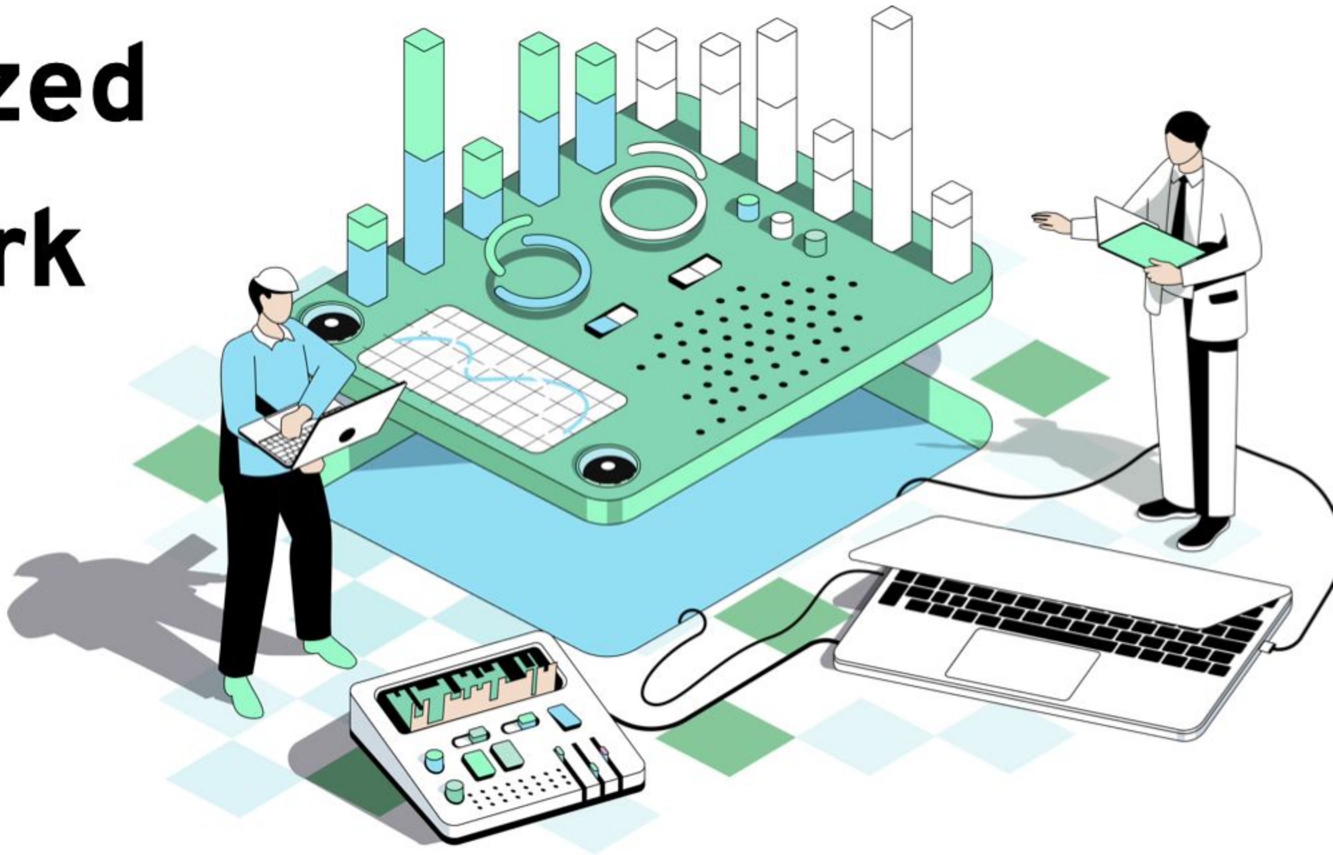
PADO

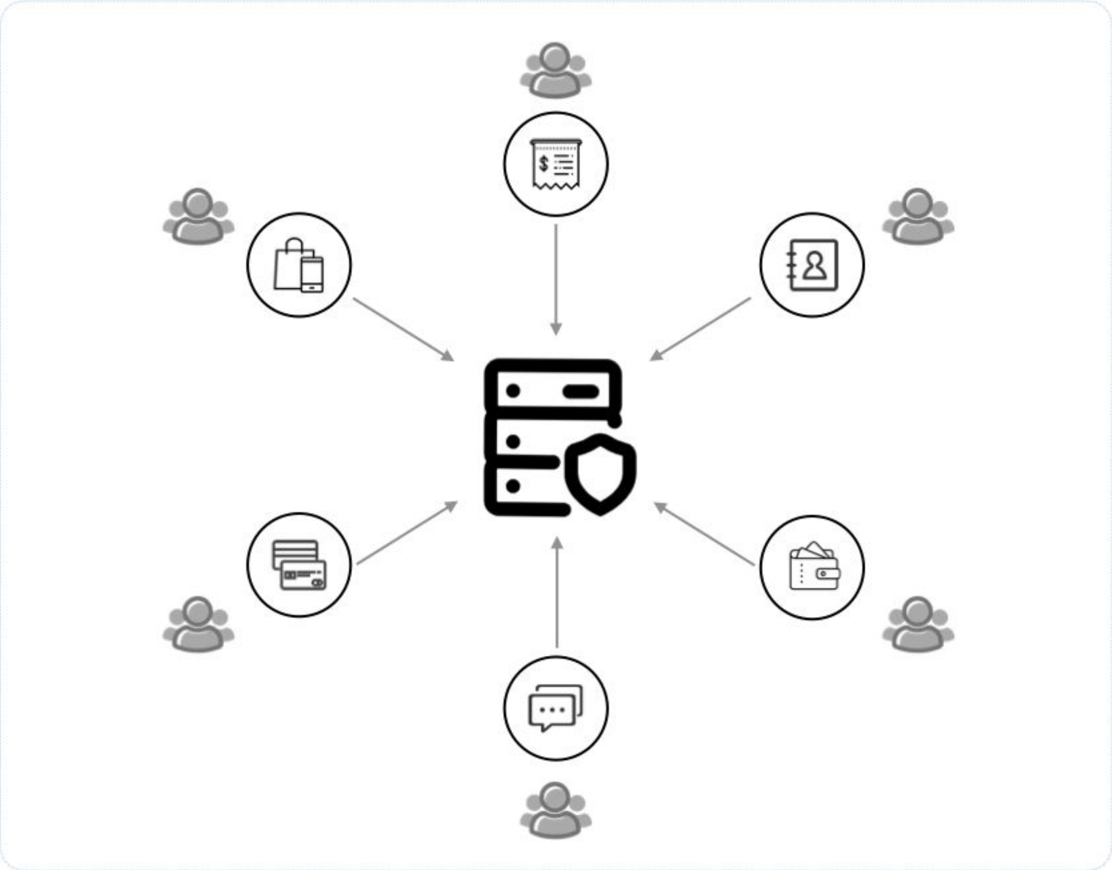
A zkFHE Decentralized Computation Network



