OpenZeppelin

Cheap Contract Deployment

Through Clones

zpl.in/contracts-workshop

Hadrien Croubois
hadrien@openzeppelin.com
@amxx

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

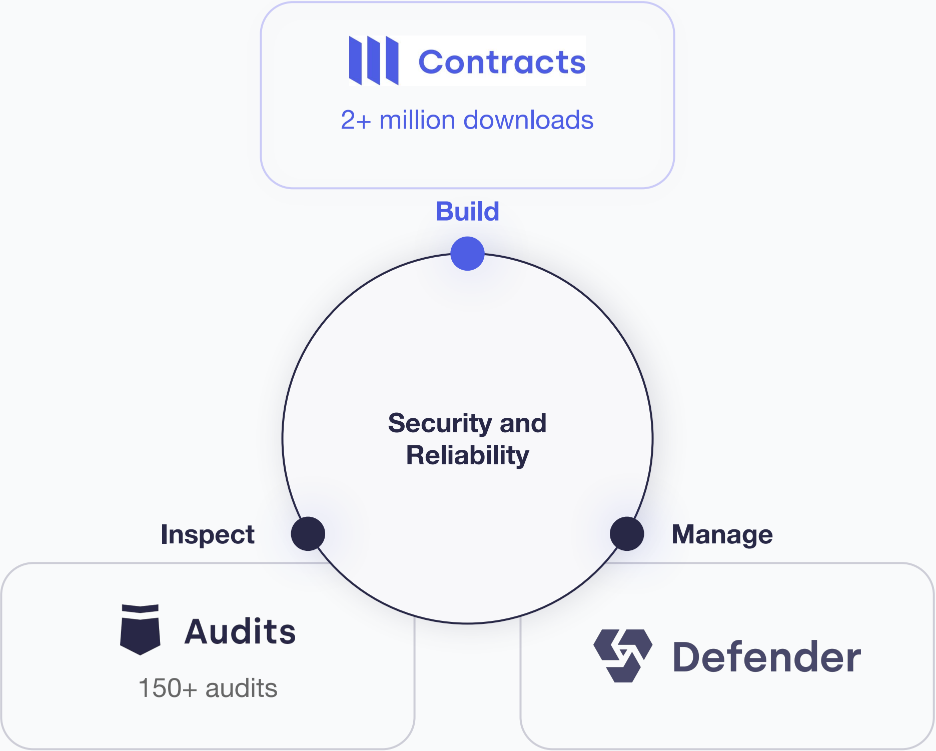
Balancer ethereum foundation augur

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.



