OpenZeppelin

Building a LaunchPad Order Book with CivTrade

using OpenZeppelin Defender

DexMan
civ@civfund.org
@civ100

Nami Shah
nami@openzeppelin.com
@nami_sh

OpenZeppelin

Our mission is to protect the open economy

OpenZeppelin is a software company that provides **security audits** and **products** for decentralized systems.

Projects from any size -from new startups to established organizations- trust OpenZeppelin to build, inspect and connect to the open economy.

Compound coinbase AAVE

δY/δX brave UMA

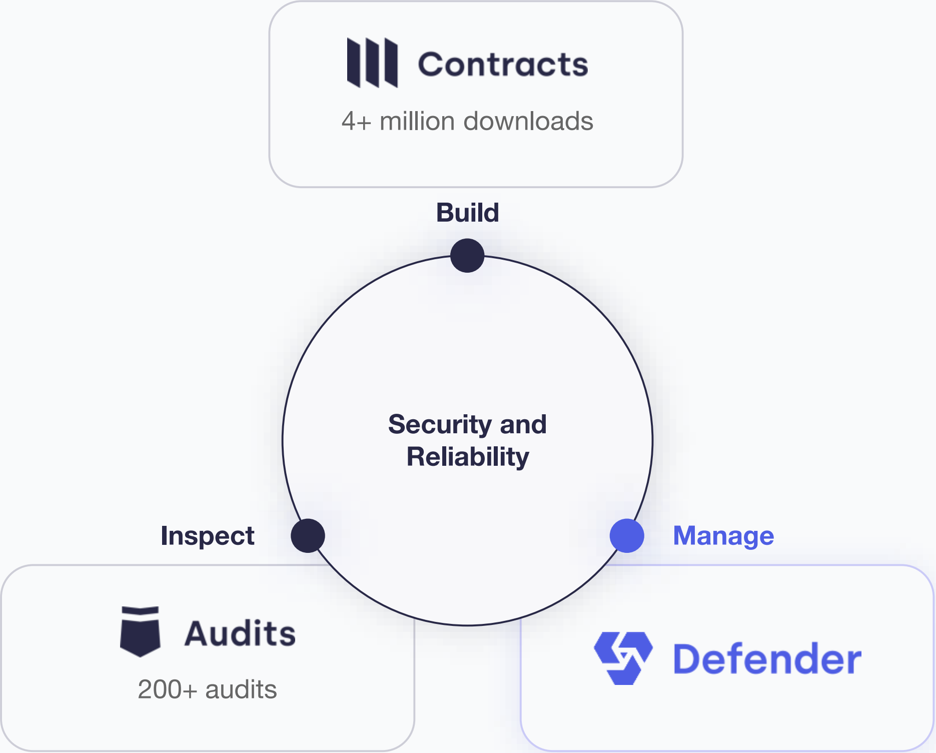
Balancer ethereum foundation augur

celo CIRCLE BitGo

pool together Set opyn

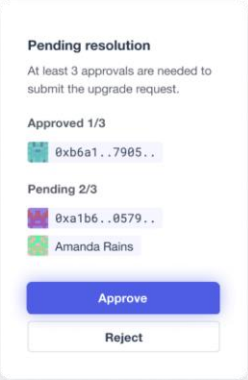
Security, Reliability and Risk Management

OpenZeppelin provides a complete suite of **security and reliability products** to build, manage, and inspect all aspects of software development and operations for Ethereum projects.



Follow along in Defender

- Defender is now **free**!
- Head over to **zpl.in/def** to sign up and follow along the workshop in real time



Pending resolution

At least 3 approvals are needed to submit the upgrade request.

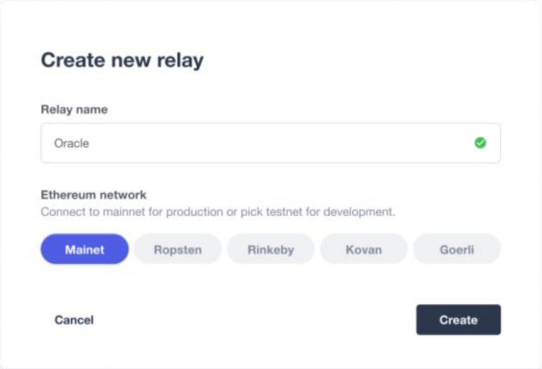
Approved 1/3

0xb6a1..7905..

