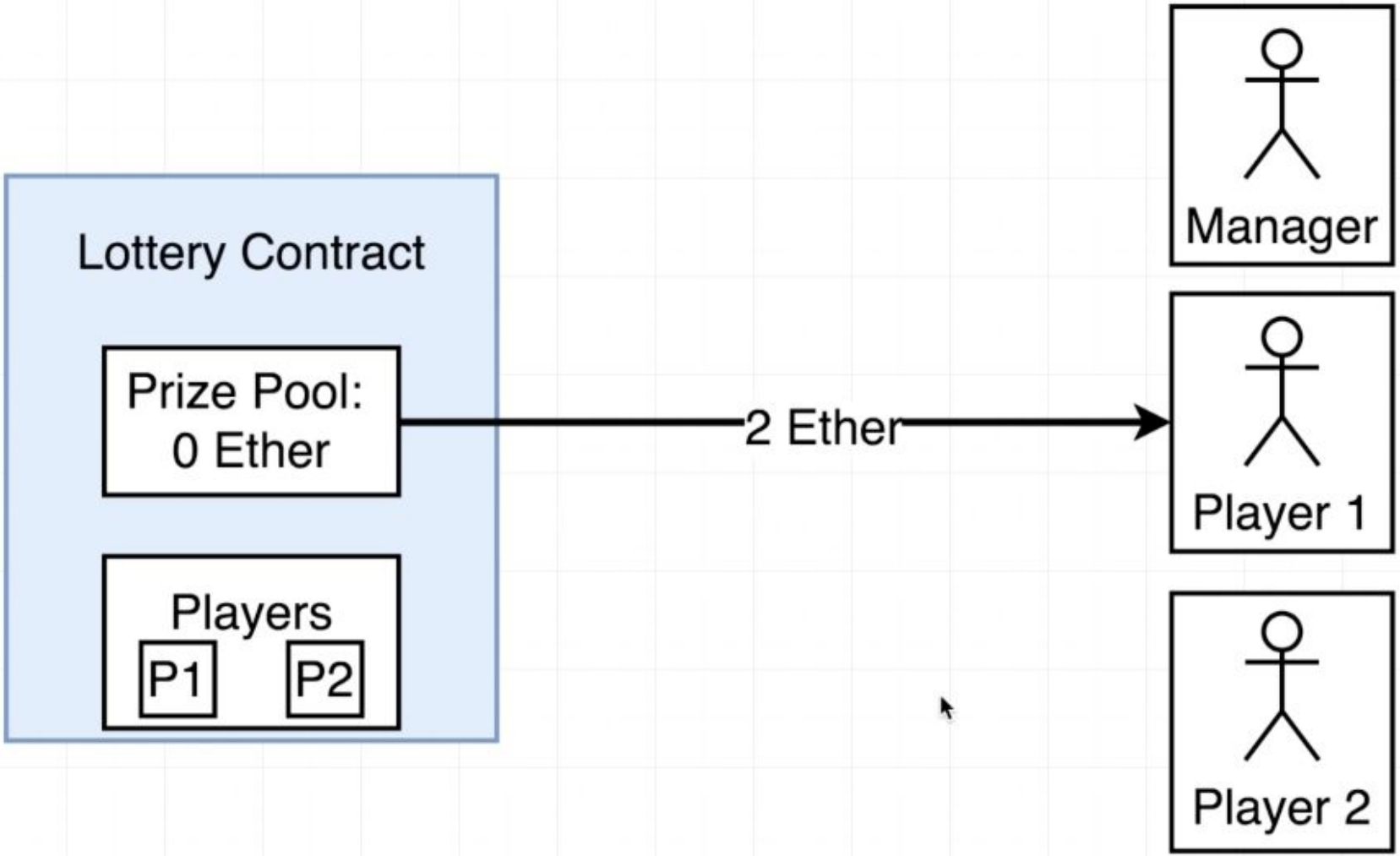
