Project writeup

Background

In this project a token called Tom Property Listing TPL to represent owner title to the properties. Before a token is minted, owner need to verify his ownership to his property. zk-SNARKs is used to create a verification system which can prove owner has title to the property without revealing that specific information on the property.

Once the token has been verified you will place it on a blockchain market place (OpenSea) for others to purchase.

Technical specification

Version

Truffle v5.1.21 (core: 5.1.21)
Solidity - 0.5.2 (solc-js)
Node v9.4.0
Web3.js v1.2.1

Contract Address: 0x47FB7b2E4Dfb78A90306B2feCBF16BaF0c78d7Ea

Setup development environment

Code: https://github.com/ymlai87416/blockchain-nanodegree-capstone

Install

This repository contains Smart Contract code in Solidity (using Truffle), tests (also using Truffle), webapp (using HTML, CSS and JS)

To install, download or clone the repo, then:

```
npm install
cd eth-contracts
truffle compile
```

Develop Client

Ganache is required to click start the project.

To run Ganache

```
ganache-cli -m "candy maple cake sugar pudding cream honey rich smooth
crumble sweet treat" -a 50 -l 9999999 -q
```

To run truffle tests:

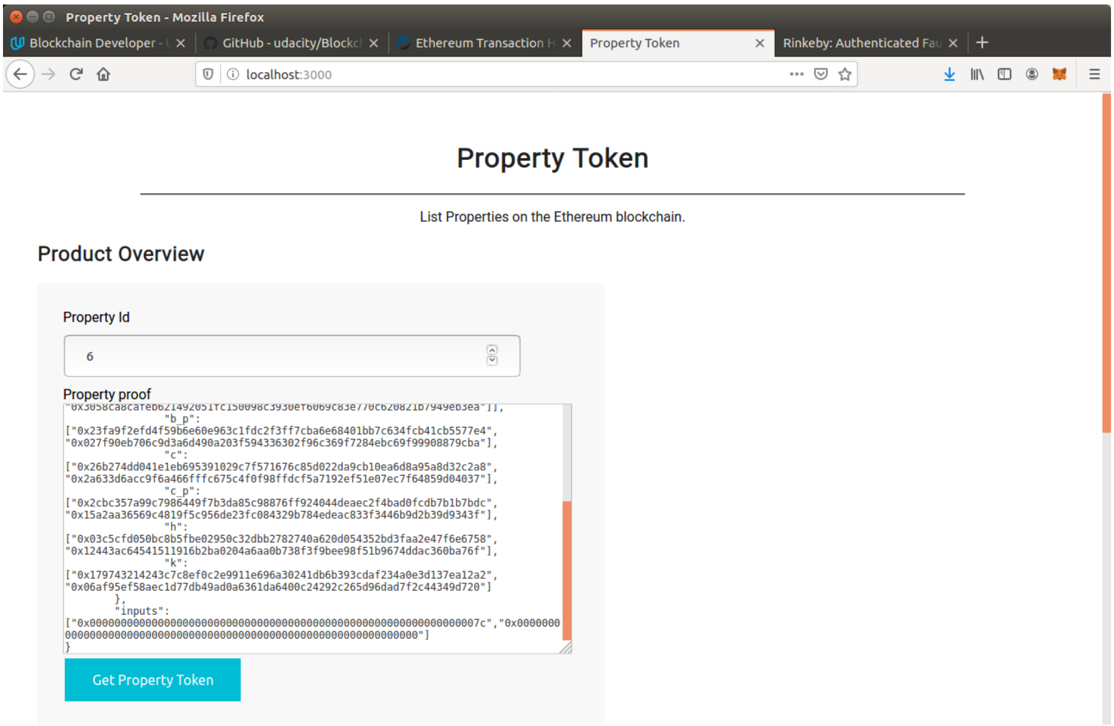
```
truffle test ./test/TestERC721Mintable.js
truffle test ./test/TestSolnSquareVerifier.js
truffle test ./test/TestSquareVerifier.js
```

To use the webapp

```
truffle migrate --reset --network development
npm run dev
```

To view dapp:

```
http://localhost:3000
```



Property Token

List Properties on the Ethereum blockchain.

