OpenZeppelin

OpenZeppelin Contracts

Past and future roadmap

EthCC[5] - July 2022

Hadrien Croubois
hadrien@openzeppelin.com
@Amxx

OpenZeppelin’s thesis

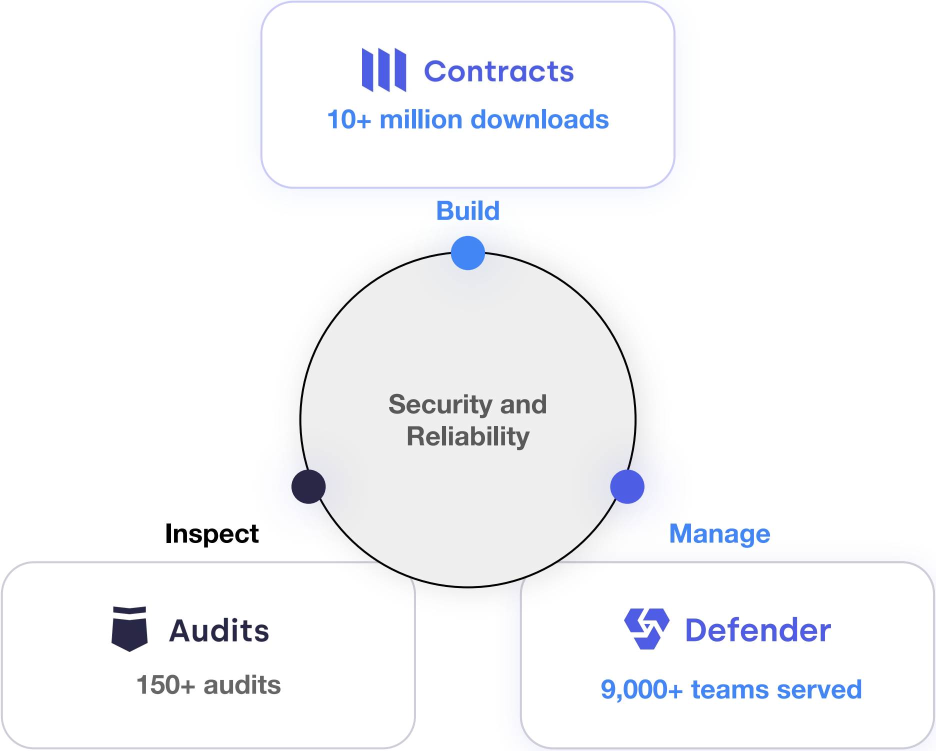
- There will be a **trillion dollar open economy** built on blockchains and **powered by smart contracts**

- This new, open economy will be **built by teams of creative people developing new applications used by billions of people**

- These teams **will need a set of tools, products and services** to make sure that what they are building is **safe and reliable**

- OpenZeppelin will be a **leading provider of these solutions,** allowing teams to **build faster with lower risk**

OpenZeppelin’s products



Contracts

10+ million downloads

Build

Security and Reliability

Inspect

Manage

Audits

150+ audits

Defender

9,000+ teams served

L1 / L2 Networks

ethereum

polygon

Polkadot.

AVALANCHE

ARBITRUM

STARKWARE

OPTIMISM

celo

fantom

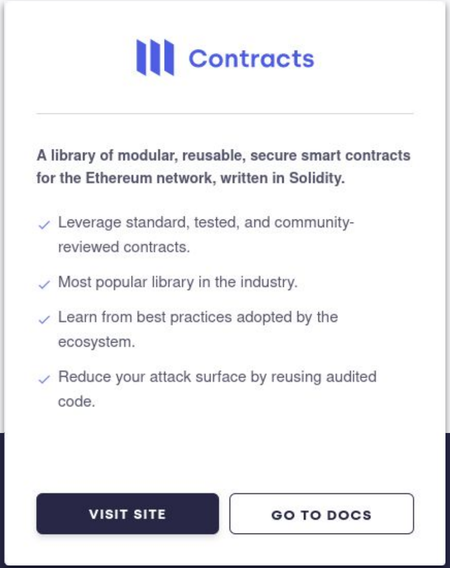
BINANCE SMART CHAIN

Hedera

Contracts

@openzeppelin/contracts@4.7.0

@openzeppelin/contracts-upgradable@4.7.0

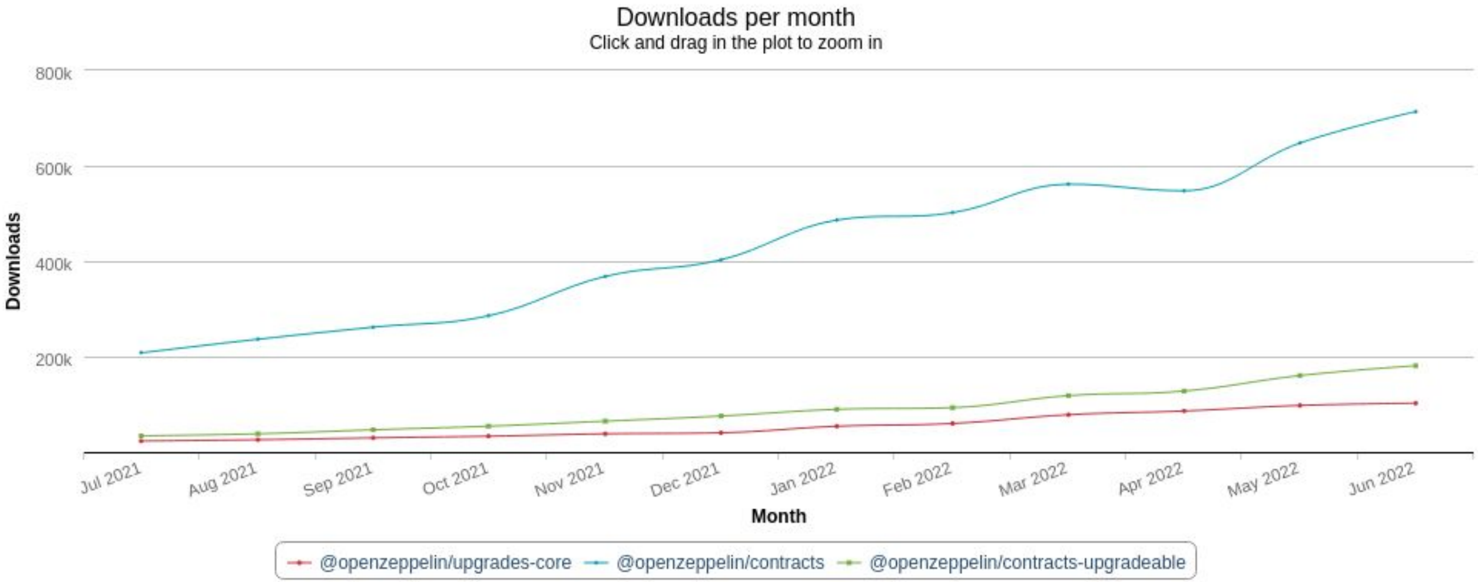


Contracts

A library of modular, reusable, secure smart contracts for the Ethereum network, written in Solidity.

- ✓ Leverage standard, tested, and community-reviewed contracts.
- ✓ Most popular library in the industry.
- ✓ Learn from best practices adopted by the ecosystem.
- ✓ Reduce your attack surface by reusing audited code.

