# 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

Text

Description automatically generated

Here is a sample transaction as an example. Record the Block number so you can find your transaction in the blockchain. Over 100,000 blocks in the chain already! Wow.

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, application

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

The contract address is in the first block  
Text, email

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

### Answer 1: A Problem with the Site

When you try to send a made up walletID and proofs to the BSRS site, it tells you (rudely) that you are not on the Merkle tree and cannot purchase an NFT. This is expected.  
Text

Description automatically generated

When you look at the request the browser sends to BSRS (this is the Network tab of Firefox web developer tools) you see something interesting.  
Graphical user interface, text, application, email

Description automatically generated

The browser needs to send the WalletID, Proof, and Session key, but why does it send Root? The root of a Merkle tree is unique to the tree—you could say that it specifies the tree. If we can get them to check our WalletID and Proof against a Root that we give them, we could trick them into validating that we are in our own tree instead of validating our presence in their tree.

In the early days of the Internet, some web stores allowed the browser to send the price of an item in the purchase request to the server. Enterprising people soon learned they could change the price of the item sent to the store. Then you could buy a $500 TV for $1! The BSRS site allowing the browser to send the Root of the tree is essentially making the same mistake.

So, if we create a tree that includes our WalletID, we can send our Root instead of theirs. Before we can create a tree, we need to install the [software in Prof. Q’s repo](https://github.com/QPetabyte/Merkle_Trees).

### 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.

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

Git and Docker are supported on most major operating systems. Here are [instructions for installing Git](https://git-scm.com/book/en/v2/Getting-Started-Installing-Git), and here are [instructions for installing Docker](https://docs.docker.com/engine/install/).

Once you have Git and Docker installed just clone Prof. Q’s repo, build it, and run it in Docker. These commands will work in Ubuntu.  
git clone <https://github.com/QPetabyte/Merkle_Trees.git>  
cd Merkle\_Trees  
sudo docker build -t merkletrees .  
sudo docker run -it --rm --name=merkletrees merkletrees

### Question 3: Create a Merkle Tree

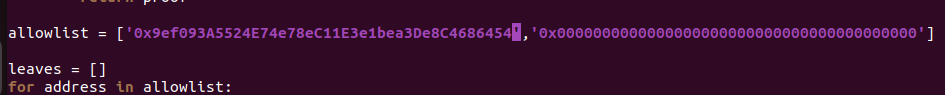
Create a Merkle tree that has your WalletID in the allow list. I found it best to use the simplest tree possible (two leaves) and put my ID into the first value of the list.

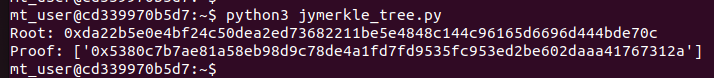
### Answer 3: Create a Merkle Tree

You will need to edit merkle\_tree.py to put your WalletID into the allow list. However, you do not have the permissions to do that.  


Just copy the file, and you will have the correct permissions for the copy.  
Text

Description automatically generated

Edit merkle\_tree.py with vim or nano to insert your WalletID into the allow list. I chose to replace the entry for 0x1337133713371337133713371337133713371337 with my WalletID. By default, the program computes the proof for the first item [0] in allowlist. 

The program will give you the root and the proof that go with your tree and WalletID.  


### 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.

### Answer 4: Plant Your Merkle Tree

Firefox has a useful feature under the Network tab called Edit and Resend. It is helpful when you do not want to bother with spinning up Burp Suite.

Using Firefox, enter your walletID and your proof into the BSRS presale page so that all you will have to edit is the root value. Open the webdev tools if you haven’t already, and select the Network tab. Then click Go! on the BSRS presale page. They will deny your request saying that you are not on the list, but that is fine, the attack is coming.

Find the packet you just sent in the Networking tab and right-click on it. One of the choices is Edit and Resend, which is exactly what we want to do.  
Graphical user interface, text, application

Description automatically generated

The Body is shown at the bottom of the page. If you put your walletID and proof into the web page before you clicked Go, all you edit is the root. Change the root to the value you got from the merkle\_tree.py script. Now you are telling BSRS to check that your walletID is in the tree you created, and not theirs. The silly sporcs do it.

Graphical user interface, text, application, email

Description automatically generated

You should get a message telling you that you have been validated and can purchase an NFT.

### 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.

### Answer 5: Buy an NFT

Follow the steps properly, and the BSRS site will take your 100 KC and give you this message.

*Success! You are now the proud owner of BSRS Token #000147. You can find more information at* [*https://boredsporcrowboatsociety.com/TOKENS/BSRS147,*](https://boredsporcrowboatsociety.com/TOKENS/BSRS147,) *or check it out in the gallery!<br>Transaction: 0xccad6b3c139676d81d4f488f1cbd731d0ef7c4bee8b421548bf279f1bc782a85, Block: 58630<br><br>Remember: Just like we planned, tell everyone you know to <u><em>BUY A BoredSporc</em></u>.<br>When general sales start, and the humans start buying them up, the prices will skyrocket, and we all sell at once!<br><br>The market will tank, but we'll all be rich!!!*

The link will show you your NFT. Your NFT is also available in the BSRS Gallery, although you may have to scroll for a while to find it. You can look up your Block number in the Blockchain Explorer and see your transaction recorded there all time (or at least while the blockchain exists.) Congratulations!