Product Overview

Property Id

6

Property proof

```
"0x3058ca8cafeb6214920 51fc150098c3930ef6069c83e770c620821b7949eb3ea"]],
                "b_p":
["0x23fa9f2efd4f59b6e60e963c1fdc2f3ff7cba6e68401bb7c634fcb41cb5577e4",
"0x027f90eb706c9d3a6d490a203f594336302f96c369f7284ebc69f99908879cba"],
                "c":
["0x26b274dd041e1eb695391029c7f571676c85d022da9cb10ea6d8a95a8d32c2a8",
"0x2a633d6acc9f6a466fffc675c4f0f98ffdcf5a7192ef51e07ec7f64859d04037"],
                "c_p":
["0x2cbc357a99c7986449f7b3da85c98876ff924044deaec2f4bad0fcdb7b1b7bdc",
"0x15a2aa36569c4819f5c956de23fc084329b784edeac833f3446b9d2b39d9343f"],
                "h":
["0x03c5cfd050bc8b5fbe02950c32dbb2782740a620d054352bd3faa2e47f6e6758",
"0x12443ac64541511916b2ba0204a6aa0b738f3f9bee98f51b9674ddac360ba76f"],
                "k":
["0x179743214243c7c8ef0c2e9911e696a30241db6b393cdaf234a0e3d137ea12a2",
"0x06af95ef58aec1d77db49ad0a6361da6400c24292c265d96dad7f2c44349d720"]
        },
        "inputs":
["0x000000000000000000000000000000000000000000000000000000000000007c","0x0000000
000000000000000000000000000000000000000000000000000000000"]
}
```

Project specification

ERC721 is implemented in eth-contracts\contracts\ERC721Mintable.sol

The test code is at: eth-contracts\test\TestERC721Mintable.js

Zokrates program which test user ability to calculate square of a number
DSL code: zokrates\code\square\square.code
Verifier contract: zokrates\code\square\verifier.sol
Proof example: User proof that he knows how to calculate square, and give the answer of 3^2 = 9

```
{

    "proof": {

        "a": ["0x1e738b5a44c64d7b772ccc2638496b61ce2e852a95b4ec05246a492f0bab3328",

"0x0260c2177894ced90fc0e8ba79170fc0931c07f7ce777af678abd19132e9bb51"],

        "a_p": ["0x076ff328f180b1e0836b13292a484908ea0708dff5b67e8b9da93081d060d6b4",

"0x12eab1a35b78d57be773f508653d6cebb655cfeecbd0f66167b768118f087548"],

        "b": [["0x1564b152ed44ae5fe0ff3c6a4666ddfc82a74cb1b1c2695bb0f7519f18d27c2b",

"0x26500b7902b193c5d6563ef82671b2d1a64598fcc74e37ac0422c3f0ba42850a"],

["0x1ef319e08716bbcd5c54cc3a4c441493e1f01311879cfc7ab14169769adb8a7f",

"0x18cf7d855a38cacd2ffd9089fa5abb64361d9457cf3e57e807ca728f41cbf35f"]],
        "b_p": ["0x09acf2c8afbc862a53af9e33c56ff411b40aa8d4d68491d7bb78c2d15bfeb57a",
"0x06dde9b2e64642ca6563772a9180eabaad94cc2cfc00d4a7309b0c1ac7fd5ff7"],
        "c": ["0x1857b53c85560029c4bed676d75ee9867fb981b35193503f39323e1f4d3f231e",
"0x1565ab0ecbf9369484a944e7ad9998a4f53b5fb7d7d4247a5398f8e142da08ad"],
        "c_p": ["0x2026b17ff8900e55e4ef72321a733effeb56abbff35ba482c3aedec8e4336dbd",
"0x29ca5e93cff02132c9e78cac9aa69754a341657223bd44800f9e089a6fadf62e"],
        "h": ["0x23fb5b0fcf2ef8d11c655dd7f48bd17ceda9734f85481cabe897ee8839b596fe",
"0x16405a652c433ca5a5f59a97aea4e3e6ac3fe5898fc39fa0a6f6371176329726"],
        "k": ["0x0e434812f972a2f3eeaeea21a8fb78d4cecfc823aa66d82b8d8b9228de9c7bdb",
"0x2753b6627019c510fd6dfe9fe31dfc2d6a10cd44e172b886c6ccbdf94e0596e9"]
    },
    "inputs":
["0x0000000000000000000000000000000000000000000000000000000000000009","0x0000000000000
000000000000000000000000000000000000000000000000001"]
}
```

The final contract SolnSquareVerifier is an ERC721 token contract, and only mint ERC721 tokens upon user proof that they can calculate the square of a number.