Pending 2/3

0xa1b6..0579..

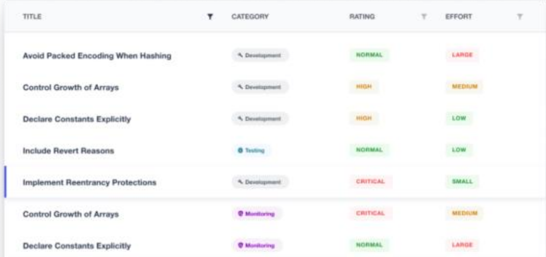
Amanda Rains



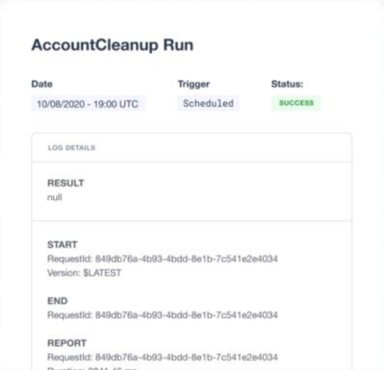
Create new relay

Relay name: Oracle

Ethereum network
Connect to mainnet for production or pick testnet for development.



TITLE	CATEGORY	RATING	EFFORT
Avoid Packed Encoding When Hashing	Development	NORMAL	LARGE
Control Growth of Arrays	Development	HIGH	MEDIUM
Declare Constants Explicitly	Development	HIGH	LOW
Include Revert Reasons	Testing	NORMAL	LOW
Implement Reentrancy Protections	Development	CRITICAL	SMALL
Control Growth of Arrays	Monitoring	CRITICAL	MEDIUM
Declare Constants Explicitly	Monitoring	NORMAL	LARGE



AccountCleanup Run

Date: 10/08/2020 - 19:00 UTC
Trigger: Scheduled
Status: SUCCESS

```
LOG DETAILS

RESULT
null

START
RequestId: 849db76a-4b93-4bdd-8e1b-7c541e2e4034
Version: $LATEST

END
RequestId: 849db76a-4b93-4bdd-8e1b-7c541e2e4034

REPORT
RequestId: 849db76a-4b93-4bdd-8e1b-7c541e2e4034
```

