Production on the World Computer

Hi, I'm Kaushal

- SDE2 at Pedals Up
- CTO and Cofounder at getriff.xyz
- Builder

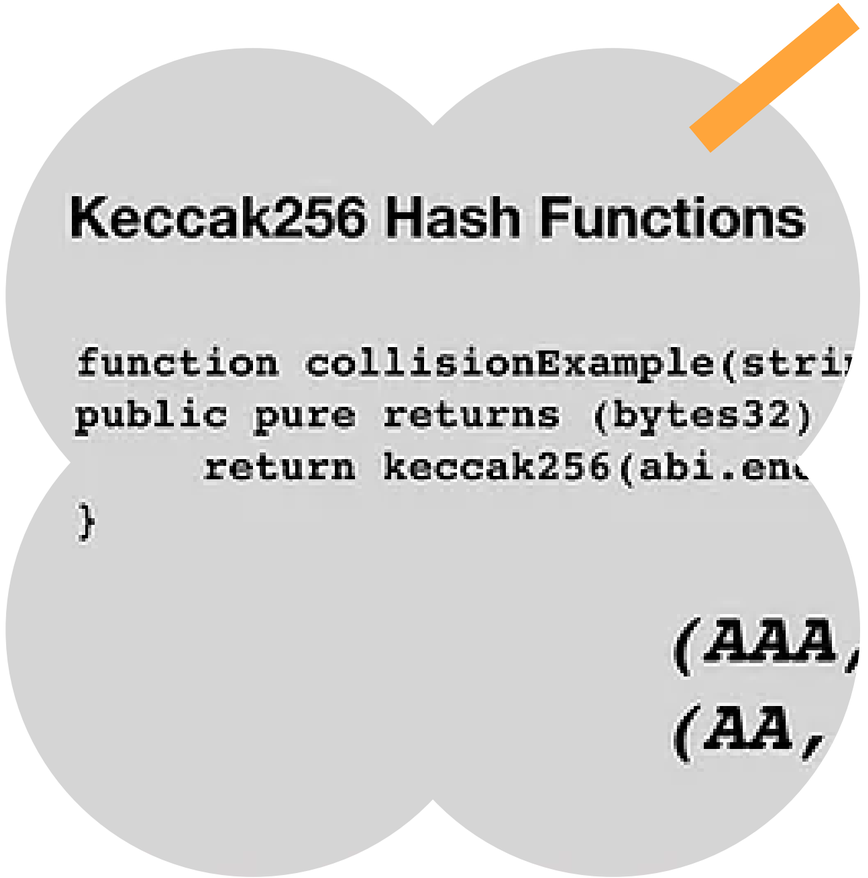
Twitter, Linkedin, Github, Instagram

ABI Encoding and Decoding

- Solidity Docs
- More Information

Hash In Solidity

- Hash
- Medium Blog on Keccak256
- Applied



Function Selectors

When a function is called, the first 4 bytes of calldata specifies which function to call. This 4 bytes is called a function selector.

```
bytes4(keccak256("foo(uint256,address,string,uint256[2])"))
```

- Solidity By Example
- Information

Delegate Calls

There exists a special variant of a message call, named delegatecall which is identical to a message call apart from the fact that the code at the target address is executed in the context of the calling contract and msg.sender and msg.value do not change their values.

Example

What can be a possible use of delegate calls?