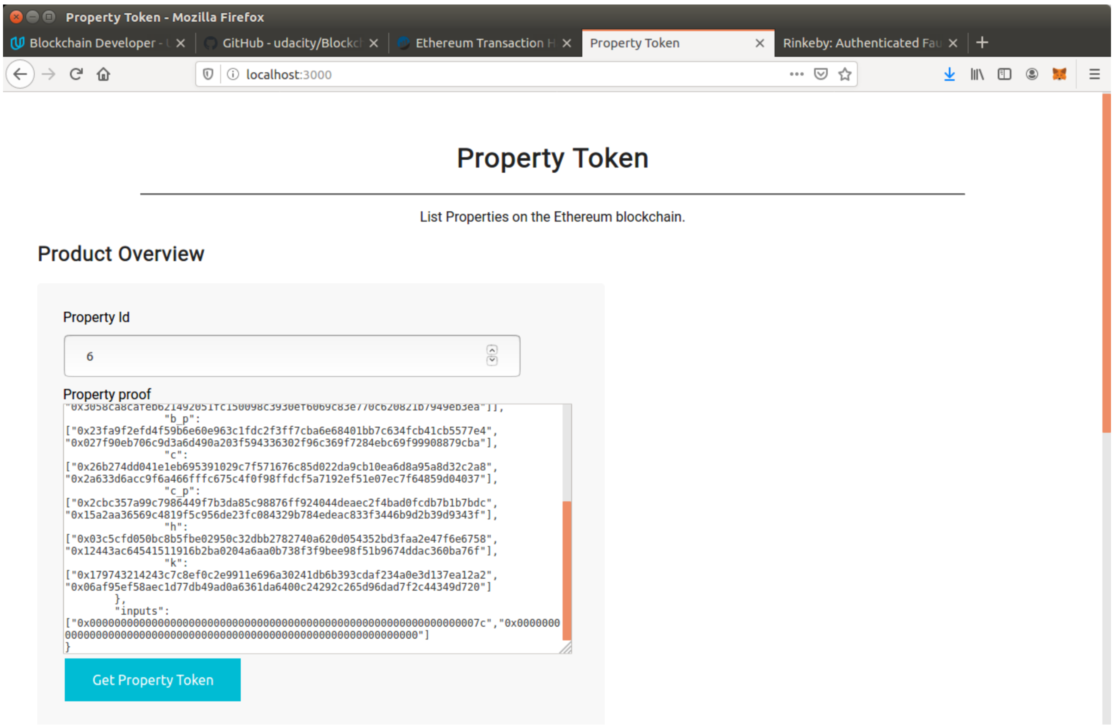
Code: `eth-contracts\contracts\SolnSquareVerifiier.sol`

Test:

- `eth-contracts\test\TestSquareVerifier.js`
- `eth-contracts\test\TestSolnSquareVerifier.js`

The contract is deployed on Rinkeby network at address:
0x47FB7b2E4Dfb78A90306B2feCBF16BaF0c78d7Ea

Using the webapp, 10 tokens are minted.
In the webapp, one has to provide the token id and the proof in order to mint a token.



Property Token

List Properties on the Ethereum blockchain.

