OpenZeppelin

On-chain Governance

with OpenZeppelin Governor and Tally

Hadrien Croubois, Martín Verzilli, Dennison Bertram

{hadrien,martin}@openzeppelin.com, dennison@withtally.com

@Amxx, @Mverzilli, @DennisonBertram

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

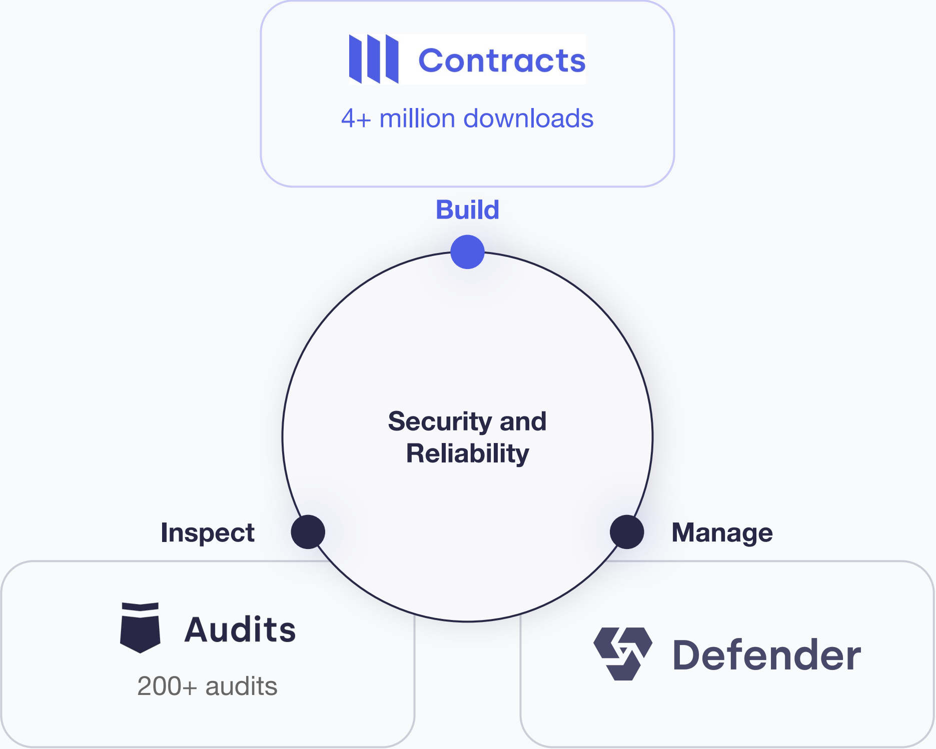
Balancer ethereum foundation augur

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.



What is governance?

Governance is all the processes of interaction [...] over a social system [...].
It is done by the government of a state, by a market, or by a network.

