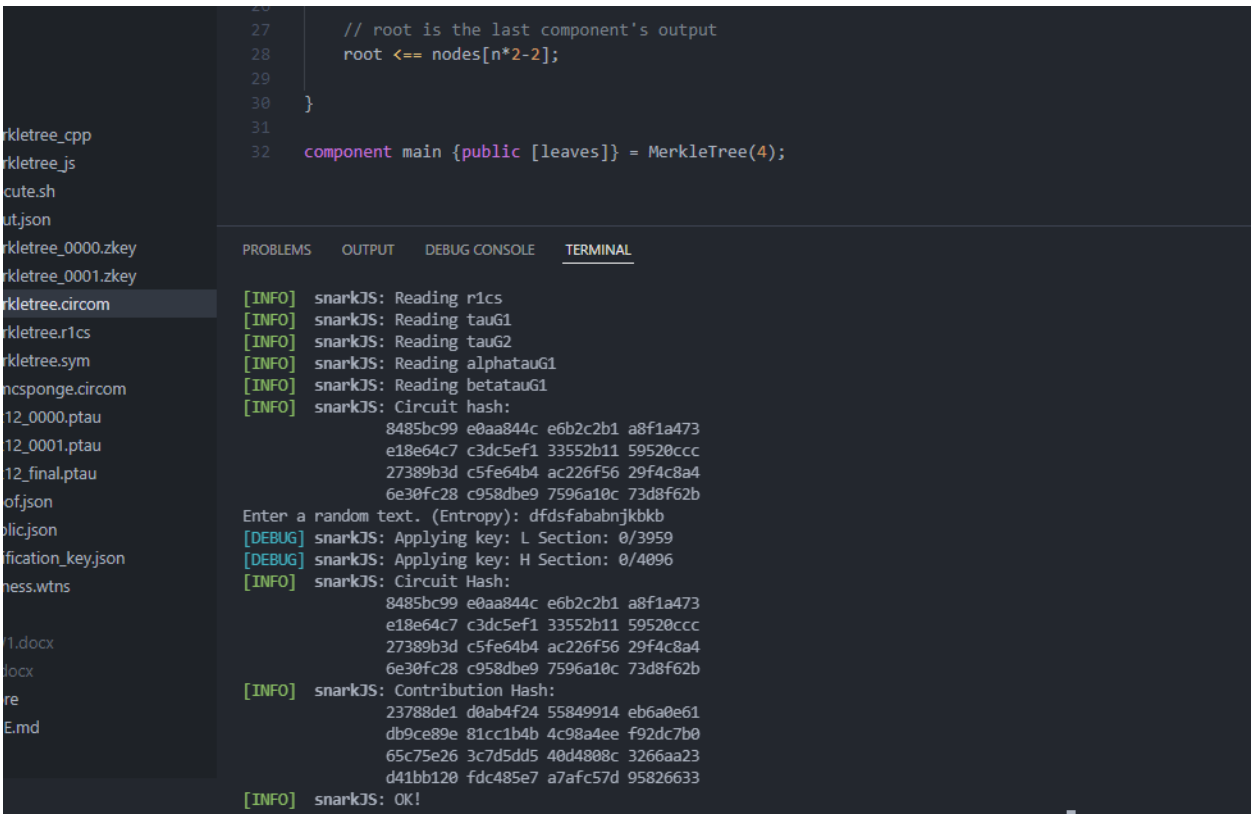
Zero Knowledge University March-April 2022 Cohort

Week 1 Assignment

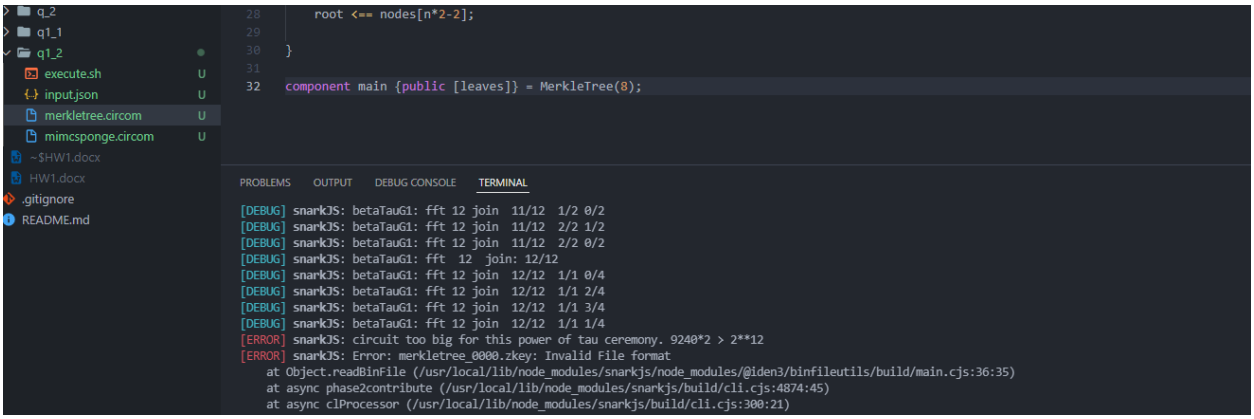
Course Registration Email: zhang.jeremy.2001@gmail.com