Contracts

2+ million downloads

Build

Security and Reliability

Inspect

Manage

Audits

150+ audits

Defender

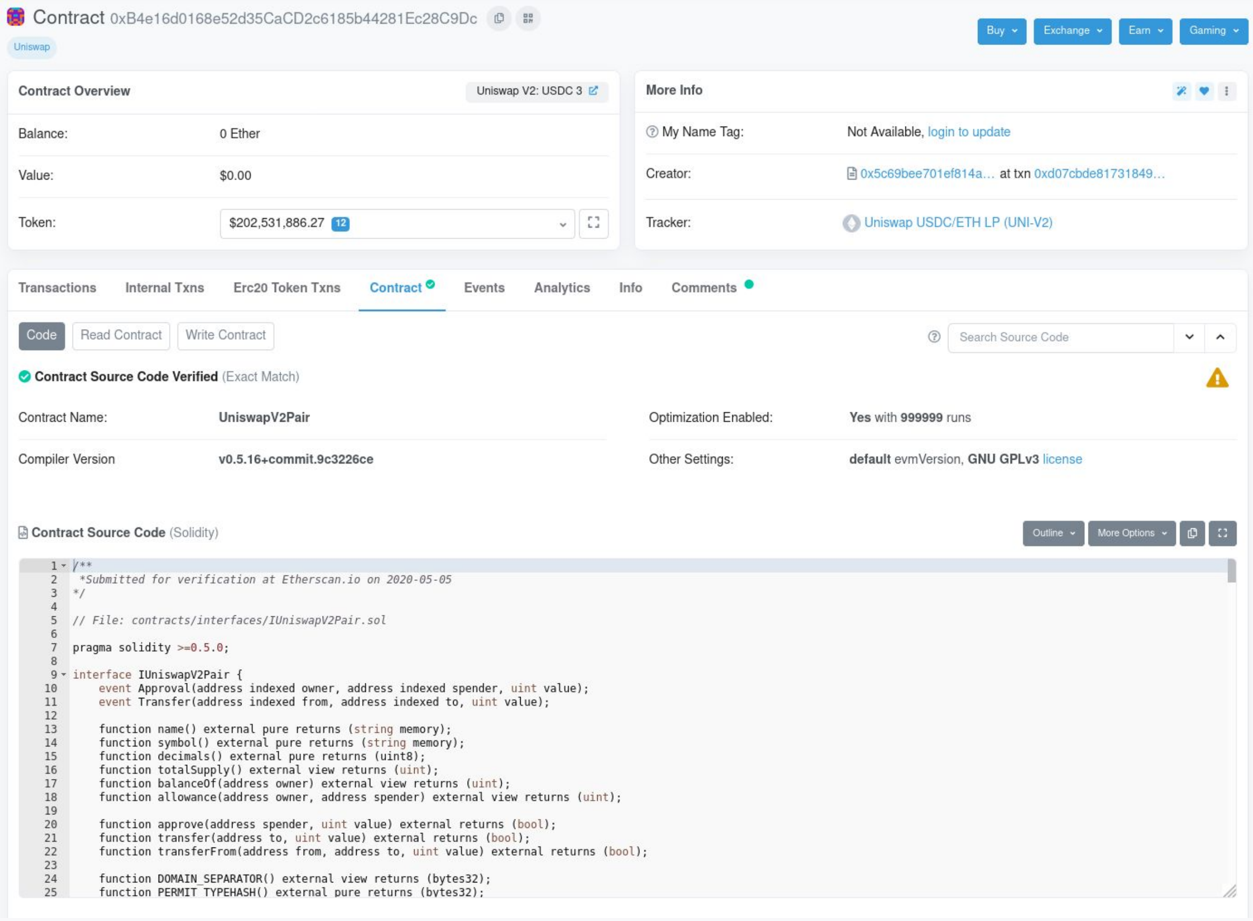
Families of smart contracts

A brief overview

UniswapV2 has over 30k registered pairs

Argent factories have been called over 35k times

In both cases, these adoption numbers are contracts deployed on mainnet



Contract 0xB4e16d0168e52d35CaCD2c6185b44281Ec28C9Dc

Contract Overview

Balance:	0 Ether
Value:	$0.00
Token:	$202,531,886.27 12

More Info

My Name Tag:	Not Available, login to update
Creator:	0x5c69bee701ef814a… at txn 0xd07cbde81731849…
Tracker:	Uniswap USDC/ETH LP (UNI-V2)