Motivation

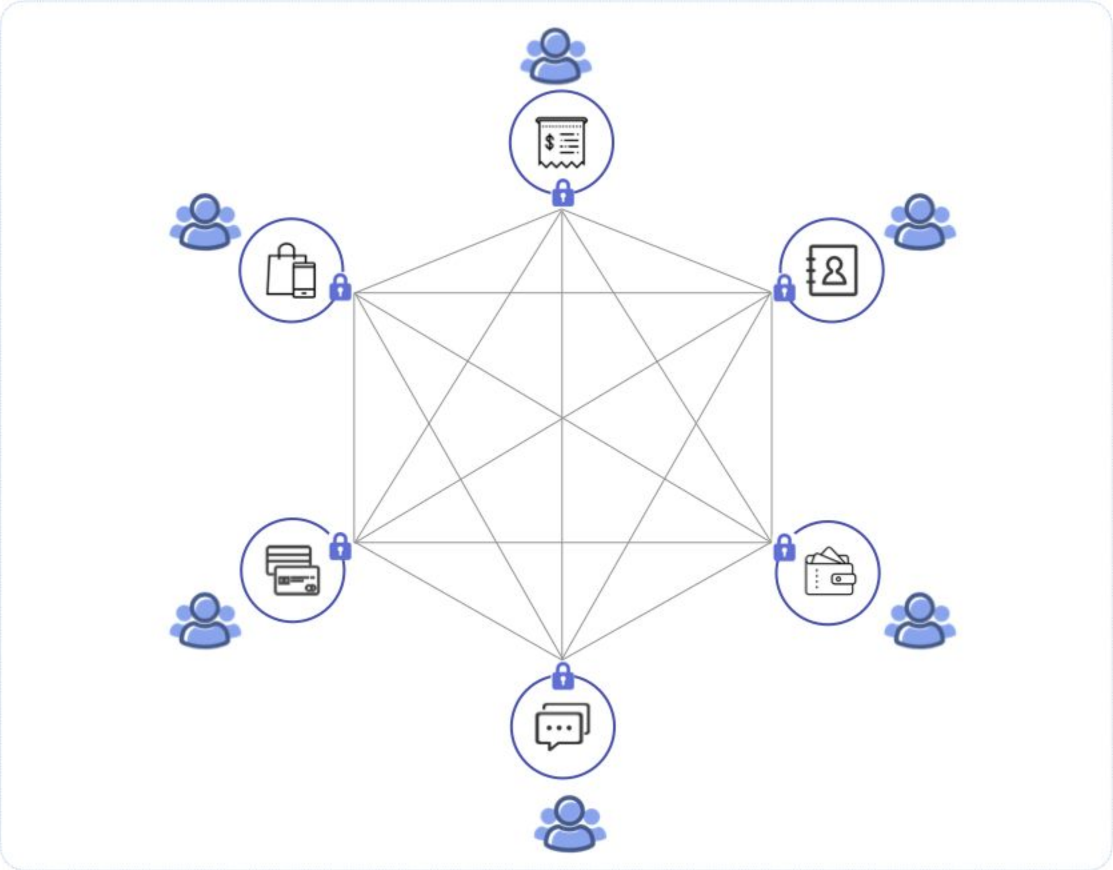
Today

Centralized Data Confidentiality



Future

Decentralized Data Confidentiality

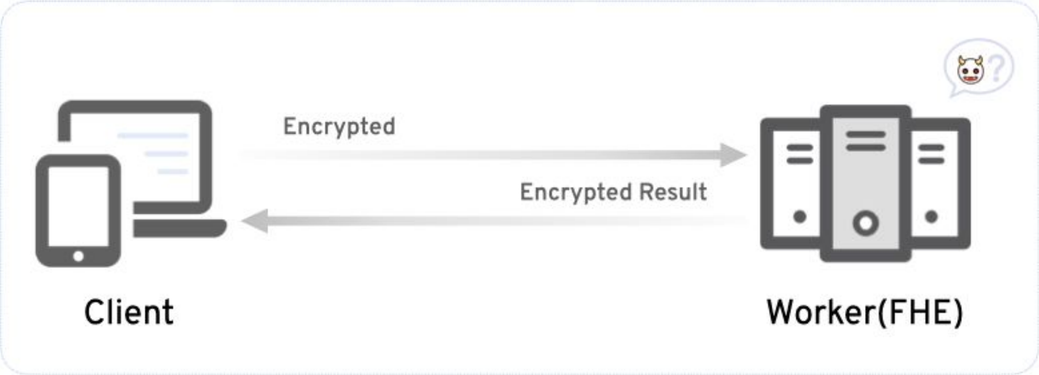


Current Approaches

Fully Homomorphic Encryption:

The client has to trust the worker in terms of computation integrity.

