LatticA

Lattice Acceleration & Alliance,
Using Fully Homomorphic Encryption, FHE16

Confidential contract: privacy rail for institutions

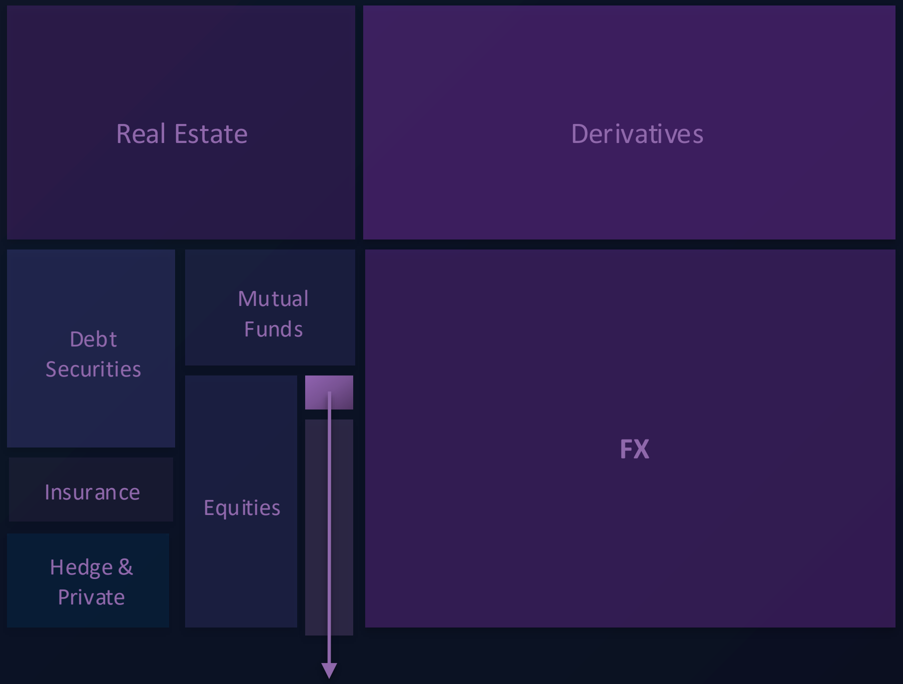
LatticA

Off-chain financial opportunities

: How to onboard onto Solana?

[Global Financial Market Size]

Unit: Trillions of Dollars



Tokenized(Crypto)assets are **small**

Our Problem

Contract with off-chain assets
Should be confidential
(for institution)

Off-chain financial opportunities

:From a confidential transfer to a confidential contract

" We want to make contract with our asset "

[Institutions with tokens]

Current

Token Extension

Confidential Transfer	Supporting Regulation	Confidential Contract		
○	○	?	=	Confidential Transaction

Solution

Token Extension + LatticA

Confidential Transfer	Supporting Regulation	Confidential Contract		
○	○	○	=	Confidential Contract