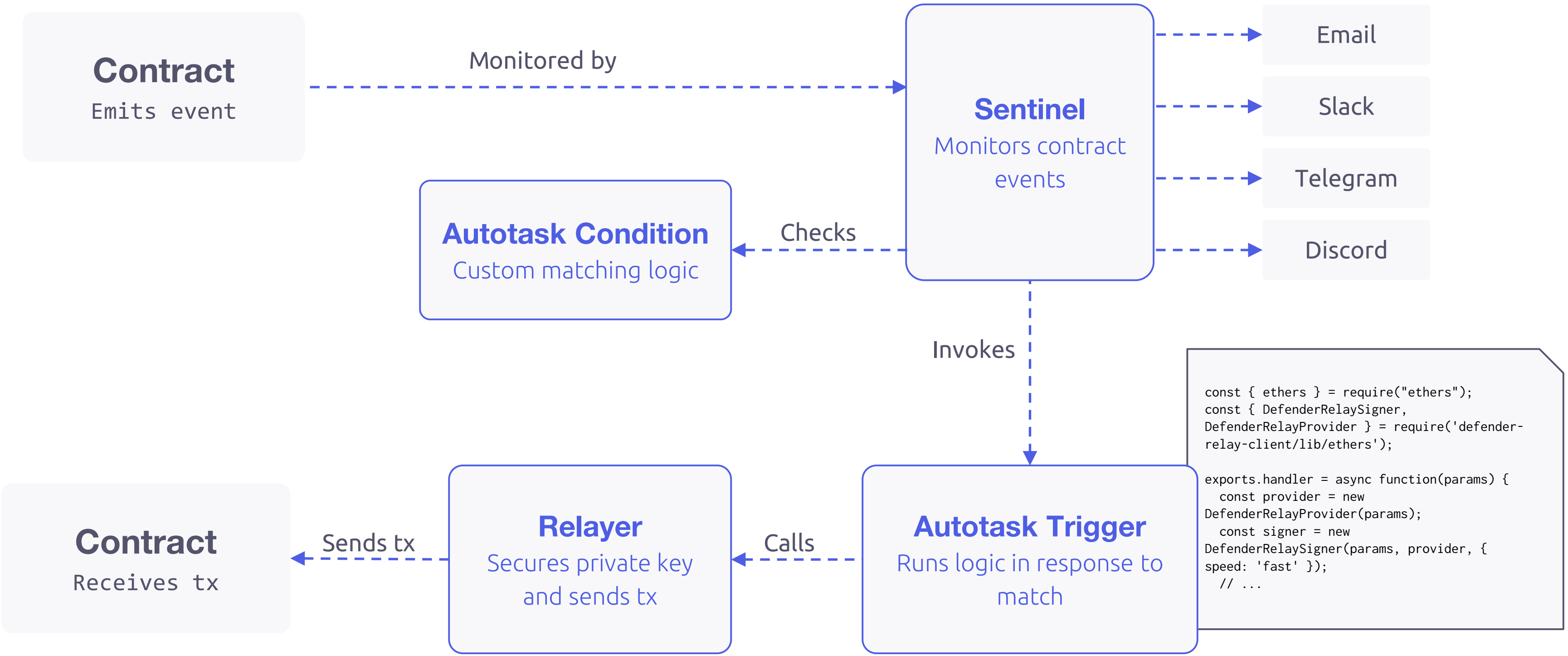
Automating
Smart Contract operations

Monitoring, sending txs, automation, administration

Defender Components

- **Admin** - Automate and secure all your smart contract administration
- **Sentinel** – Monitor smart contracts and send notifications
- **Advisor** – Learn and implement security best practices
- **Autotask** – Create automated scripts to call your smart contracts
- **Relay** - Build with private and secure transaction infrastructure

Sentinel → Autotask → Relayer



```
const { ethers } = require("ethers");
const { DefenderRelaySigner,
DefenderRelayProvider } = require('defender-
relay-client/lib/ethers');

exports.handler = async function(params) {
  const provider = new
DefenderRelayProvider(params);
  const signer = new
DefenderRelaySigner(params, provider, {
speed: 'fast' });
  // ...
```

OpenZeppelin

Use cases

- Send Transactions from a server
- Send Transactions based on an event
- Query a subgraph as part of an autotask
- Interacting with external APIs
- Running a Keep3r network keeper https://docs.openzeppelin.com/defender/guide-keep3r
- Signing a message with a private key
- Meta transactions https://blog.openzeppelin.com/gasless-metatransactions-with-openzeppelin-defender/