Some statistics



More users, more developers, more libraries

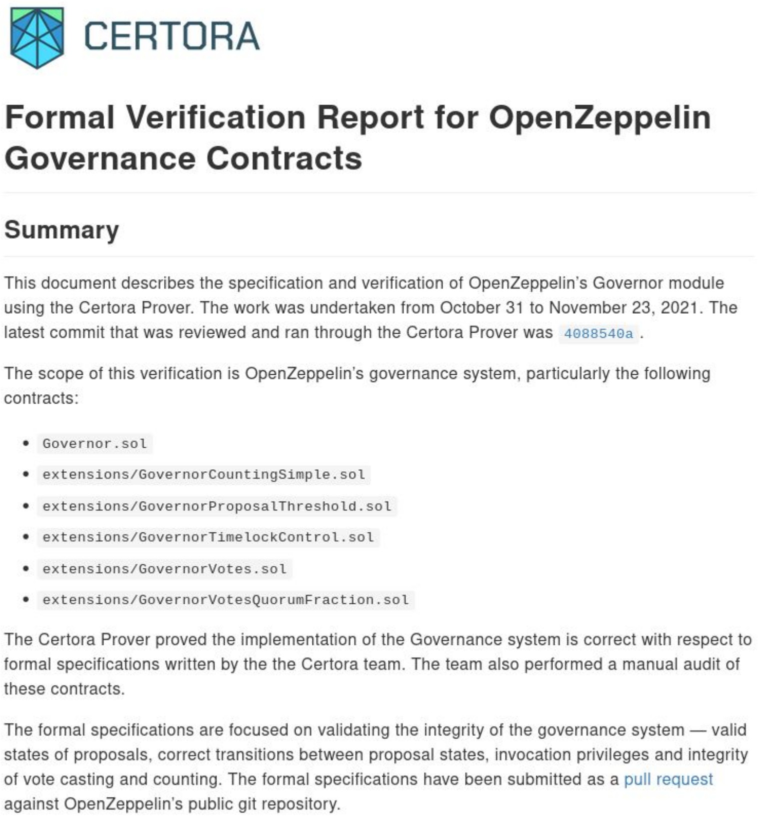
Some other relevant projects	
DappHub	ds-auth , ds-token, ds-pause, …
@transmissions11	@transmissions11/solmate
Paul Razvan Berg	@prb/math
Azuki	ERC721A

Most of these project make different design choice, and may or may not be relevant depending on your use-case.

OpenZeppelin Contracts focus on security, extensibility, customizability and readability/auditability …

… without compromising performance

More about security



CERTORA

Formal Verification Report for OpenZeppelin Governance Contracts

Summary

This document describes the specification and verification of OpenZeppelin's Governor module using the Certora Prover. The work was undertaken from October 31 to November 23, 2021. The latest commit that was reviewed and ran through the Certora Prover was `4088540a` .

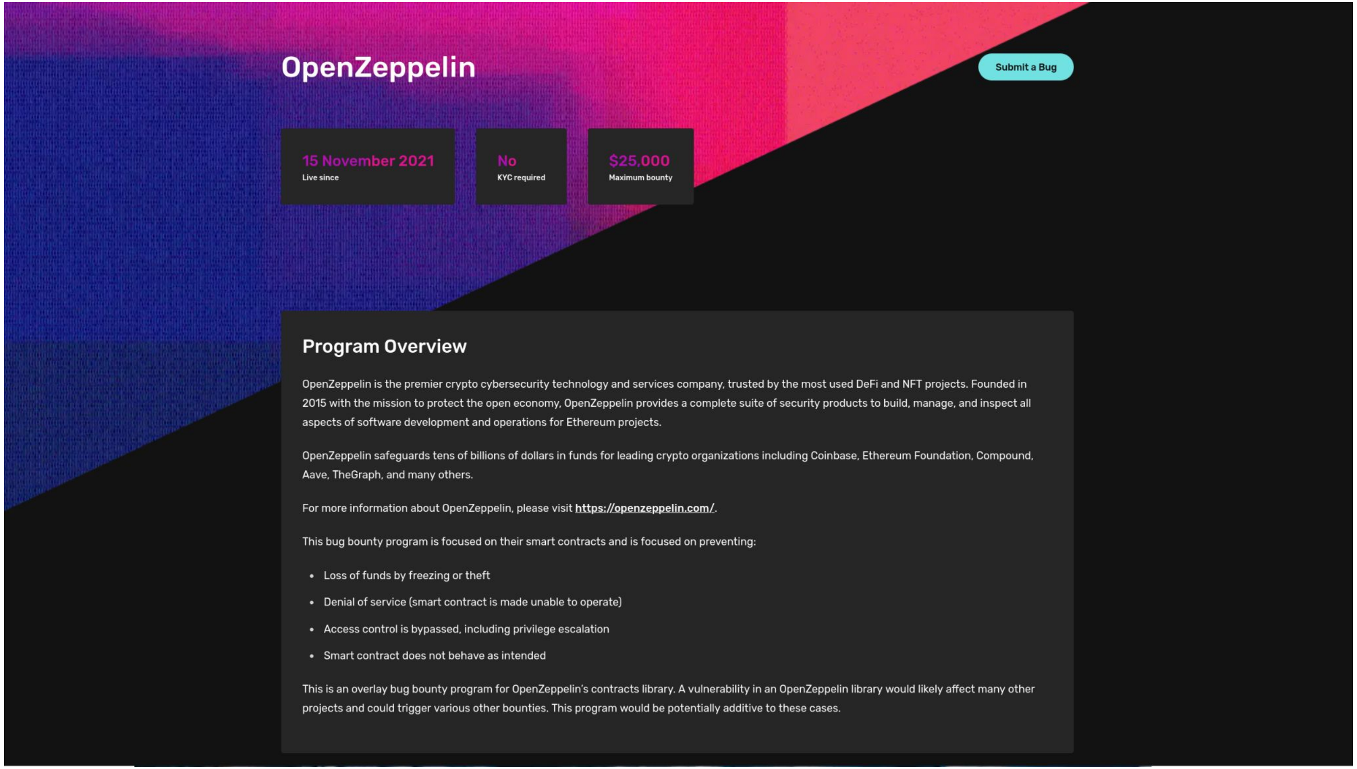
The scope of this verification is OpenZeppelin's governance system, particularly the following contracts:

- `Governor.sol`
- `extensions/GovernorCountingSimple.sol`
- `extensions/GovernorProposalThreshold.sol`
- `extensions/GovernorTimelockControl.sol`
- `extensions/GovernorVotes.sol`
- `extensions/GovernorVotesQuorumFraction.sol`

The Certora Prover proved the implementation of the Governance system is correct with respect to formal specifications written by the the Certora team. The team also performed a manual audit of these contracts.

The formal specifications are focused on validating the integrity of the governance system — valid states of proposals, correct transitions between proposal states, invocation privileges and integrity of vote casting and counting. The formal specifications have been submitted as a pull request against OpenZeppelin's public git repository.

Immunefi bug bounty



15 November 2021
Live since

No
KYC required

$25,000
Maximum bounty

Program Overview

OpenZeppelin is the premier crypto cybersecurity technology and services company, trusted by the most used DeFi and NFT projects. Founded in 2015 with the mission to protect the open economy, OpenZeppelin provides a complete suite of security products to build, manage, and inspect all aspects of software development and operations for Ethereum projects.

OpenZeppelin safeguards tens of billions of dollars in funds for leading crypto organizations including Coinbase, Ethereum Foundation, Compound, Aave, TheGraph, and many others.

For more information about OpenZeppelin, please visit **https://openzeppelin.com/**.

This bug bounty program is focused on their smart contracts and is focused on preventing:

- Loss of funds by freezing or theft
- Denial of service (smart contract is made unable to operate)
- Access control is bypassed, including privilege escalation
- Smart contract does not behave as intended

This is an overlay bug bounty program for OpenZeppelin's contracts library. A vulnerability in an OpenZeppelin library would likely affect many other projects and could trigger various other bounties. This program would be potentially additive to these cases.

Community calls

Give visibility to new features & improvements

Involve you in the process:

- Provide feedback
- Request features
- Engage discussion
- Review the code

Some key features

released last year

The OpenZeppelin Governor system

introduced in @openzeppelin/contracts@4.3.0

Token

and

Governor

(modular, based on Compound’s Governor)

and

Timelock

(optional)

and

Defender, Tally, TheGraph ...

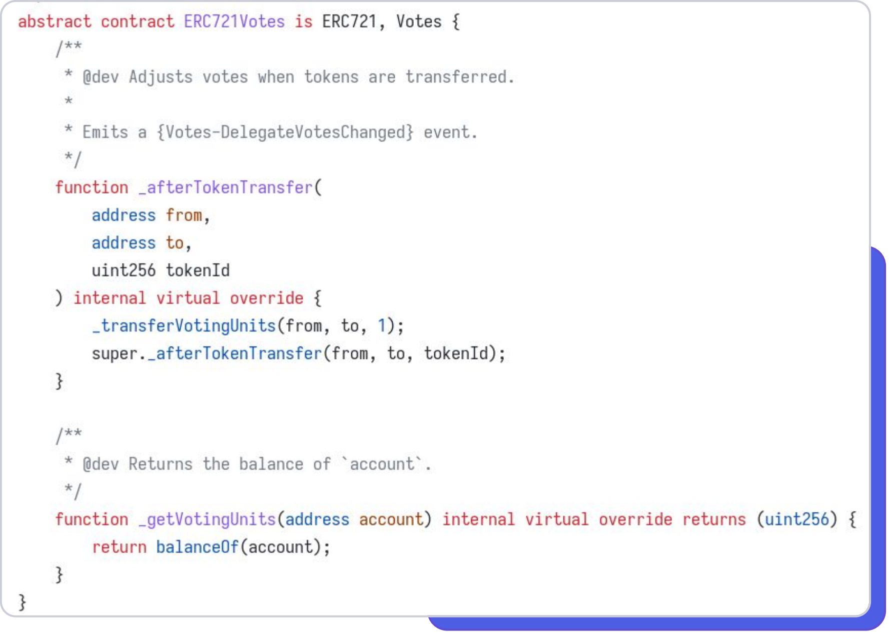
Used by @ensdomains. Currently +30 active instances on mainnet.

