NFT Locker: Decentralized Application to lock NFTs

Majid Babaei, Michael Buchar, Ezra Gomolin, Ege Karadibak, Dominic Chan (DP-37)

Vision

- Since blockchain was invented and numerous cryptocurrencies and other tools started using this technology, it has become rather evident that this technology has enormous potential.
- Blockchain is highly popular and seems not to be going away anytime soon, so it is crucial to consider it an essential technology.
- Moreover, many people use this technology for malicious activities, and scams in the crypto space have skyrocketed in the past years.
- Blockchain is widespread, and there are so many scams in the crypto space; we use NFTs and saw some problems in this technology.
- This project aims to increase the security aspects of NFTs for users from possible phishing attacks.

Problem/Challenges

- NFTs are popular and valuable assets due to blockchain technology. But there are risks of scams and phishing attacks. NFT Locker is designed to prevent such problems by allowing users to store their assets in a smart contract.
- One of the main challenges of the project is developing a secure smart contract that can effectively lock and transfer the ownership of the NFTs to the contract. This requires a thorough understanding of blockchain technology and smart contract development, as well as a keen attention to detail to ensure that the smart contract functions as intended.
- Another challenge is ensuring that the website is user-friendly and easy to navigate. This requires a focus on user experience design and implementing intuitive features that allow users to easily lock and unlock their NFTs.
- Overall, the proposed project aims to address the challenges of NFT ownership through the development of a secure and user-friendly website that allows users to lock their NFTs using a smart contract

Target Audience

- Are you interested in new technologies? Interested in Blockchain?
- Have you delved into Blockchain yet and got some Ether or any other crypto?
- Are you afraid of cyber scams and keeping your assets such as NFTs safe?
- If you said yes to any of these, this website is for you! We are creating a simple, easy-to-use application where you can securely store your NFTs (Non-Fungible Tokens) for as many days as you want.
- It is really easy to get started and get your first NFTs, simply log into or create your Metamask wallet and import your wallet in the application.
- You will never have to worry about being scammed again since the NFTs cannot be retrieved until the locking period expires!

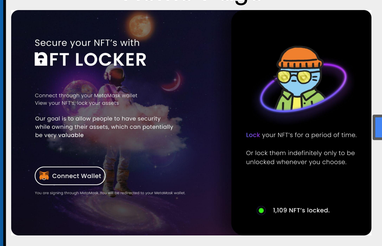
Security

- For each user we must create our own data structure and have a list of that data structure for each user to keep track of which NFTs they have staked, for how long and what NFT smart contract they belong to. Most staking contracts at the moment just have to store a list corresponding to tokenIDs that a user is staking because it is hardcoded into their contract which NFT collection (their own) can be stored in their contract.
- Security is a very important component for our application, and when designing our smart contract we had to ensure it was easy to understand, robust and simple.
- The most important aspect of our application was to ensure that the NFT that a user locks up can only be returned to that user. This is really the only security concern and to ensure that it was important that we searched the mapping and added to the mapping of the user msg.sender. msg.sender in solidity is essentially the user that has submitted the transaction on the blockchain; this means that no one can ever remove or add NFTs to the mapping of anyone but themselves as that only occurs upon a transaction.

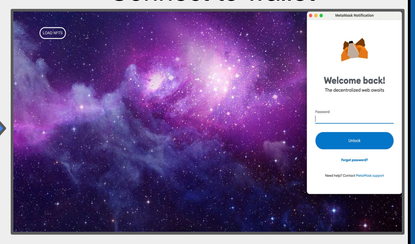
Methodology

- Our solution was to create a website application that allows users to lock their NFTs safely and securely.
- The user can use our application to select the NFTs they want locked, so that it cannot be subject to scams and malicious activity unbeknownst to the user.
- This feature works by transferring the ownership of the user's NFT to the smart contract designed for the website, where it will stay locked and secured until the number of days the user has chosen to lock it for passes.
- The NFT can then be unlocked and transferred back to the user's wallet from the smart contract.