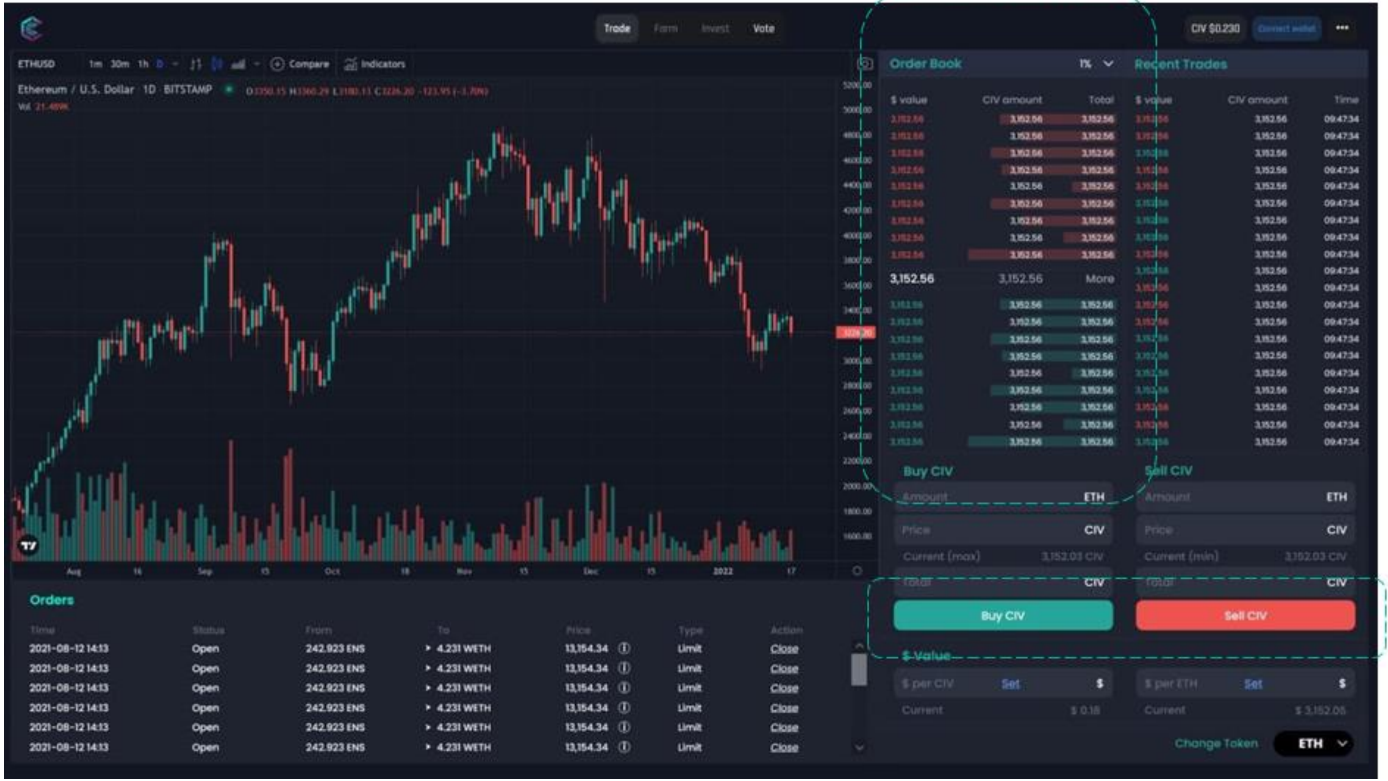
OpenZeppelin

Introducing the CivTrade OrderBook

With OpenZeppelin Defender

The DeFi order book

Like Binance, but DeFi



Order Book 1%

$ value	CIV amount	Total
3,152.56	3,152.56	3,152.56
3,152.56	3,152.56	3,152.56
3,152.56	3,152.56	3,152.56
3,152.56	3,152.56	3,152.56
3,152.56	3,152.56	3,152.56
3,152.56	3,152.56	3,152.56
3,152.56	3,152.56	3,152.56
3,152.56	3,152.56	3,152.56
3,152.56	3,152.56	3,152.56
3,152.56	3,152.56	More
3,152.56	3,152.56	3,152.56
3,152.56	3,152.56	3,152.56
3,152.56	3,152.56	3,152.56
3,152.56	3,152.56	3,152.56
3,152.56	3,152.56	3,152.56
3,152.56	3,152.56	3,152.56
3,152.56	3,152.56	3,152.56
3,152.56	3,152.56	3,152.56
3,152.56	3,152.56	3,152.56

Recent Trades

$ value	CIV amount	Time
3,152.56	3,152.56	09:47:34
3,152.56	3,152.56	09:47:34
3,152.56	3,152.56	09:47:34
3,152.56	3,152.56	09:47:34
3,152.56	3,152.56	09:47:34
3,152.56	3,152.56	09:47:34
3,152.56	3,152.56	09:47:34
3,152.56	3,152.56	09:47:34
3,152.56	3,152.56	09:47:34
3,152.56	3,152.56	09:47:34
3,152.56	3,152.56	09:47:34
3,152.56	3,152.56	09:47:34
3,152.56	3,152.56	09:47:34
3,152.56	3,152.56	09:47:34
3,152.56	3,152.56	09:47:34
3,152.56	3,152.56	09:47:34
3,152.56	3,152.56	09:47:34
3,152.56	3,152.56	09:47:34
3,152.56	3,152.56	09:47:34
3,152.56	3,152.56	09:47:34

Buy CIV

Amount ETH

Price CIV

Current (max) 3,152.03 CIV

Total CIV

Buy CIV

Sell CIV

Amount ETH

Price CIV

Current (min) 3,152.03 CIV

Total CIV

Sell CIV

$ Value

$ per CIV Set $

Current $ 0.18

$ per ETH Set $

Current $ 3,152.05

Change Token ETH

Orders

Time	Status	From	To	Price	Type	Action
2021-08-12 14:13	Open	242.923 ENS	▸ 4.231 WETH	13,154.34 ⓘ	Limit	Close
2021-08-12 14:13	Open	242.923 ENS	▸ 4.231 WETH	13,154.34 ⓘ	Limit	Close
2021-08-12 14:13	Open	242.923 ENS	▸ 4.231 WETH	13,154.34 ⓘ	Limit	Close
2021-08-12 14:13	Open	242.923 ENS	▸ 4.231 WETH	13,154.34 ⓘ	Limit	Close
2021-08-12 14:13	Open	242.923 ENS	▸ 4.231 WETH	13,154.34 ⓘ	Limit	Close
2021-08-12 14:13	Open	242.923 ENS	▸ 4.231 WETH	13,154.34 ⓘ	Limit	Close