Different types of governance

Off-chain governance

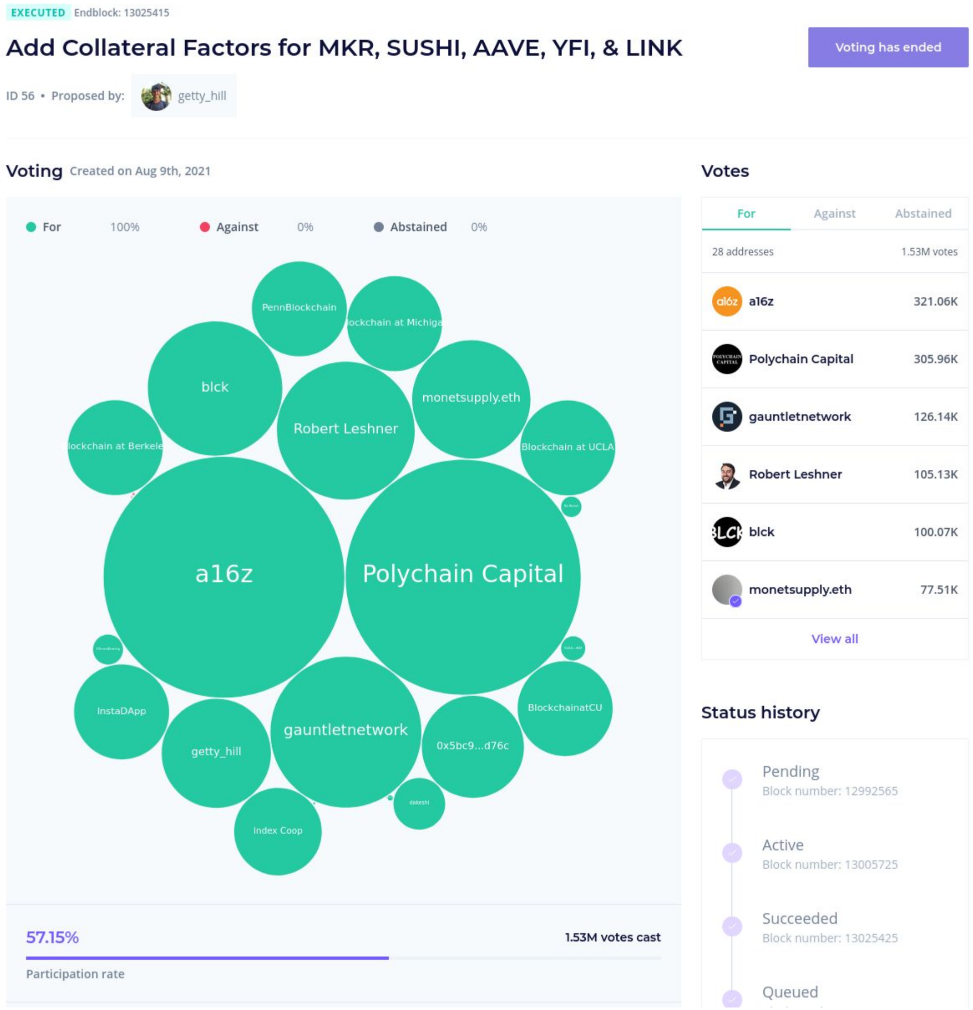
- A person (EOA), or a group of persons (Multisig), is in control,
- Community members can express their opinions,
- Pool results are non-bindings.

Example: https://sybil.org/

On-chain governance

- Specific governor contract is in control,
- Community members votes are submitted to this contract,
- Actions can only be taken if approved by a vote.

Example: https://compound.finance/governance



EXECUTED Endblock: 13025415

Add Collateral Factors for MKR, SUSHI, AAVE, YFI, & LINK

Voting has ended

ID 56 • Proposed by: getty_hill

Voting Created on Aug 9th, 2021

● For 100% ● Against 0% ● Abstained 0%

57.15% 1.53M votes cast

Participation rate

Votes

For | Against | Abstained

28 addresses	1.53M votes
a16z	321.06K
Polychain Capital	305.96K
gauntletnetwork	126.14K
Robert Leshner	105.13K
blck	100.07K
monetsupply.eth	77.51K

