/FPGA 동일 결  
과

**Compliance**

**금융 규제 대응**

AML/KYC + 감사 로그 내  
장

**Production Ready - PoC 즉시 진행 가능**

출처: ePrint 2025/2150

# 협력 방안: 코스콤과 함께

## PHASE 1

1-2개월

**POC 구축**

테스트넷에  
서 검증

## PHASE 2

3-4개월

**파일럿**

선별 고객  
사 실증

## PHASE 3

6개월+

**상용화**

STO 결제  
시스템 통  
합

KOSCOM | 금융위 STO 가이드라인



# 감사합니다

LatticA | ZK + FHE Infrastructure

 [contact@lattica.io](mailto:contact@lattica.io)

 [lattica.io](https://lattica.io)