Project 3
Floriane Beyegue, Fareed Freihat, Josh Jaggat, Cassandra Johnson, Ken Lindgren, and Aparna Pooleri

Whole Lotto Tokens

Modernizing lottery systems through smart contracts

Lottery Contract

Create an interactive lottery system through smart contracts utilizing Solidity

1.

Project Background!

Here's a bit more about our idea.

Objectives

First	Second	Third	Last
Allow multiple addresses to purchase lottery tickets for a set price	Pool the earnings from the ticket purchase	Select a randomized winner	Pay out the earnings to the winner and reset to zero

Definitions

Blockchain

A network of nodes linked peer-to-peer that facilitates transactions similar to a distributed ledger.

Block Hash

A function that converts an input of letters and numbers into an encrypted output.

Smart Contract

Computer code that automatically executes all or parts of an agreement and is stored on a blockchain-based platform.

Wallet Address

A digital wallet used to store cryptocurrencies and conduct secure transactions.

Constructor

A special method that gets called whenever an object of a class is initialized.

Token

A virtual asset or utility that resides on their own blockchain.

Coding Roadmap

1. A constructor sets up the token on the Ethereum network.
2. An array stores the addresses of ticket purchasers. The index = lottery ticket number.
3. The Buy function sets the ticket price and pushes each purchaser's address into the array.
4. The contract generates a random number within a set range to determine the winner.
5. Lottery proceeds can be withdrawn by the winner.
6. The contract resets everything to zero.

Testing

Phase 1

A single person purchased multiple lottery tickets from several accounts. This initial test verified the contract would select a random winner.

Phase 2

Several different individuals purchased lottery tickets. This test verified others could import the contract and buy a ticket.

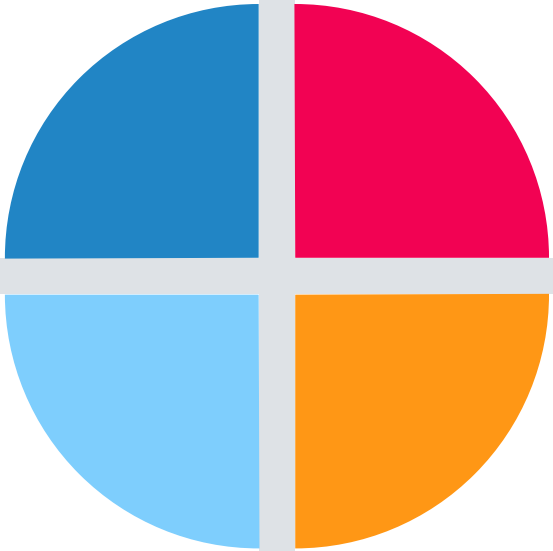
2.

Demo!

Ethere-UM, you just won the lottery!

Challenges

Getting a random number generator to work.



Determining how to give multiple people the ability to buy tickets.

Conversion rate of Ethereum to our Lottery Token.

Getting prompted by MetaMask to send Ether for the token.

Next Steps

Exchange Rate

Use multiple types of cryptocurrency in the same contract

Other Methods

Have users pick a number to win instead of assigning a random winner

More Security

Restrict certain functionality to the contract owner

Thanks!

Any questions?

We'll miss you guys.