View all

Status history

Pending
Block number: 12992565

Active
Block number: 13005725

Succeeded
Block number: 13025425

Queued

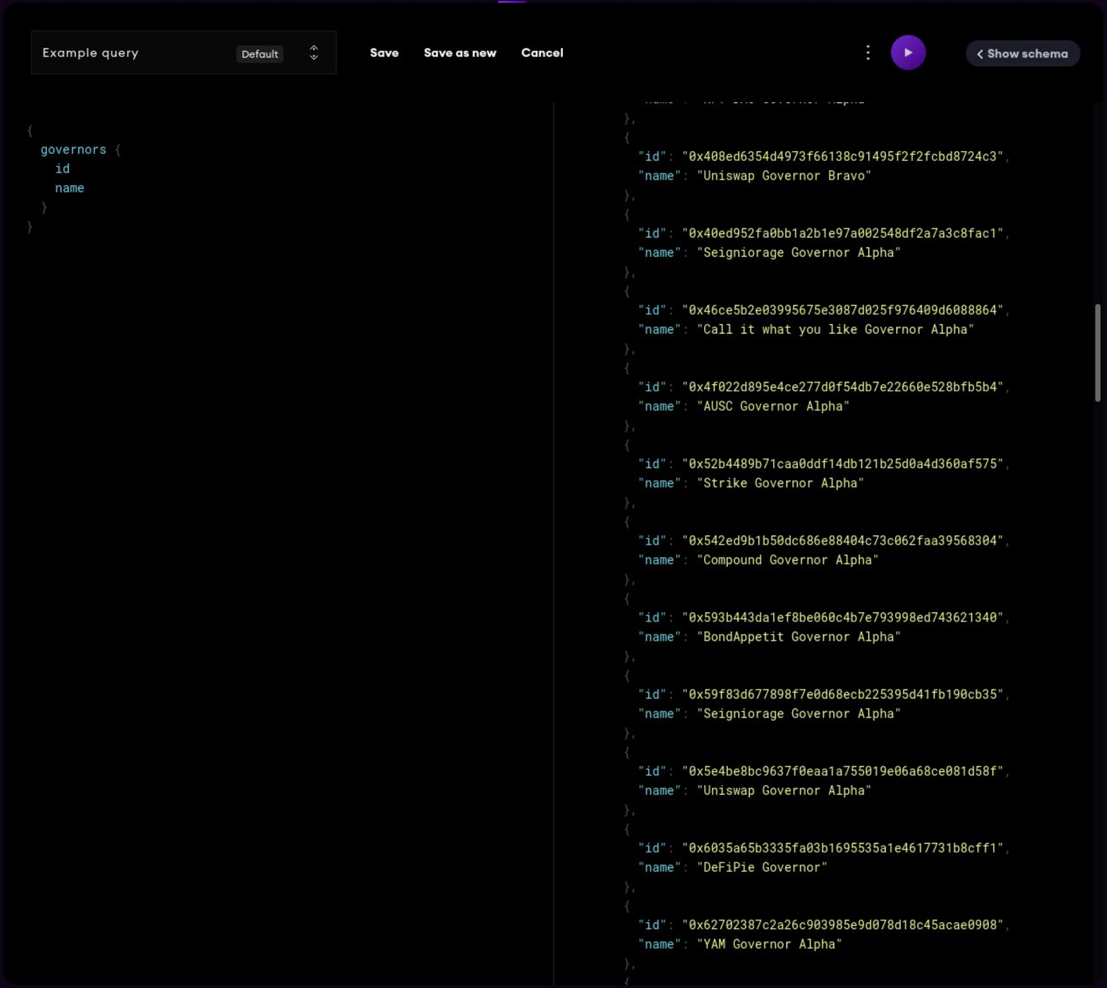
Compound Governors

Over 80 instances on mainnet:

- Governor Alpha;
- Governor Bravo;
- Variations of the above.

A lot of variations, a lot of incompatibilities:

- Event signatures;
- Function arguments;
- Behaviors.



```
{
  governors {
    id
    name
  }
}
```

```
  },
  {
    "id": "0x408ed6354d4973f66138c91495f2f2fcbd8724c3",
    "name": "Uniswap Governor Bravo"
  },
  {
    "id": "0x40ed952fa0bb1a2b1e97a002548df2a7a3c8fac1",
    "name": "Seigniorage Governor Alpha"
  },
  {
    "id": "0x46ce5b2e03995675e3087d025f976409d6088864",
    "name": "Call it what you like Governor Alpha"
  },
  {
    "id": "0x4f022d895e4ce277d0f54db7e22660e528bfb5b4",
    "name": "AUSC Governor Alpha"
  },
  {
    "id": "0x52b4489b71caa0ddf14db121b25d0a4d360af575",
    "name": "Strike Governor Alpha"
  },
  {
    "id": "0x542ed9b1b50dc686e88404c73c062faa39568304",
    "name": "Compound Governor Alpha"
  },
  {
    "id": "0x593b443da1ef8be060c4b7e793998ed743621340",
    "name": "BondAppetit Governor Alpha"
  },
  {
    "id": "0x59f83d677898f7e0d68ecb225395d41fb190cb35",
    "name": "Seigniorage Governor Alpha"
  },
  {
    "id": "0x5e4be8bc9637f0eaa1a755019e06a68ce081d58f",
    "name": "Uniswap Governor Alpha"
  },
  {
    "id": "0x6035a65b3335fa03b1695535a1e4617731b8cff1",
    "name": "DeFiPie Governor"
  },
  {
    "id": "0x62702387c2a26c903985e9d078d18c45acae0908",
    "name": "YAM Governor Alpha"
  },
  {
```

Introducing OpenZeppelin Governor

Available since version 4.3.0

@openzeppelin/contracts/governance/Governor.sol
@openzeppelin/contracts/governance/extensions/...

Designed with modularity in mind

Just like ERC20, ERC721 and ERC1155.

OpenZeppelin Governor Modules

Required modules

- **Votes:** Where do the users get their voting power from?
- **Counting:** What options do users have when voting, and how are votes counted?

Optional Modules

- **Timelock:** Perform operations through a timelock contract.
- **Threshold:** Limit some operation (proposal) to users with enough tokens.
- Many more to come?

Required module: Voting

Where do users get their voting power form?