Discord Username: xyz5368#1102

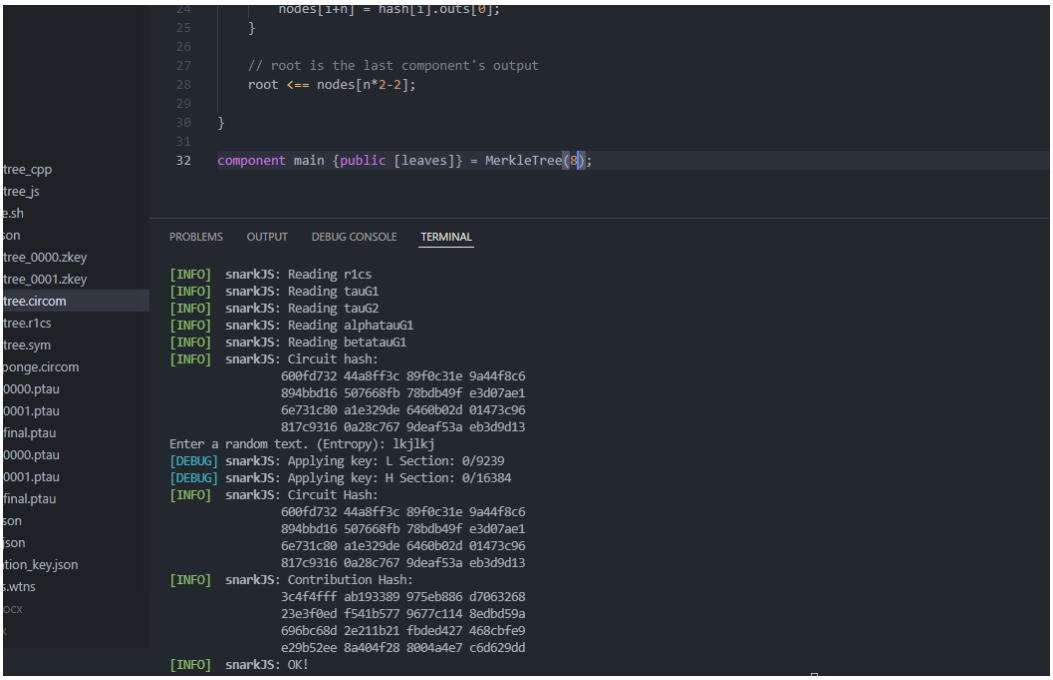
1. Intro to Circom
    a. See https://github.com/jeremyzhang1/zku-submissions/blob/main/week1/hw/q1_1/merkletree.circom. Here is a screenshot of the successful execution.



    b. See https://github.com/jeremyzhang1/zku-submissions/blob/main/week1/hw/q1_2/merkletree.circom. While running the code, I ran into an error stating that the circuit was too big for the power of tau ceremony. See picture below:



To fix this problem, I increased the powers of tau from 12 to 14, which solved the problem. Here is a screenshot of the successful execution.



c. Zero knowledge proofs are not really necessary for all of this. Creating a Merkle tree on chain like the example provided in the solidity by example documentation could work as well. When the user commits some information, only the hash values would be stored, so it would still be completely anonymous. We would then give the root hash and perhaps a few intermediate hashes to let the user know that their transaction was successful.

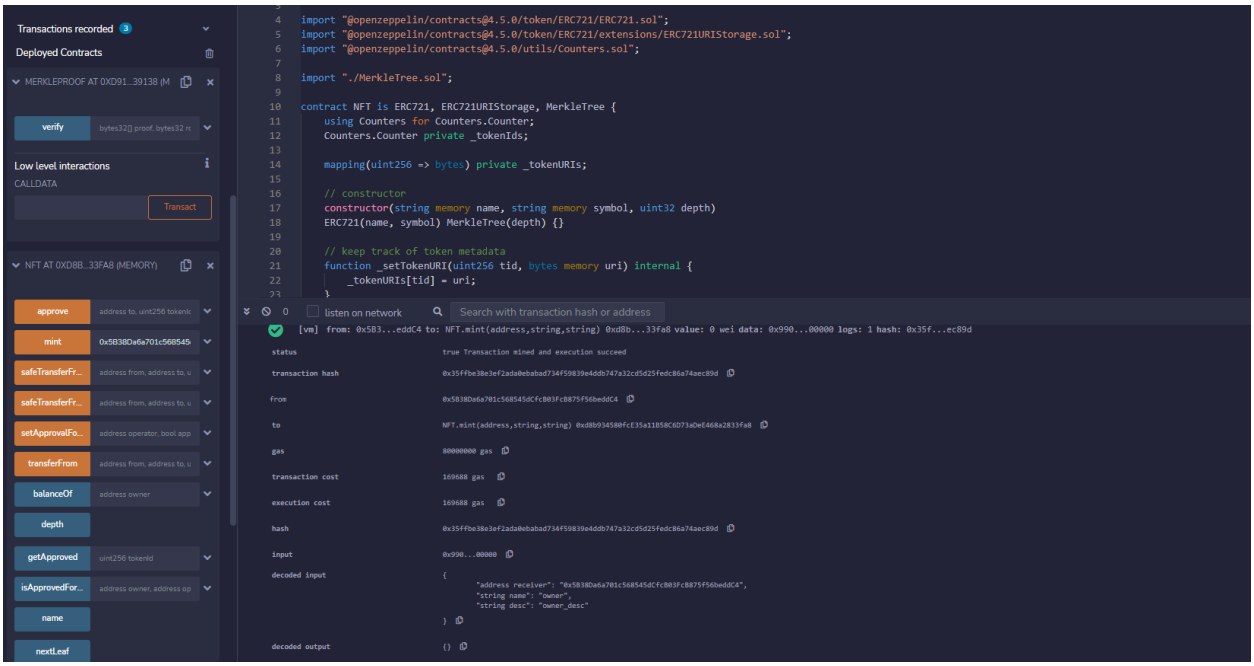
d. See https://github.com/jeremyzhang1/zku-submissions/blob/main/week1/hw/q1_2/execute.sh