Votes & ERC721Votes

introduced in @openzeppelin/contracts@4.5.0

Enables governance protocols with NFT-based voting.

(1 NFT = 1 vote)



```
abstract contract ERC721Votes is ERC721, Votes {
    /**
     * @dev Adjusts votes when tokens are transferred.
     *
     * Emits a {Votes-DelegateVotesChanged} event.
     */
    function _afterTokenTransfer(
        address from,
        address to,
        uint256 tokenId
    ) internal virtual override {
        _transferVotingUnits(from, to, 1);
        super._afterTokenTransfer(from, to, tokenId);
    }

    /**
     * @dev Returns the balance of `account`.
     */
    function _getVotingUnits(address account) internal virtual override returns (uint256) {
        return balanceOf(account);
    }
}
```

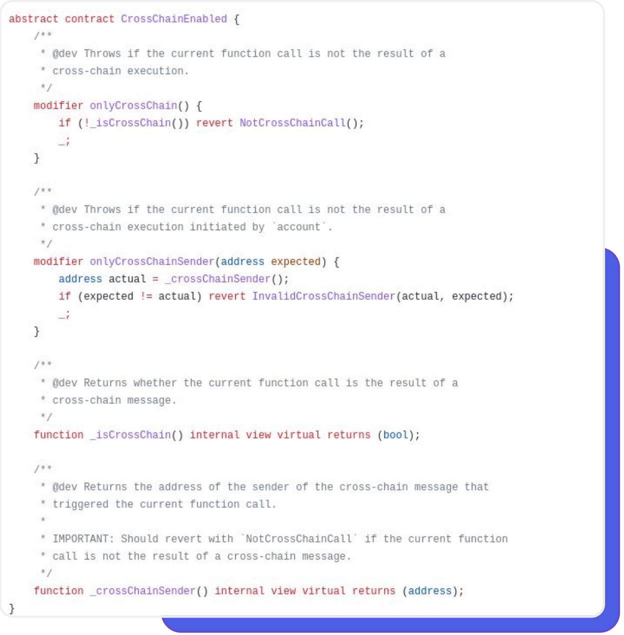
CrossChainEnabled

introduced in @openzeppelin/contracts@4.6.0

An abstraction to build cross-chain aware contracts. Includes internal functions and modifiers to restrict cross chain operations.

Implementations available for:

- AMB (gnosis chain)
- Arbitrum
- Optimism
- Polygon (Root → Child)



```
abstract contract CrossChainEnabled {
    /**
     * @dev Throws if the current function call is not the result of a
     * cross-chain execution.
     */
    modifier onlyCrossChain() {
        if (!_isCrossChain()) revert NotCrossChainCall();
        _;
    }

    /**
     * @dev Throws if the current function call is not the result of a
     * cross-chain execution initiated by `account`.
     */
    modifier onlyCrossChainSender(address expected) {
        address actual = _crossChainSender();
        if (expected != actual) revert InvalidCrossChainSender(actual, expected);
        _;
    }

    /**
     * @dev Returns whether the current function call is the result of a
     * cross-chain message.
     */
    function _isCrossChain() internal view virtual returns (bool);

    /**
     * @dev Returns the address of the sender of the cross-chain message that
     * triggered the current function call.
     *
     * IMPORTANT: Should revert with `NotCrossChainCall` if the current function
     * call is not the result of a cross-chain message.
     */
    function _crossChainSender() internal view virtual returns (address);
}
```

One year of features: 4.3.0 to 4.7.0

Governance

- Governor (with many modules)
- ERC721Votes

Cross chain operations

- CrossChainEnabled

DeFi

- ERC3156 (ERC20FlashMint)
- ERC4626
- VestingWallet
- PaymentSplitter support for ERC20

NFTs

- ERC2981 royalty standard

Upgradeability

- Improved security for UUPS proxies
- Re-initializers patterns

Utilities

- DoubleEndedQueue
- More EnumerableMap types
- Math (muldiv & sqrt)
- SignedMath
- Base64

Upgrades plugin

- Beacon proxy support
- Etherscan code verification

And many more…

Our objectives for the next year

DeFi

- Staking

Governance

- Timestamp based governance

Cross-chain

- Send message
- Participating to bridge design discussions

General design

- Generalize the use of custom errors

Upgradeability

- Transition to diamond storage

Upgrades plugin

- Support storage gap
- Validation of parent initializers

Developer tools

- AccessControlExplorer

Standardization process

- Voting interface ERC

Contracts for Cairo

```
pip install openzeppelin-cairo-contracts==0.2.1
```

Contract for Cairo

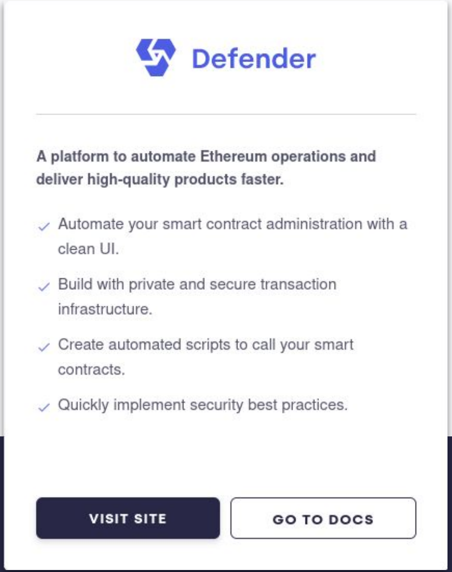
Currently available

- Account contracts (Stark and Ethereum keys)
- Tokens
  - ERC20
  - ERC721
  - Presets! (pausable, upgradable, etc)
- Access Control and Ownable
- Upgrades and Proxy
- Security
  - Pausable
  - ReentrancyGuard
  - SafeMath

On the roadmap

- More tokens
  - ERC1155
- Timelock
- Data Structures
  - EnumerableSet
  - EnumerableMap
- More presets!

https://zpl.in/wizard/cairo



Defender

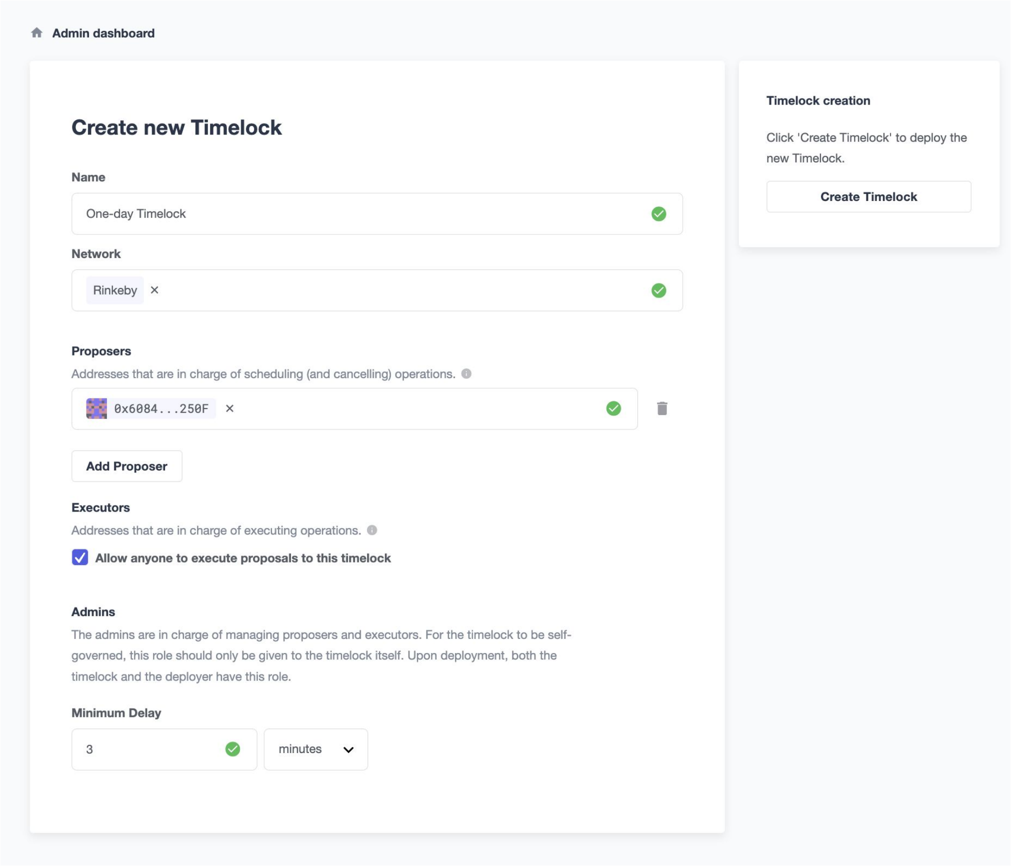
A platform to automate Ethereum operations and deliver high-quality products faster.