V2: less gas than Uniswap

OpenZeppelin

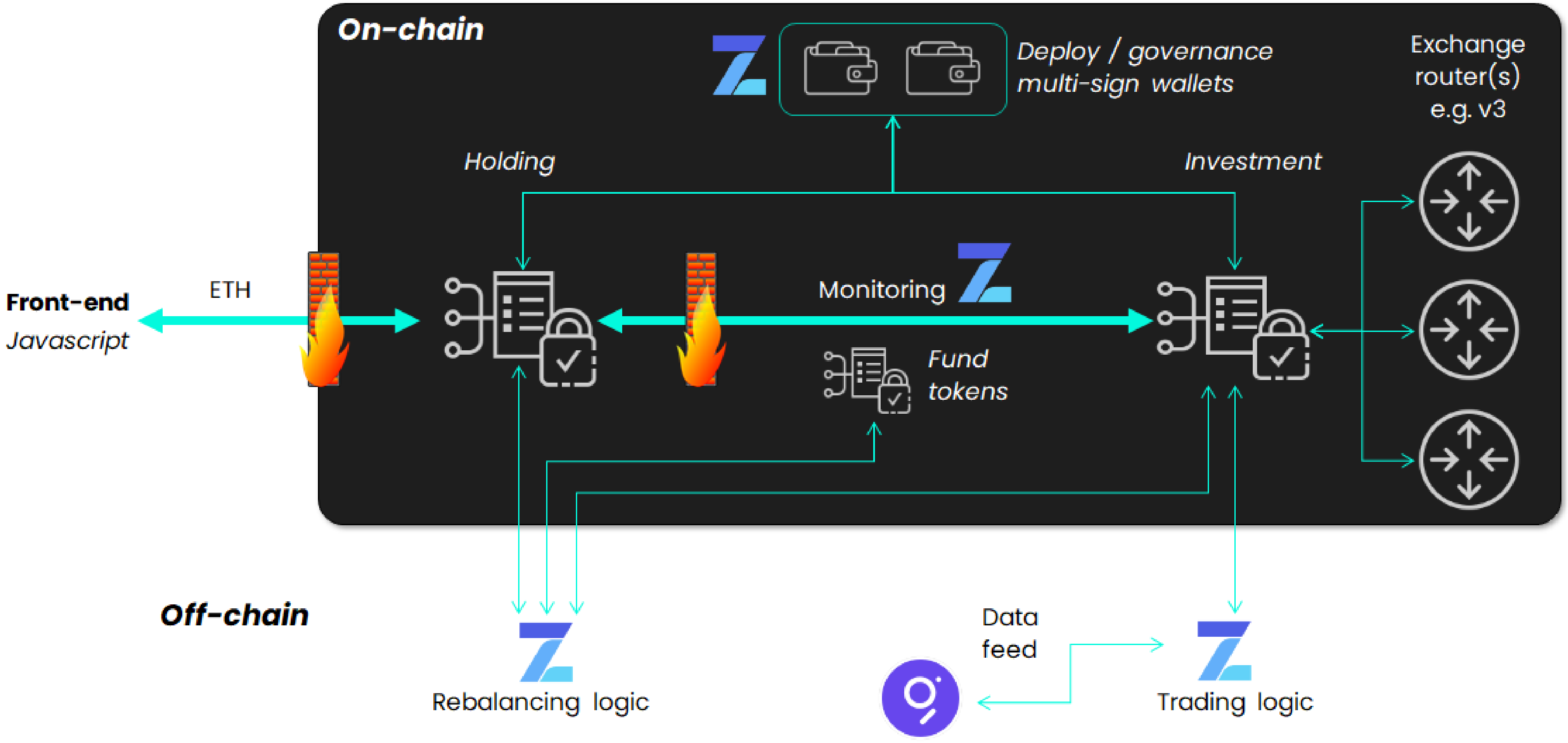
The original idea

- **Price control** for limit trades
- **Zero** price impact, slippage, liquidity fees
- **Risk** of front-running and bots eliminated