LatticA

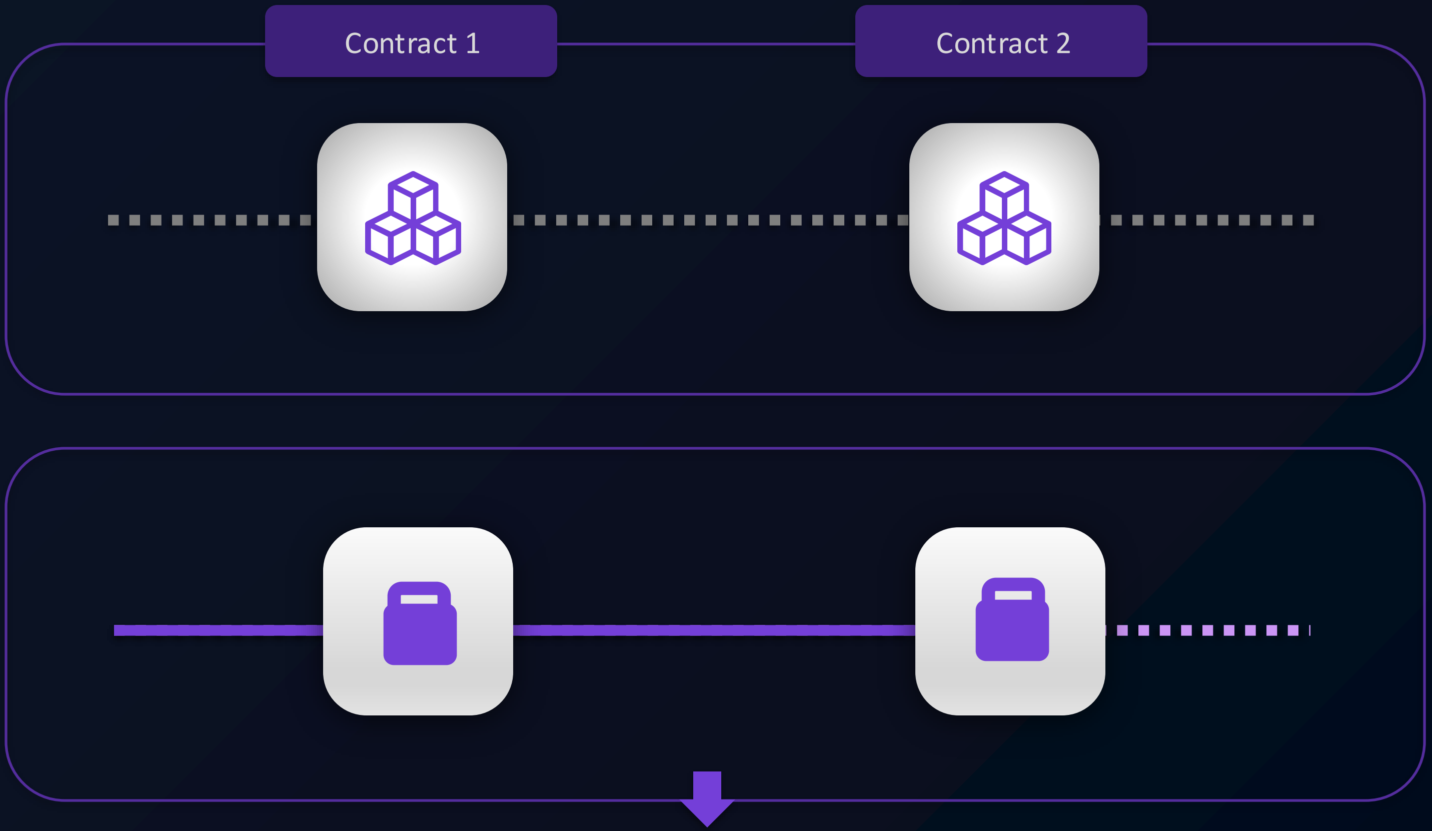
LatticA bridges every institution, every chain
- by FHE16

