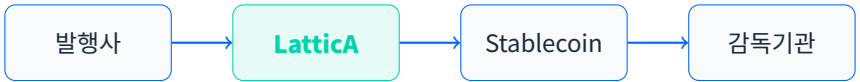
CONFIDENTIAL

코스콤 토큰증권 인프라 제안

Stablecoin 결제의 프라이버시 레이어

자본시장법 제117조 준수 하에 거래 정보 기밀성 확보

FHE 기반 암호화 연산 — 감사 가능성 100% 유지



1.9x **100%** **₩14.6조**

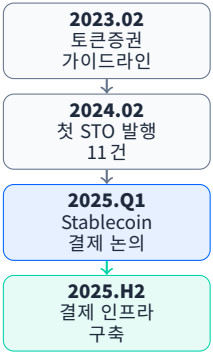
한국 STO 시장: 결제 인프라 공백

01. 시장 현황

시장 규모 전망

구분	2024	2025E	2027E	출처
국내 STO 발행	3,200억	1.2조	**14.6조**	한투
글로벌 토큰화	$50B	$100B	**$2T**	BCG
발행 기업 수	11개	25개+	100개+	금융위

규제 타임라인



핵심 기회

Stablecoin 결제 도입 시 **거래 프라이버시 문제** 발생 필연적

블록체인 투명성 vs 기업 기밀성

02. 문제 정의

× 현재 문제

거래 금액 완전 노출

모든 Stablecoin 이체 금액 온체인 공개

→ Etherscan에서 실시간 조회 가능

거래 상대방 추적

지갑 주소 기반 네트워크 분석 가능

→ Chainalysis, Nansen 이미 상용화

기업 전략 정보 유출

M&A, 투자, 파트너십 정보 노출

→ 대규모 거래 시 시장 교란 가능

✓ 규제 요구사항

자본시장법 제117조

투자자 정보 제3자 제공 금지

특정금융정보법 제5조의2

AML/KYC 의무, 의심거래 보고

전자금융거래법 제21조

5년간 거래기록 보존 및 제출 의무

핵심 딜레마: 기업 요구 (거래 정보 비공개) **vs** 규제 요구 (감사 접근권 보장)

→ **LatticA: 암호화 상태로 감사 수행 = 양립 가능**

기존 솔루션의 구조적 한계

03. 경쟁 분석

기준	Aztec	Penumbra	Token Ext.	LatticA
프라이버시 범위	금액만	금액+주소	금액만	**완전 보호**
규제 감사	불가	불가	제한적	**완전 지원**
EVM 호환	부분	불가	불가	**완전**
연산 지원	이체만	이체+스왑	이체만	**범용 연산**
규제 리스크	높음	중간	낮음	**최소**

선례: Tornado Cash 제재 (2022.08 OFAC)

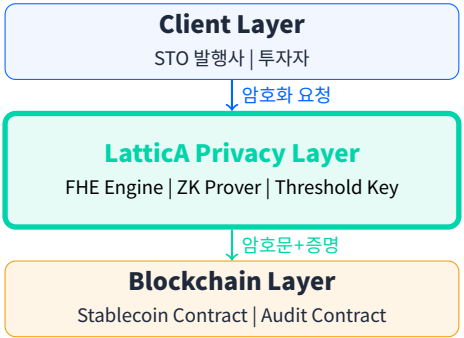
제재 근거: “불법 자금 세탁에 사용될 수 있는 인프라 제공”
핵심 쟁점: 감독 기관이 거래 내역 접근 불가 → 법 집행 불가능
교훈: **프라이버시 솔루션은 규제 감사 기능 필수**

출처: OFAC Tornado Cash 제재 | Aztec Network | Solana Token Extension

ZK + FHE 하이브리드 아키텍처

04. 기술 아키텍처

3-Layer Architecture



성능 벤치마크

Metric	Value
Bootstrapping	**2.89ms**
vs ZAMA tfhe-rs	**1.9x**
연산 방식	NTT (결정론적)
오차 예측 정확도	**<1%**

