AEGIS

ETH Oxford 2026

Sofie Rüffer, Matthew Wilson, Aakash Gnanavelu

The Problem

Currently, customers have to provide their private key or deposit funds into a developer-controlled wallet, which requires custodial trust

You're trusting strangers not to steal your money

AEGIS

Autonomous trading bot that generates its own private keys inside an Intel TDX Trusted Execution Environment (TEE) via Oasis ROFL

Generates its own private key inside the TEE, which is used to create a wallet and sign transactions

Why TEE?

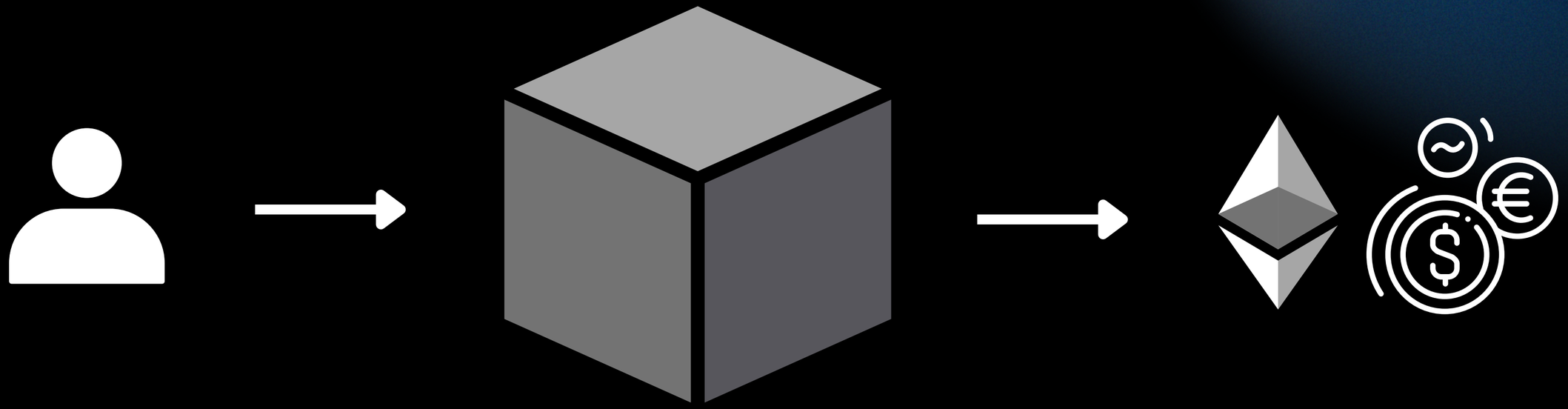
Key generated inside hardware, developer never sees it

Theft is physically impossible (enforced by the chip)

Remote attestation cryptographically proves the exact code

Auditable logs produced inside the TEE

AEGIS



USER SENDS ETH

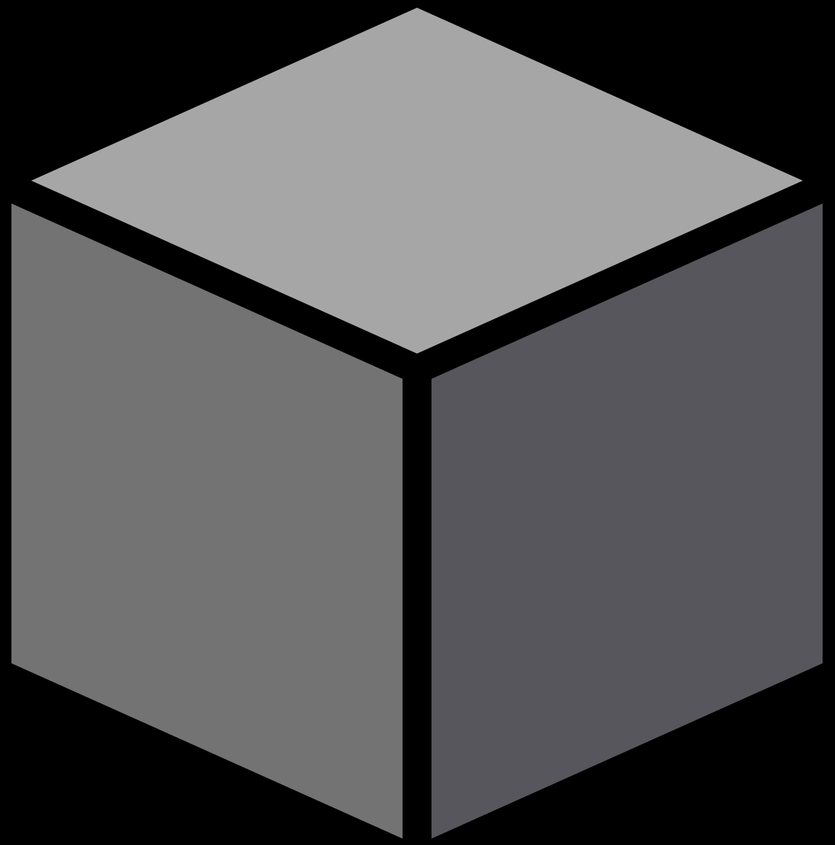
INTEL TDX TRUSTED EXECUTION ENVIRONMENT (TEE)

TRANSACTION ON BASE SEPOLIA

AEGIS

AEGIS is built as 5 modules that run in sequence every cycle

AEGIS



WALLET:
Generate private key

STRATEGY:
Makes DECISION based on market data and RSI over seven days of hourly candles

POLICY:
A safety layer that runs inside the TEE

TRADER:
Constructs and submits swaps on Uniswap V2

ORCHESTRATOR:
Ties it all together in a continuous loop

AEGIS

WALLET

Generates and manages private keys with hardware entropy

Keys are encrypted at rest using AES-256-CBC and never logged or exported

In the TEE, keys are derived from hardware.

Outside, they are derived from a passphrase-encrypted file.

AEGIS

STRATEGY

Pulls price data from two independent oracles (CoinGecko + CryptoCompare) and computes RSI over 7 days of hourly candles

If the oracles disagree by more than 2%, the bot holds as a safety measure

RSI value below 30 → BUY (oversold)

RSI value avoe 70 → SELL (overbought)

RSI value between 30-70 → HOLD (neutral)

AEGIS

POLICY

A safety layer that runs inside the TEE, that encodes:

- Maximum trade size per swap
- Daily trading volume cap (resets at midnight)
- Rate limiting between trades
- Token whitelist (only approved pairs)
- Emergency stop switch.

AEGIS

TRADER

Constructs and submits swaps on Uniswap V2 with:

- Configurable slippage tolerance
- Gas estimation
- ETH ↔ USDC path routing

Supports Sepolia, Base Sepolia, and any EVM chain.

AEGIS

ORCHESTR.

Ties it all together in a continuous loop:

Signal → *Policy Check* → *Execute* → *Wait* → *Repeat*

Handles errors and shuts down when necessary

Key Innovation

The agent never reads a raw private key

Locally it uses a passphrase-encrypted wallet.enc (AES-256-CBC); in the TEE the same file can be sealed in the enclave

The private key is generated inside the process (hardware entropy), encrypted and only used for signing (never exported or logged)

AEGIS

TEE-Secured Trading