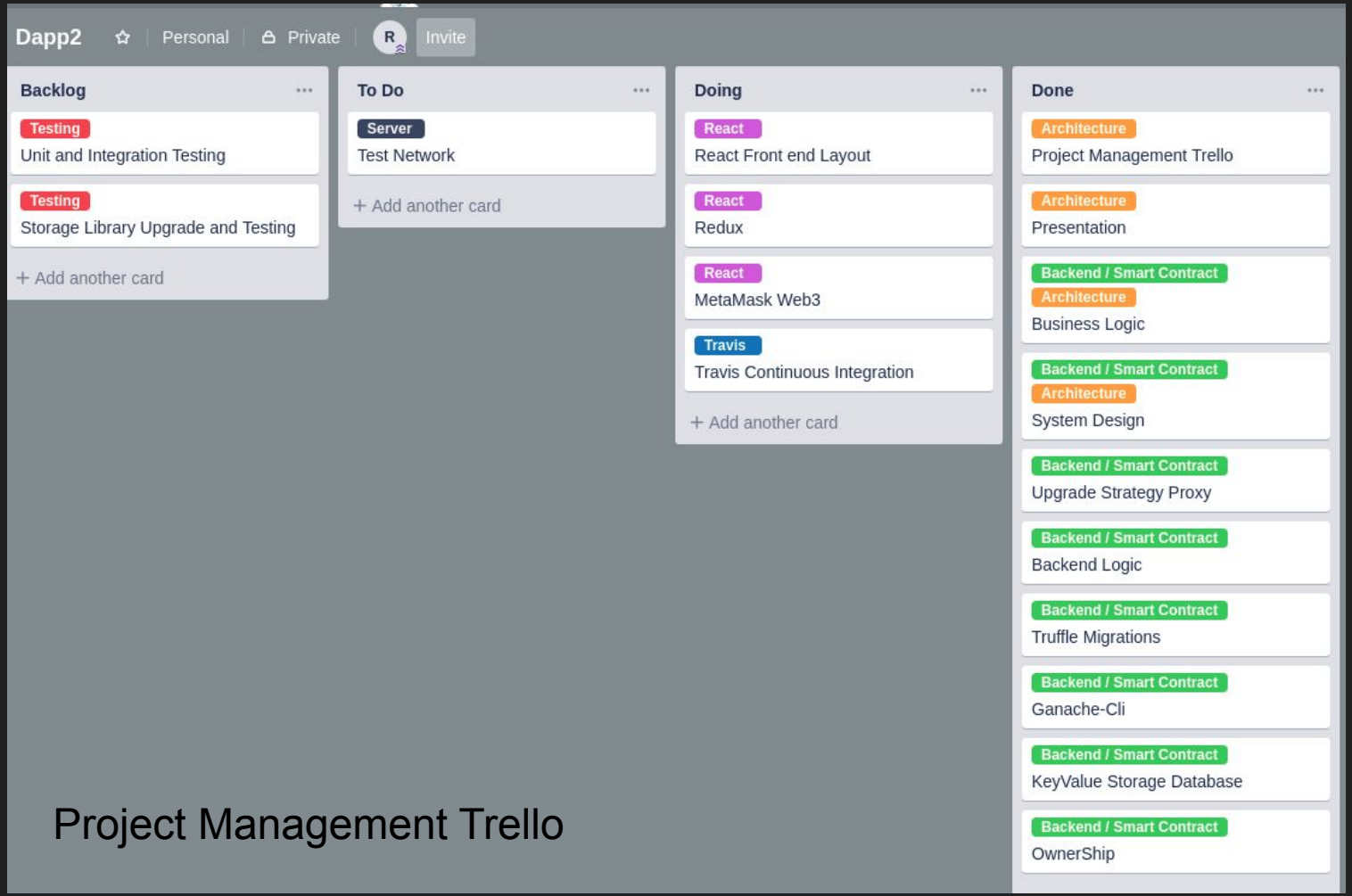
Upgradable Smart Contract

Proxy Contract



Project Management Trello

Why Upgrade Logic?