Product Overview

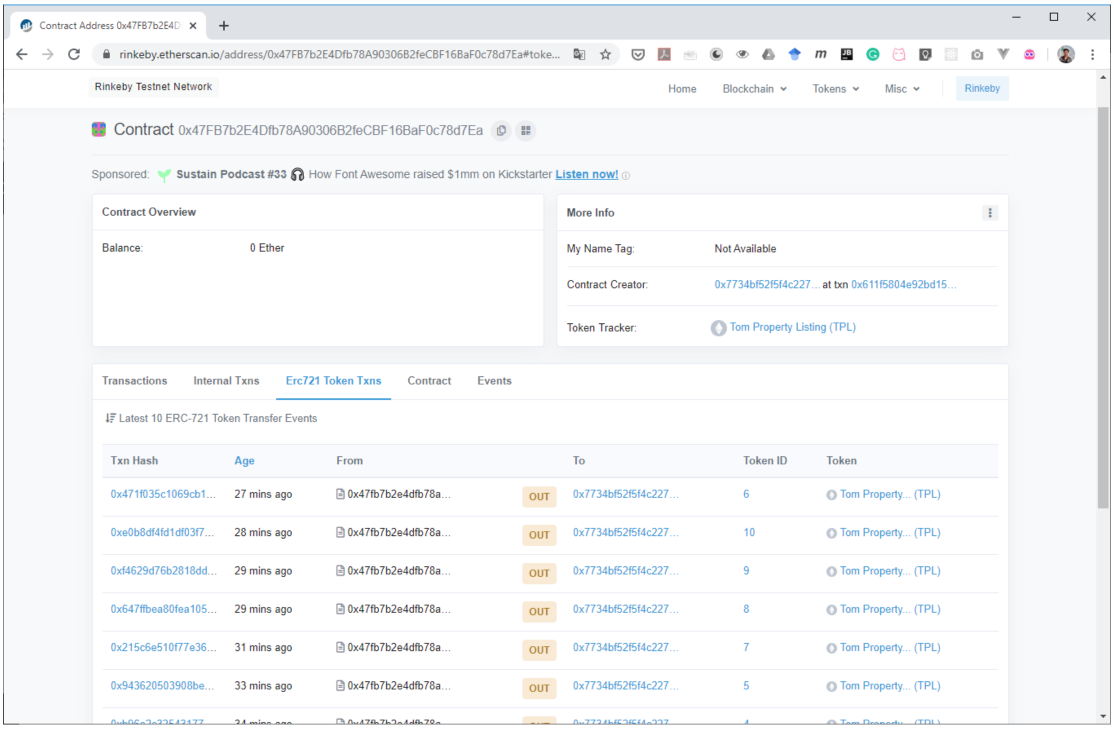
Property Id

6

Property proof

```
"0x3058ca8cafeb6214920 51fc150098c3930ef6069c83e770c620821b7949eb3ea"]],
                "b_p":
["0x23fa9f2efd4f59b6e60e963c1fdc2f3ff7cba6e68401bb7c634fcb41cb5577e4",
"0x027f90eb706c9d3a6d490a203f594336302f96c369f7284ebc69f99908879cba"],
                "c":
["0x26b274dd041e1eb695391029c7f571676c85d022da9cb10ea6d8a95a8d32c2a8",
"0x2a633d6acc9f6a466fffc675c4f0f98ffdcf5a7192ef51e07ec7f64859d04037"],
                "c_p":
["0x2cbc357a99c7986449f7b3da85c98876ff924044deaec2f4bad0fcdb7b1b7bdc",
"0x15a2aa36569c4819f5c956de23fc084329b784edeac833f3446b9d2b39d9343f"],
                "h":
["0x03c5cfd050bc8b5fbe02950c32dbb2782740a620d054352bd3faa2e47f6e6758",
"0x12443ac64541511916b2ba0204a6aa0b738f3f9bee98f51b9674ddac360ba76f"],
                "k":
["0x179743214243c7c8ef0c2e9911e696a30241db6b393cdaf234a0e3d137ea12a2",
"0x06af95ef58aec1d77db49ad0a6361da6400c24292c265d96dad7f2c44349d720"]
        },
        "inputs":
["0x000000000000000000000000000000000000000000000000000000000000007c","0x0000000
000000000000000000000000000000000000000000000000000000000"]
}
```

Here are the 10 tokens from Etherscan https://rinkeby.etherscan.io/address/0x47FB7b2E4Dfb78A90306B2feCBF16BaF0c78d7Ea#tokentxnsErc721



Contract Address 0x47FB7b2E4D
rinkeby.etherscan.io/address/0x47FB7b2E4Dfb78A90306B2feCBF16BaF0c78d7Ea#toke...
Rinkeby Testnet Network
Home
Blockchain
Tokens
Misc
Rinkeby

Contract 0x47FB7b2E4Dfb78A90306B2feCBF16BaF0c78d7Ea

Sponsored: Sustain Podcast #33 How Font Awesome raised $1mm on Kickstarter Listen now!

Contract Overview

Balance: 0 Ether

More Info

My Name Tag: Not Available

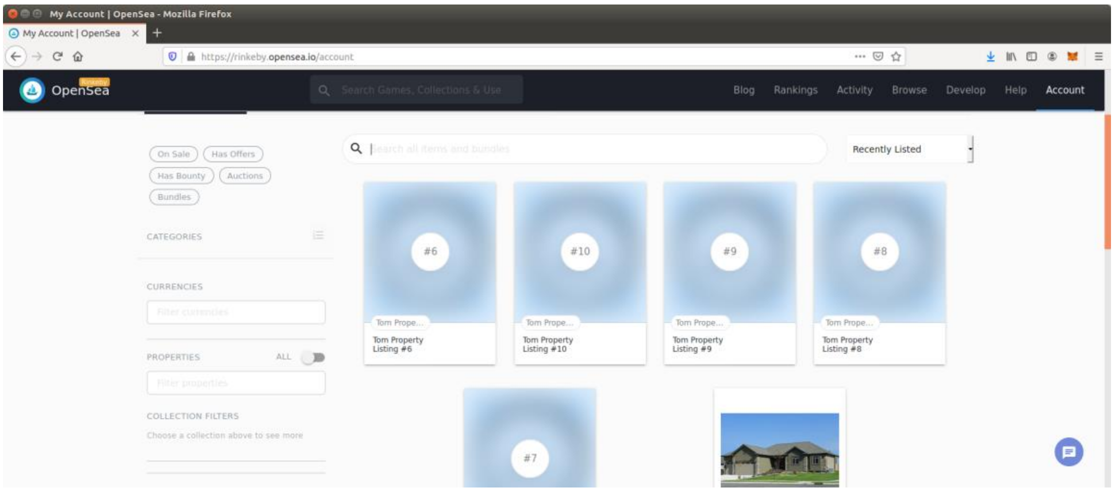
Contract Creator: 0x7734bf52f5f4c227... at txn 0x611f5804e92bd15...