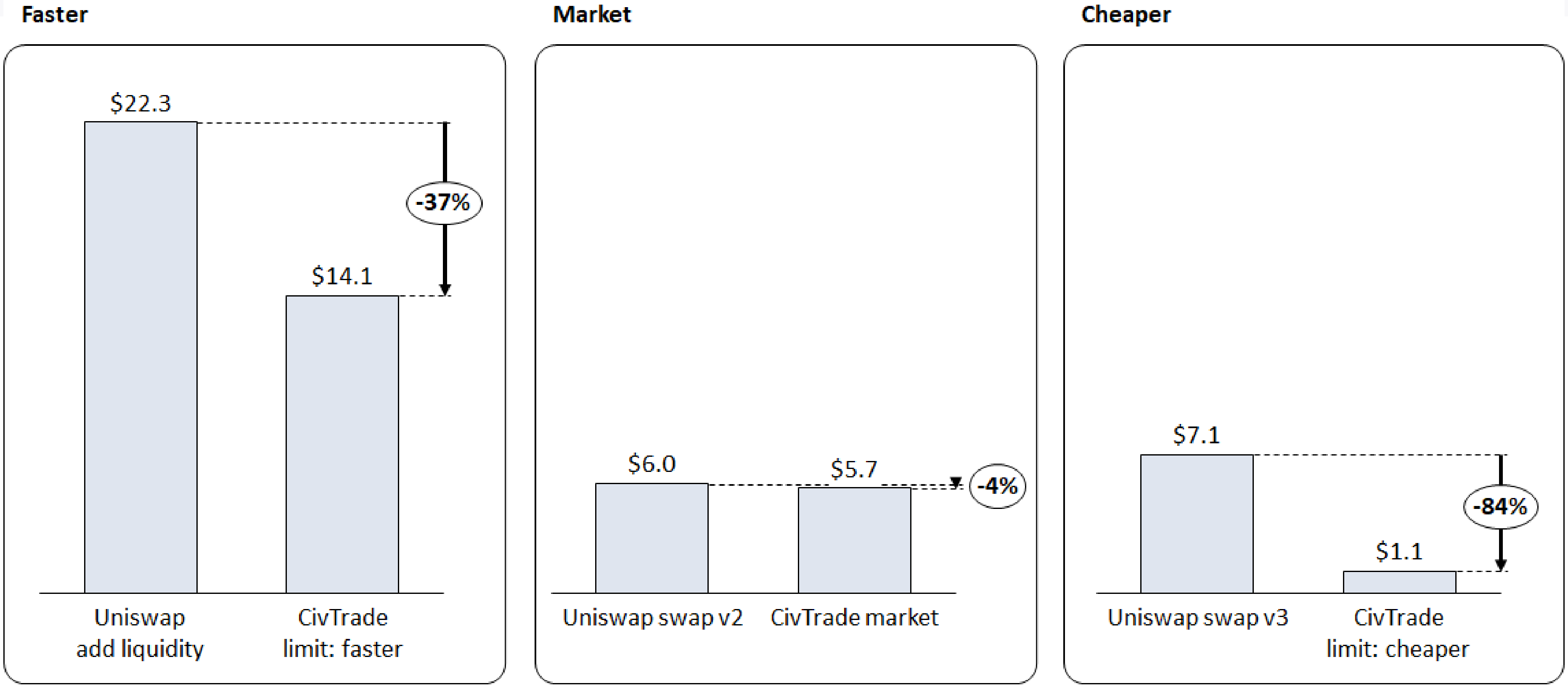
Using **Defender**

& Uniswap v3

Defender activates our smart contracts: relaying, monitoring and automation



From 4% to 84% gas savings versus Uniswap’s router



Average $ gas prices at 30 gwei per unit of gas and $3,000 per ETH

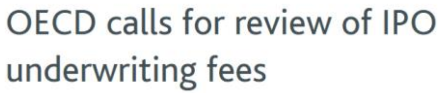
OpenZeppelin

Creating a DeFi LaunchPad Order Book

With OpenZeppelin Defender

Example use-case: DeFi launchpad. Why? The rationale

- **Off-chain:** IPO costs of 4-11% of amount raised
- **On-chain:** bots, click-first events, outright fraud



OECD calls for review of IPO underwriting fees

Beware of The Crypto ICO and IDO “Rug Pull”

Can new DeFi tools reduce risk and costs?