*Previous Chains

Contract logics and results are Immediately open

*FHE16

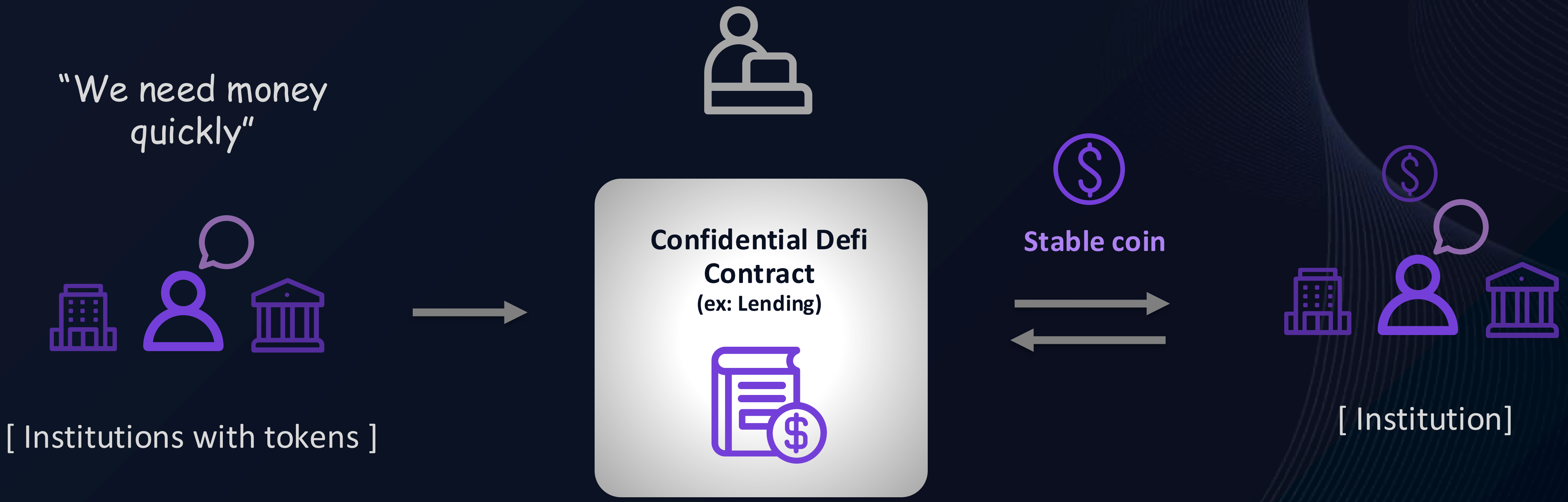
Contract is made on the ciphertext



‘ Time — Controlled Reveal - Free Optional Feature! ‘

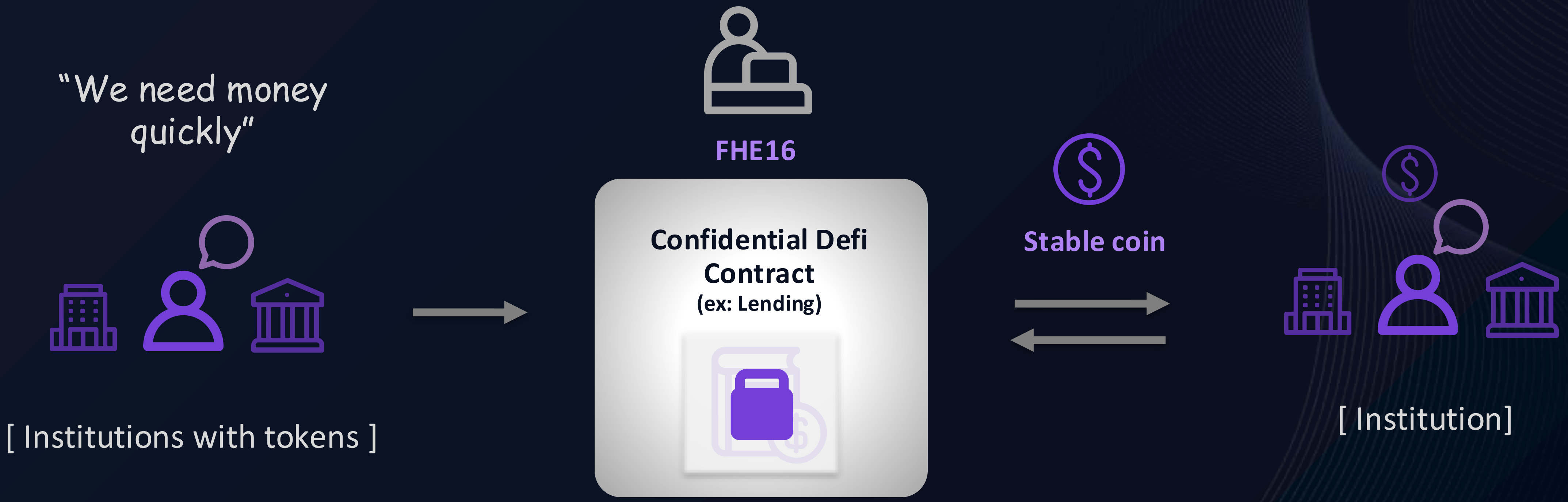
LatticA

Confidential Transactions, Verifiable Results
- with FHE



FHE16 keeps your contract confidential.