Token Tracker: Tom Property Listing (TPL)

Latest 10 ERC-721 Token Transfer Events

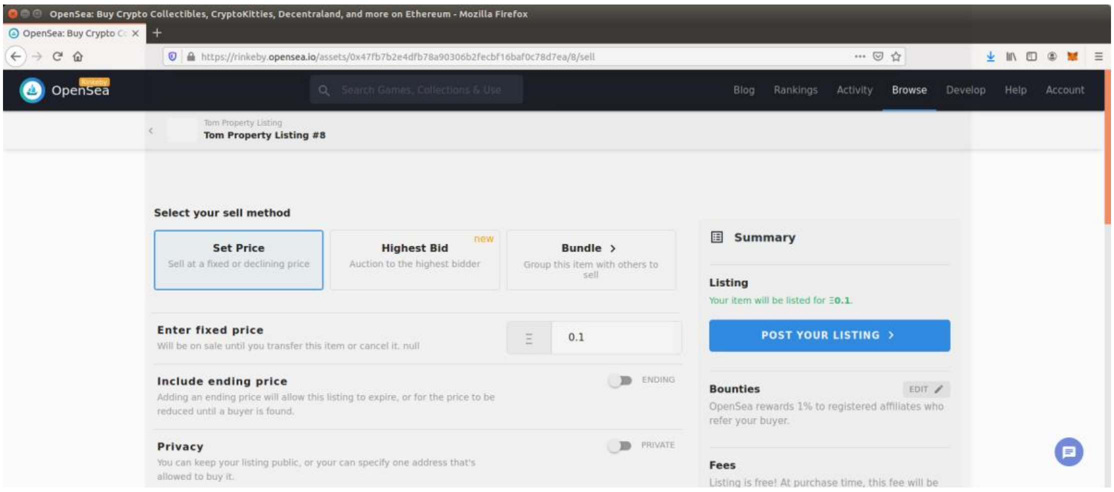
Txn Hash	Age	From		To	Token ID	Token
0x471f035c1069cb1...	27 mins ago	0x47fb7b2e4dfb78a...	OUT	0x7734bf52f5f4c227...	6	Tom Property... (TPL)
0xe0b8df4fd1df03f7...	28 mins ago	0x47fb7b2e4dfb78a...	OUT	0x7734bf52f5f4c227...	10	Tom Property... (TPL)
0xf4629d76b2818dd...	29 mins ago	0x47fb7b2e4dfb78a...	OUT	0x7734bf52f5f4c227...	9	Tom Property... (TPL)
0x647ffbea80fea105...	29 mins ago	0x47fb7b2e4dfb78a...	OUT	0x7734bf52f5f4c227...	8	Tom Property... (TPL)
0x215c6e510f77e36...	31 mins ago	0x47fb7b2e4dfb78a...	OUT	0x7734bf52f5f4c227...	7	Tom Property... (TPL)
0x943620503908be...	33 mins ago	0x47fb7b2e4dfb78a...	OUT	0x7734bf52f5f4c227...	5	Tom Property... (TPL)

OpenSea list the TPL token 0x7734bF52F5F4C2278d3bA2B6f0C2Fa76d2356273 owns.



The following demo how token 6, 7, 8, 9 and 10 are sold on OpenSea Marketplace for 0.1 ETH.

Set the price for token 8 = 0.1ETH



OpenSea: Buy Crypto Collectibles, CryptoKitties, Decentraland, and more on Ethereum - Mozilla Firefox
https://rinkeby.opensea.io/assets/0x47fb7b2e4dfb78a90306b2fecbf16baf0c78d7ea/8/sell
OpenSea
Search Games, Collections & Use
Blog
Rankings
Activity
Browse
Develop
Help
Account
Tom Property Listing
Tom Property Listing #8

Select your sell method

Set Price
Sell at a fixed or declining price

Highest Bid (new)
Auction to the highest bidder

Bundle
Group this item with others to sell

Enter fixed price
Will be on sale until you transfer this item or cancel it. null

Ξ 0.1

Include ending price (ENDING)
Adding an ending price will allow this listing to expire, or for the price to be reduced until a buyer is found.

Privacy (PRIVATE)
You can keep your listing public, or your can specify one address that's allowed to buy it.