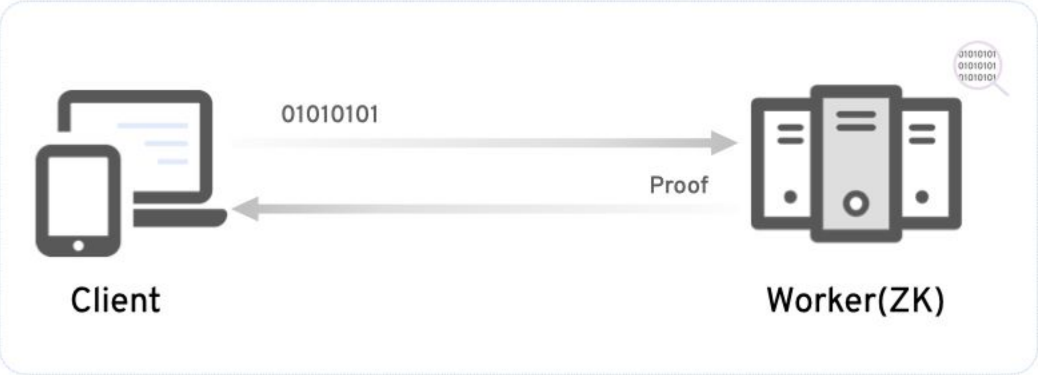
Lack of verifiability!



Zero-Knowledge Proof:

The client delegates private data to the worker, raising privacy concerns.

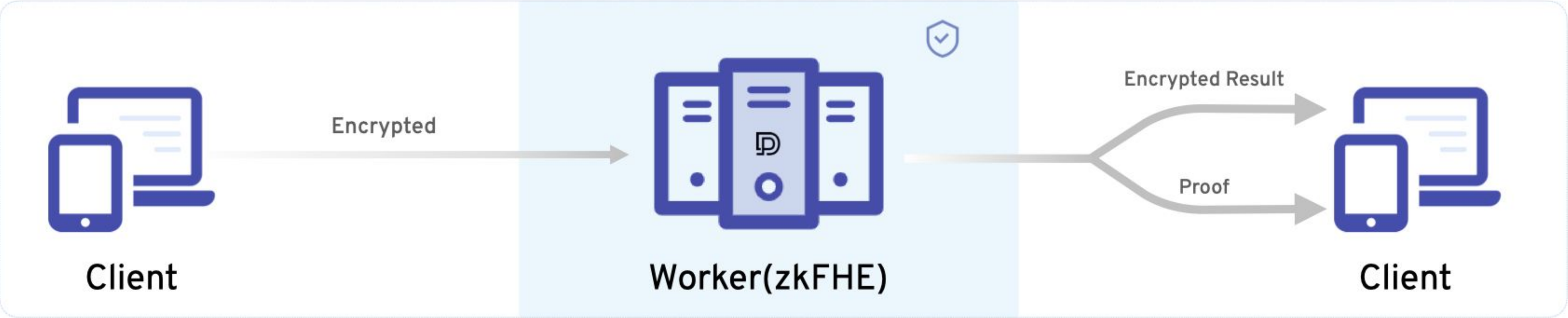
Lack of confidentiality!



Our Solution

zkFHE: Win-Win

The client can outsource computation to a trustless worker without sacrificing privacy and computation integrity.



Performance

Existing method:

Lack of generality and efficiency

Compiling FHE code into zkVM for simple operations, like validating ciphertext, is slow and can take hours to prove.

Our result:

00:03

Boosting compatibility and efficiency

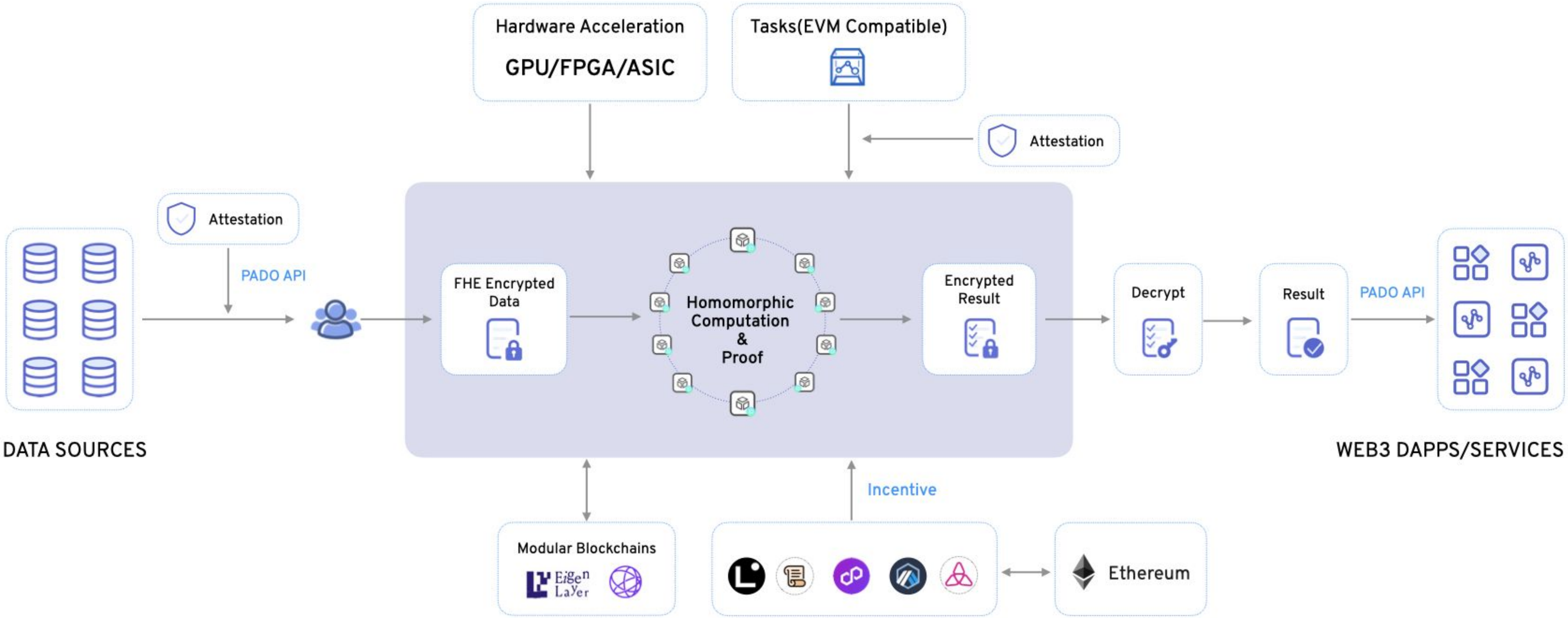
We can prove the core operation (bootstrapping) of FHE **in a few seconds**, we can still improve it.

How we achieve it:

- Efficient NTT/INTT operation proofs
- Sumcheck and PCS protocol with small prime fields
- FHE adaptation for small prime fields
- Parallel proof generation and hardware compatibility