- ✓ Automate your smart contract administration with a clean UI.
- ✓ Build with private and secure transaction infrastructure.
- ✓ Create automated scripts to call your smart contracts.
- ✓ Quickly implement security best practices.

Contracts support in Defender

Features currently available

Creating a Timelock



Admin dashboard

Create new Timelock

Name

One-day Timelock ✓

Network

Rinkeby × ✓

Proposers

Addresses that are in charge of scheduling (and cancelling) operations.

0x6084...250F × ✓

Add Proposer

Executors

Addresses that are in charge of executing operations.

☑ Allow anyone to execute proposals to this timelock

Admins

The admins are in charge of managing proposers and executors. For the timelock to be self-governed, this role should only be given to the timelock itself. Upon deployment, both the timelock and the deployer have this role.

Minimum Delay

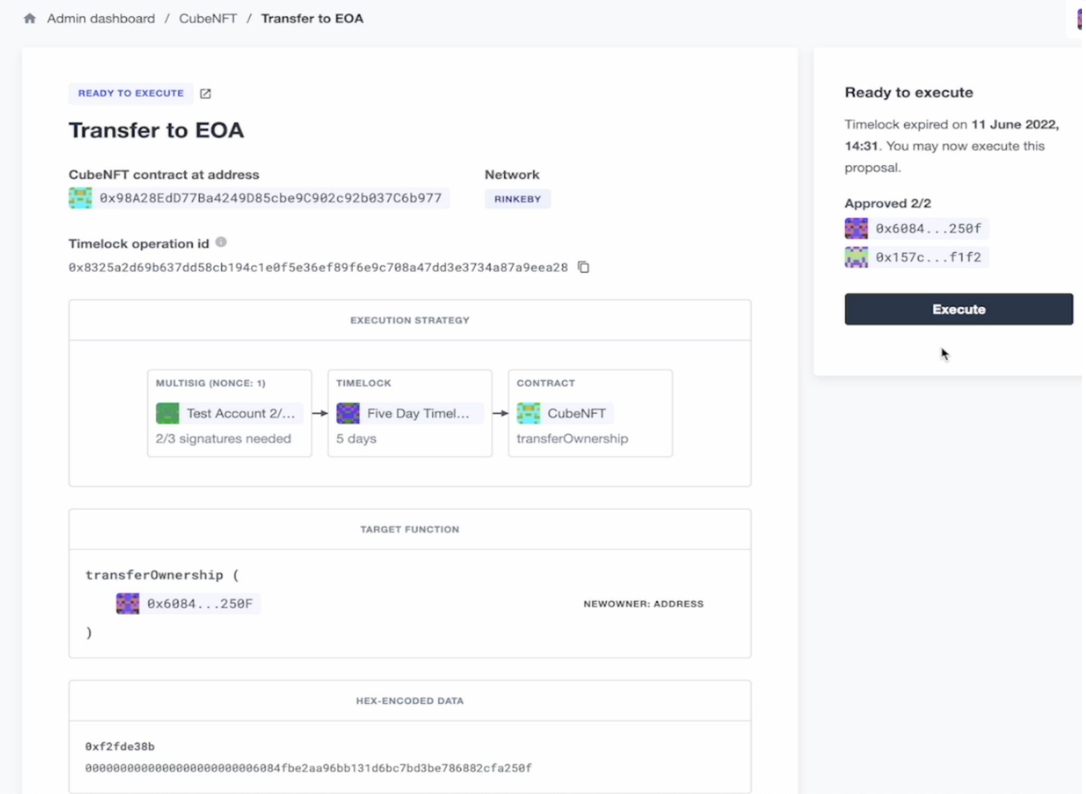
3 ✓ minutes

Timelock creation

Click 'Create Timelock' to deploy the new Timelock.

Create Timelock

Full support for calling any public function via Multisig, Governor, or Timelock



Admin dashboard / CubeNFT / Transfer to EOA

READY TO EXECUTE

Transfer to EOA

CubeNFT contract at address
0x98A28EdD77Ba4249D85cbe9C902c92b037C6b977

Network
RINKEBY

Timelock operation id
0x8325a2d69b637dd58cb194c1e0f5e36ef89f6e9c708a47dd3e3734a87a9eea28

EXECUTION STRATEGY

MULTISIG (NONCE: 1)
Test Account 2/...
2/3 signatures needed
→
TIMELOCK
Five Day Timel...
5 days
→
CONTRACT
CubeNFT
transferOwnership

TARGET FUNCTION

```
transferOwnership (
    0x6084...250F                                NEWOWNER: ADDRESS
)
```

HEX-ENCODED DATA

```
0xf2fde38b
0000000000000000000000006084fbe2aa96bb131d6bc7bd3be786882cfa250f
```

Ready to execute

Timelock expired on **11 June 2022, 14:31**. You may now execute this proposal.

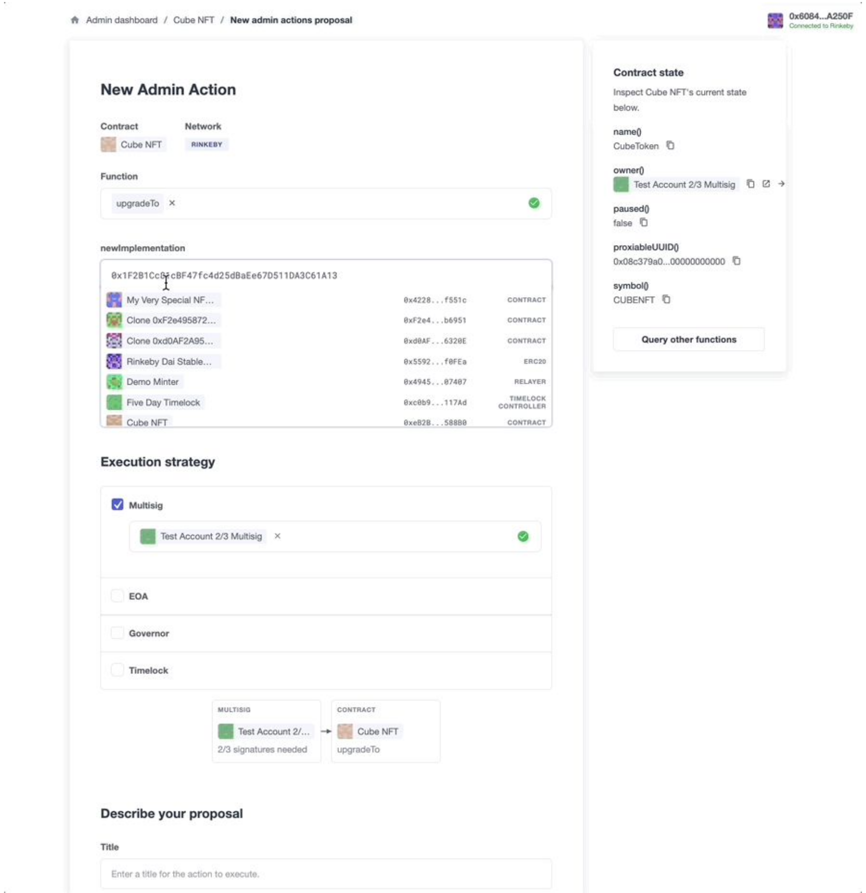
Approved 2/2
0x6084...250f
0x157c...f1f2

Execute

OpenZeppelin

https://openzeppelin.com

Contract upgrades



Admin dashboard / Cube NFT / **New admin actions proposal**

0x6084...A250F
Connected to Rinkeby

New Admin Action

Contract: Cube NFT

Network: RINKEBY

Function

upgradeTo ×

newImplementation

0x1F2B1CcB[illegible]cBF47fc4d25dBaEe67D511DA3C61A13

My Very Special NF...	0x4228...f551c	CONTRACT
Clone 0xF2e495872...	0xF2e4...b6951	CONTRACT
Clone 0xd0AF2A95...	0xd0AF...6320E	CONTRACT
Rinkeby Dai Stable...	0x5592...f0FEa	ERC20
Demo Minter	0x4945...07407	RELAYER
Five Day Timelock	0xc0b9...117Ad	TIMELOCK CONTROLLER
Cube NFT	0xeB2B...588B0	CONTRACT

Execution strategy

☑ Multisig

Test Account 2/3 Multisig ×

□ EOA

□ Governor

□ Timelock

MULTISIG: Test Account 2/... → CONTRACT: Cube NFT
2/3 signatures needed — upgradeTo

Describe your proposal

Title

Enter a title for the action to execute.