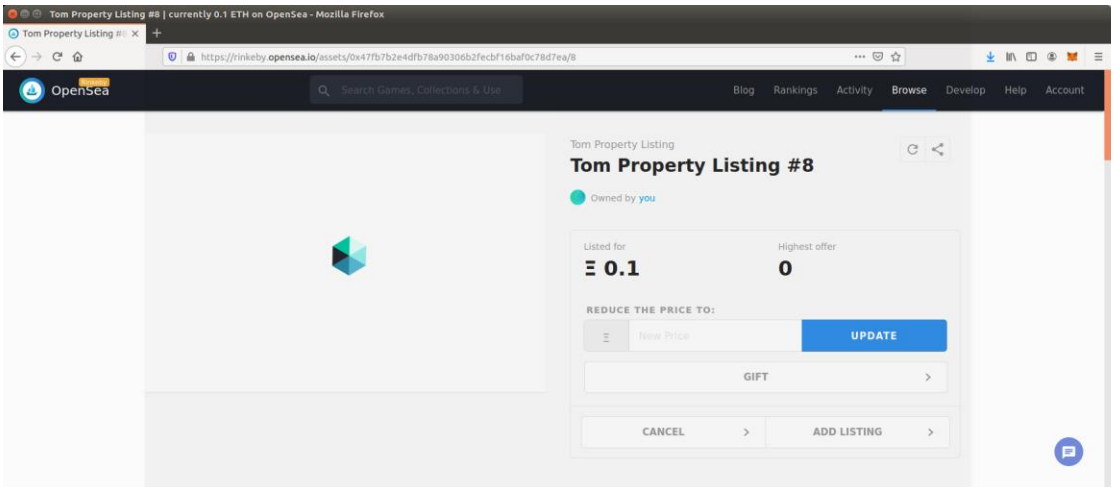
Summary

Listing
Your item will be listed for Ξ0.1.

POST YOUR LISTING

Bounties (EDIT)
OpenSea rewards 1% to registered affiliates who refer your buyer.

Fees
Listing is free! At purchase time, this fee will be



Tom Property Listing #8 | currently 0.1 ETH on OpenSea - Mozilla Firefox
https://rinkeby.opensea.io/assets/0x47fb7b2e4dfb78a90306b2fecbf16baf0c78d7ea/8
OpenSea
Search Games, Collections & Use
Blog
Rankings
Activity
Browse
Develop
Help
Account

Tom Property Listing
Tom Property Listing #8
Owned by you

Listed for
Ξ 0.1

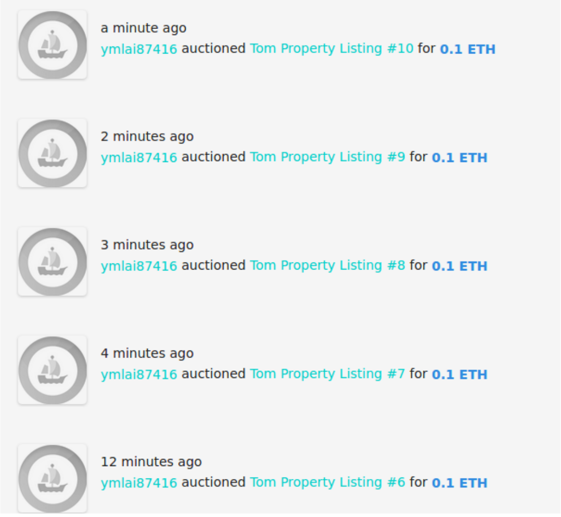
Highest offer
0

REDUCE THE PRICE TO:
Ξ New Price
UPDATE

GIFT

CANCEL
ADD LISTING

OpenSea shows that TPL token 6-10 are listed on the market.



a minute ago
ymlai87416 auctioned Tom Property Listing #10 for 0.1 ETH

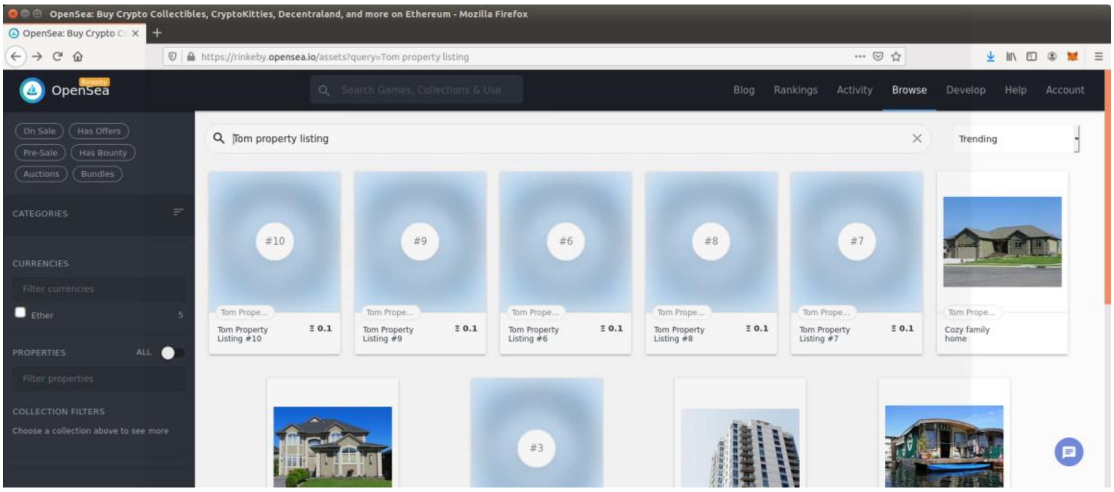
2 minutes ago
ymlai87416 auctioned Tom Property Listing #9 for 0.1 ETH