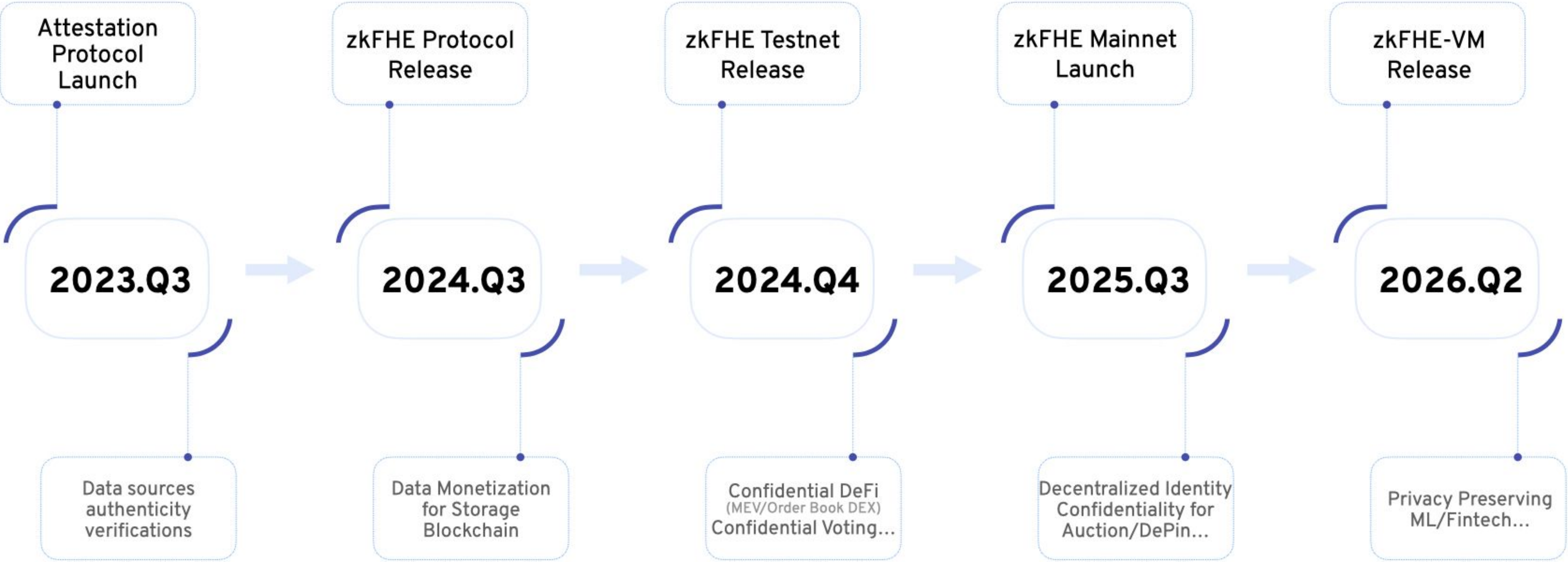
Ultimate Goal

Build a zkFHE Decentralized Computation Network



© PADO Labs 2024

Roadmap



2023.Q3

Attestation Protocol Launch

Data sources authenticity verifications

2024.Q3

zkFHE Protocol Release