Contract state

Inspect Cube NFT's current state below.

name()
CubeToken

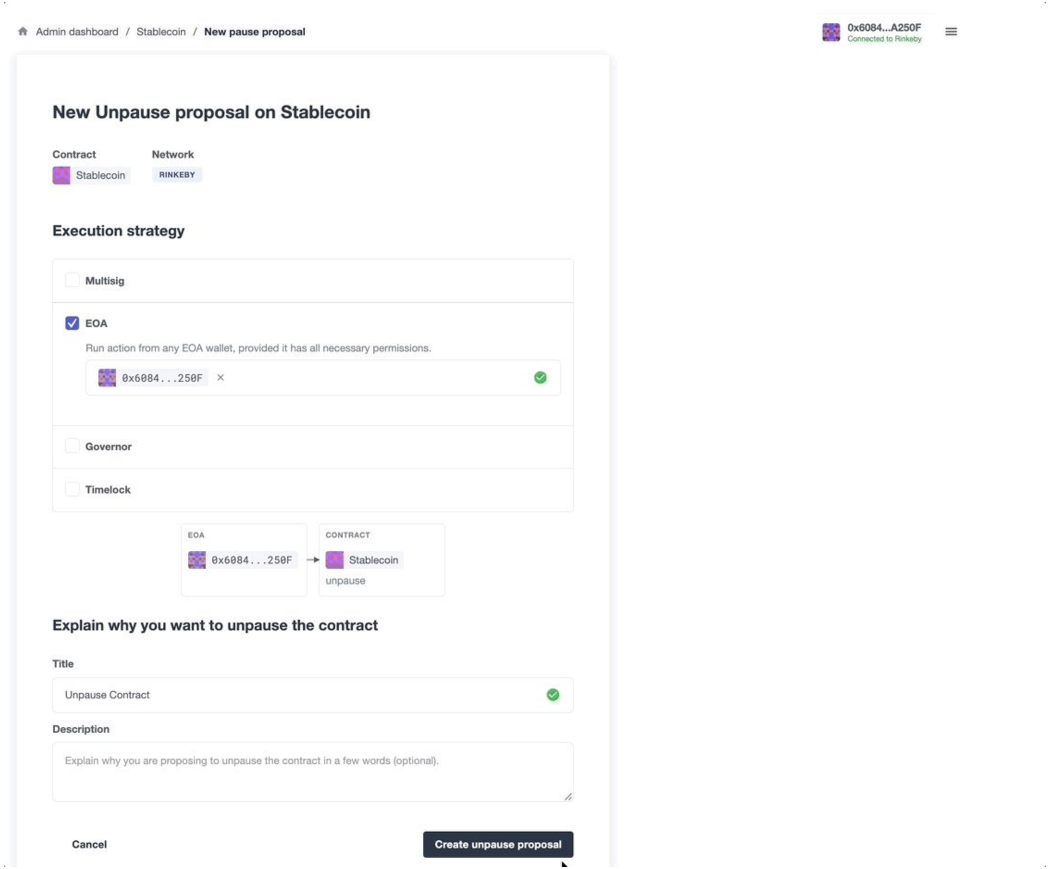
owner()
Test Account 2/3 Multisig

paused()
false

proxiableUUID()
0x08c379a0...00000000000

symbol()
CUBENFT

Pause / Unpause



Admin dashboard / Stablecoin / New pause proposal

0x6084...A250F
Connected to Rinkeby

New Unpause proposal on Stablecoin

Contract	Network
Stablecoin	RINKEBY

Execution strategy

□ Multisig

☑ EOA

Run action from any EOA wallet, provided it has all necessary permissions.

0x6084...250F ×

□ Governor

□ Timelock

EOA		CONTRACT
0x6084...250F	→	Stablecoin unpause

Explain why you want to unpause the contract

Title

Unpause Contract

Description

Explain why you are proposing to unpause the contract in a few words (optional).

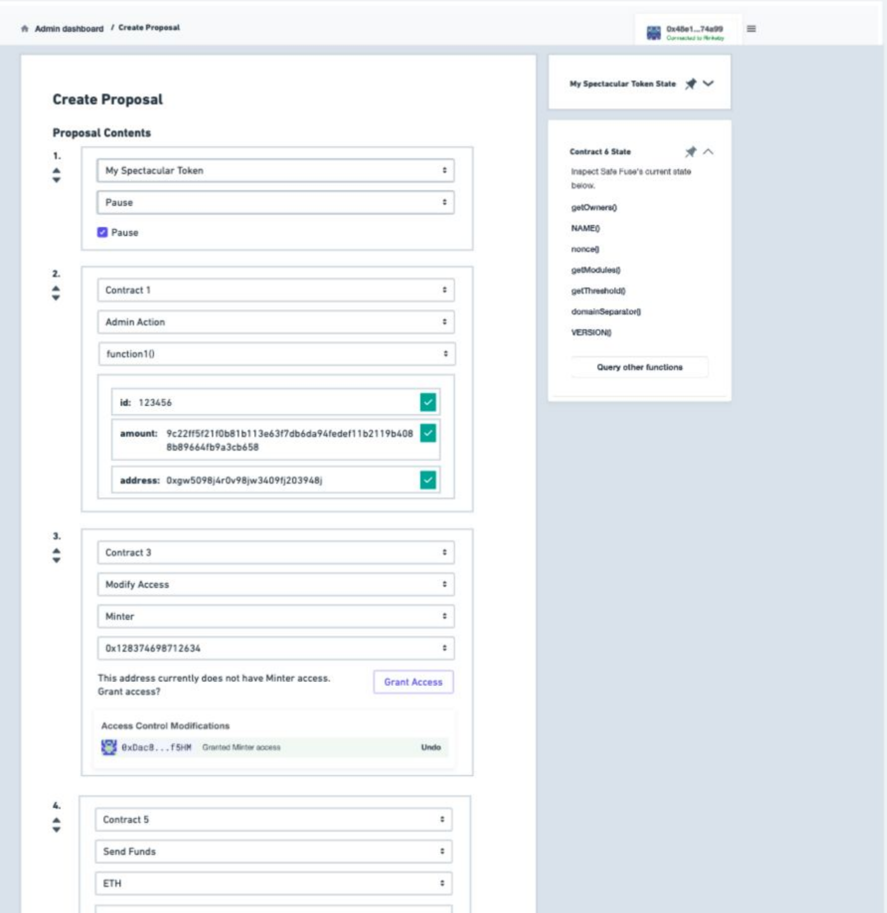
OpenZeppelin

https://openzeppelin.com

Coming Soon

Upcoming new features for Q3

Transaction Batching



Create Proposal

Proposal Contents

1.
- My Spectacular Token
- Pause
- ☑ Pause

2.
- Contract 1
- Admin Action
- function1()
- **id:** 123456 ✓
- **amount:** 9c22ff5f21f0b81b113e63f7db6da94fedef11b2119b408 8b89664fb9a3cb658 ✓
- **address:** 0xgw5098j4r0v98jw3409fj203948j ✓

3.
- Contract 3
- Modify Access
- Minter
- 0x128374698712634

This address currently does not have Minter access. Grant access?

