Blockchain Project 2022

Primiano Arminio Cristino: primiano.cristino@studio.unibo.it
Francesco Palmisano: francesco.palmisano2@studio.unibo.it

Outlines

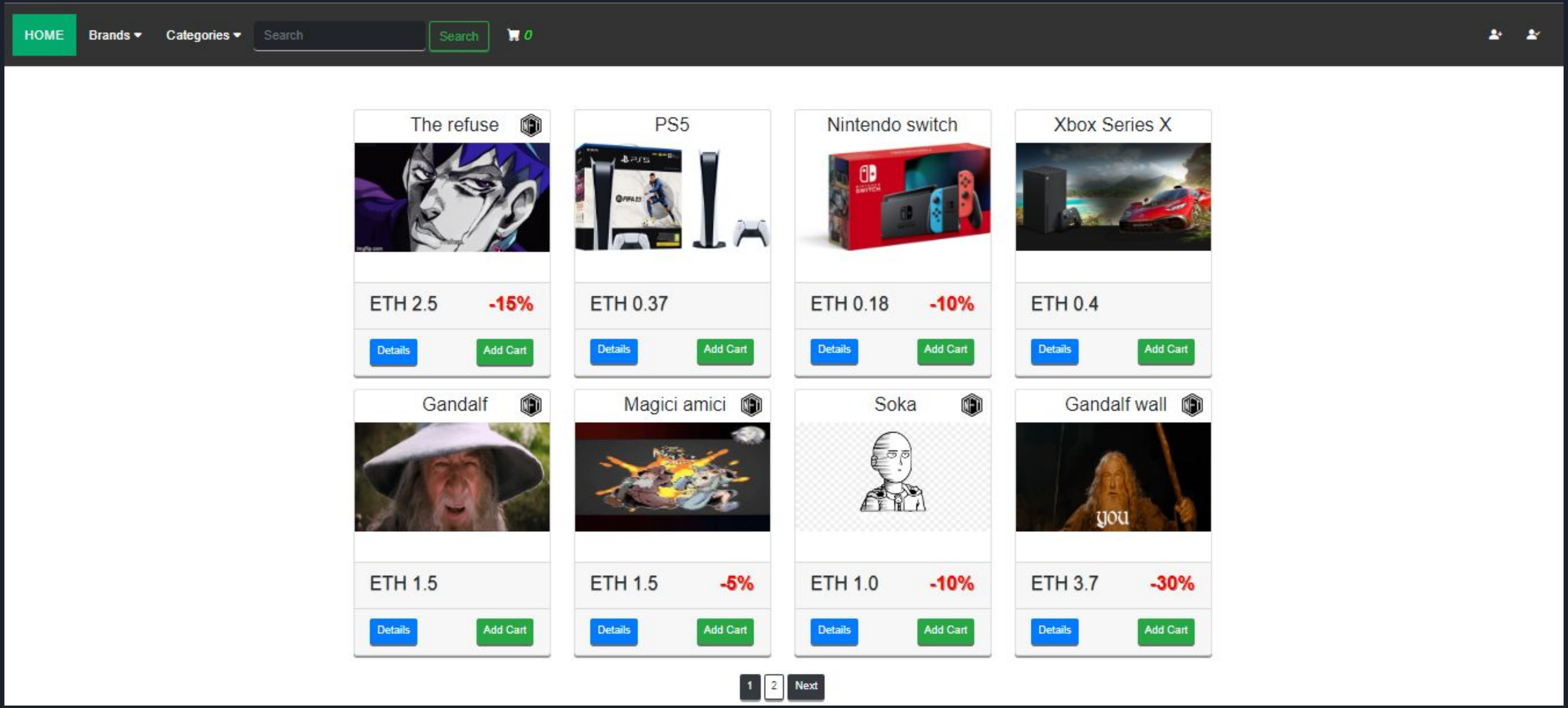
- DAPP infrastructure
  - Metamask
  - Buying & Selling
- Contract infrastructure
  - DEX
  - ERC-20 Token
  - ERC-721 Token
- Security treats
  - NFT term conditions
  - NFT forging and stealing
- Conclusion