- Scalability
- Secure Code
- Unforeseen Bugs / Errors
- Gas Efficiency
- Code Readability
- Best Practices

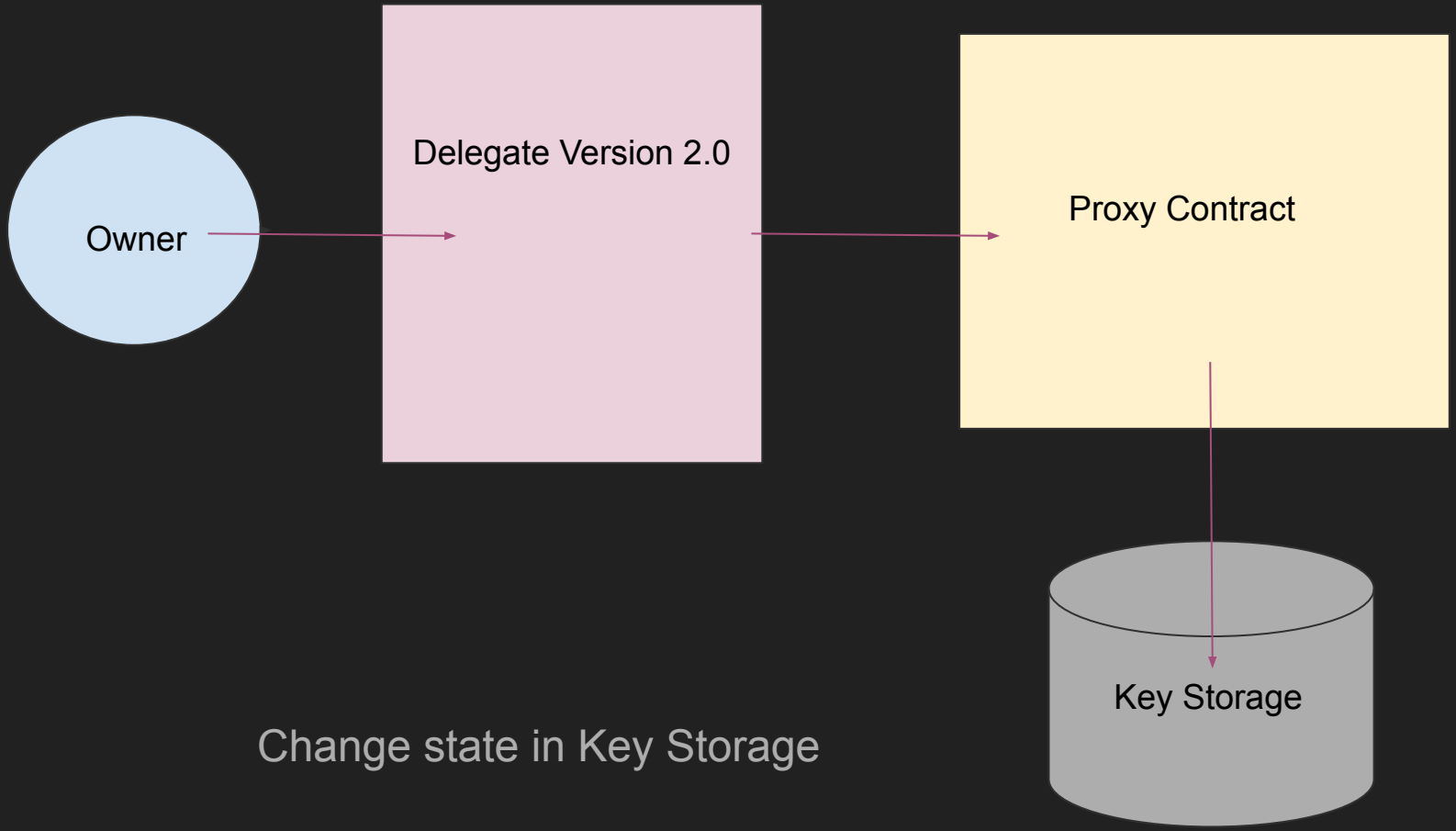
Pros:

- Offers more flexibility for Developers
- Easier for users migration

- Preserve State of original Contract
- External Storage via proxy contract
- Separate contract functionality
    - Allows multiple contracts to share the same state

Cons

- Ethics
- Trust in Developers
- Immutability:
  - Storage vs
  - Logic (unforeseen future bugs)

