OpenZeppelin

Deploying More Efficient Upgradeable Contracts

UUPS Proxies

zpl.in/contracts-workshop

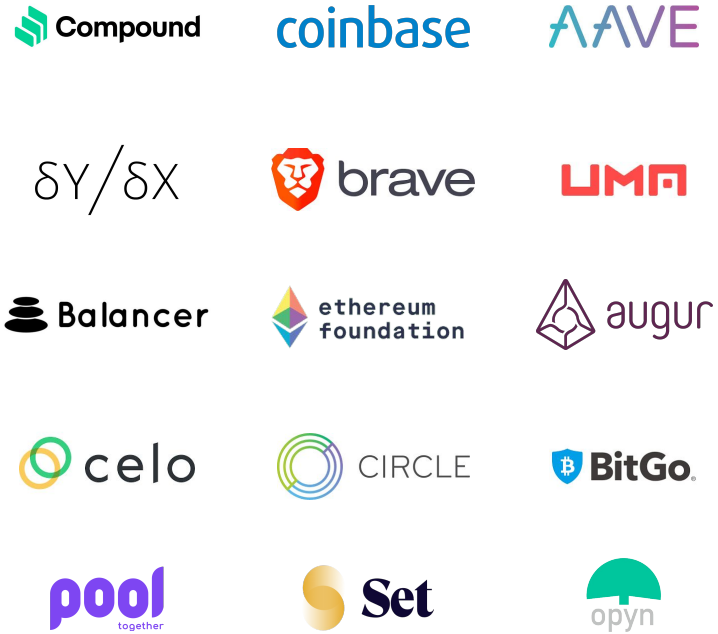
Francisco Giordano
frangio@openzeppelin.com
@frangio_

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.



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.

OpenZeppelin Contracts

Token Standards
ERC20, ERC721, ...

+ Extensions
Pausable, snapshots, ...

Proxies
Upgradeability, clones

Security modules
Reentrancy guard,
pull payments

Utilities
Cryptography, math, create2,
data structures, ...

→ Upgrades Plugins
Automated upgradeability with
security checks

Governance
Timelock, & more coming...

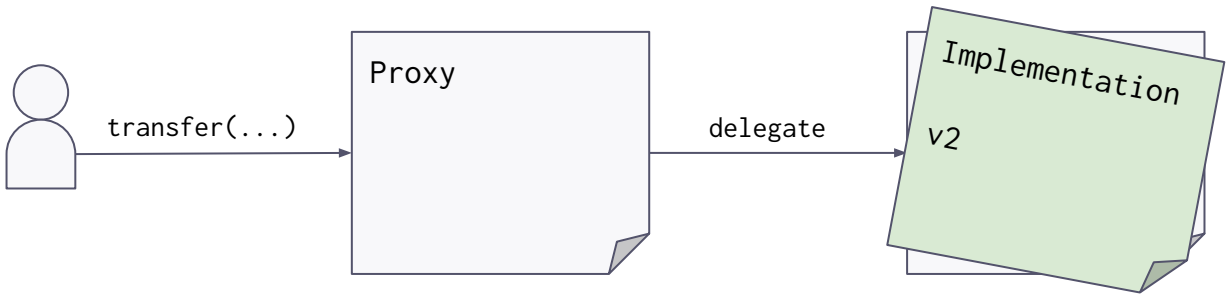
Access Control
Ownable & Roles

Outline

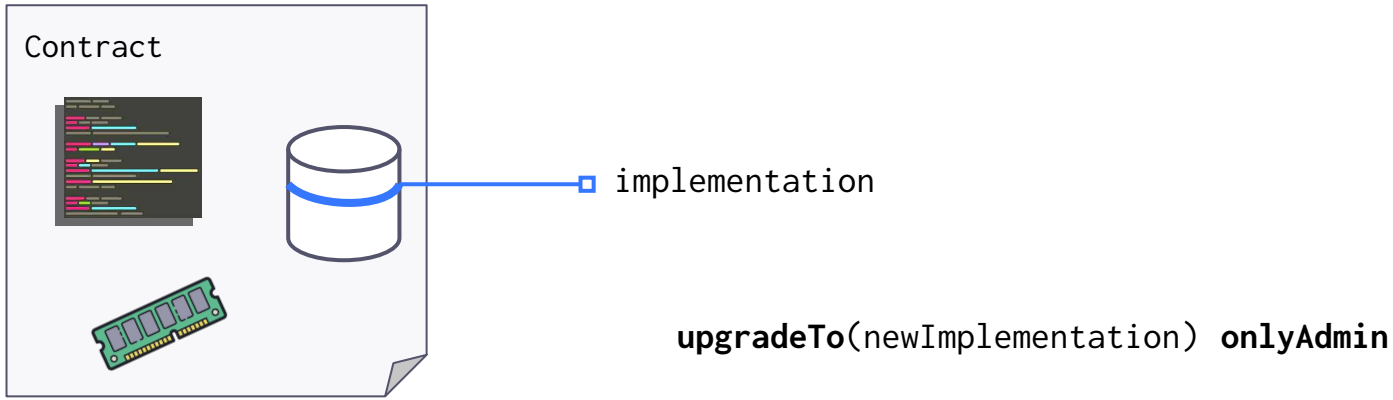
1. Theory
    * Build up to UUPS
    * Comparison with Transparent Proxy
2. Practice
    * Writing upgradeable contracts for UUPS
    * Developing with Upgrades Plugins

