NOX LABS
(EX. LUMOS LABS)
3 FRASER STREET, #04-23A
SINGAPORE, (189352)
DUO TOWER

Private Vault for ERC-20 tokens

We're creating a "private vault" that can attach to any ERC20 token, letting users hold and send funds without showing amounts publicly

01

A universal upgrade for any ERC20 token

02

Lets users move tokens from their public balance into a private one

03

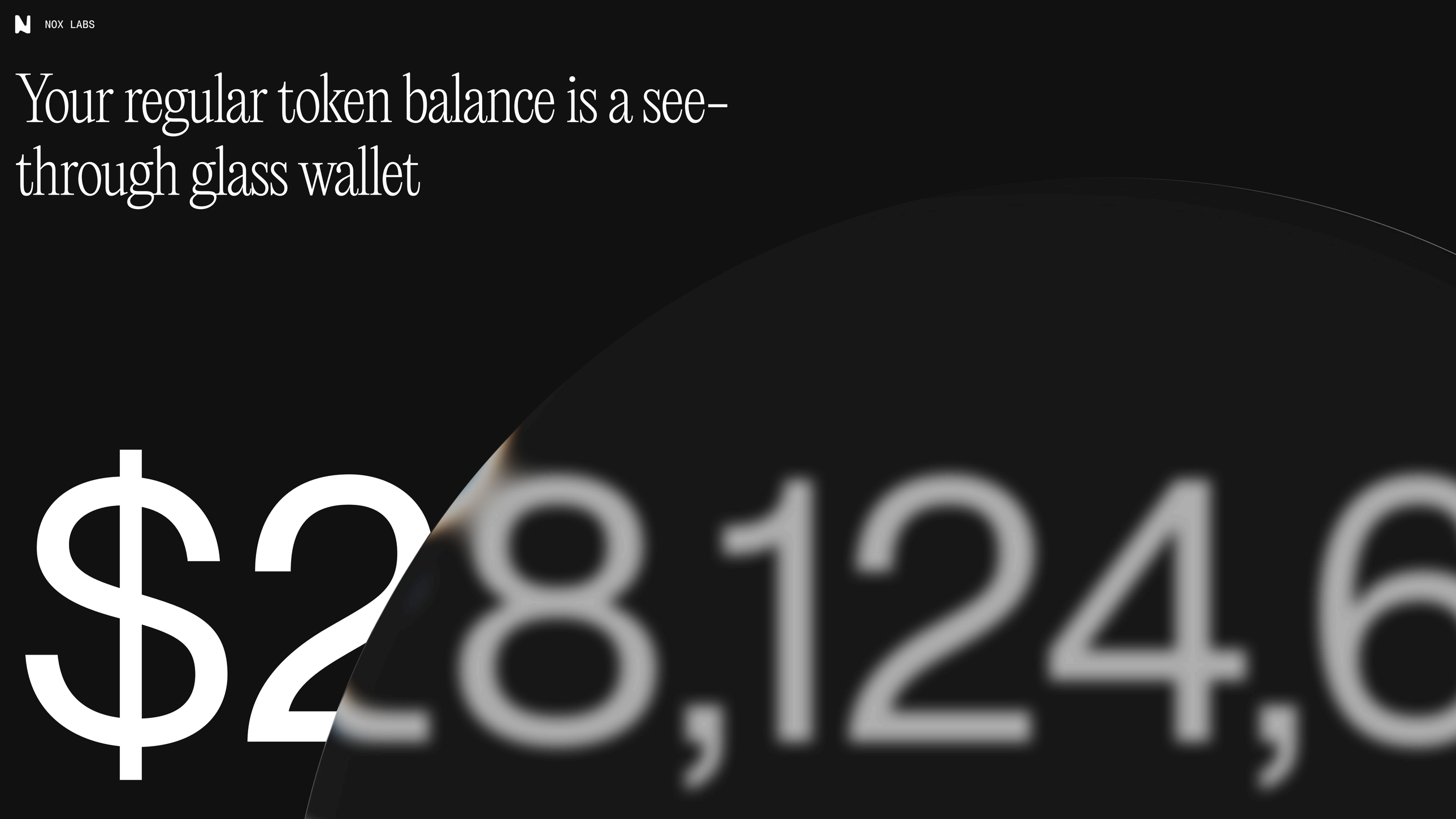
Inside this private system, all amounts stay hidden — only the fact that a transfer happened is visible

04

Users can move funds back out to the public world whenever they need to

NOX LABS

Your regular token balance is a see-through glass wallet



Our feature adds a secure, opaque vault to it

On public blockchains, every transaction is visible to everyone

No Privacy

Every payment, balance, and transfer can be seen by competitors, analysts, or anyone watching.

Strategic Disadvantage

This exposes sensitive business details like:

- Payments to partners,
- Payroll amounts,
- Treasury moves,
- Upcoming large trades or investments,

Barrier to Adoption

For institutions, total transparency is unacceptable. They need financial privacy to operate. Without it, many high-value use cases can’t exist on public chains.

Use Cases

NOX LABS

Confidential B2B Payments

Pay suppliers and partners without showing payment terms or amounts to competitors.