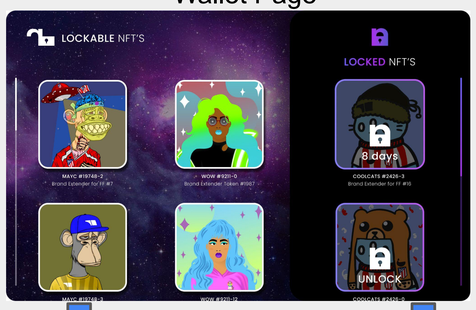
Home Page



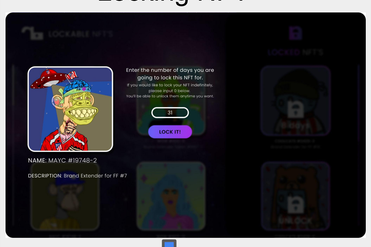
Connect to wallet



Wallet Page

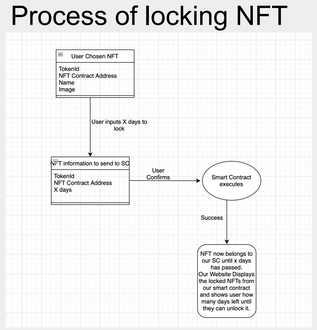


Locking NFT

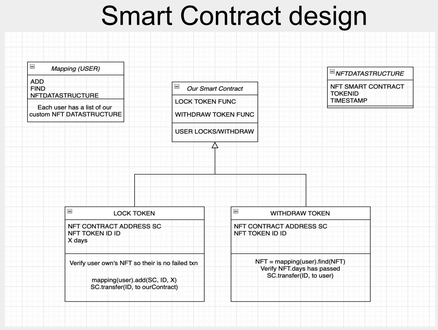


Unlocking NFT

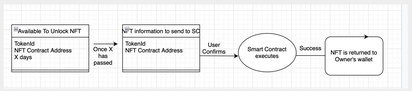
Process of locking NFT



Smart Contract design



Process of unlocking NFT



Smart Contract

- The smart contract contains a struct which defines a NFT object, with tokenId, add, withdrawal date, and imageLink as its properties.
- The mapping function maps a list of custom data structures for each user's Ethereum address, which is used for locking and unlocking NFTs by adding and removing them to/from this list.
- The locking functionality allows for the transfer of NFTs to the smart contract and storing them in the user's mapping for later withdrawal.
- The unlocking functionality iterates through the mapping, verifies the withdrawal date, transfers the token back to the user, and removes the NFT from the mapping.

Work Accomplished

- Frontend: React.JS; React was used as it allows for the use of existing Web3.js libraries to easily allow us to connect our website to the Blockchain as well as easily interacting with external APIs.
- Our contract has two main functionalities, one being locking a token and the second being withdrawing a token. The figure on the left outlines the design of our smart contract which will be developed next semester. Utilizing the Web3.js javascript library we will be able to send transactions to our smart contract from our front end.
- Walkthrough:
  - A user first signs into our application using their Ethereum Public key.
  - When a user clicks on sign in, it prompts Metamask using Web3.js library and allows the user to connect to our website.
  - Once connected when a user wishes to view all their NFTs, our website uses Alchemy's API (a free API for NFTs) in order to retrieve all the NFTs that a user owns and display them as a gallery.
  - Then a user can lock a given NFT by clicking on it and specifying the number of days (non-negative number) they want to lock the NFT for.
- Front-end application almost complete:
  - A user can sign in to our application with their metamask wallet and our website displays their NFTs as a gallery.
  - The user can browse through this gallery and can input how many days they want to lock their NFT for.
  - Then this information gets sent to the smart contract that locks the NFT and fulfills the request.
  - Only minor tweaks with regards to the front-end are planned and that is changing the colors and fonts to make the text a little more readable and making the connect wallet functionality somewhat more seamless.

Conclusion

- With the rise of NFTs also came many attackers against specific individuals in order to retrieve their valuable assets and capitalize off them. Inadvertently clicking on a hyperlink or approving a seemingly authentic transaction has resulted in significant financial losses ranging from hundreds to hundreds of thousands of dollars for numerous individuals.
- Our project holds immense significance and worth, as we aim to enhance the security measures surrounding people's assets, thus curtailing several of these malicious assaults.
- Our ultimate objective is to develop an all-inclusive decentralized application that enables users to interface with the blockchain via our web application.
- Our web app displays all their NFTs and enables users to lock them up in a smart contract that only releases them to their rightful owner after the time they requested has passed.
- The underlying drive of this project is to facilitate individuals with a safeguarded means of possessing their assets, which may hold considerable value.