`@openzeppelin/contracts/governance/extensions/GovernorVotes.sol`

- Get voters weight for an ERC20Votes contract.

`@openzeppelin/contracts/governance/extensions/GovernorVotesComp.sol`

- Get voters weight for a Comp token contract.

`@openzeppelin/contracts/governance/extensions/GovernorVotesQuorumFraction.sol`

- Get voters weight for an ERC20Votes contract, and set the quorum to a ratio of the total supply.

For a proposal to pass, 5% of the total supply must vote

Required module: Counting

What options do users have when voting, and how are votes counted?

`@openzeppelin/contracts/governance/extensions/GovernorVotesComp.sol`

- User can vote for, against, or abstain.
- A proposal must have (strictly) more “for” votes then “against” votes to pass.
- “For” and “abstain” votes count toward the quorum. “Against” votes don’t.
- Counting is described as

```
function COUNTING_MODE() public pure virtual override returns (string memory) { return "support=bravo&quorum=for,abstain"; }
```

Optional module: Timelock

Perform operations through a timelock contract.

`@openzeppelin/contracts/governance/extensions/GovernorTimelockControl.sol`

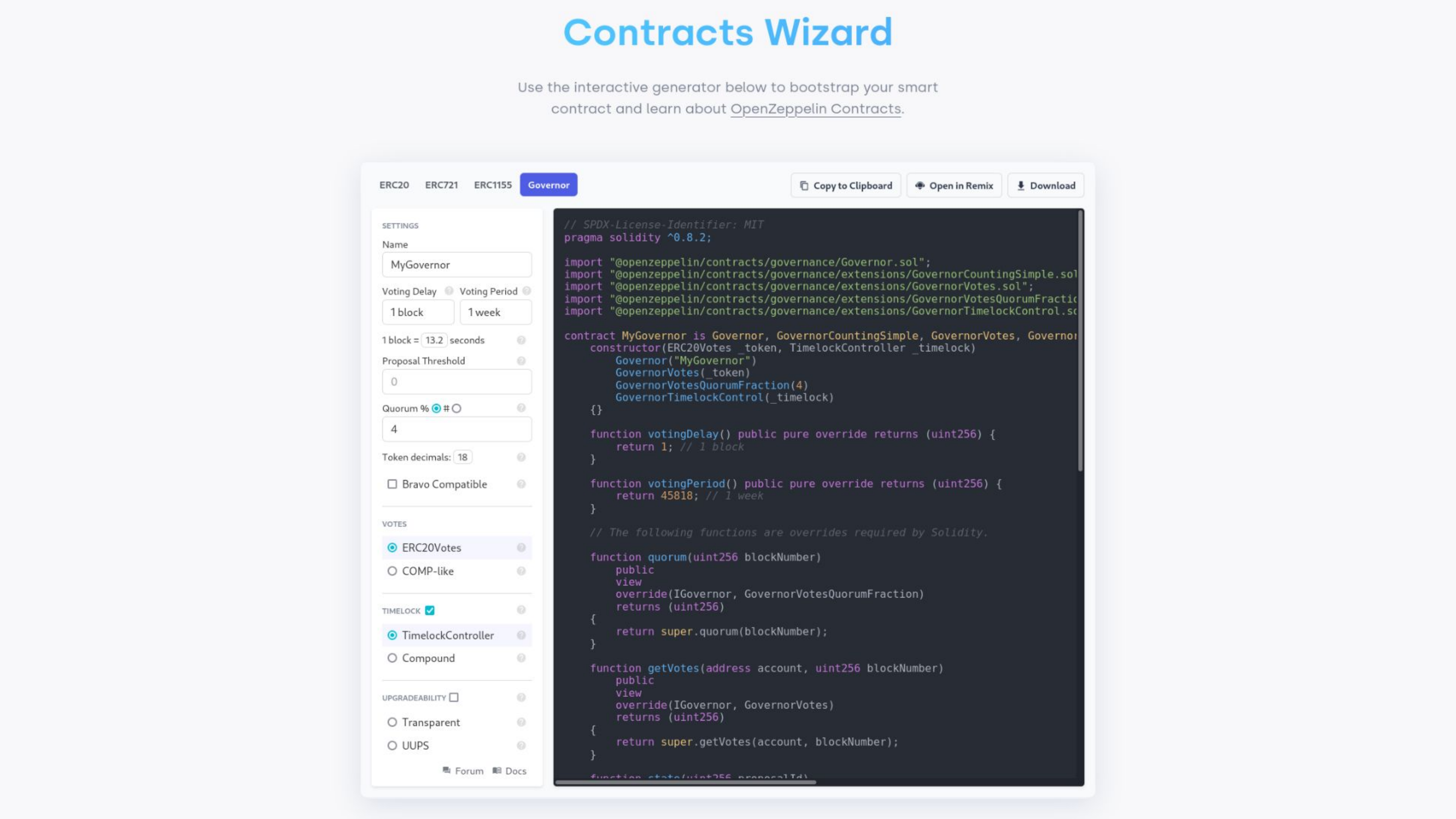
- Add a “queue” function, and execute successful operations through a TimelockController.