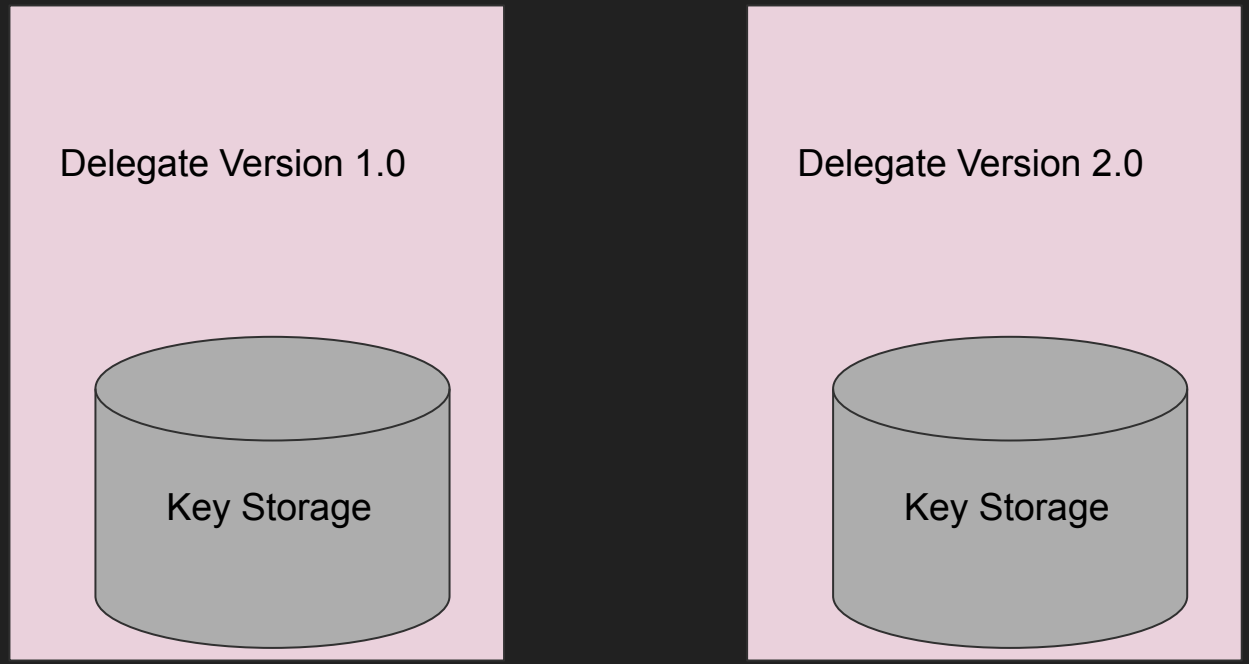


Change state in Key Storage

Implementation

- Delegate contract: Functionality / Logic

- Proxy Contract: Immutable Storage Contract
  - Storage Structure must be Compatible with one another
  - Order defined


Delegate Version 1.0
Key Storage
Delegate Version 2.0
Key Storage

Delegate Contract

- Dapp Functionality
- Local Copy of Key Storage
- If future bug is found:
  - Create new version
  - New Contract will also contain local copy
  - Reference to actual key storage deployed on Ethereum

- Potential bugs:
  - Modifiers
  - Safe Math
  - Etc

Key Storage Contract

- Common Storage
- Shared State Variables
  - All versions
- Getter and Setter functions
  - Update from Delegate Contract
  - Only Authorized Calls (msg.sender)
- Immutable
- Mappings
  - `mapping(address => mapping(bytes32 => address)) storageAddress;`
  - `mapping(address => mapping(bytes32 => uint256)) storageNum;`

Proxy Contract

- Logic contract is updated
  - Calling states in proxy contract
- Every user interacts with new Version

- Delegate call OpCode:

`0xf4`	DELEGATECALL	Message-call into this account with an alternative account's code, but persisting into this account with an alternative account's code	-	Complicated

Delegate Call

- Proxy Contracts accepts new address from Delegate Contract
  - Dynamically load code from a different address during runtime
  - Only code logic is taken from the called address
  - Storage, addresses still refer to Proxy contract

  - Both contracts need to define the same storage memory
    - Same order
  - Able to reuse library code in Proxy Storage Contract