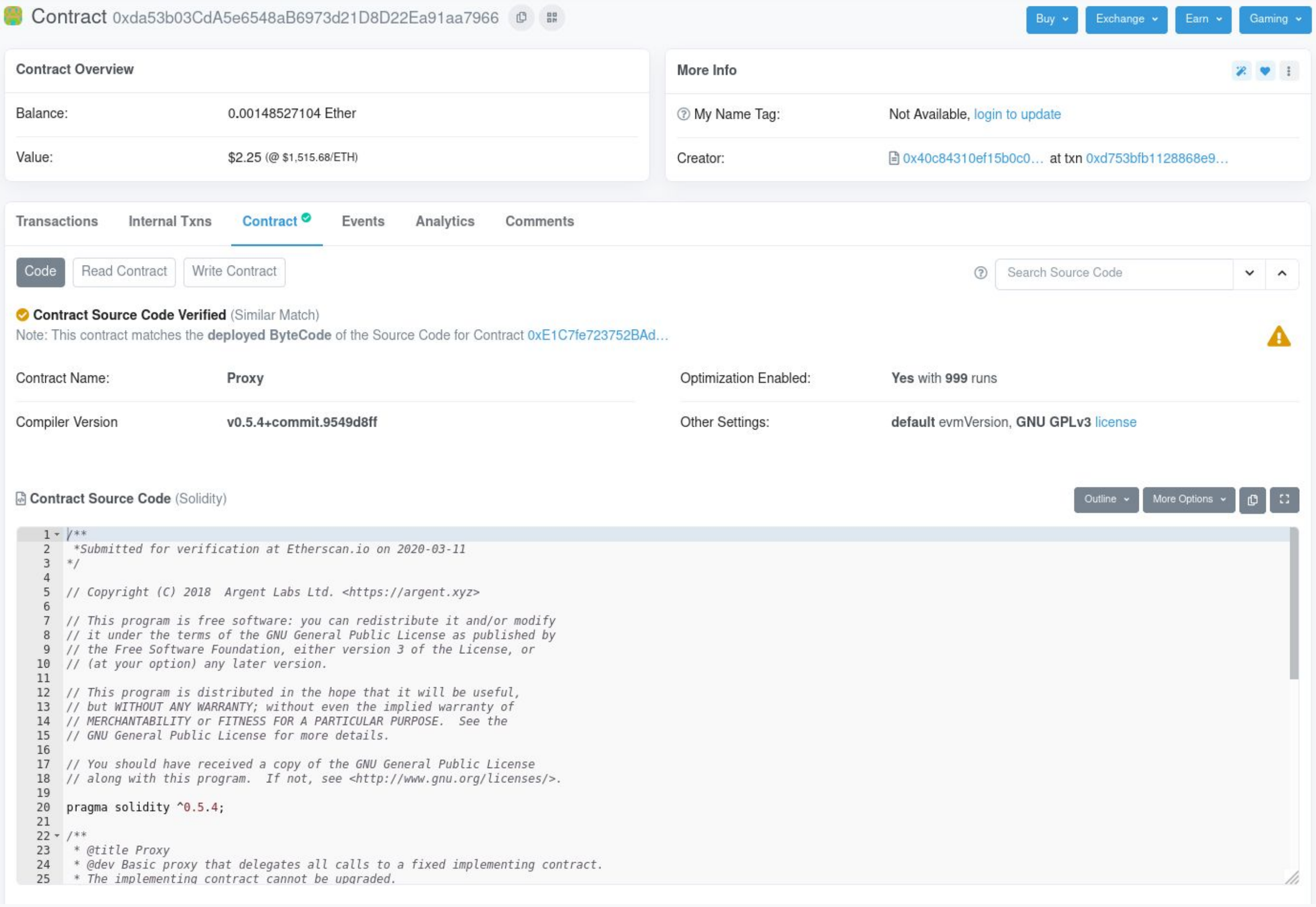
Contract Source Code Verified (Exact Match)

Contract Name:	UniswapV2Pair	Optimization Enabled:	Yes with 999999 runs
Compiler Version	v0.5.16+commit.9c3226ce	Other Settings:	default evmVersion, GNU GPLv3 license

Contract Source Code (Solidity)

```
/**
 *Submitted for verification at Etherscan.io on 2020-05-05
*/

// File: contracts/interfaces/IUniswapV2Pair.sol

pragma solidity >=0.5.0;

interface IUniswapV2Pair {
    event Approval(address indexed owner, address indexed spender, uint value);
    event Transfer(address indexed from, address indexed to, uint value);

    function name() external pure returns (string memory);
    function symbol() external pure returns (string memory);
    function decimals() external pure returns (uint8);
    function totalSupply() external view returns (uint);
    function balanceOf(address owner) external view returns (uint);
    function allowance(address owner, address spender) external view returns (uint);

    function approve(address spender, uint value) external returns (bool);
    function transfer(address to, uint value) external returns (bool);
    function transferFrom(address from, address to, uint value) external returns (bool);

    function DOMAIN_SEPARATOR() external view returns (bytes32);
    function PERMIT_TYPEHASH() external pure returns (bytes32);
```

Creation cost: 2,513,386 gas



Contract 0xda53b03CdA5e6548aB6973d21D8D22Ea91aa7966

Contract Overview

Balance:	0.00148527104 Ether
Value:	$2.25 (@ $1,515.68/ETH)

More Info

My Name Tag:	Not Available, login to update
Creator:	0x40c84310ef15b0c0… at txn 0xd753bfb1128868e9…

Contract Source Code Verified (Similar Match)
Note: This contract matches the **deployed ByteCode** of the Source Code for Contract 0xE1C7fe723752BAd…