`@openzeppelin/contracts/governance/extensions/GovernorTimelockCompound.sol`

- Add a “queue” function, and execute successful operations through a CompoundTimelock

➢ Both modules implement the same interface, and emit compound governor alpha/bravo compatible events

➢ Warning: with these modules, assets and permissions must be given to the timelock, not the governor!



Contracts Wizard

Use the interactive generator below to bootstrap your smart contract and learn about OpenZeppelin Contracts.

SETTINGS

Name: MyGovernor

Voting Delay: 1 block

Voting Period: 1 week

1 block = 13.2 seconds

Proposal Threshold: 0

Quorum % ● # ○: 4

Token decimals: 18

☐ Bravo Compatible

VOTES

● ERC20Votes

○ COMP-like

TIMELOCK ☑

● TimelockController

○ Compound

UPGRADEABILITY ☐

○ Transparent

○ UUPS

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.2;

import "@openzeppelin/contracts/governance/Governor.sol";
import "@openzeppelin/contracts/governance/extensions/GovernorCountingSimple.sol
import "@openzeppelin/contracts/governance/extensions/GovernorVotes.sol";
import "@openzeppelin/contracts/governance/extensions/GovernorVotesQuorumFractic
import "@openzeppelin/contracts/governance/extensions/GovernorTimelockControl.sc

contract MyGovernor is Governor, GovernorCountingSimple, GovernorVotes, Governor
    constructor(ERC20Votes _token, TimelockController _timelock)
        Governor("MyGovernor")
        GovernorVotes(_token)
        GovernorVotesQuorumFraction(4)
        GovernorTimelockControl(_timelock)
    {}

    function votingDelay() public pure override returns (uint256) {
        return 1; // 1 block
    }

    function votingPeriod() public pure override returns (uint256) {
        return 45818; // 1 week
    }

    // The following functions are overrides required by Solidity.

    function quorum(uint256 blockNumber)
        public
        view
        override(IGovernor, GovernorVotesQuorumFraction)
        returns (uint256)
    {
        return super.quorum(blockNumber);
    }

    function getVotes(address account, uint256 blockNumber)
        public
        view
        override(IGovernor, GovernorVotes)
        returns (uint256)
    {
        return super.getVotes(account, blockNumber);
    }

    function state(uint256 proposalId)
```

Another module: GovernorCompatibilityBravo

Extending Compatibility with Governor Bravo

`@openzeppelin/contracts/governance/compatibility/GovernorCompatibilityBravo.sol`

- By default, OpenZeppelin Governor uses the same event signatures as Compound
- OpenZeppelin Govenor is designed to be more gas efficient with minimal on-chain storage.
- Some key function signatures are different (queue, execute)

○ The compatibility layer reproduces the Governor Bravo experience

➢ Implement the missing functions
➢ Comes with a built-in counting module
➢ More expensive in terms of gas …
➢ ... allows backward compatibility with tools designed for Compound

Creating Governor proposals with Defender

Defender Components

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

Creating Governor proposals from Defender Admin

1. Use Admin’s transaction builder to create the proposal.

2. Select the Governor contract that will manage the proposal.

3. Point your community to Tally to vote.

4. Defender tracks proposal status.

Demo:
Create a proposal with Defender

Demo:
Walk through of the Tally Site

Learn more about Tally

www.withTally.com

Discord:

https://discord.gg/fPz4VugbjJ

OpenZeppelin Governor

is supported in

@openzeppelin/subgraphs

@openzeppelin/contracts

docs.openzeppelin.com

forum.openzeppelin.com

defender.openzeppelin.com

Thank you!

Learn more

openzeppelin.com/**contracts**

forum.openzeppelin.com

docs.openzeppelin.com

Contact

{hadrien,mverzilli}@openzeppelin.com

dennison@withtally.com