Theory

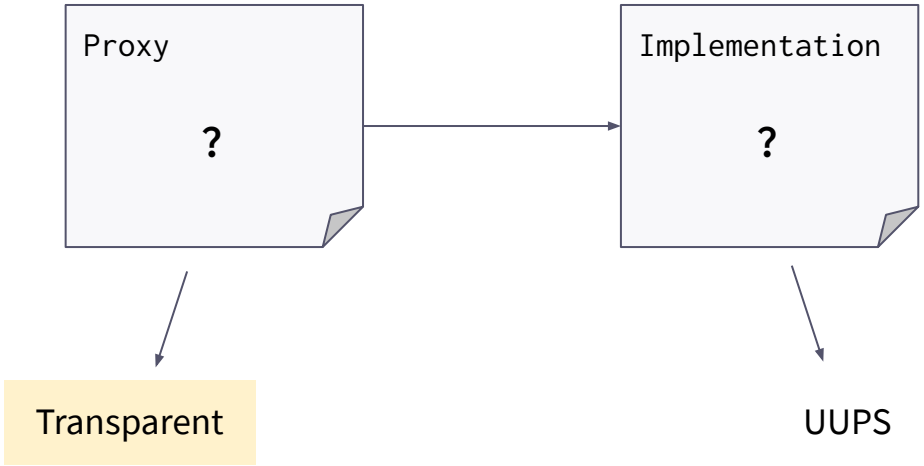
Proxy Pattern



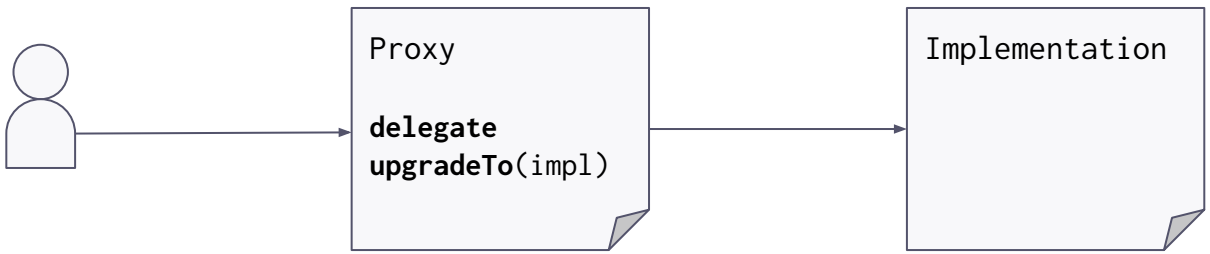
Storage


Contract
implementation
upgradeTo(newImplementation) onlyAdmin

Upgrade - Where?



Transparent Proxy



Malicious backdoors in Ethereum Proxies

A detailed explanation on how the Proxy pattern for smart contract upgradeability can be exploited.

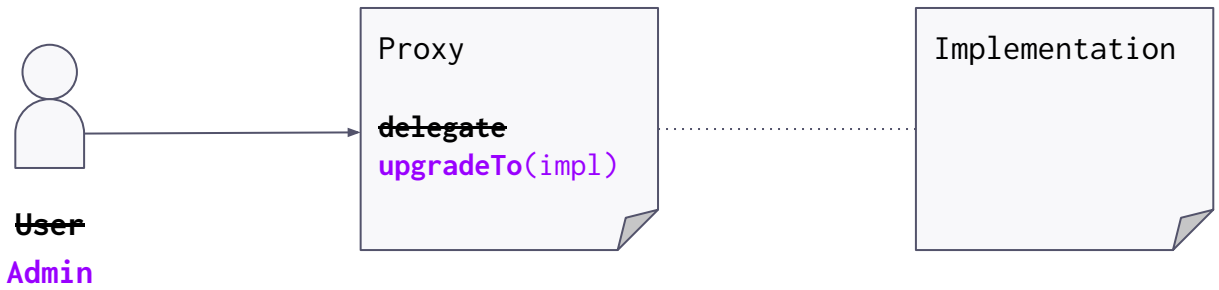
Patricio Palladino Follow
Jun 1, 2018 · 5 min read