Contract Name:	**Proxy**	Optimization Enabled:	**Yes** with **999** runs
Compiler Version	**v0.5.4+commit.9549d8ff**	Other Settings:	**default** evmVersion, **GNU GPLv3** license

Contract Source Code (Solidity)

```
/**
 *Submitted for verification at Etherscan.io on 2020-03-11
*/

// Copyright (C) 2018  Argent Labs Ltd. <https://argent.xyz>

// This program is free software: you can redistribute it and/or modify
// it under the terms of the GNU General Public License as published by
// the Free Software Foundation, either version 3 of the License, or
// (at your option) any later version.

// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
// GNU General Public License for more details.

// You should have received a copy of the GNU General Public License
// along with this program.  If not, see <http://www.gnu.org/licenses/>.

pragma solidity ^0.5.4;

/**
 * @title Proxy
 * @dev Basic proxy that delegates all calls to a fixed implementing contract.
 * The implementing contract cannot be upgraded.
```

Creation cost: 919,704 gas

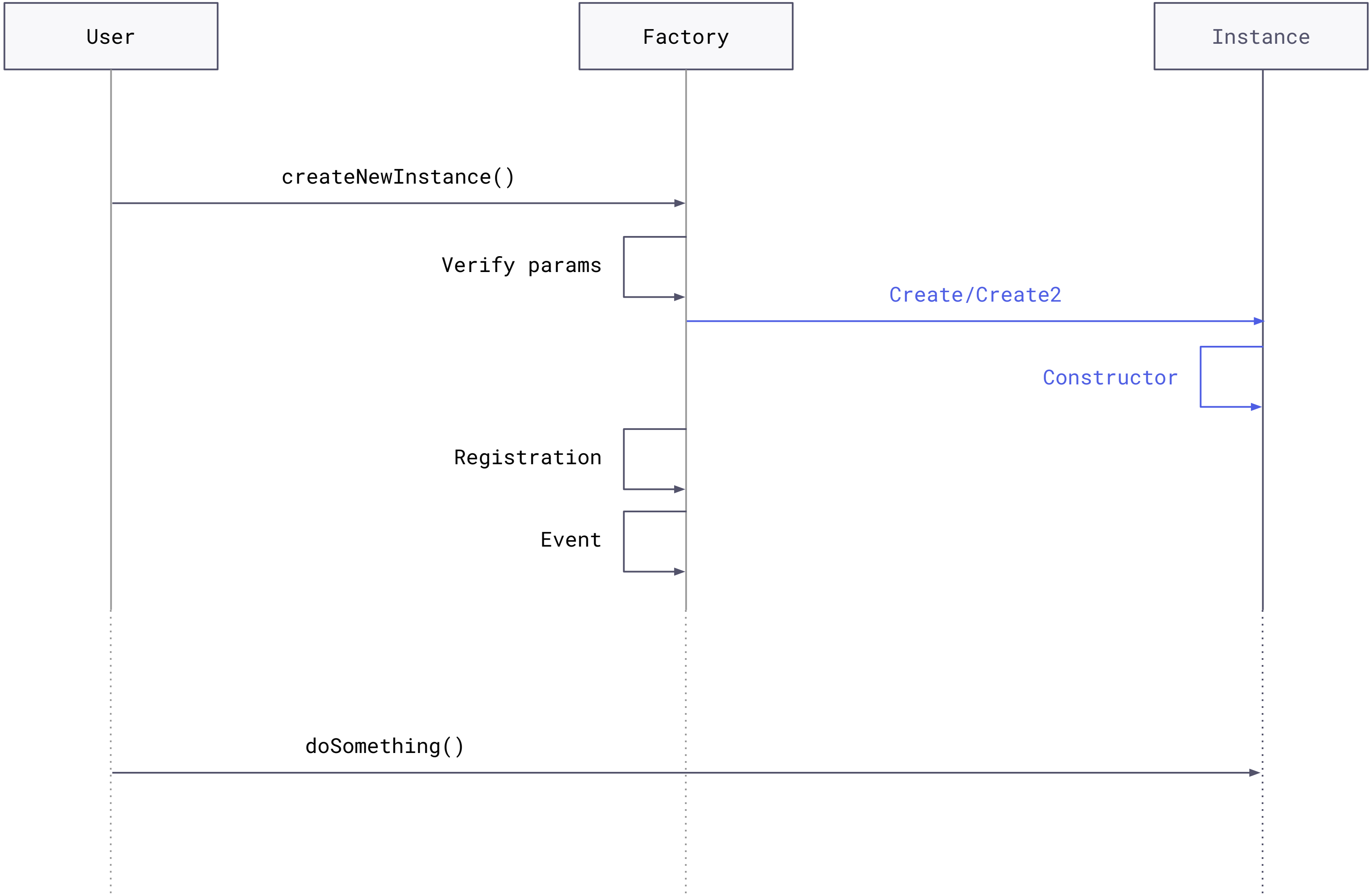
Why so expensive?