Confidential Transactions, Verifiable Results
- with FHE



"We need money quickly"

[Institutions with tokens]

FHE16

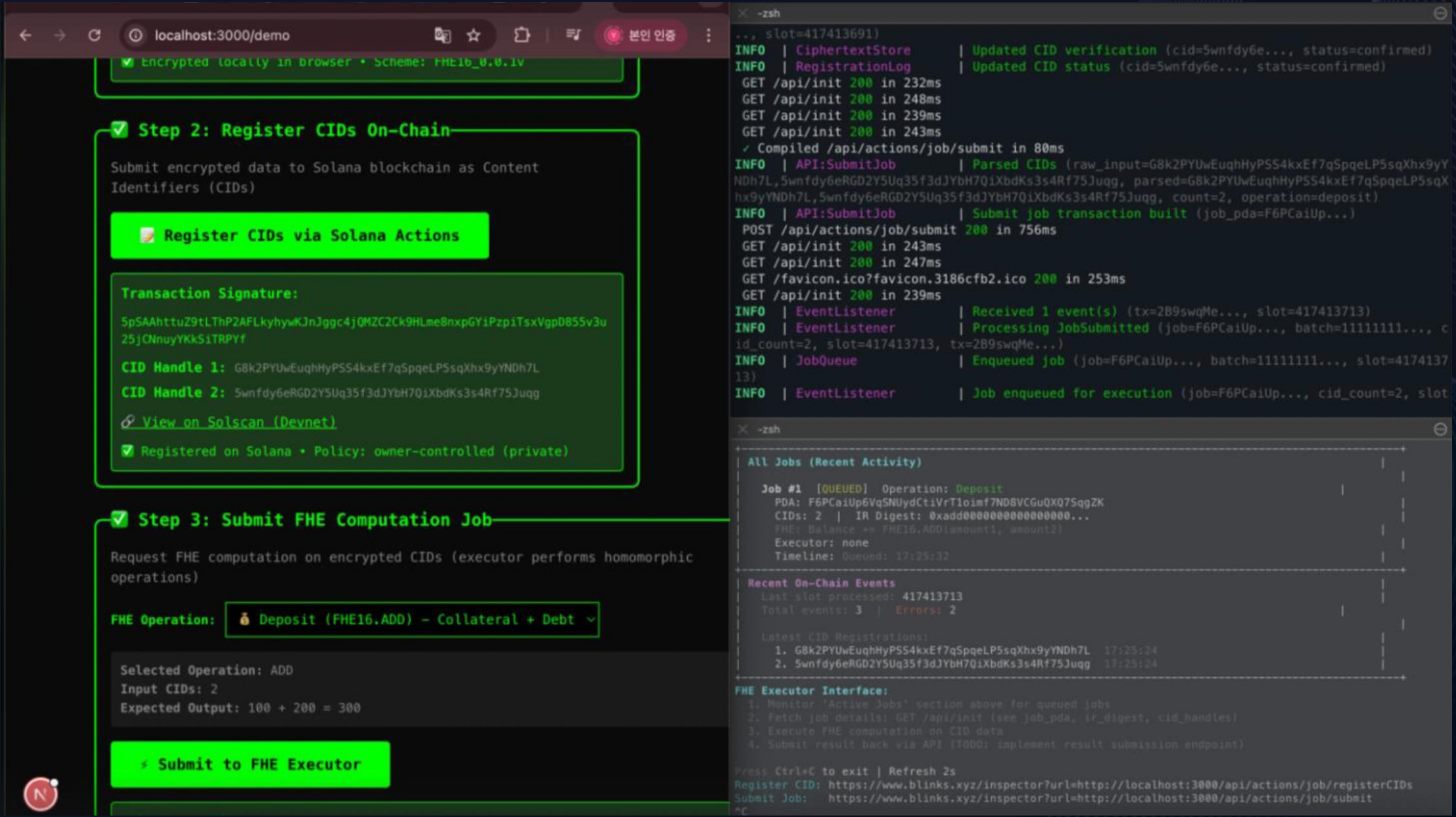
Confidential Defi Contract
(ex: Lending)

Stable coin

[Institution]

FHE16 keeps your contract confidential.