DAPP infrastructure

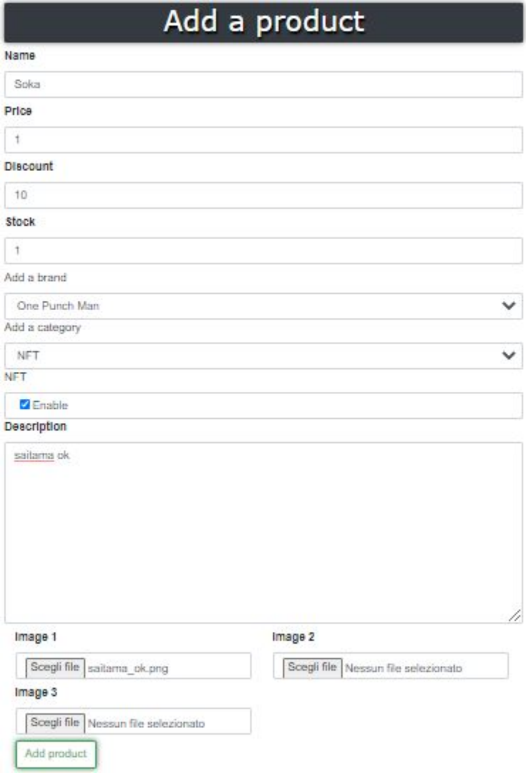
MetaMask

- To test the interaction with contracts we tried to use the Web3 python library.
- Web3py directly manages users private key.
- For this reason we decided to use Web3js that interacts with a proper remote wallet (e.g. MetaMask).
- Thus, we created a MetaMask wrapper to execute solidity transactions.

Home Page


HOME
Brands ▾
Categories ▾
Search
Search
0
The refuse
ETH 2.5
-15%
Details
Add Cart
PS5
ETH 0.37
Details
Add Cart
Nintendo switch
ETH 0.18
-10%
Details
Add Cart
Xbox Series X
ETH 0.4
Details
Add Cart
Gandalf
ETH 1.5
Details
Add Cart
Magici amici
ETH 1.5
-5%
Details
Add Cart
Soka
ETH 1.0
-10%
Details
Add Cart
Gandalf wall
you
ETH 3.7
-30%
Details
Add Cart
1
2
Next

Add and edit a product



Add a product

Name: Soka

Price: 1

Discount: 10

Stock: 1

Add a brand: One Punch Man

Add a category: NFT

NFT: ☑ Enable

Description: saitama ok

Image 1: Scegli file saitama_ok.png

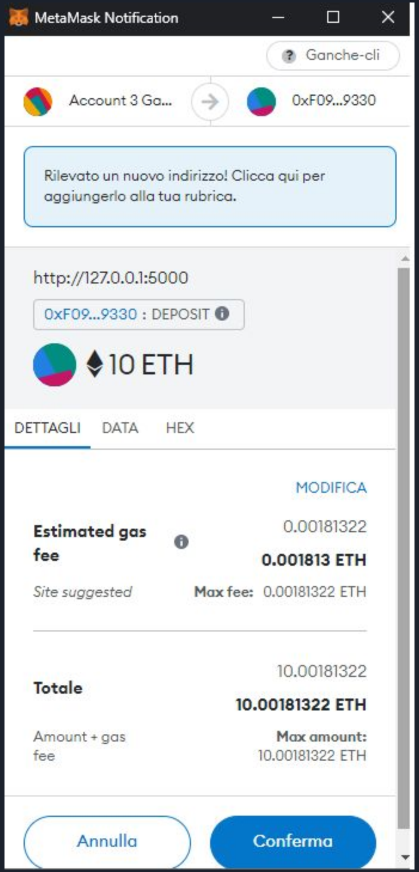
Image 2: Scegli file Nessun file selezionato

Image 3: Scegli file Nessun file selezionato

- When a product is added, the customer can decide whether the product is an NFT or not.