감사 질의 데모

감독기관 질의:

```
sum(tx.amount) > 1B WHERE entity=``X사''
```

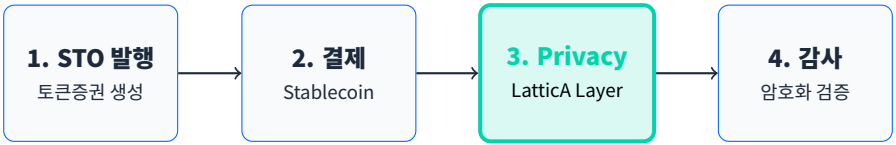
FHE 응답:

```
TRUE + ZK proof (금액 비공개)
```

출처: FHE16 (ePrint 2024/1916) | Primitive Gate (ePrint 2025/2150) | Error Analysis (ePrint 2026/269)

코스콤 STO 플랫폼 통합 시나리오

05. 적용 시나리오



기업 고객

- ✓ 경쟁사에 거래 정보 비공개
- ✓ M&A, 전략적 투자 보호
- ✓ 자본시장법 117조 준수

코스콤

- ✓ 차별화된 STO 인프라
- ✓ 프리미엄 서비스 라인업
- ✓ 글로벌 시장 진출 기반

금융당국

- ✓ 암호화 상태 감사 가능
- ✓ AML/KYC 100% 준수
- ✓ Tornado Cash 리스크 회피

코스콤 가치 제안: 시장 최초 Privacy-Enabled STO 인프라 구축으로
기업 고객 유치 경쟁력 확보 및 규제 선도 기관 포지셔닝

Why LatticA: 검증된 연구 역량

06. 기술 우위

ePrint 2024/1916

FHE16: Fast, Compact Bootstrapping

Seunghwan Lee, Dohyuk Kim, Dong-Joon Shin

2.89ms Bootstrapping (n=512)

16-bit 정수 연산 기반, MIMC 병렬화로 1.9x 성능

ePrint 2025/2150

Primitive Gate Bootstrapping

Dohyuk Kim, Sin Kim, Seunghwan Lee, et al.

PGF Primitive Gate Family

단일 Bootstrapping으로 다중 입력 게이트 지원

ePrint 2026/269

Exact Error Analysis for Blind Rotation

Sin Kim, Seunghwan Lee, et al.

<1% 오차 예측 정확도

기존 휴리스틱 대비 50% 오차 감소

Crypto 2025 — ePrint 2025/810

Actively Secure MPC

Seunghwan Lee et al.

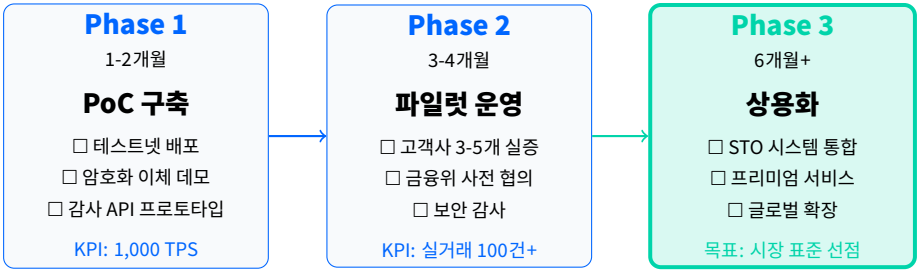
Active Security Dishonest Majority

Circuit-privacy 최초 도입, O(1) 복잡도

NTT 기반 정밀 연산 Threshold 복호화 Production Ready

코스콤과 함께

07. 협력 제안



코스콤 STO 플랫폼에 프라이버시 레이어 구축

시장 최초 규제 준수형 Privacy Infrastructure

Email
contact@lattica.io

Website
lattica.io

LinkedIn
linkedin.com/company/lattica