Demo scenario-Confidential Defi Contact



☑ Encrypted locally in browser • Scheme: FHE16_0.0.1v

☑ Step 2: Register CIDs On-Chain

Submit encrypted data to Solana blockchain as Content Identifiers (CIDs)

Transaction Signature:

5pSAAhttuZ9tLThP2AFLkyhywKJnJggc4jQMZC2Ck9HLme8nxpGYiPzpiTsxVgpD855v3u25jCNnuyYKkSiTRPYf

CID Handle 1: G8k2PYUwEuqhHyPSS4kxEf7qSpqeLP5sqXhx9yYNDh7L

CID Handle 2: 5wnfdy6eRGD2Y5Uq35f3dJYbH7QiXbdKs3s4Rf75Juqg

🔗 View on Solscan (Devnet)

☑ Registered on Solana • Policy: owner-controlled (private)

☑ Step 3: Submit FHE Computation Job

Request FHE computation on encrypted CIDs (executor performs homomorphic operations)

FHE Operation: 💰 Deposit (FHE16.ADD) - Collateral + Debt

Selected Operation: ADD
Input CIDs: 2
Expected Output: 100 + 200 = 300

```
..., slot=417413691)
INFO  | CiphertextStore       | Updated CID verification (cid=5wnfdy6e..., status=confirmed)
INFO  | RegistrationLog       | Updated CID status (cid=5wnfdy6e..., status=confirmed)
 GET /api/init 200 in 232ms
 GET /api/init 200 in 248ms
 GET /api/init 200 in 239ms
 GET /api/init 200 in 243ms
 ✓ Compiled /api/actions/job/submit in 80ms
INFO  | API:SubmitJob         | Parsed CIDs (raw_input=G8k2PYUwEuqhHyPSS4kxEf7qSpqeLP5sqXhx9yY
NDh7L,5wnfdy6eRGD2Y5Uq35f3dJYbH7QiXbdKs3s4Rf75Juqg, parsed=G8k2PYUwEuqhHyPSS4kxEf7qSpqeLP5sqX
hx9yYNDh7L,5wnfdy6eRGD2Y5Uq35f3dJYbH7QiXbdKs3s4Rf75Juqg, count=2, operation=deposit)
INFO  | API:SubmitJob         | Submit job transaction built (job_pda=F6PCaiUp...)
 POST /api/actions/job/submit 200 in 756ms
 GET /api/init 200 in 243ms
 GET /api/init 200 in 247ms
 GET /favicon.ico?favicon.3186cfb2.ico 200 in 253ms
 GET /api/init 200 in 239ms
INFO  | EventListener         | Received 1 event(s) (tx=2B9swqMe..., slot=417413713)
INFO  | EventListener         | Processing JobSubmitted (job=F6PCaiUp..., batch=11111111..., c
id_count=2, slot=417413713, tx=2B9swqMe...)
INFO  | JobQueue              | Enqueued job (job=F6PCaiUp..., batch=11111111..., slot=4174137
13)
INFO  | EventListener         | Job enqueued for execution (job=F6PCaiUp..., cid_count=2, slot
```

```
+--------------------------------------------------------------------------------+
| All Jobs (Recent Activity)                                                    |
|                                                                                |
|   Job #1  [QUEUED]  Operation: Deposit                                      |
|     PDA: F6PCaiUp6VqSNUydCtiVrT1oimf7ND8VCGuQXQ7SqgZK                          |
|     CIDs: 2  |  IR Digest: 0xadd0000000000000000...                          |
|     FHE: Balance += FHE16.ADD(amount1, amount2)                               |
|     Executor: none                                                             |
|     Timeline: Queued: 17:25:32                                                |
+--------------------------------------------------------------------------------+
| Recent On-Chain Events                                                        |
|   Last slot processed: 417413713                                              |
|   Total events: 3  |  Errors: 2                                             |
|                                                                                |
|   Latest CID Registrations:                                                   |
|     1. G8k2PYUwEuqhHyPSS4kxEf7qSpqeLP5sqXhx9yYNDh7L  17:25:24                  |
|     2. 5wnfdy6eRGD2Y5Uq35f3dJYbH7QiXbdKs3s4Rf75Juqg  17:25:24                  |
+--------------------------------------------------------------------------------+
FHE Executor Interface:
  1. Monitor 'Active Jobs' section above for queued jobs
  2. Fetch job details: GET /api/init (see job_pda, ir_digest, cid_handles)
  3. Execute FHE computation on CID data
  4. Submit result back via API (TODO: implement result submission endpoint)

Press Ctrl+C to exit | Refresh 2s
Register CID: https://www.blinks.xyz/inspector?url=http://localhost:3000/api/actions/job/registerCIDs
Submit Job:   https://www.blinks.xyz/inspector?url=http://localhost:3000/api/actions/job/submit
^C
```