3 minutes ago
ymlai87416 auctioned Tom Property Listing #8 for 0.1 ETH

4 minutes ago
ymlai87416 auctioned Tom Property Listing #7 for 0.1 ETH

12 minutes ago
ymlai87416 auctioned Tom Property Listing #6 for 0.1 ETH

TPL token 6-10 on the market



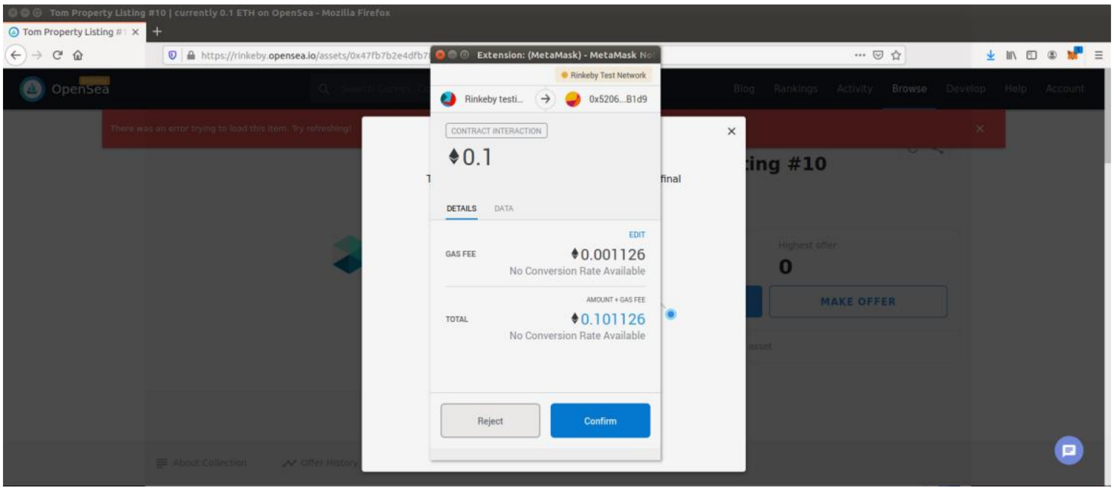
OpenSea: Buy Crypto Collectibles, CryptoKitties, Decentraland, and more on Ethereum - Mozilla Firefox

https://rinkeby.opensea.io/assets?query=Tom property listing

Tom property listing

Tom Prope...	Tom Prope...	Tom Prope...	Tom Prope...	Tom Prope...	Tom Prope...
Tom Property Listing #10 Ξ 0.1	Tom Property Listing #9 Ξ 0.1	Tom Property Listing #6 Ξ 0.1	Tom Property Listing #8 Ξ 0.1	Tom Property Listing #7 Ξ 0.1	Cozy family home

Now another address 0xb6e72643161e3a01b2f22faec0afe7710bedb51b wants to purchase TPL token 10.