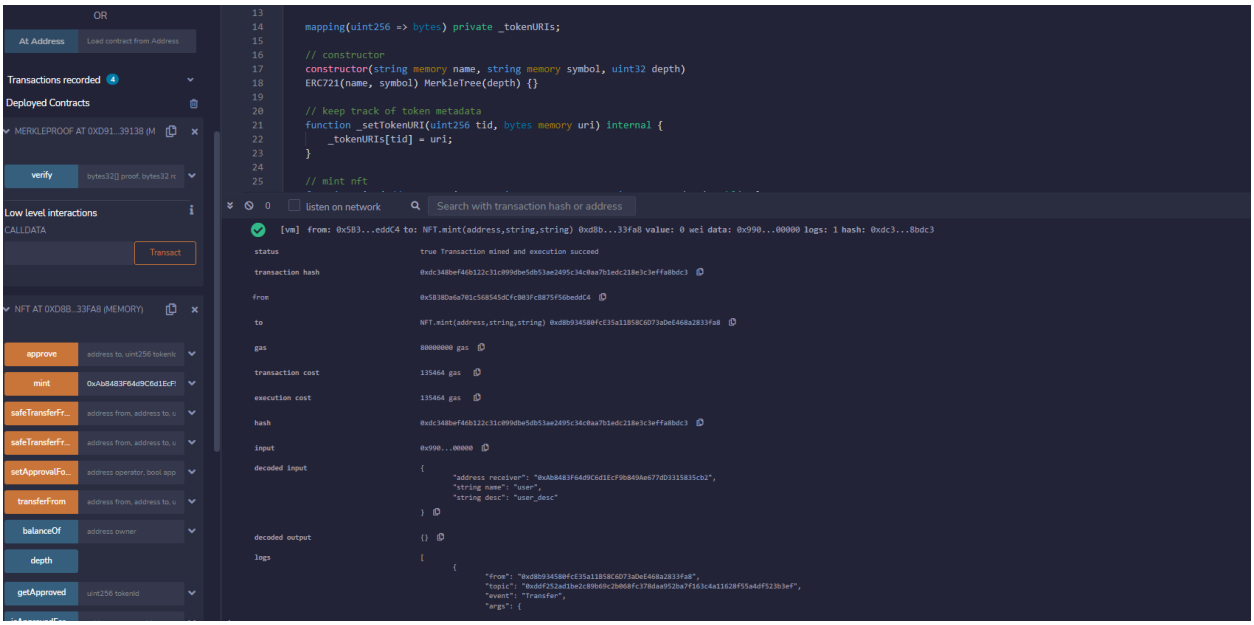
2. Minting an NFT and committing the mint data to a Merkle Tree

a. See https://github.com/jeremyzhang1/zku-submissions/blob/main/week1/hw/q2/NFT.sol

b. See https://github.com/jeremyzhang1/zku-submissions/blob/main/week1/hw/q2/MerkleTree.sol

c. The first screenshot is an NFT mint to the contract owner, the second screenshot is an NFT mint to another user.





d. Minimal frontend bonus not attempted.

e. Extra bonus not attempted.

3. Understanding and generating ideas about ZK technologies

a. SNARK relies on elliptic curves, which can be solved with a quantum computer whereas STARK uses hashing algorithms that are more secure. SNARK needs a trusted setup ritual whereas STARK does not. SNARK has a smaller proof size and thus takes less time to verify than STARK.

b. Groth16 is not a universally trusted setup whereas PLONK is. This essentially means that every time the circom circuit file is modified, you need to go through the trusted setup process again with Groth16.
c. You can anonymize NFT transactions, so that owners of NFTs would be able to prove that they are the owner without revealing who they actually are. You could also prevent the resale of NFTs by providing some sort of information or original certificate of authenticity. When the NFT is resold, this information is not passed along, and since the new owner does not have that information, they cannot verify into the Merkle tree to prove ownership.
d. In addition to voting, ZK can be used to verify identity without members of the DAO having to break the anonymity barrier. DAOs would be able to verify the identity or membership status of the member without knowing who that member is.