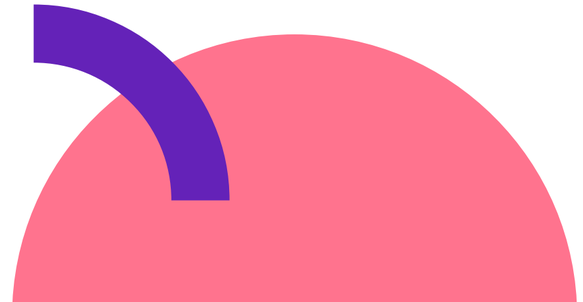
Proxy Contracts

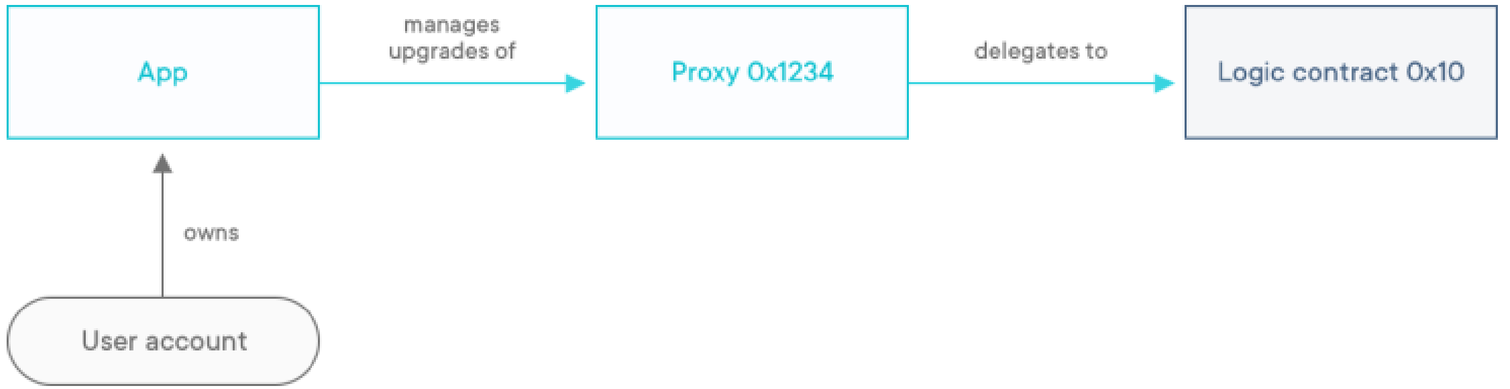
Advanced Resource: https://blog.openzeppelin.com/proxy-patterns/

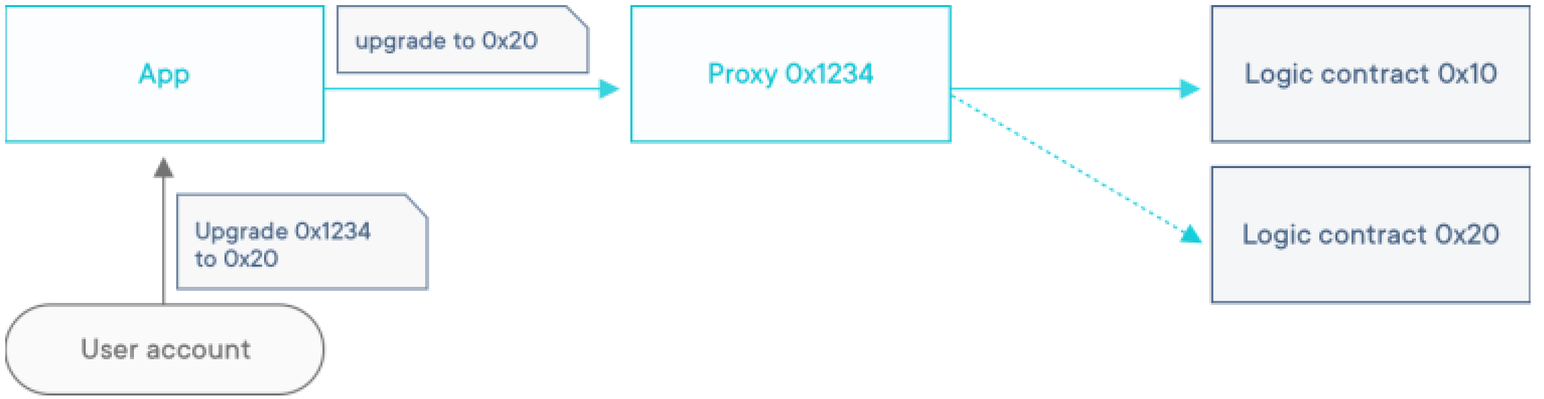
Transaparent Proxies

As explained, proxies work by delegating all calls to a logic contract that holds the actual code to be executed. Nevertheless, upgradeable proxies require certain functions for management of the proxy itself. At the very least, an `upgradeTo(address newImplementation)` function is needed in order to be able to upgrade the proxy to a new logic contract.

What can be the solution ?







msg.sender	owner()	upgradeTo()	transfer()
Admin	returns proxy owner	upgrades proxy	reverts
Other account	returns ERC20 owner	reverts	sends ERC20 transfer

Proxies

Solidity Storage

- Storage is a persistent read-write word-addressable space
- It is a key-value mapping of 2^256 slots of 32 bytes each. A contract can neither read nor write to any storage apart from its own. All locations are initially defined as zero.

Source

ERC-1967: Proxy Storage Slots

Before the big guns.

Let's discuss some applications

Vesting and Staking

Staking Interface as defined by EIP-900

Liquidity Pools

The term refers to a collection of tokens or digital assets locked in a smart contract that provide essential liquidity to decentralized exchanges.

Uses:

- Lending Tokens
- Swapping Tokens
- Trading Tokens

How do we design a liquidity pool smart contract?

Let's View a Full Stack Blockchain Application

Let's view some production ready smart contract code!

Diamonds, Multi-Facet Proxy

- EIP Proposal
- Everything Diamonds

Factory Pattern For Contracts

Resource