The cost of deploying a contract

Common factory workflow: the naive approach

- Initiate transaction
- (Verify parameters)
- Create a new contract
  - Constructor
- (New contract registration)
- (Emit event)

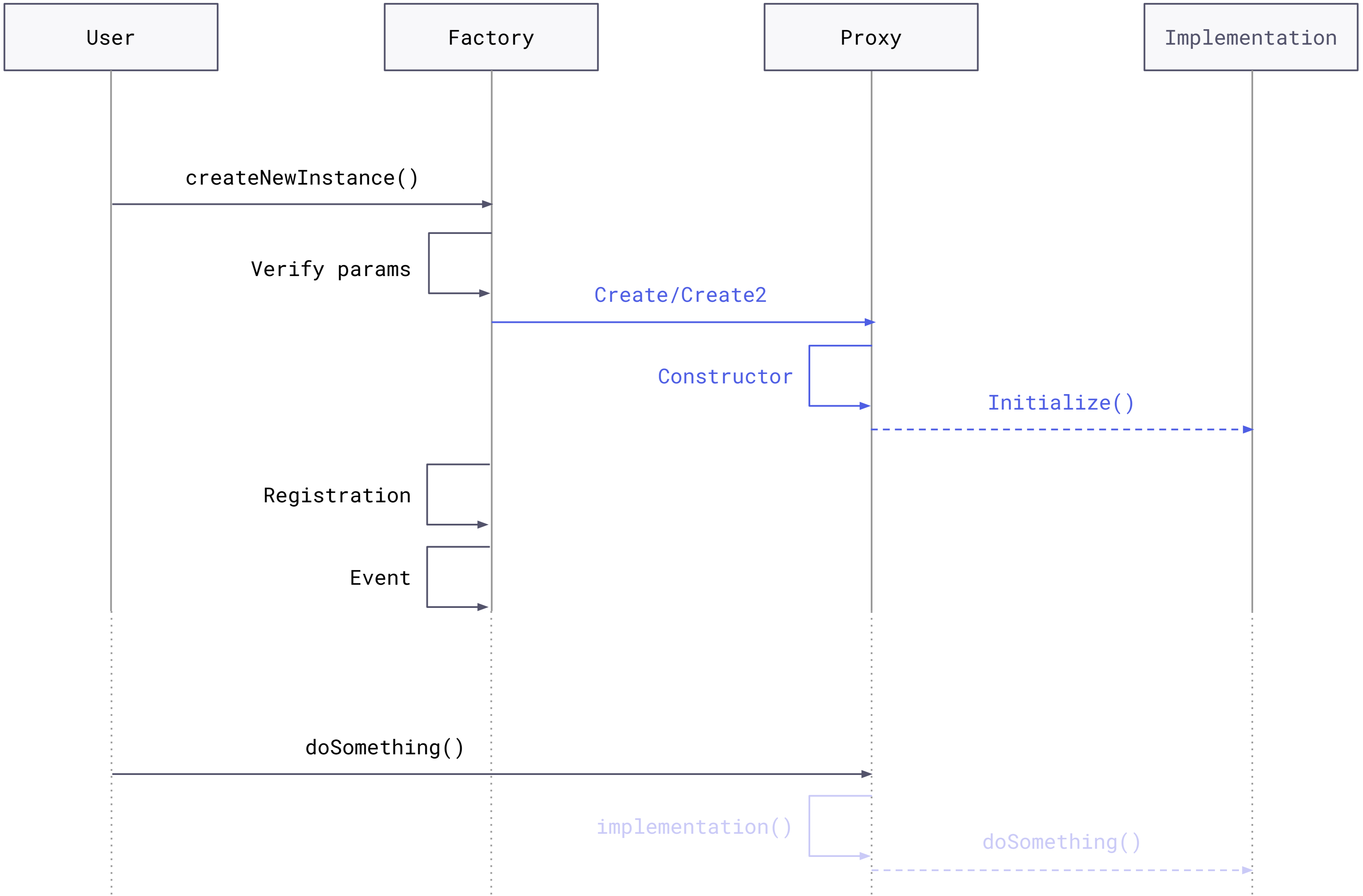
The very expensive part*


User
Factory
Instance
createNewInstance()
Verify params
Create/Create2
Constructor
Registration
Event
doSomething()

Alternative factory workflow: the proxy approach

- Initiate transaction
- (Verify parameters)
- Create a new proxy
    - Constructor
- Initialize the underlying logic
- (New contract registration)
- (Emit event)