- In particular the stock and image for an NFT must be one.

Deposit and Withdraw



Rilevato un nuovo indirizzo! Clicca qui per aggiungerlo alla tua rubrica.

http://127.0.0.1:5000

0xF09...9330 : DEPOSIT

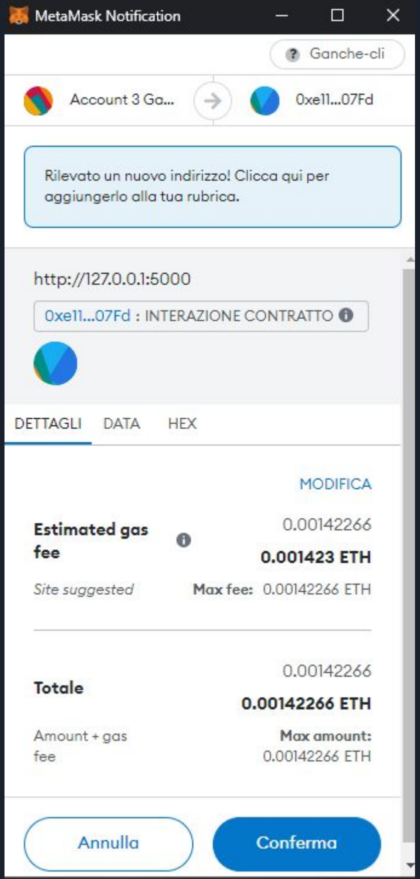
10 ETH

Estimated gas fee 0.00181322 **0.001813 ETH**

Site suggested **Max fee:** 0.00181322 ETH

Totale 10.00181322 **10.00181322 ETH**

Amount + gas fee **Max amount:** 10.00181322 ETH



Rilevato un nuovo indirizzo! Clicca qui per aggiungerlo alla tua rubrica.

http://127.0.0.1:5000

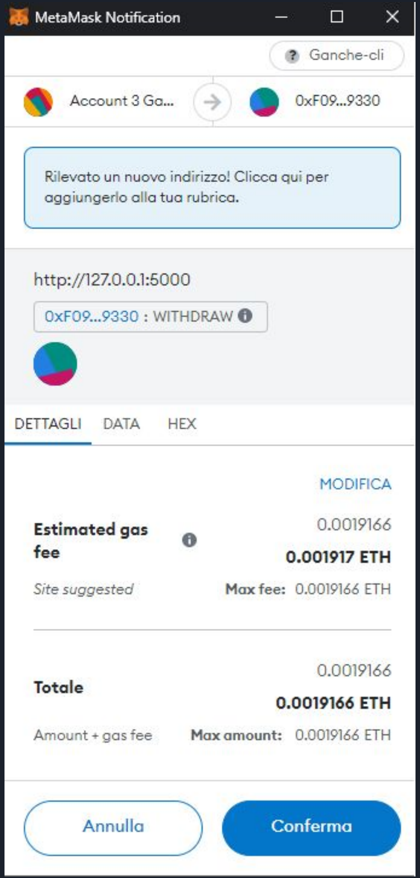
0xe11...07Fd : INTERAZIONE CONTRATTO

Estimated gas fee 0.00142266 **0.001423 ETH**

Site suggested **Max fee:** 0.00142266 ETH

Totale 0.00142266 **0.00142266 ETH**

Amount + gas fee **Max amount:** 0.00142266 ETH



Rilevato un nuovo indirizzo! Clicca qui per aggiungerlo alla tua rubrica.

