# Case Study

Given that we have access already to a rendering pipeline, media cluster, marketplace and backend wallet manager, we first have to separate what will be done by the smart contracts with what will be done off chain and what interfaces are required for the users to interact with.

First and foremost, since we are building a marketplace, we require a front end that is connected to our marketplace smart contract allowing trades of the assets  
  
We require a way for users to upload their projects and files to the media cluster and this will be our first smart contract, considering that the media cluster works similarly to Pinata then folders will separate the metadata and images as well as code for each project.  
Futhermore this smart contract (can also be separate) will also act as a project generator meaning it this is where the number of iterations are created and we can call this the generator contract. This will return a string pointing to the newly created folders of the user within their project.

All of this can easily be controlled via an interface so that the users never have to write their own smart contract.

## NFT Contract

In the next step, users can find an interface with various input fields allowing them to paste their ipfs link, set the number of editions (error checking required via the interface), set the price, opening time, link to their code, link to the project details which can be taken from the previous step or inserted by the user, list of splits, setting royalties and access lists. These input fields are directly correlated to variables in the smart contract that can be created upon hitting deploy and the user paying the fees.   
The smart contract itself will have predefined variables set by the user via the interface, with the possibility of editing them later. One of these variables is the whitelist location which is in the form of a link and we are using the merkle method to keep the list secure.

Some libraries we are importing are:  
 1.ERC721A since we are using fungible tokens and want to save some gas for people minting multiple nfts at once.

2.Ownable.sol to make sure that the user creating the contract is the owner and only they can change functions such as setting the price or enabling public mint.

3. ReentrancyGuard.sol to ensure that we do not have any reentrancies while minting and withdrawing at the same time.  
As an addition we can add a receive function to act as our fallback for when we are receiving ether without anyone minting

The project has a reveal and hide state which we can control by simply changing the link address which will be an onchain reveal function using the reveal function of the contract or simply filling the current link with the items we will be revealing or replacing the items of the current link with other items (note: In order to do this, we would have to avoid the use of IPFS). Lastly, we can also reveal and unreveal through the website by hiding the address and providing a placeholder container.

Our contract starts off as paused and we are using block timestamp as well as a set timer function to make sure that the minting does not start before the timer runs out.

Since we are using variables and with the correct privileges depending on the function call we are able to retrieve these variables, we are also able to send them to a database using an API while still giving access to the features of our smart contract to the users.

## Oracle and seed phrase

One of the tricky parts of the contract is seed generation since we do not want this to be predictable, we will avoid using blockhash or block.difficulty and instead use VRF with oracle functionality. The oracle itself in addition to the VRF can have a random number generation logic similar to our prototype oracle file we created here:

Marketplace  
We will assume at this point that our wallet has access to everything and no issue signing any of these transactions but if it does have issues then we would go about implementing it in the same way we are implementing metamask features or using a different token protocol for the tokens.  
  
The last piece of our ecosystem we have to create is a contract that handles the marketplace transactions that can also act as a monitoring tool for our users to research different projects on our website.  
For the purpose of saving time we are not implementing any external libraries at the moment but normally this contract would need to be written with care as to avoid many attacks. Our current setup allows users to use a marketplace with similar functions to seaport allowing them to list NFTs, make offers for tokens, make offers for projects, check some statistics and view various information such as metadata.  
  
Concerns

Some of these can be simple attacks like reentrancies or fallbacks but others can be harder to spot such as delegate calls, low level attacks, poor logic or even cross site scripting similar to the attack on opensea.  
Following this, access control is a major point for all contracts and making sure the correct view types are given to functions can make or break a contract.  
Furthermore gas is another concern for all of our contracts and having a smaller time constraint would allow us to make use of calldata, assembly code and using cheaper opcode functions and using custom errors to save gas rather than asserting, reverting etc..

Lastly, we want to make use of functions such as abi.encodePacked(), ecrecover, wad, manually setting v, r and s, permits, having checks for the nonce to avoid replay attacks and ensuring the security, anonymity or unpredictability of the random number generator, whitelist spots, contracts to be released and NFT transactions.

## Further Improvements

We can use proxies for NFT contracts, in particular beacon proxies if we want to hide some further logic and we could even use proxies for the random number generation.

We can avoid the use of constructors and also use upgradeable libraries such as safe erc20 upgradeable to make our NFT contracts upgradeable in case users want to release another collection as part of the same project and want to be able to show both of those collections on the same page in the marketplace.

Zero knowledge can also play a big part in our transactions whether we want to use them to have a better whitelist form or prove that we generate random numbers in a more authentic way.

## Examples to look at

Similar marketplace protocol done well: [ProjectOpenSea/seaport: Seaport is a marketplace protocol for safely and efficiently buying and selling NFTs. (github.com)](https://github.com/ProjectOpenSea/seaport)

Wallet: [Safe Core SDK Packages - Developer Docs](https://docs.safe.global/learn/safe-core/safe-core-account-abstraction-sdk/protocol-kit/core-sdk)

Oracle: [Generate Provably Fair Random Numbers in Solidity With Chainlink VRF](https://chain.link/vrf?&utm_medium=paid-search&utm_source=google&agid=051i73y9sn0e&cnid=44v2tu4ilo0a&utm_term=vrf&utm_campaign=FY23Q2_Always+On+-+Ad+Words_Conversion+-+VRF&utm_source=adwords&utm_medium=ppc&hsa_acc=8091600258&hsa_cam=19912913975&hsa_grp=146911387639&hsa_ad=652920215427&hsa_src=g&hsa_tgt=kwd-32737346&hsa_kw=vrf&hsa_mt=b&hsa_net=adwords&hsa_ver=3&gad=1&gclid=CjwKCAjwpayjBhAnEiwA-7enazqCrgNmspqaIg8q4g-HlKCfFvurT0bZpYikt1MfcViPlpVpFVSd6BoCDVYQAvD_BwE)

General EVM: [Ethereum Yellow Paper: a formal specification of Ethereum, a programmable blockchain](https://ethereum.github.io/yellowpaper/paper.pdf)  
Best Practices: [x676f64/secureum-mind\_map: Central Repository for the Epoch 0 coursework and quizzes. Contains all the content, cross-referenced and linked. (github.com)](https://github.com/x676f64/secureum-mind_map)  
Fuzzing tool (I personally contributed!! ;p ): [crytic/slither: Static Analyzer for Solidity (github.com)](https://github.com/crytic/slither)

Testing suite: [Introduction - Foundry Book (getfoundry.sh)](https://book.getfoundry.sh/)

IDE to test some attacks on goerli: [Remix - Ethereum IDE](https://remix.ethereum.org/)

OpenZeppelin libraries in depth: [Proxies - OpenZeppelin Docs](https://docs.openzeppelin.com/contracts/4.x/api/proxy)