Data Monetization for Storage Blockchain

2024.Q4

zkFHE Testnet Release

Confidential DeFi
(MEV/Order Book DEX)
Confidential Voting...

2025.Q3

zkFHE Mainnet Launch

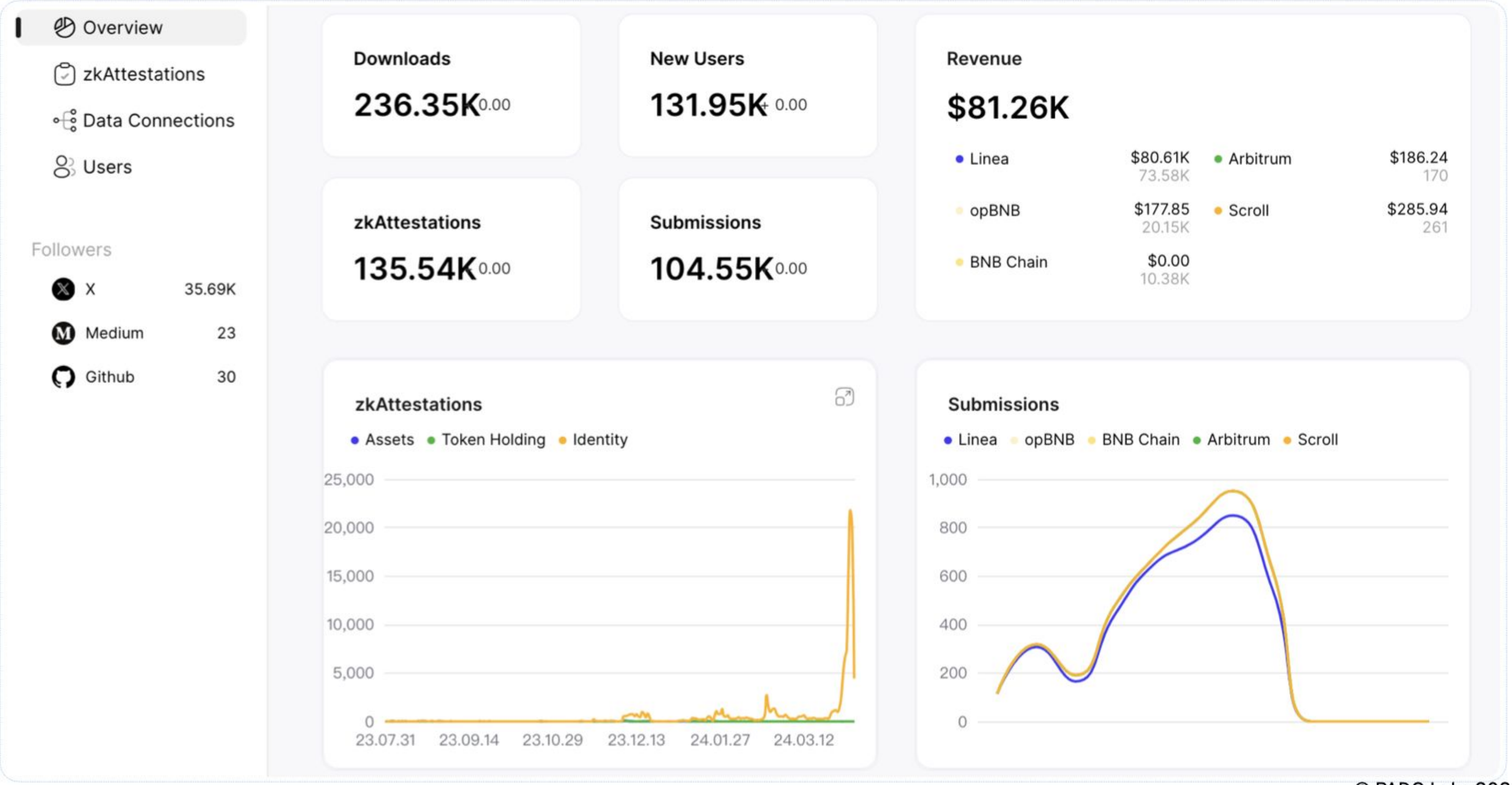
Decentralized Identity
Confidentiality for Auction/DePin...