Beware of the proxy: learn how to exploit function clashing

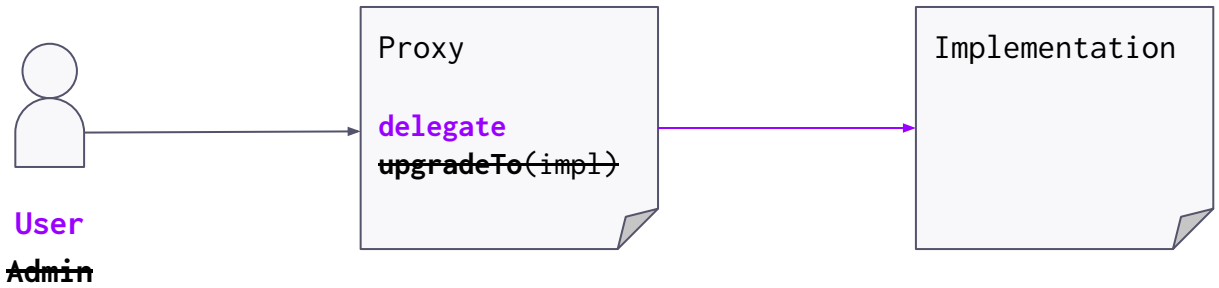
Security

tinchoabbate ⚡ OpenZeppelin Team 2 Jul '19

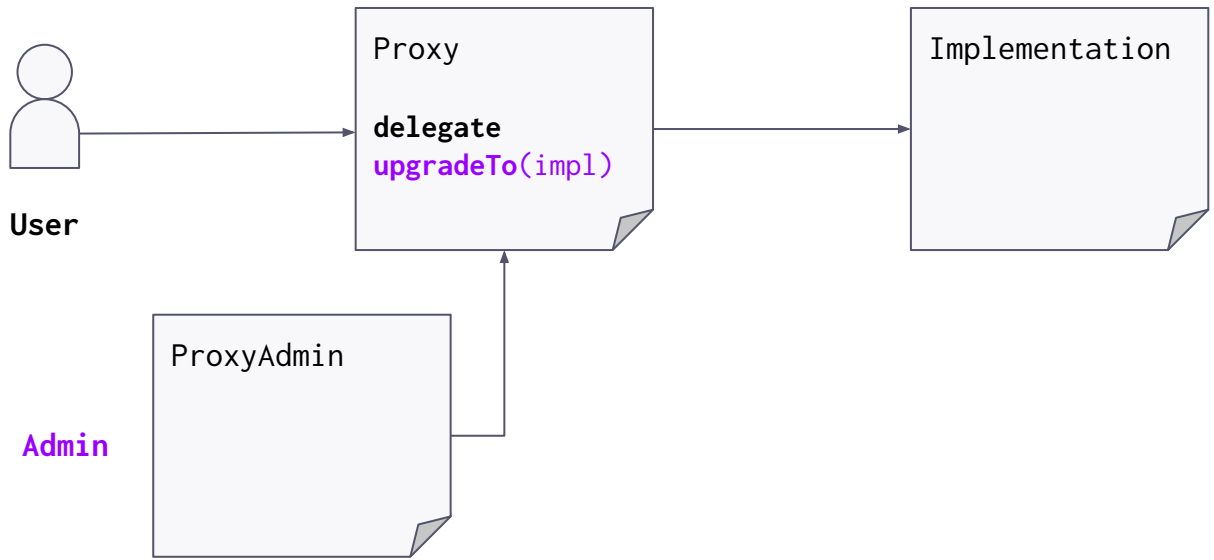
Transparent Proxy



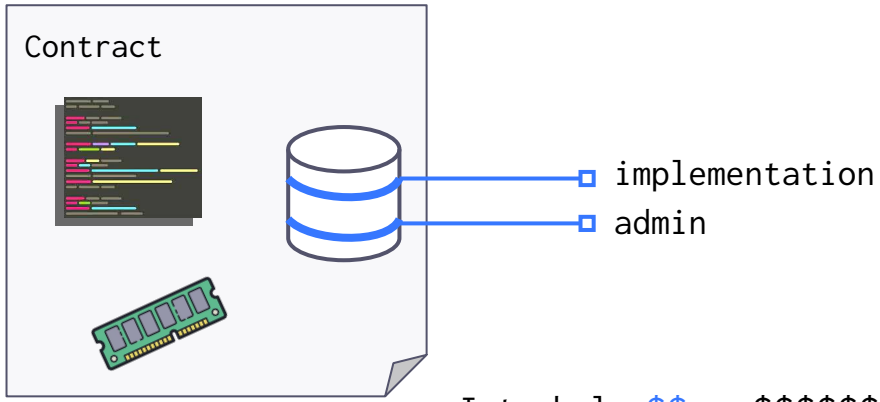
Transparent Proxy



Transparent Proxy



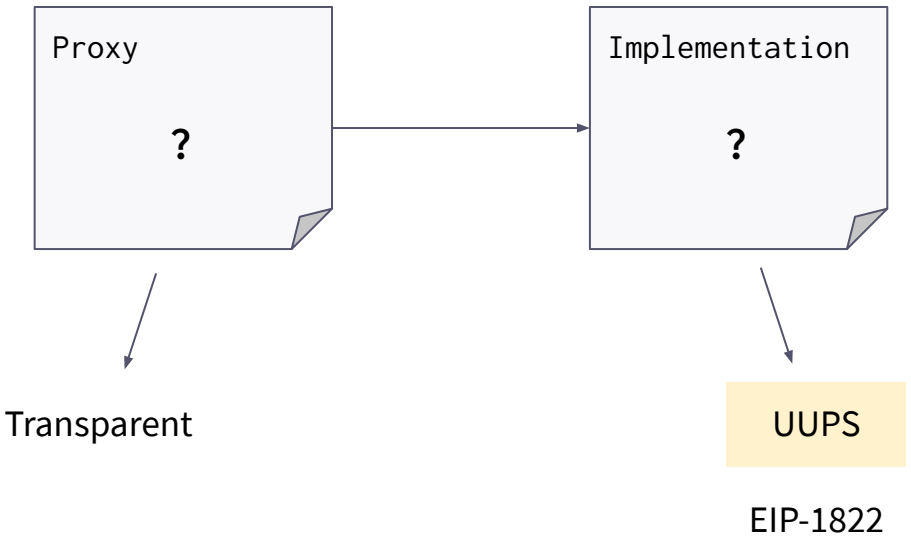
Transparent Proxy



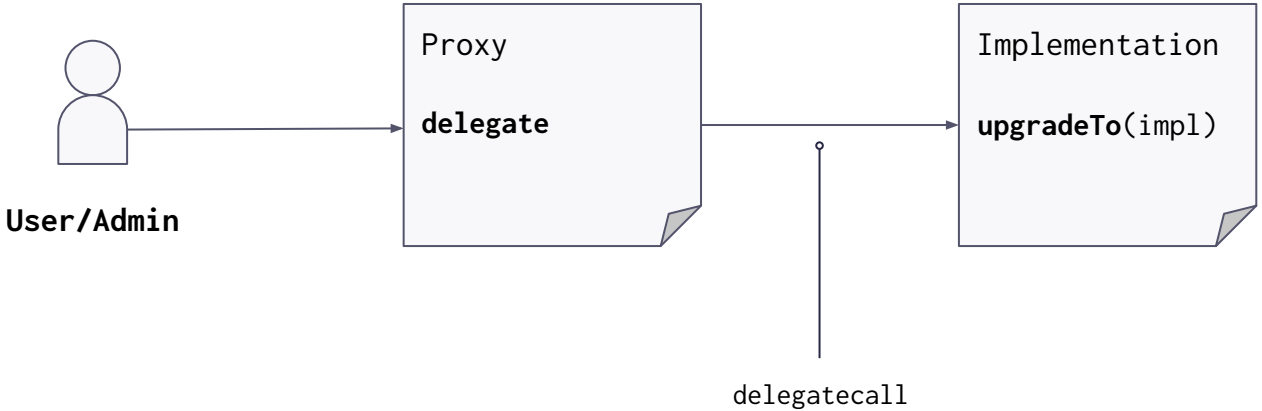
Istanbul $$ → $$$$$$$$

Berlin $$$$$$$$ → $$$$$$$$$$$$$$$$$$$$

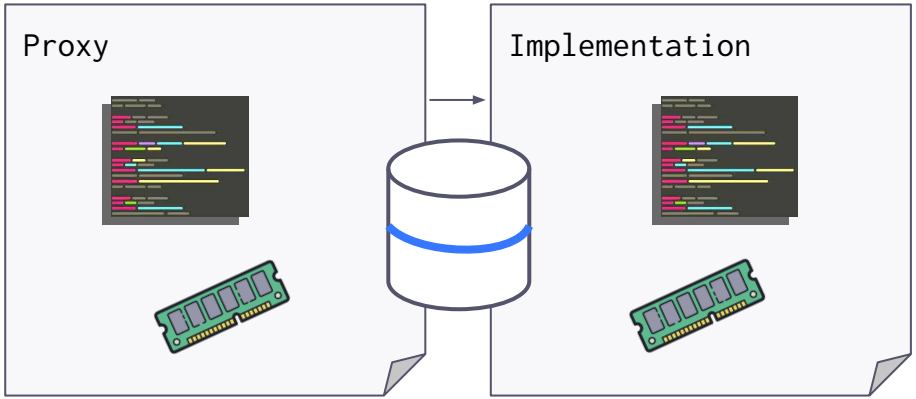
Upgrade - Where?



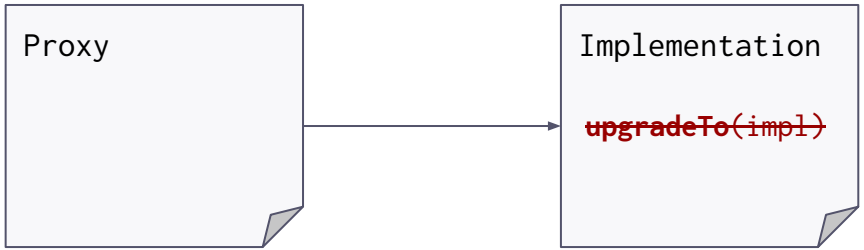
UUPS


Proxy
delegate
Implementation
upgradeTo(impl)