Fallback Function - Assembly code

```
function () external payable {
       assembly {
           let ptr := mload(0x40)
           calldatacopy(ptr, 0, calldatasize)
           let result := delegatecall(gas, _current, ptr, calldatasize, 0, 0)
           let size := returndatasize
           returndatacopy(ptr, 0, size)

           switch result
           case 0 { revert(ptr, size) }
           default { return(ptr, size) }
       }
}
```

Reference: https://blog.zeppelin.solutions/proxy-libraries-in-solidity-79fbe4b970fd

Truffle Migrate

```
1_initial_migration.js
======================

   Deploying 'Migrations'
   ----------------------
   > transaction hash:    0x96b71cec3fab688be37f9557b8bb5487e620491dec66e5c30186a06d2b4c4b29
   > Blocks: 0            Seconds: 0
   > contract address:    0x0034b5a05FBA7e91F4a20407d8F7F7b683D5Dd60
   > account:             0xDB2A2A4F81fdEaFc2eF28B51eE67137059345B80
   > balance:             99.28311066
   > gas used:            284908
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.00569816 ETH

   > Saving artifacts
   -------------------------------------
   > Total cost:          0.00569816 ETH
```

```
2_Storage_migration.js
======================

   Replacing 'KeyValueStorage'
   ---------------------------
   > transaction hash:    0xa78a4390ef41e69ea2b69a305f6d1b4d565b65ad6e077ea6771c06b83be2fed9
   > Blocks: 0            Seconds: 0
   > contract address:    0xfaadb0fFDF488beCD1Dbc9E668B2dF0d8A3F5740
   > account:             0xDB2A2A4F81fdEaFc2eF28B51eE67137059345B80
   > balance:             99.26335248
   > gas used:            987909
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.01975818 ETH


   Replacing 'Proxy'
   -----------------
   > transaction hash:    0x67442f7e2c4c9107be366d4c50bb118497e80c4021f9d8dcae450cf14e40d027
   > Blocks: 0            Seconds: 0
   > contract address:    0xd314c42f6D8465f5E3cCf492cB30dFa2E1b00bfd
   > account:             0xDB2A2A4F81fdEaFc2eF28B51eE67137059345B80
   > balance:             99.2528118
   > gas used:            527034
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.01054068 ETH

   > Saving artifacts
   -------------------------------------
   > Total cost:          0.03029886 ETH
```

```
3_Final_migration.js
====================

   Replacing 'StorageLibrary'
   --------------------------
   > transaction hash:    0xe9d4be55e9bddd78c32a664dee79149f18dac3a29a77b61765711b325a2047bb
   > Blocks: 0            Seconds: 0
   > contract address:    0xA6b99520F2824394c94172433D5cF0666157F5Ed
   > account:             0xDB2A2A4F81fdEaFc2eF28B51eE67137059345B80
   > balance:             99.24526616
   > gas used:            377282
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.00754564 ETH


   Linking
   -------
   * Contract: LogicV2 <--> Library: StorageLibrary (at address: 0xA6b99520F2824394c94172433D5cF0666157F5Ed)

   Replacing 'LogicV2'
   -------------------
   > transaction hash:    0x7e7db74a22f6894307d1038007f420cb387b9478395314ff9573f6d6a74ccb35
   > Blocks: 0            Seconds: 0
   > contract address:    0xFF5D4E5553Bc0eb692752e55084De5F65C8876C6
   > account:             0xDB2A2A4F81fdEaFc2eF28B51eE67137059345B80
   > balance:             99.23299248
   > gas used:            613684
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.01227368 ETH
```

```
   Replacing 'LogicV1'
   -------------------
   > transaction hash:    0x8da139a643e0122a4cef9a4c8d838ef8f470a5b384f643633c1a956063aae903
   > Blocks: 0            Seconds: 0
   > contract address:    0x4F6E6d4ceEb55875FFEd9579D17Cd4824c364B2F
   > account:             0xDB2A2A4F81fdEaFc2eF28B51eE67137059345B80
   > balance:             99.21410464
   > gas used:            944392
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.01888784 ETH

   > Saving artifacts
   -------------------------------------
   > Total cost:          0.03870716 ETH


Summary
=======
> Total deployments:   6
> Final cost:          0.07470418 ETH
```