123456

NOX LABS

Private Treasury Management

Move large sums internally without triggering market speculation.

123456

NOX LABS

Confidential Payroll

Pay employees and contractors privately—no public salary data.

123456

NOX LABS

Discreet Investor Operations

Manage dividends, capital calls, or M&A transactions securely.

123456

Future for CEXs

Centralized exchanges can let users deposit and withdraw privately.

123456

Cross-Chain Compatibility

LayerZero integration allows confidential transfers across different blockchains.

123456

NOX LABS

The Power of Zero-Knowledge Proofs

What is a ZKP?

A cryptographic method that proves something is true without revealing the actual data.

EXAMPLE

You can prove you own a watch by correctly telling me the time several times without showing the watch itself.

How we use it

- Each user's balance is encrypted on-chain
- When transferring, the user generates a proof locally
- This proof confirms:
  - The user has enough funds
  - The math is correct
  - No money was created
- The smart contract verifies the proof, not the amount

Key takeaway

We replace visible numbers with verifiable math

NOX LABS

The Power of Zero-Knowledge Proofs

What is a ZKP?

A cryptographic method that proves something is true without revealing the actual data.

EXAMPLE

You can prove you own a watch by correctly telling me the time several times without showing the watch itself.

How we use it

- Each user's balance is encrypted on-chain
- When transferring, the user generates a proof locally
- This proof confirms:
  - The user has enough funds
  - The math is correct
  - No money was created
- The smart contract verifies the proof, not the amount

Key takeaway

We replace visible numbers with verifiable math

NOX LABS

The Power of Zero-Knowledge Proofs

What is a ZKP?

A cryptographic method that proves something is true without revealing the actual data.

EXAMPLE

You can prove you own a watch by correctly telling me the time several times without showing the watch itself.

How we use it

- Each user's balance is encrypted on-chain
- When transferring, the user generates a proof locally
- This proof confirms:
  - The user has enough funds
  - The math is correct
  - No money was created
- The smart contract verifies the proof, not the amount

Key takeaway

We replace visible numbers with verifiable math

Possible Solutions

TECHNOLOGY	HOW IT WORKS	DECISION & REASON
Mixers (e.g., Tornado Cash)	Blend funds from many users to hide sender/receiver links.	Doesn't hide amounts; regulatory issues.
Homomorphic Encryption	Blend funds from many users to hide sender/receiver links.	Too slow and expensive for Ethereum.
L2 Rollups	Move funds to a private layer.	Complex to integrate; splits liquidity.
Railgun	One private vault for all tokens.	Geared toward retail, not institutions.
Zero-Knowledge Proofs (ZKPs)	Verify transactions without revealing data.	Best mix of privacy, security, and speed.

Choosing the Right ZKP Model

MODEL	HOW IT WORKS	ASSESMENT
UTXO (like Zcash)	Uses “notes” that represent funds. Transfers spend old notes and create new ones.	Strong privacy Complex for users and relies on external systems
Account Model (like Solana)	Each user has one encrypted balance that’s updated securely.	Slightly higher gas cost Simple, self-contained, and auditable

Choosing the Right ZKP Model

MODEL	HOW IT WORKS	ASSESMENT
UTXO (like Zcash)	Uses “notes” that represent funds. Transfers spend old notes and create new ones.	Strong privacy Complex for users and relies on external systems
Account Model (like Solana)	Each user has one encrypted balance that’s updated securely.	Slightly higher gas cost Simple, self-contained, and auditable

NOX LABS

Possible Solutions

TECHNOLOGY	MODEL	AUDIENCE
Railgun / Aztec Connect	UTXO	Retail DeFi users
Tornado Cash	Mixer	Retail privacy users
Our Extension	Account	Institutional users

- Simpler, no off-chain systems
- We hide amounts and stay compliant
- Simple and auditable

- Simpler, no off-chain systems
- We hide amounts and stay compliant
- Simple and auditable

- Simpler, no off-chain systems
- We hide amounts and stay compliant
- Simple and auditable

NOX LABS

The Acceptable Price of Privacy

For large transactions (like payroll or treasury moves), gas is less than 0.1% of the total value — an acceptable cost for full confidentiality

Confidential Transfer

±1M

Standard ERC20 Transfer

±50K

Secure, Compliant, and Easy to Use

Core Engine

Account-based ZKP system using efficient zk-SNARKs

Non-Interactive Transfers

Transfers happen in two steps (Send & Apply) so receivers don’t need to be online

Auditing & Compliance

A read-only “auditor key” allows secure, controlled access for compliance

Cross-Chain Ready

Built for LayerZero, supporting future multi-chain private transfers

NOX LABS
(EX. LUMOS LABS)
3 FRASER STREET, #04-23A
SINGAPORE, (189352)
DUO TOWER

Summary

We're building a secure, compliant, and easy-to-use privacy layer for ERC20 tokens, powered by Zero-Knowledge Proofs

Why

To enable institutional-grade transactions with full financial privacy

Result

Any token becomes suitable for real business use——confidential payments, payroll, and treasury management