Access Control Modifications

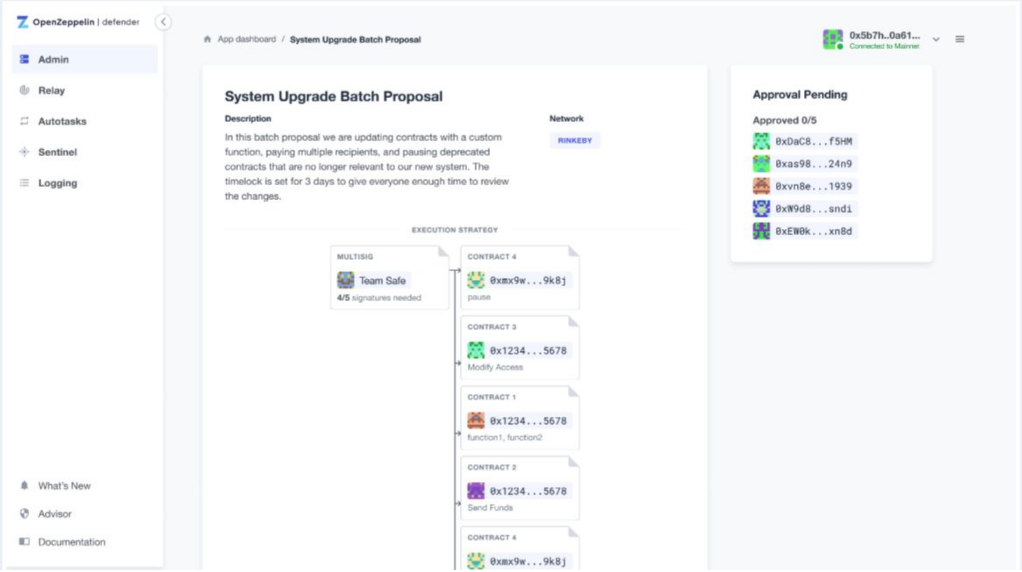
0xDac8...f5HM Granted Minter access

4.
- Contract 5
- Send Funds
- ETH

Contract 6 State

Inspect Safe Fuse's current state below.

getOwners()
NAME()
nonce()
getModules()
getThreshold()
domainSeparator()
VERSION()



System Upgrade Batch Proposal

Description

In this batch proposal we are updating contracts with a custom function, paying multiple recipients, and pausing deprecated contracts that are no longer relevant to our new system. The timelock is set for 3 days to give everyone enough time to review the changes.

Network

RINKEBY

4/5 signatures needed

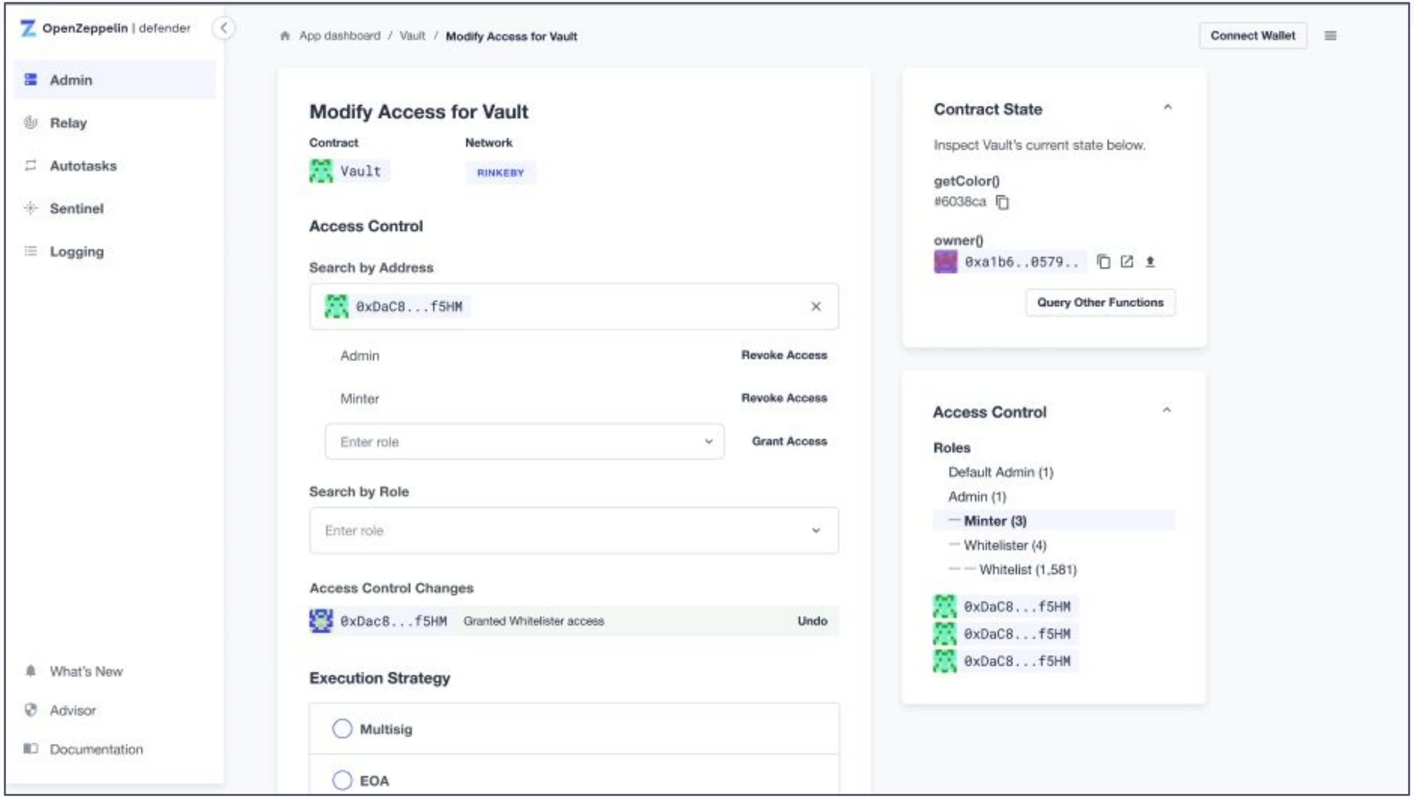
Approval Pending

Approved 0/5

- 0xDaC8...f5HM
- 0xas98...24n9
- 0xvn8e...1939
- 0xW9d8...sndi
- 0xEW0k...xn8d

https://openzeppelin.com

First-class support for AccessControl in Admin



Modify Access for Vault

Contract	Network
Vault	RINKEBY

Access Control

Search by Address

0xDaC8...f5HM ✕

Admin	Revoke Access
Minter	Revoke Access
Enter role ⌄	Grant Access

Search by Role

Enter role ⌄

Access Control Changes

0xDac8...f5HM Granted Whitelister access Undo

Execution Strategy

○ Multisig

○ EOA

Contract State ^

Inspect Vault's current state below.

getColor()
#6038ca

owner()
0xa1b6..0579..