http://127.0.0.1:5000

0xF09...9330 : WITHDRAW

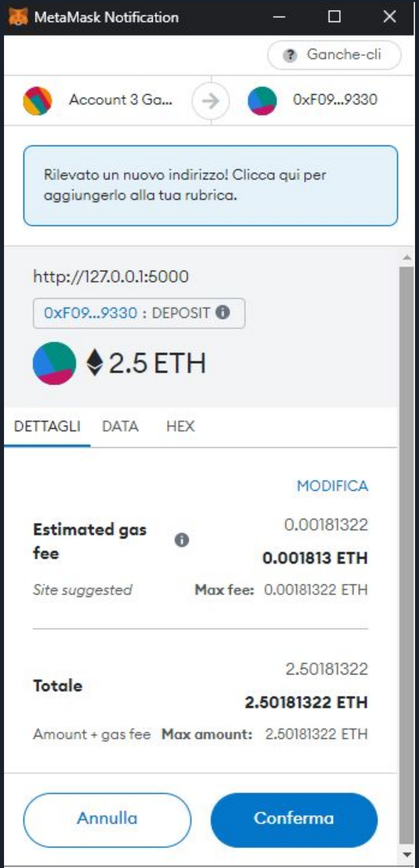
Estimated gas fee 0.0019166 **0.001917 ETH**

Site suggested **Max fee:** 0.0019166 ETH

Totale 0.0019166 **0.0019166 ETH**

Amount + gas fee **Max amount:** 0.0019166 ETH

Buy a Product



Account 3 Ga... → 0xF09...9330

Rilevato un nuovo indirizzo! Clicca qui per aggiungerlo alla tua rubrica.

http://127.0.0.1:5000

0xF09...9330 : DEPOSIT

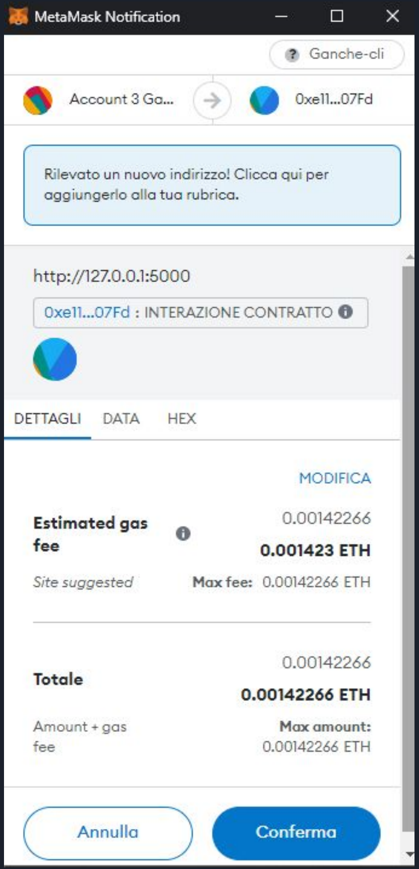
2.5 ETH

Estimated gas fee 0.00181322 **0.001813 ETH**

Site suggested **Max fee:** 0.00181322 ETH

Totale 2.50181322 **2.50181322 ETH**

Amount + gas fee **Max amount:** 2.50181322 ETH



Account 3 Ga... → 0xe11...07Fd

Rilevato un nuovo indirizzo! Clicca qui per aggiungerlo alla tua rubrica.