LatticA(FHE16) VS SOTA FHE

- **Our Technology: FHE16**
- **Decentralized computation**

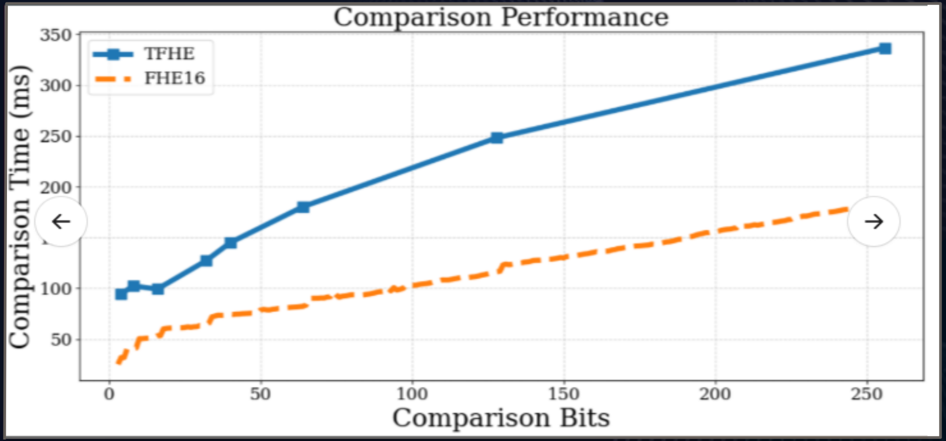
  Any-device can make confidential contracts
- **Public verification**

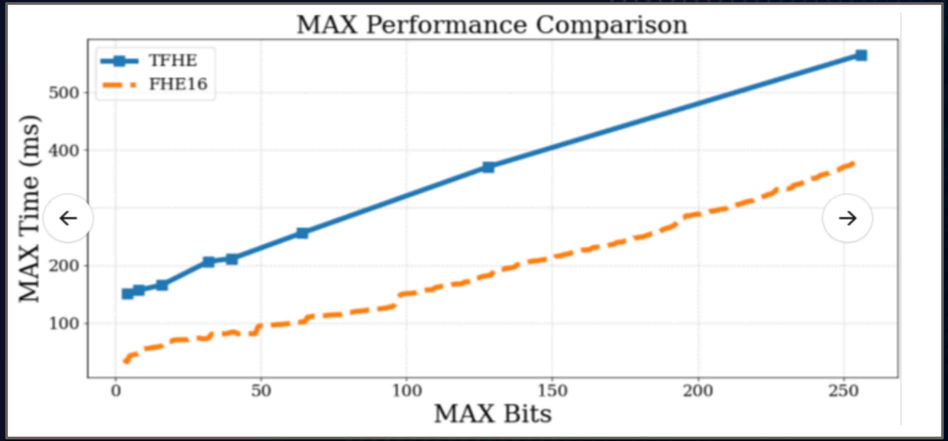
  Any-device can re-run all contracts
- **Improved computation speed**

[Speed comparison]