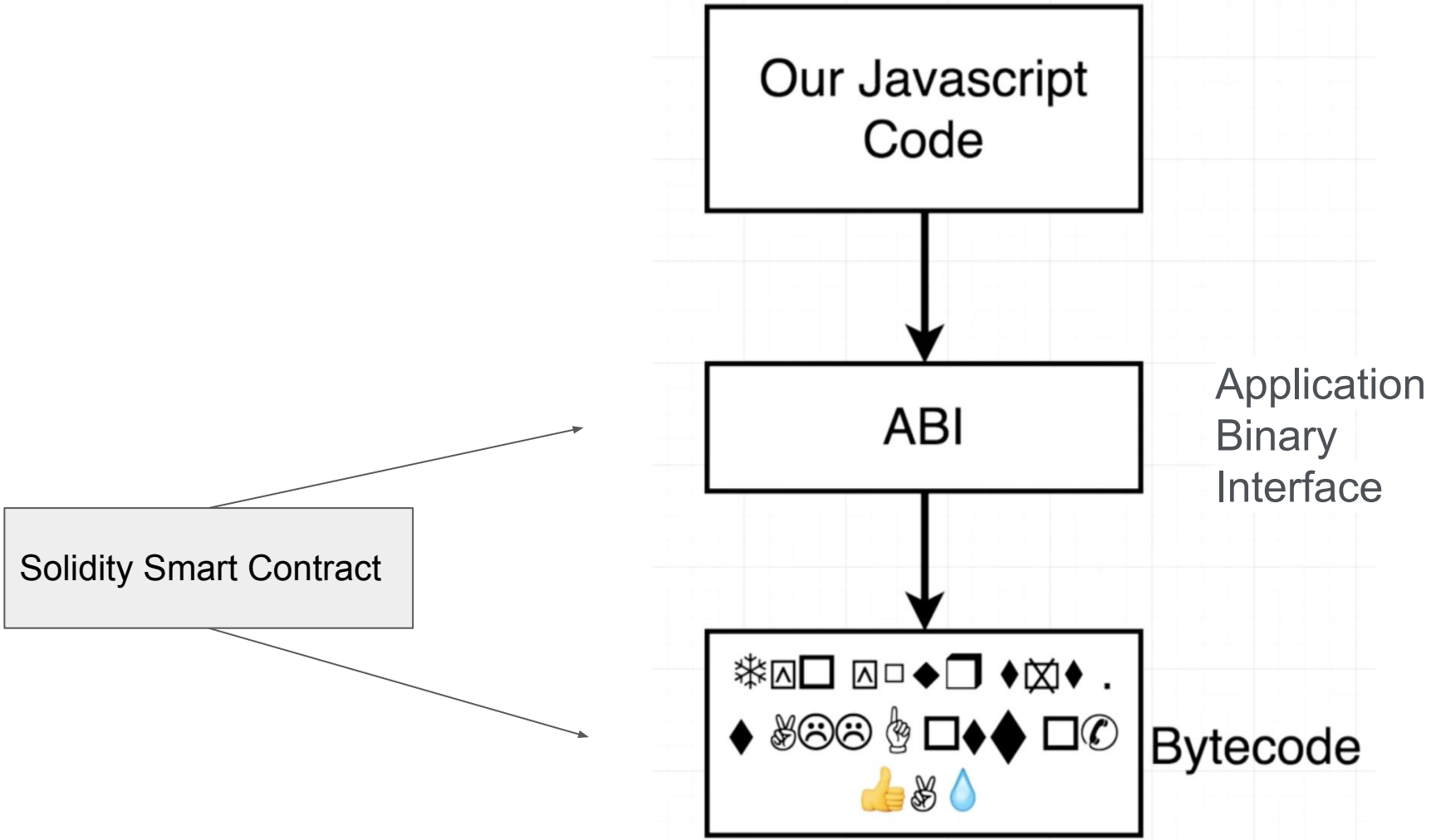
Lottery Smart Contract