http://127.0.0.1:5000

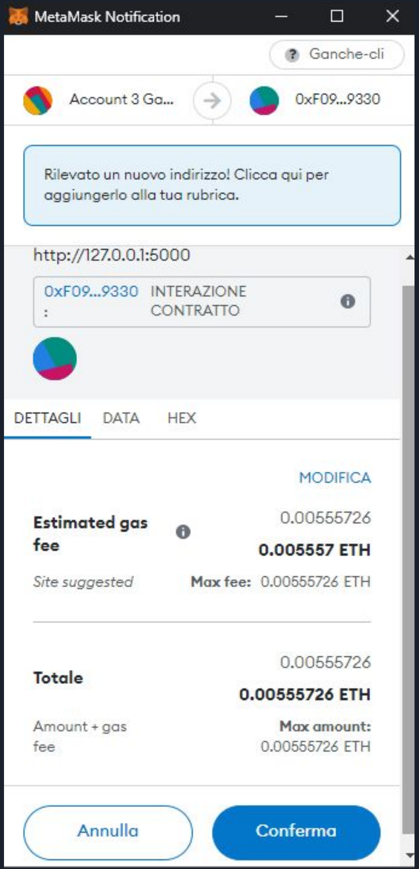
0xe11...07Fd : INTERAZIONE CONTRATTO

Estimated gas fee 0.00142266 **0.001423 ETH**

Site suggested **Max fee:** 0.00142266 ETH

Totale 0.00142266 **0.00142266 ETH**

Amount + gas fee **Max amount:** 0.00142266 ETH



Account 3 Ga... → 0xF09...9330

Rilevato un nuovo indirizzo! Clicca qui per aggiungerlo alla tua rubrica.

http://127.0.0.1:5000

0xF09...9330 : INTERAZIONE CONTRATTO

Estimated gas fee 0.00555726 **0.005557 ETH**

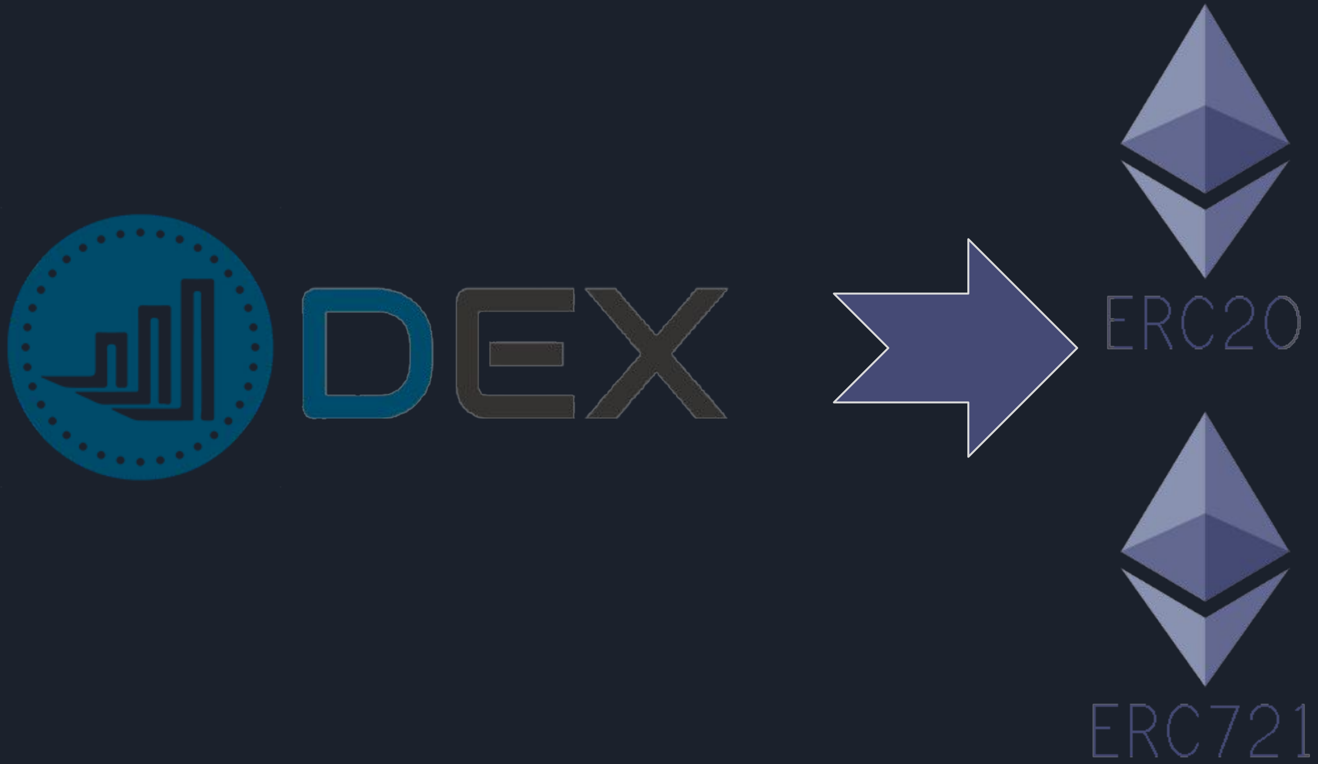
Site suggested **Max fee:** 0.00555726 ETH