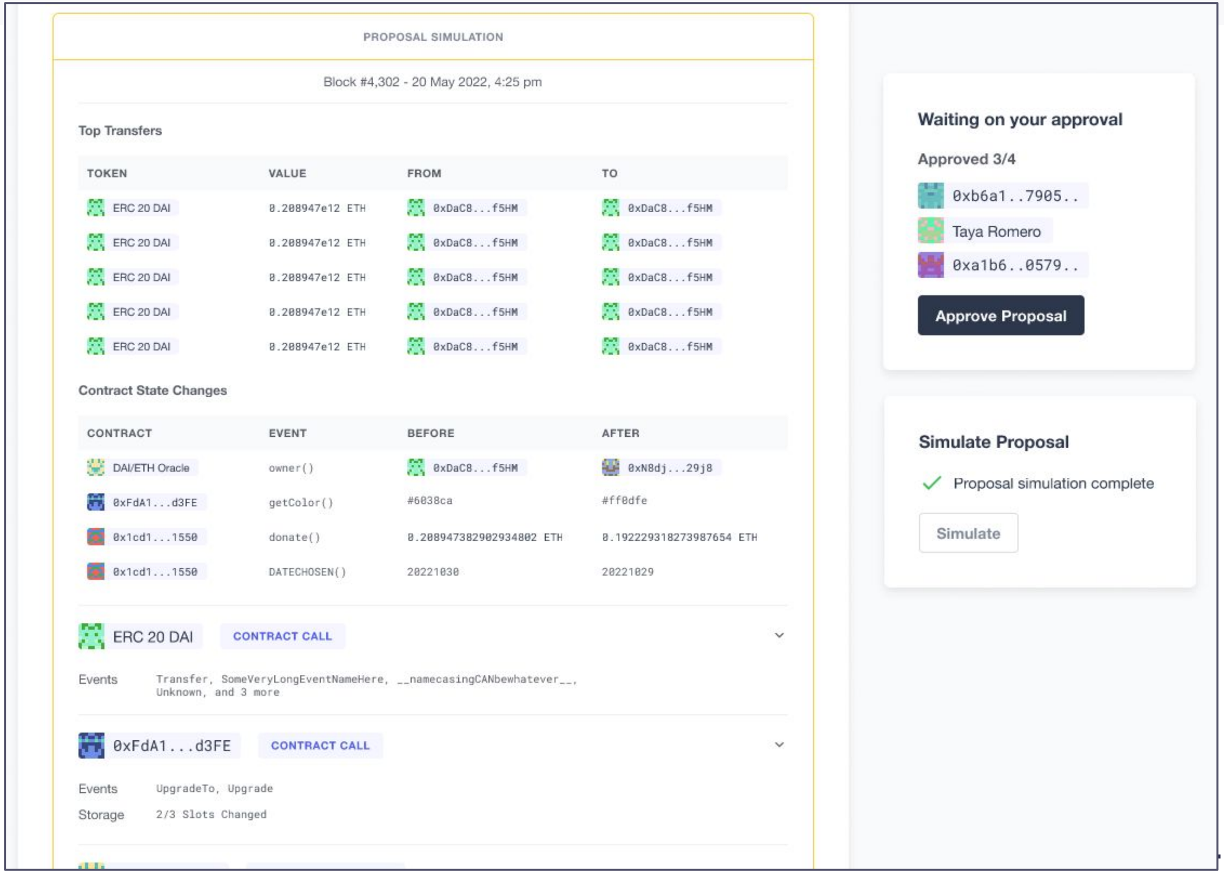
Query Other Functions

Access Control ^

Roles
- Default Admin (1)
- Admin (1)
  - Minter (3)
  - Whitelister (4)
    - Whitelist (1,581)

0xDaC8...f5HM
0xDaC8...f5HM
0xDaC8...f5HM

Transaction simulation in Admin



PROPOSAL SIMULATION

Block #4,302 - 20 May 2022, 4:25 pm

Top Transfers

TOKEN	VALUE	FROM	TO
ERC 20 DAI	0.208947e12 ETH	0xDaC8...f5HM	0xDaC8...f5HM
ERC 20 DAI	0.208947e12 ETH	0xDaC8...f5HM	0xDaC8...f5HM
ERC 20 DAI	0.208947e12 ETH	0xDaC8...f5HM	0xDaC8...f5HM
ERC 20 DAI	0.208947e12 ETH	0xDaC8...f5HM	0xDaC8...f5HM
ERC 20 DAI	0.208947e12 ETH	0xDaC8...f5HM	0xDaC8...f5HM

Contract State Changes

CONTRACT	EVENT	BEFORE	AFTER
DAI/ETH Oracle	owner()	0xDaC8...f5HM	0xN8dj...29j8
0xFdA1...d3FE	getColor()	#6038ca	#ff0dfe
0x1cd1...1550	donate()	0.208947382902934802 ETH	0.192229318273987654 ETH
0x1cd1...1550	DATECHOSEN()	20221030	20221029

ERC 20 DAI CONTRACT CALL

Events Transfer, SomeVeryLongEventNameHere, __namecasingCANbewhatever__, Unknown, and 3 more

0xFdA1...d3FE CONTRACT CALL

Events UpgradeTo, Upgrade

Storage 2/3 Slots Changed

Waiting on your approval

Approved 3/4

0xb6a1..7905..

Taya Romero

0xa1b6..0579..

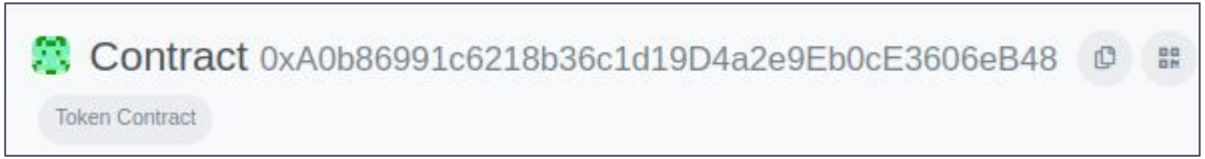
Approve Proposal

Simulate Proposal

✓ Proposal simulation complete

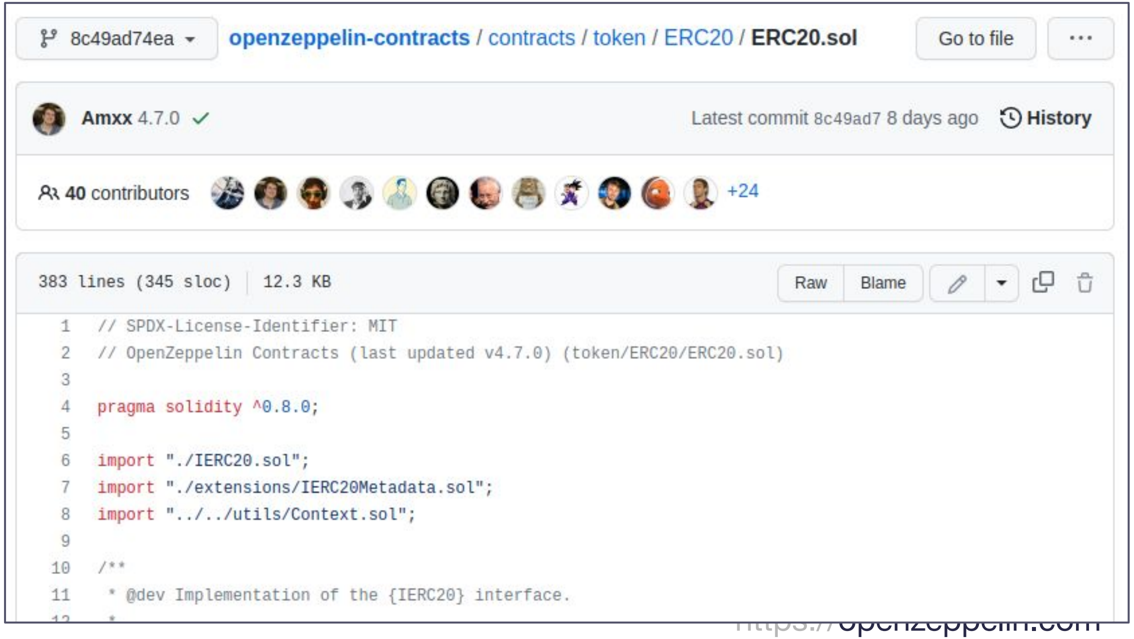
Simulate

Verify deployed code back to the source code repository



Contract 0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48

Token Contract



8c49ad74ea ▾ openzeppelin-contracts / contracts / token / ERC20 / ERC20.sol

Go to file

Amxx 4.7.0 ✓ Latest commit 8c49ad7 8 days ago History

40 contributors +24

383 lines (345 sloc) | 12.3 KB

Raw Blame

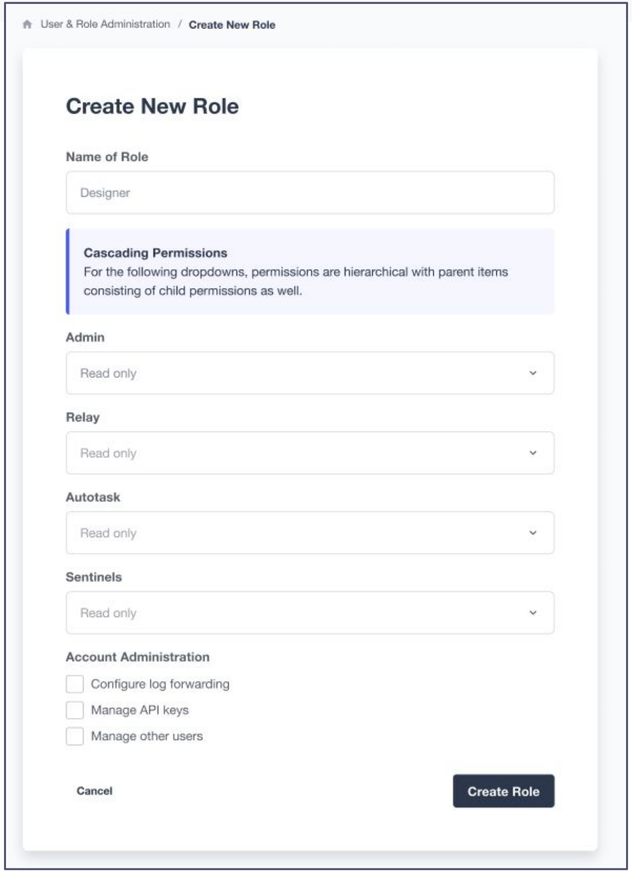
```
// SPDX-License-Identifier: MIT
// OpenZeppelin Contracts (last updated v4.7.0) (token/ERC20/ERC20.sol)

pragma solidity ^0.8.0;

import "./IERC20.sol";
import "./extensions/IERC20Metadata.sol";
import "../../utils/Context.sol";

/**
 * @dev Implementation of the {IERC20} interface.
 *
```

User roles and permissions



User & Role Administration / **Create New Role**

Create New Role

Name of Role

Designer

Cascading Permissions
For the following dropdowns, permissions are hierarchical with parent items consisting of child permissions as well.