LatticA is 2-3 times faster than SOTA FHE

SOTA FHE ------ FHE16





Our Team

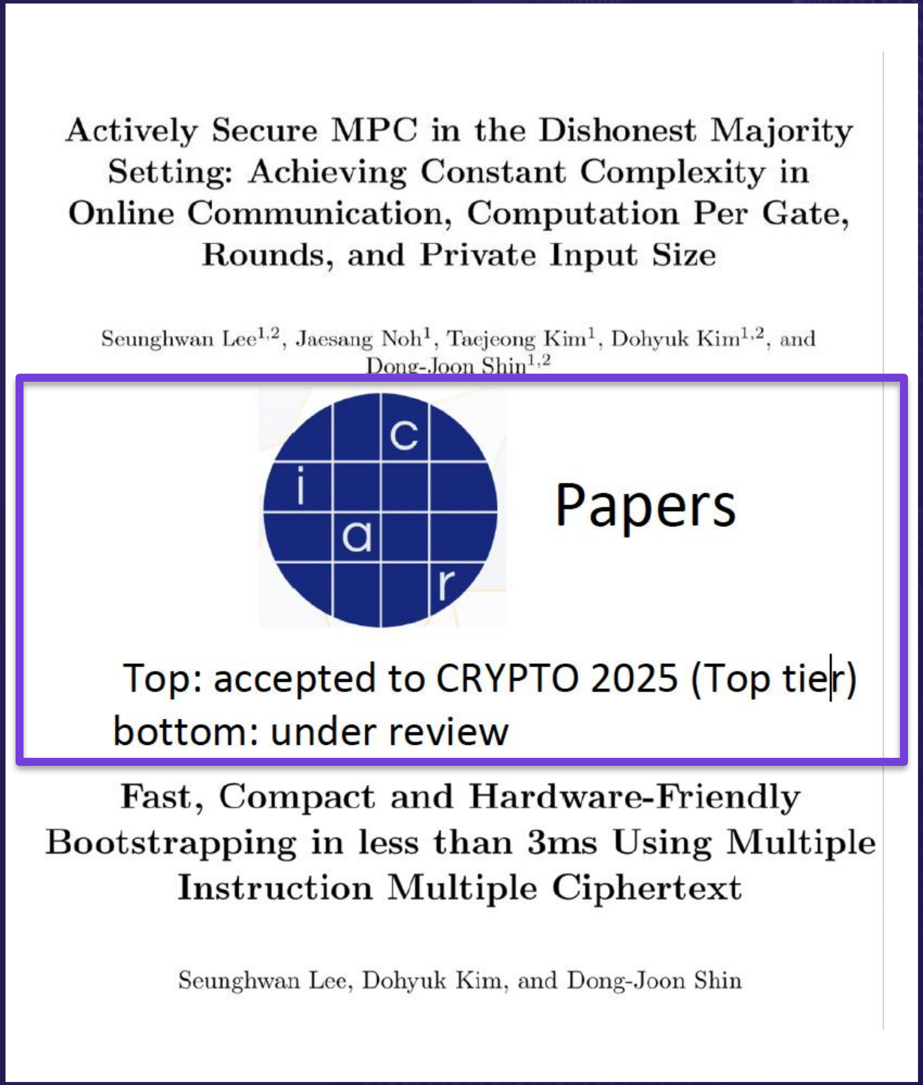
Seunghwan Lee_CEO
Ph.D
(2019~2025, Hanyang,Korea)

Dohyuk Kim_CTO
Ph.D Candidate
(2023~, Hanyang,Korea)

Dong-Joon Shin_CSO
Tenured professor
(2000~, Hanyang,Korea)

Yunsik Ham, Youngjun Kim
Skilled WEB3 Developers

Kiin Shin, Jiin Shin
Skilled WEB3 Designers



Actively Secure MPC in the Dishonest Majority Setting: Achieving Constant Complexity in Online Communication, Computation Per Gate, Rounds, and Private Input Size

Seunghwan Lee[1,2], Jaesang Noh[1], Taejeong Kim[1], Dohyuk Kim[1,2], and Dong-Joon Shin[1,2]

Papers

Top: accepted to CRYPTO 2025 (Top tier)
bottom: under review

Fast, Compact and Hardware-Friendly Bootstrapping in less than 3ms Using Multiple Instruction Multiple Ciphertext

Seunghwan Lee, Dohyuk Kim, and Dong-Joon Shin

FHE16

Let’s build confidential contracts on Ciphertexts!

Goodbye **Front-running,** Hello **Institutions**

@SCARROTS

LatticA

Seunghwan Lee
(shlee@walllnut.com)