User/Admin
delegatecall

Hm? Delegatecall



UUPS - Drawbacks



* Complexity in implementation

* Risk of killing upgrades

Cost Comparison

	Transparent	UUPS
Proxy Deployment	740k + 480k ProxyAdmin	390k
Implementation Deployment	+ 0	+ 320k
Runtime Overhead	7.3k	4.9k

(unit = gas)

Upgrade the upgrade

* Customize authorization mechanism
    * Access control
    * Domain specific logic

Practice

Tools

OpenZeppelin Upgradeable Contracts

* @openzeppelin/contracts-upgradeable
  - UUPSUpgradeable
  - Ownable

OpenZeppelin Upgrades Plugins (Hardhat/Truffle)

* Security checks
* Deployment

Documentation

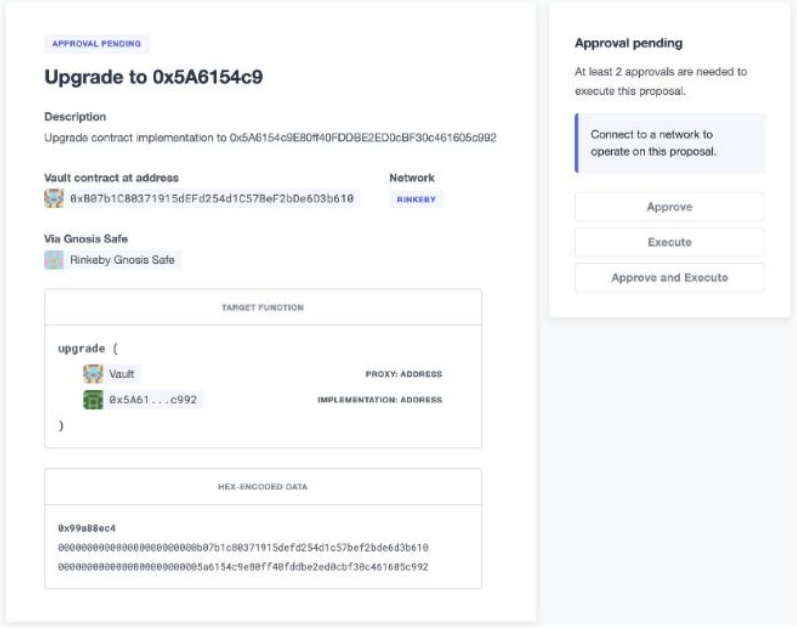
https://zpl.in/docs/upgrades

Defender Admin - Automate and secure all your smart contract administration

Use **multi-sigs** to administrate your contract to:

- Tweak critical parameters
- **Pause** in the event of an emergency
- **Upgrade** your contract to a new implementation

- No need for privileged access for Defender
- Simple UI
- Trigger workflows via API



docs.openzeppelin.com
blog.openzeppelin.com
forum.openzeppelin.com
defender.openzeppelin.com

Thank you!

Learn more

openzeppelin.com/**contracts**
forum.openzeppelin.com
docs.openzeppelin.com

Contact

@frangio_
frangio@openzeppelin.com