Totale 0.00555726 **0.00555726 ETH**

Amount + gas fee **Max amount:** 0.00555726 ETH

Contracts infrastructure

DEX (Decentralized Exchange)



DEX

ERC20

ERC721

DEX (Decentralized Exchange)

- Deposit/Withdraw tokens
- Add/Update/Delete products
- Store products information

ERC-20 Token

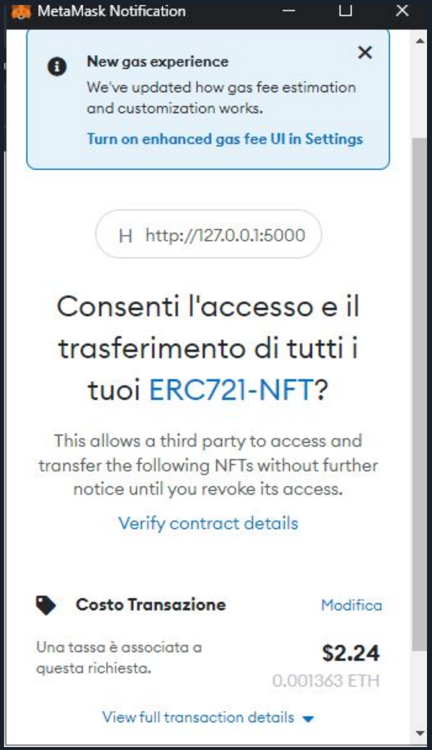
- Approve and transfer tokens from and address to another with DEX as intermediate.
- Associate a proper allowance to DEX contract.

ERC-721 Token

- Generate/Burn NFTs.
- Ensure NFT uniqueness.
- Avoid NFT stealing and forging (contract-side).
- Provide NFT URI.

Security threats

NFT Term conditions



New gas experience

We've updated how gas fee estimation and customization works.

Turn on enhanced gas fee UI in Settings

H http://127.0.0.1:5000

Consenti l'accesso e il trasferimento di tutti i tuoi ERC721-NFT?

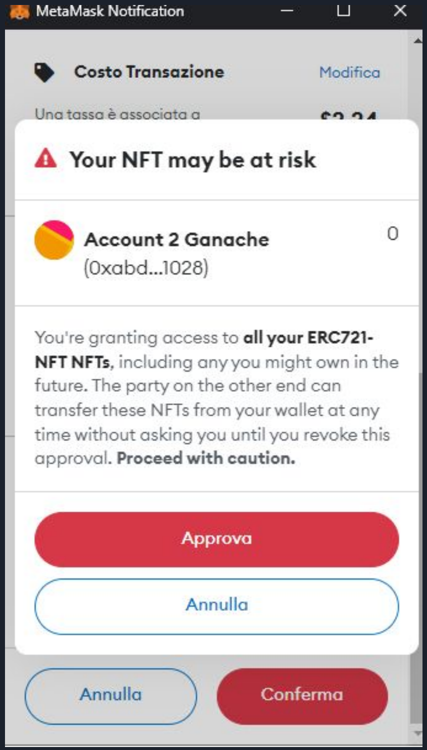
This allows a third party to access and transfer the following NFTs without further notice until you revoke its access.