Admin

Read only

Relay

Read only

Autotask

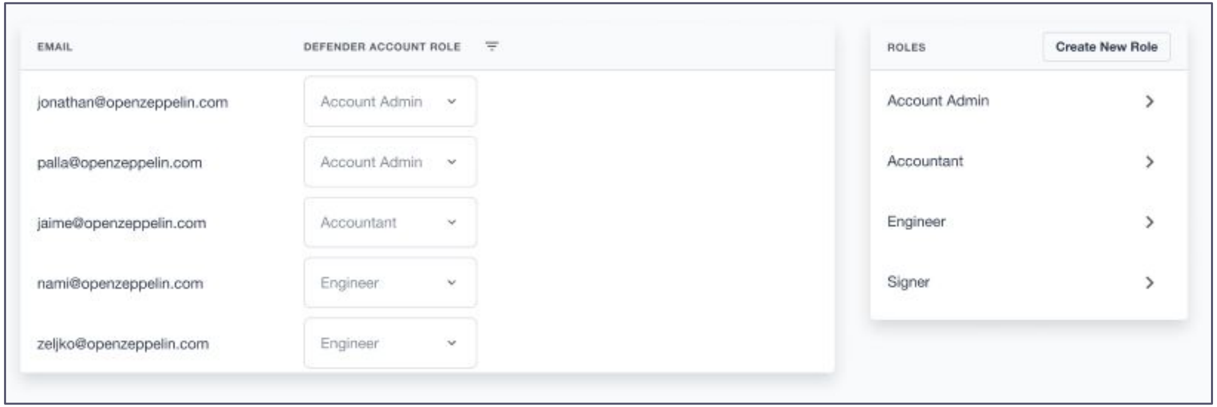
Read only

Sentinels

Read only

Account Administration

□ Configure log forwarding
□ Manage API keys
□ Manage other users



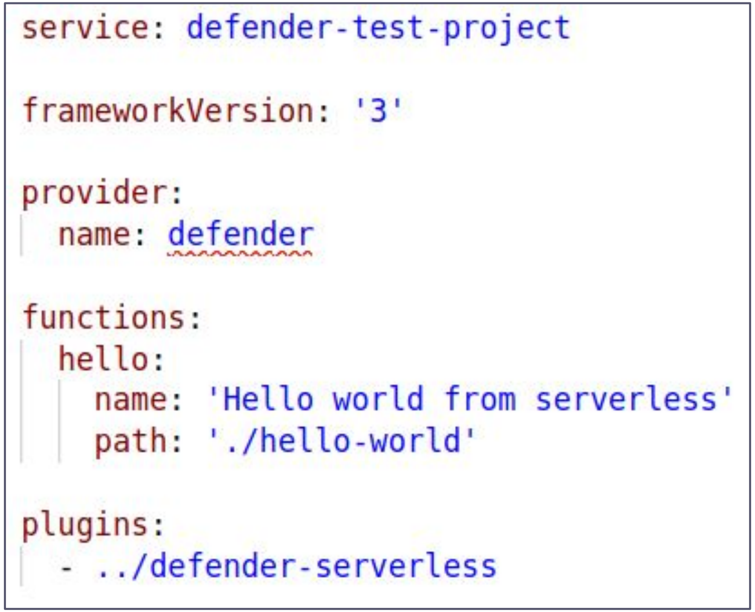
EMAIL	DEFENDER ACCOUNT ROLE
jonathan@openzeppelin.com	Account Admin
palla@openzeppelin.com	Account Admin
jaime@openzeppelin.com	Accountant
nami@openzeppelin.com	Engineer
zeljko@openzeppelin.com	Engineer

ROLES

- Account Admin
- Accountant
- Engineer
- Signer

https://openzeppelin.com

Infra-as-code via Terraform or Serverless



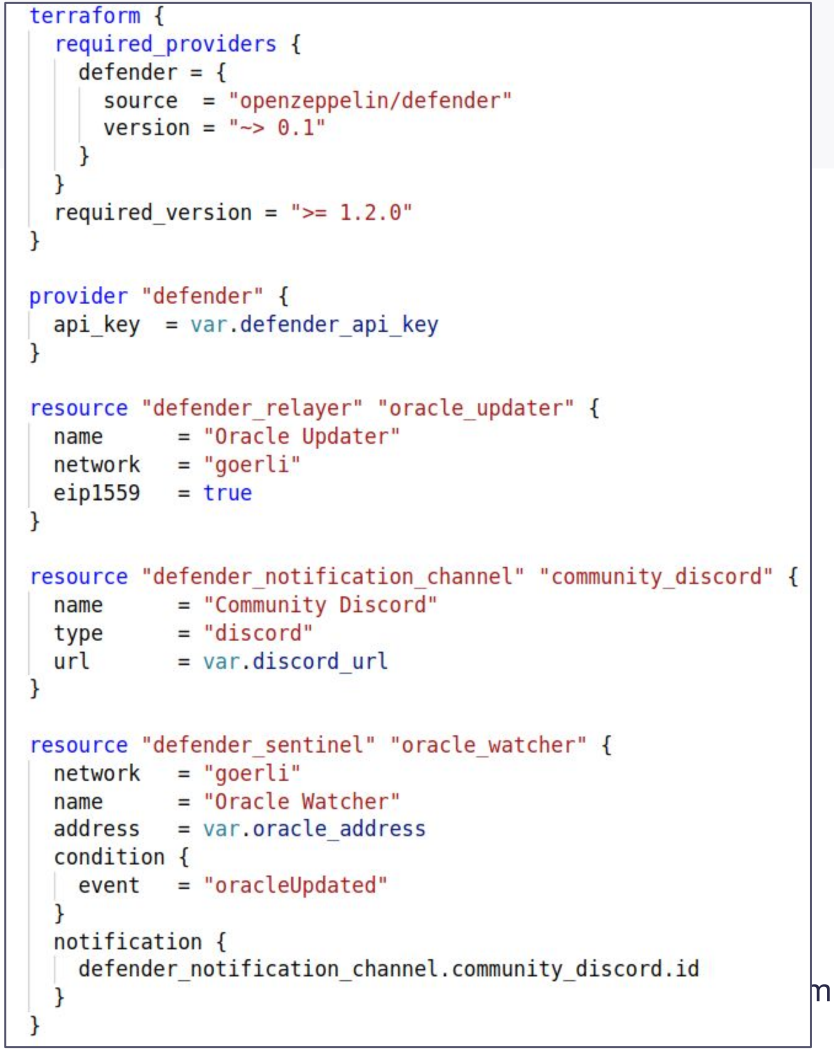
```yaml
service: defender-test-project

frameworkVersion: '3'

provider:
  name: defender

functions:
  hello:
    name: 'Hello world from serverless'
    path: './hello-world'

plugins:
  - ../defender-serverless
```



```hcl
terraform {
  required_providers {
    defender = {
      source  = "openzeppelin/defender"
      version = "~> 0.1"
    }
  }
  required_version = ">= 1.2.0"
}

provider "defender" {
  api_key  = var.defender_api_key
}

resource "defender_relayer" "oracle_updater" {
  name       = "Oracle Updater"
  network    = "goerli"
  eip1559    = true
}

resource "defender_notification_channel" "community_discord" {
  name       = "Community Discord"
  type       = "discord"
  url        = var.discord_url
}

resource "defender_sentinel" "oracle_watcher" {
  network    = "goerli"
  name       = "Oracle Watcher"
  address    = var.oracle_address
  condition {
    event    = "oracleUpdated"
  }
  notification {
    defender_notification_channel.community_discord.id
  }
}
```

OpenZeppelin

m

@openzeppelin/contracts

docs.openzeppelin.com

forum.openzeppelin.com

defender.openzeppelin.com

We are Hiring!
Come join our team!

Contact info

Reach out now if you are interested to chat with our Recruiter on site here at EthCC:

david_bessin@openzeppelin.com

Telegram: David Bessin

OpenZeppelin

https://openzeppelin.com