Tom Property Listing #10 | currently 0.1 ETH on OpenSea - Mozilla Firefox

https://rinkeby.opensea.io/assets/0x47fb7b2e4dfb7

Extension: (MetaMask) - MetaMask No

Rinkeby Test Network

Rinkeby testi... → 0x5206...B1d9

CONTRACT INTERACTION

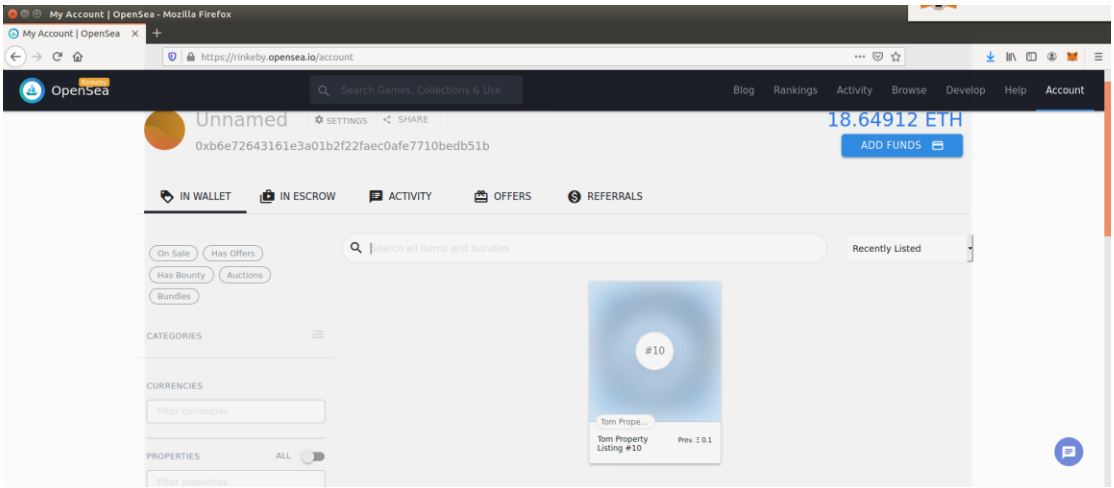
0.1

GAS FEE 0.001126
No Conversion Rate Available

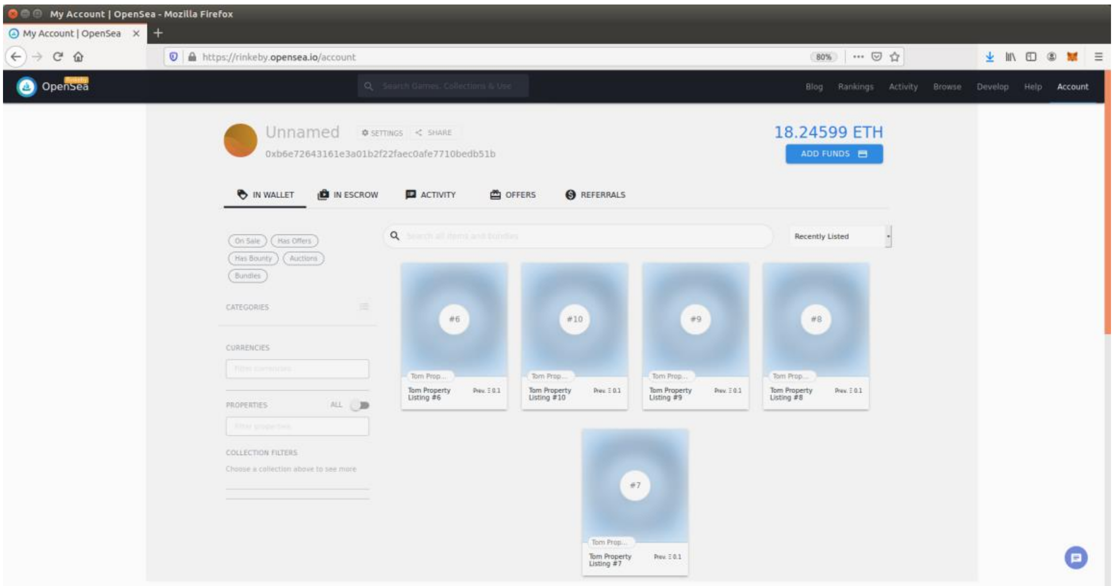
AMOUNT + GAS FEE
TOTAL 0.101126
No Conversion Rate Available

There was an error trying to load this item. Try refreshing!

Transaction successful



Now 0xb6e72643161e3a01b2f22faec0afe7710bedb51b have all 5 tokens sold by 0x7734bf52f5f4c2278d3ba2b6f0c2fa76d2356273.


My Account | OpenSea - Mozilla Firefox
https://rinkeby.opensea.io/account
80%
OpenSea
Search Games, Collections & Use
Blog
Rankings
Activity
Browse
Develop
Help
Account
Unnamed
SETTINGS
SHARE
0xb6e72643161e3a01b2f22faec0afe7710bedb51b
18.24599 ETH
ADD FUNDS
IN WALLET
IN ESCROW
ACTIVITY
OFFERS
REFERRALS
On Sale
Has Offers
Has Bounty
Auctions
Bundles
CATEGORIES
CURRENCIES
Filter currencies
PROPERTIES
ALL
Filter properties
COLLECTION FILTERS
Choose a collection above to see more
Search all items and bundles
Recently Listed
#6
Tom Prop...
Tom Property Listing #6
Prev. Ξ 0.1
#10
Tom Prop...
Tom Property Listing #10
Prev. Ξ 0.1
#9
Tom Prop...
Tom Property Listing #9
Prev. Ξ 0.1
#8
Tom Prop...
Tom Property Listing #8
Prev. Ξ 0.1
#7
Tom Prop...
Tom Property Listing #7
Prev. Ξ 0.1