2026.Q2

zkFHE-VM Release

Privacy Preserving ML/Fintech...

First Stage



Followers

X	35.69K
Medium	23
Github	30

Downloads
236.35K 0.00

New Users
131.95K 0.00

zkAttestations
135.54K 0.00

Submissions
104.55K 0.00

Revenue
$81.26K

● Linea	$80.61K 73.58K	● Arbitrum	$186.24 170
● opBNB	$177.85 20.15K	● Scroll	$285.94 261
● BNB Chain	$0.00 10.38K		

zkAttestations

Submissions

Highlights

ethereum foundation

Granted by Ethereum Foundation & PSE

consensys Fellowship

Accepted by the first cohort of Consensys Fellowship Program

BERKELEY BLOCKCHAIN XCELERATOR

Selected by Cohort 7 of Berkeley Blockchain Xcelerator

polygon Village

Selected by Polygon Village Startup Support Program

40+

Published 40+ papers in top-tier cryptography conferences

IZK

Invented the state-of-the-art interactive ZK protocols

Team

14
People

6
PhDs

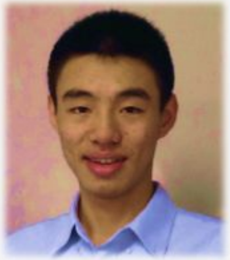
4
Professors

12
Interns

Xiang Xie

CEO/Co-Founder

Ph.D. in Cryptography. 6 years experience in crypto industry.



Xiao Wang

Chief Scientist

Assistant professor of computer science at Northwestern University.

Vicky Zhang

CMO/Co-Founder

Emory University double major with 3 years in Web3 marketing.

Tie Qi

COO/Co-Founder

FinTech serial entrepreneur with 20 years in financial security.

Yu Yu

Academic Partner

Professor at Shanghai Jiao Tong University.

Seeking Collaboration

Fundraise

Pre-A round fundraise targeting at leading investors

Collaboration

Seeking collaborations with the game-changing projects in the industry

Talent

Looking for research cryptographers, and token economy advisors

Marketing

Looking for market and BD leads, branding and social media experts