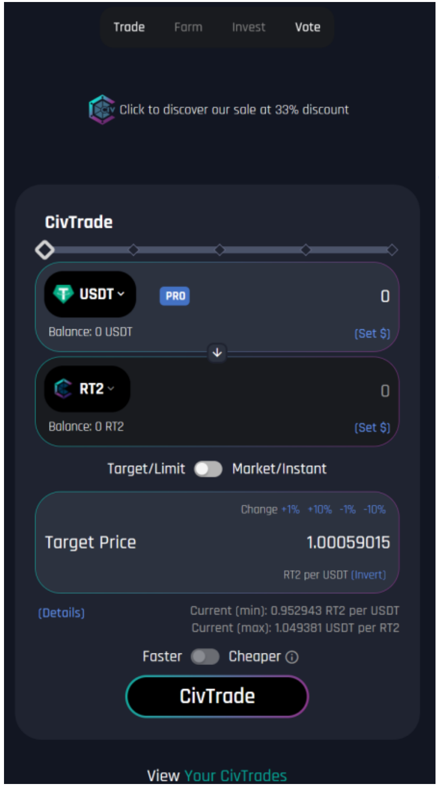
Using CivTrade and OpenZeppelin

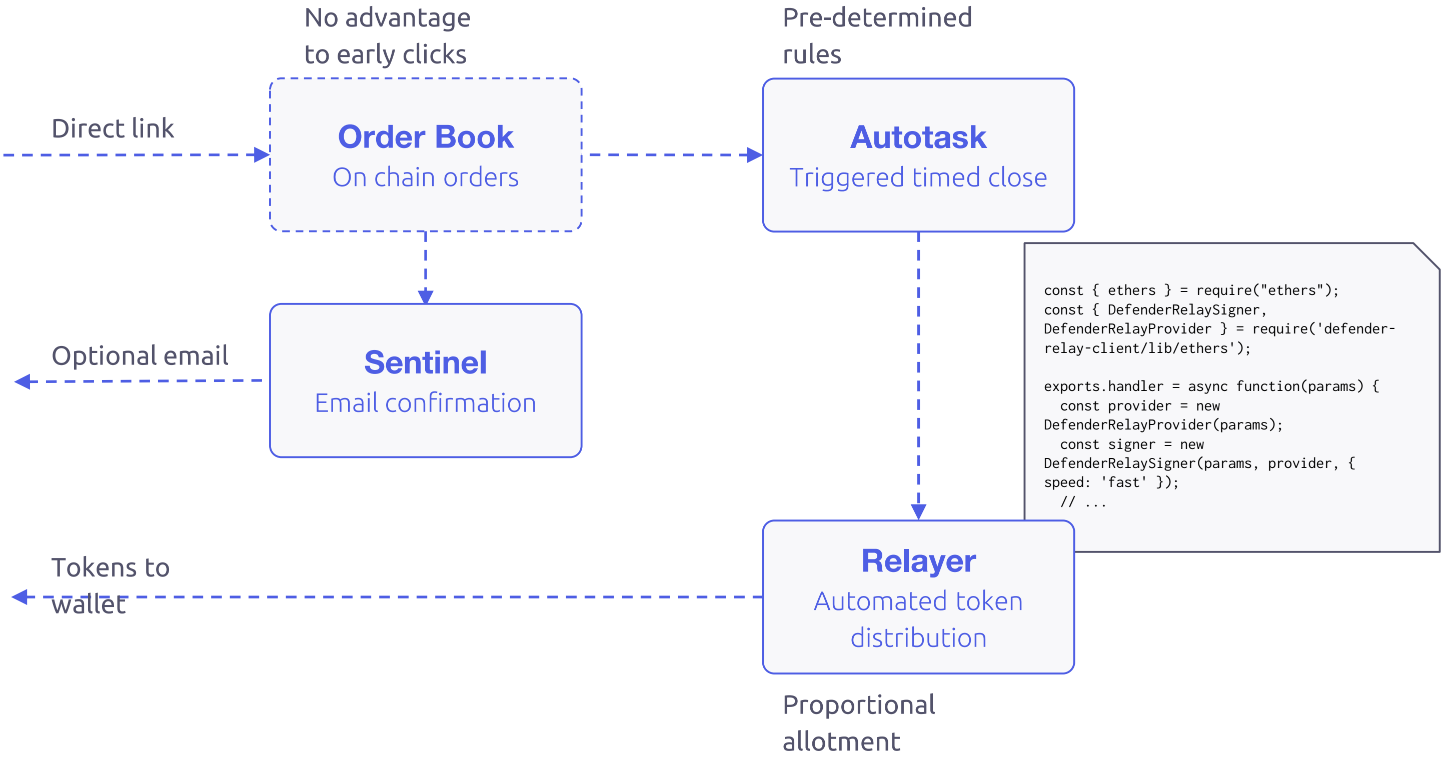
- **Order book** built with DeFi tools
- **Fair allocation** with proportional allotment
- **Low gas** total cost of ~$10 per participant: $5-18 per entry

