# Objective: Recover the Ring of Fire

In this objective you will get a brief introduction to blockchain, cryptocurrency, and the blockchain’s cousin, the Merkle tree. Your first task is to listen to curmudgeon Tom Liston’s talk about cryptocurrency.

The Kringlecoin (KC) tellers are real cryptocurrency wallets, only useful at Kringlecon. Every time you have received KC or bought a hat your transaction is recorded in the KC blockchain. You will use KC to purchase a Non-Fungible Token (NFT) through a Merkle tree once you learn how to bypass the sporc’s evil plans.

Map

Description automatically generated with low confidence

After Tom’s talk, listen to Prof. Petabyte’s talk about NFT’s. He does not recommend them, except as a learning experience here at Kringlecon. You will need his information about Merkle trees to complete the challenge.

Text

Description automatically generated  
<http://www.youtube.com/watch?v=r3zj9DPC8VY>

Text

Description automatically generated  
<http://www.youtube.com/watch?v=Qt_RWBq63S8>

## Buy a Hat

The purpose of this objective is to show you the process for making a purchase using a Kringlecoin Teller Machine (KTM). It is fun, and you get to choose a cool hat for your avatar.

A screenshot of a computer

Description automatically generated with medium confidence

The process should be simple. Select a hat at the vending machine, then go to the KTM and authorize a transfer for the price of the hat to the vending machine’s wallet. Return to the vending machine to complete the purchase.

A picture containing text, several

Description automatically generated

## Blockchain Divination

Enjoy examining the blockchain with the Blockchain Explorer terminal. See if you can find the block that contains your hat purchase. At the beginning of the chain, block 1 creates the KC smart contract, block 2 creates the NFT smart contract, and block 6 appears to be the first award of KC for a player that completed orientation. The hints come from hidden chests, but you probably will not need them.

Text

Description automatically generated

A picture containing text, sign

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

## Exploit a Smart Contract

The sporcs have an evil plan. They have created an NFT but restricted access to their friends. Once the NFTs become popular they hope the price will skyrocket and they can sell their own NFTs for a huge profit. They are using a Merkle tree to limit access to NFTs. Your mission is to buy an NFT even though you aren’t in their tree.

Graphical user interface, text

Description automatically generated

Be sure to listen to [Prof. Q’s talk on Merkle trees](http://www.youtube.com/watch?v=Qt_RWBq63S8) if you haven’t already. The hint, Plant a Merkle Tree is essential as it gives you the link to [Prof. Q’s Git repo for making Merkle trees](https://github.com/QPetabyte/Merkle_Trees). (It was in a chest hidden under the table in the Tolkien Ring.)

A green screen with white text

Description automatically generated with medium confidence  
   
Text

Description automatically generated with medium confidence

Take this opportunity to browse through the KC blockchain, which is a real Ethereum blockchain. Skim through the Solidity code that creates KC (block 1) and the NFTs (block 2). Read the notes in [Prof. Q’s Git repo](https://github.com/QPetabyte/Merkle_Trees) about how Merkle trees work. It may not solve the challenge for you, but a lot of work went into creating a captive blockchain and NFTs so we could have an example to study.

### Question 1: A Problem with the Site

Visit the Bored Sporc Rowing Society (BSRS) website and investigate its working. Try to purchase an NFT and see what the browser sends to the BSRS site. Now that you understand Merkle trees, you should see that the site allows the browser to send one piece of information that should be kept on the server. What is it?

Graphical user interface

Description automatically generated with medium confidence

### Question 2: Install merkle\_tree.py

In addition to building cloud applications, containers are also used to distribute applications that may be complicated to install. The application and all its prerequisites can be delivered together so that all the user needs to do is install the Dockerfile. Of course, they may also need to install Git and Docker first.

Install the Dockerfile that Prof. Q provides in his repo.

### Question 3: Create a Merkle Tree

Create a Merkle tree that has your WalletID in the allow list. I found it best to use the simplest tree possible (two leaves) and put my ID into the first value of the list.

### Question 4: Plant Your Merkle Tree

Now it is time to insert our own root into the traffic that is sent to the BSRS site. At Glamtariel’s Fountain we used Burp Proxy and Repeater. Since this is a simple insertion, the Firefox Edit and Resend feature will work well. Insert your root into the traffic to the BSRS site so the site will check your tree and not its own.

### Question 5: Buy an NFT

Follow the instructions on the Pre-Sale page. Pre-approve a transfer of 100 KC to the address they give; there is a KTM in the level above you. Repeat the procedure, except with the Validate box unchecked.