Verify contract details

Costo Transazione Modifica

Una tassa è associata a questa richiesta. **$2.24** 0.001363 ETH

View full transaction details



Costo Transazione Modifica

Una tassa è associata a

Your NFT may be at risk

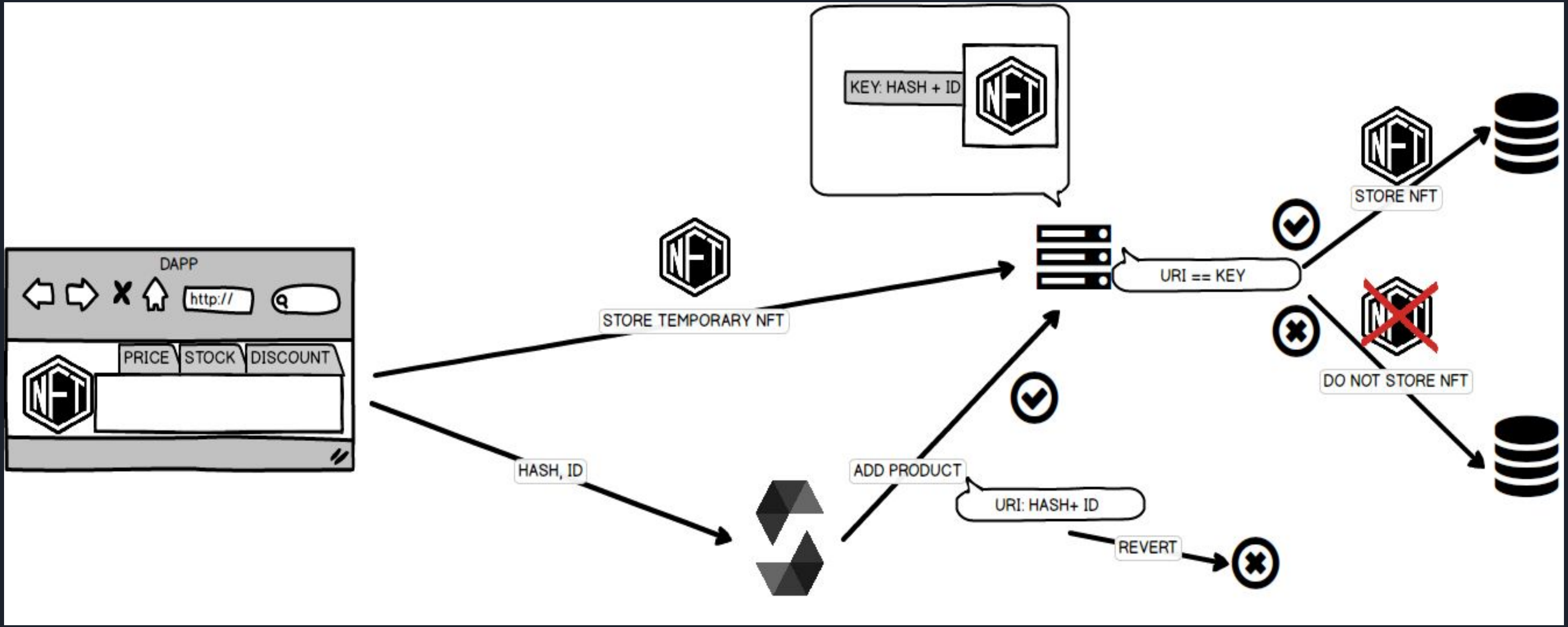
Account 2 Ganache 0
(0xabd...1028)

You're granting access to **all your ERC721-NFT NFTs**, including any you might own in the future. The party on the other end can transfer these NFTs from your wallet at any time without asking you until you revoke this approval. **Proceed with caution.**

As soon as a new customer registers at the DAPP, he/she can decide whether let the application managing its NTFs.

Otherwise, the customer can approve them singularly.

Dealing with NFT



Conclusion

Let’s see the demo.