→ 150 participants = ~$1,500 gas for $500,000 raised in 1 hour

→ Total gas burnt = 0.3% of total raised

User experience




Direct link

No advantage to early clicks

Order Book
On chain orders

Pre-determined rules

Autotask
Triggered timed close

Sentinel
Email confirmation

Optional email

Relayer
Automated token distribution

Tokens to wallet

Proportional allotment

```
const { ethers } = require("ethers");
const { DefenderRelaySigner,
DefenderRelayProvider } = require('defender-
relay-client/lib/ethers');

exports.handler = async function(params) {
  const provider = new
DefenderRelayProvider(params);
  const signer = new
DefenderRelaySigner(params, provider, {
speed: 'fast' });
  // ...
```

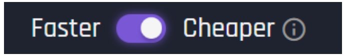
OpenZeppelin

Simple Autotask monitoring code

```
const ethers = require('ethers');
const { DefenderRelaySigner, DefenderRelayProvider } = require('defender-relay-client/lib/ethers');
const { Relayer } = require('defender-relay-client');
const { axios } = require('axios');
const { getCivPosMgrAddress } = require('./imports/contractAddresses');
const { civPosMgrAbi } = require('./imports/civPosMgrAbi');

exports.handler = async function(credentials) {
  const provider = new DefenderRelayProvider(credentials);
  const network = await provider.getNetwork();
  const chainId = network.chainId;
  const signer = new DefenderRelaySigner(credentials, provider, { speed: 'fast' });
  const civposmgr = new ethers.Contract(getCivPosMgrAddress(chainId), civPosMgrAbi, signer);

  let response
  let linkTarget = 'https://api.civfund.org/getReadyToClose?chainId='+chainId
  try {
    response = await fetch(linkTarget, { method: 'GET', headers: { 'Content-Type': 'application/json' }, });
    response = await response.json();
  } catch (err) { console.log("Fetch error", err); }

  for (let trade of response) {
      console.log ('Check orderId: '+trade.orderId);
      console.log (await civposmgr.civTrade(trade.orderId));
      console.log ('Now closing orderId: '+trade.orderId);
      console.log (await civposmgr.closePos(trade.orderId));
      console.log ('CLOSED orderId: '+trade.orderId);
  }
  return 'Number of positions closed: ' + counter;
}
```

Bonus future extension opportunity: pay gas for users

```
// follows our custom validation code
if (!accepts) throw new Error(`Rejected request to ${request.to}`);
  console.log(`Accepted`, accepts);

// Validate request on the forwarder contract
const valid = await forwarder.verify(request.from, request.to, request.nativeValue, request.nonce, request.data, signature);
if (!valid) throw new Error(`Invalid request`);
  console.log(`Signature validated`, valid);

// Send transaction on behalf of user
return await forwarder.executeWithLogs(request.from, request.to, request.nativeValue, maxGas, request.nonce, request.data,
signature, extraData, { gasLimit: maxGas, value: request.nativeValue });
```



- **Relayers already** enable *Cheaper* trade type
- **Cool wow factor** to build user gas into the trade itself
- **Launchpad integration** remains future improvement opportunity

Benefits of the OpenZeppelin Defender Launchpad

- Transparent on-chain collection of orders
- Trustless pre-programmed event for everyone’s benefit
- Automation with low gas costs
- Proportional allocation with no advantage to clicking fast
- Tokens delivered directly to wallet at pre-determined time

Thank you!

Learn more

openzeppelin.com/**defender**
forum.openzeppelin.com
docs.openzeppelin.com

Contact

🐦 @nami_sh
nami@openzeppelin.com

🐦 @civ100
civ@civfund.org