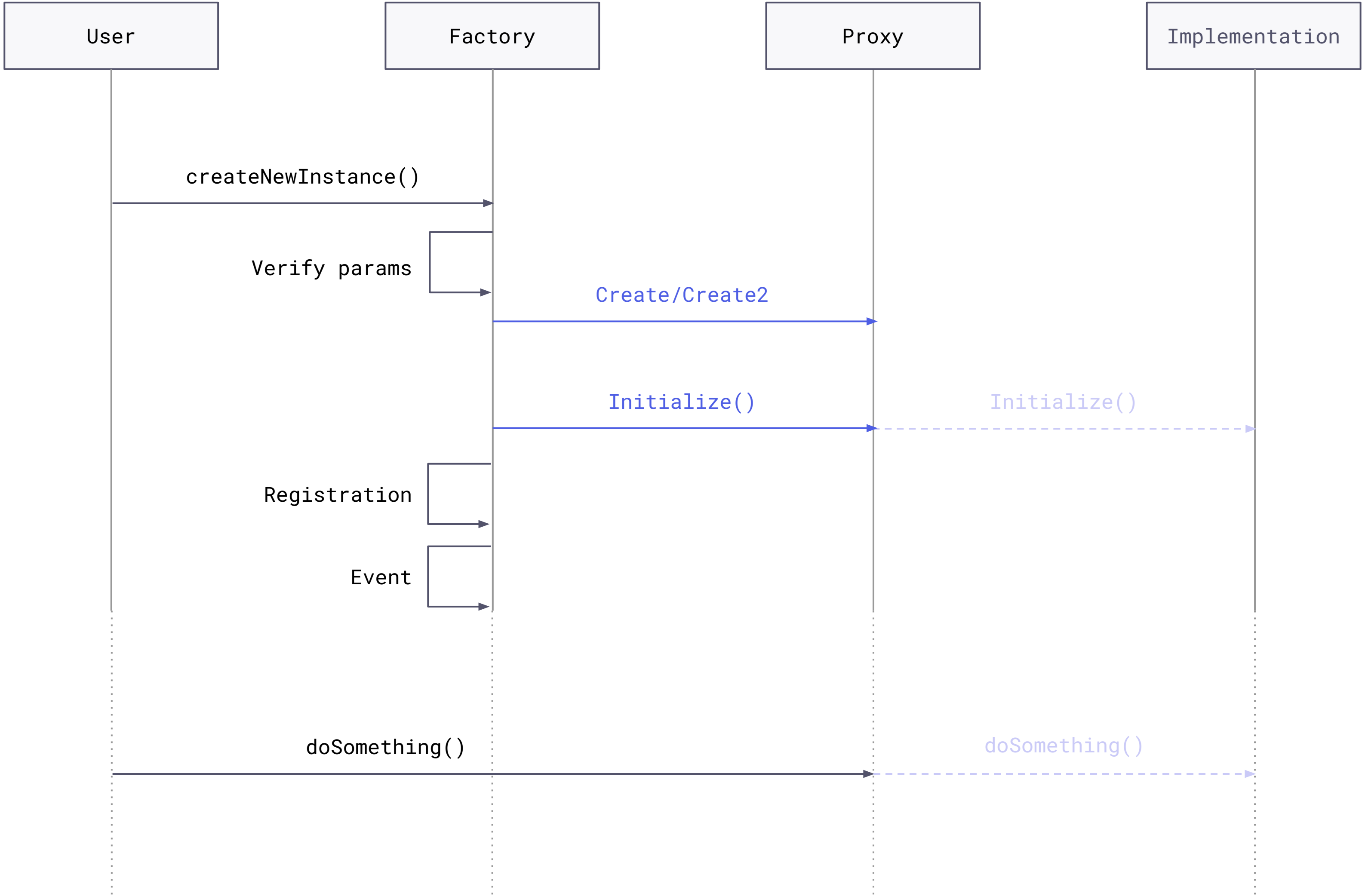
The expensive part*


User
Factory
Proxy
Implementation
createNewInstance()
Verify params
Create/Create2
Constructor
Initialize()
Registration
Event
doSomething()
implementation()
doSomething()

Alternative factory workflow: the clone approach

- Initiate transaction
- (Verify parameters)
- Create a new clone (EIP1167)
- Initialize the underlying logic
- (New contract registration)
- (Emit event)

} The not quite as expensive part*


User
Factory
Proxy
Implementation
createNewInstance()
Verify params
Create/Create2
Initialize()
Initialize()
Registration
Event
doSomething()
doSomething()

Demo Time

Hands-on with the code

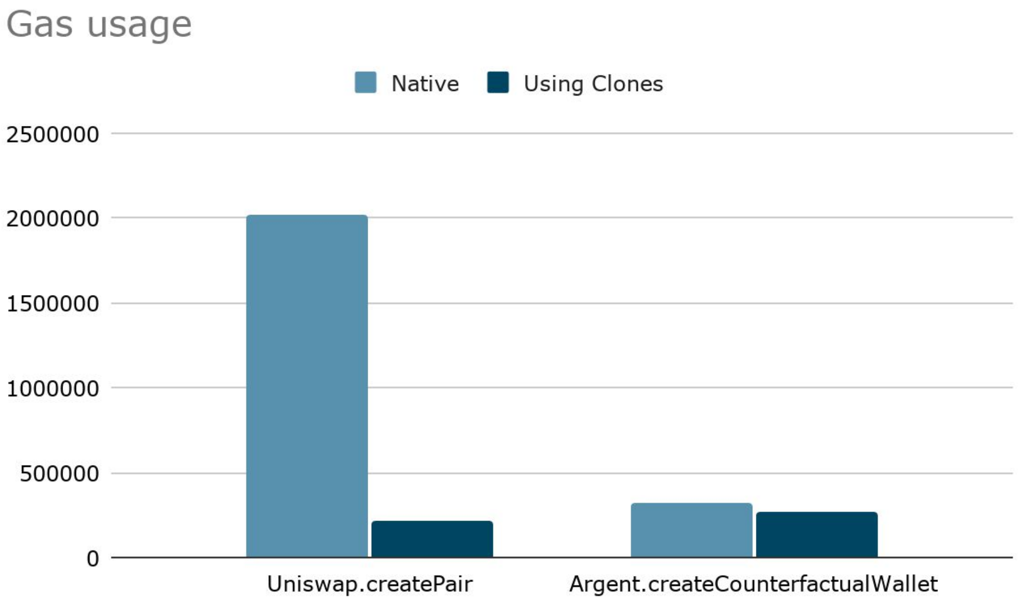
zpl.in/contracts-workshop

Clones are part of @openzeppelin/contracts

```
import "@openzeppelin/contracts/proxy/Clones.sol";
```

- function **clone(address)** returns (address)
- function **cloneDeterministic(address, bytes32)** returns (address)
- function **predictDeterministicAddress(address, bytes32)** view returns (address)
- function **predictDeterministicAddress(address, bytes32, address)** pure returns (address)

Cost of using clones compared to other methods



Advantages and drawbacks of clones

- Very cheap deployment
- Easily compatible current proxy based factories
- Cheaper to call than a “storage based” proxy
- Non upgradeable
- More expensive to call than a native contract (+700 gas/call)

@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

🐦 @amxx

hadrien@openzeppelin.com