K.Y. Shen

1.Rinkerby Faucet
https://faucet.rinkeby.io/
2.Deploy contract using Infura
https://infura.io/
Sign up account and get your link and mnemonic words
npm install
node deploy.js
3.Deploy frontend on Netlify
npm install
npm run start
npm run build
Note: the version of solidity inside package.json should be equal to Lottery.sol(0.4.17)


Lottery Contract
Prize Pool:
0 Ether
Players
P1
P2
2 Ether
Manager
Player 1
Player 2


Our Javascript Code
ABI
Application Binary Interface
Solidity Smart Contract
Bytecode

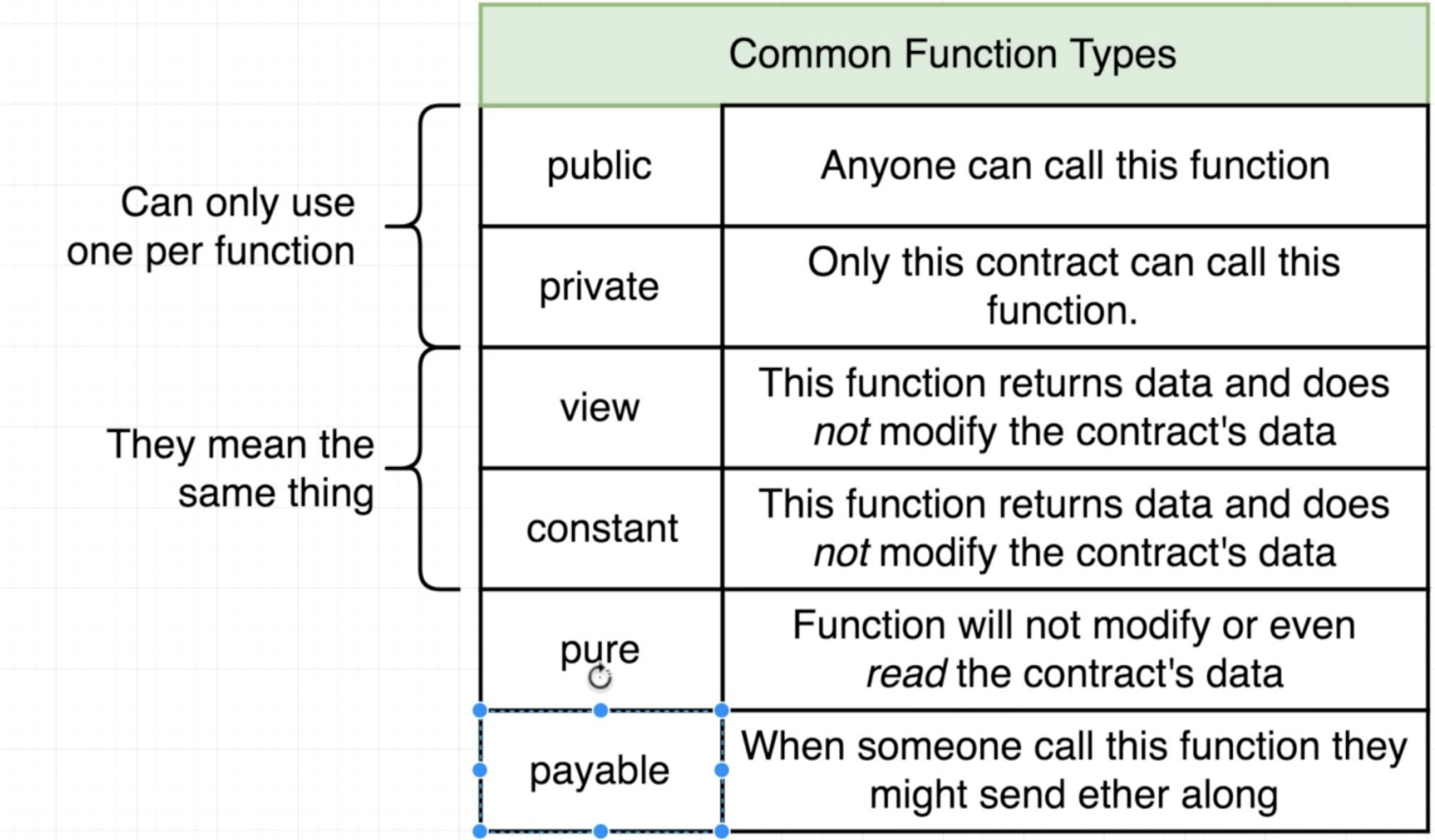
Lottery Contract

Variables

Name	Purpose
manager	Address of person who created the contract
players	Array of addresses of people who have entered

Functions

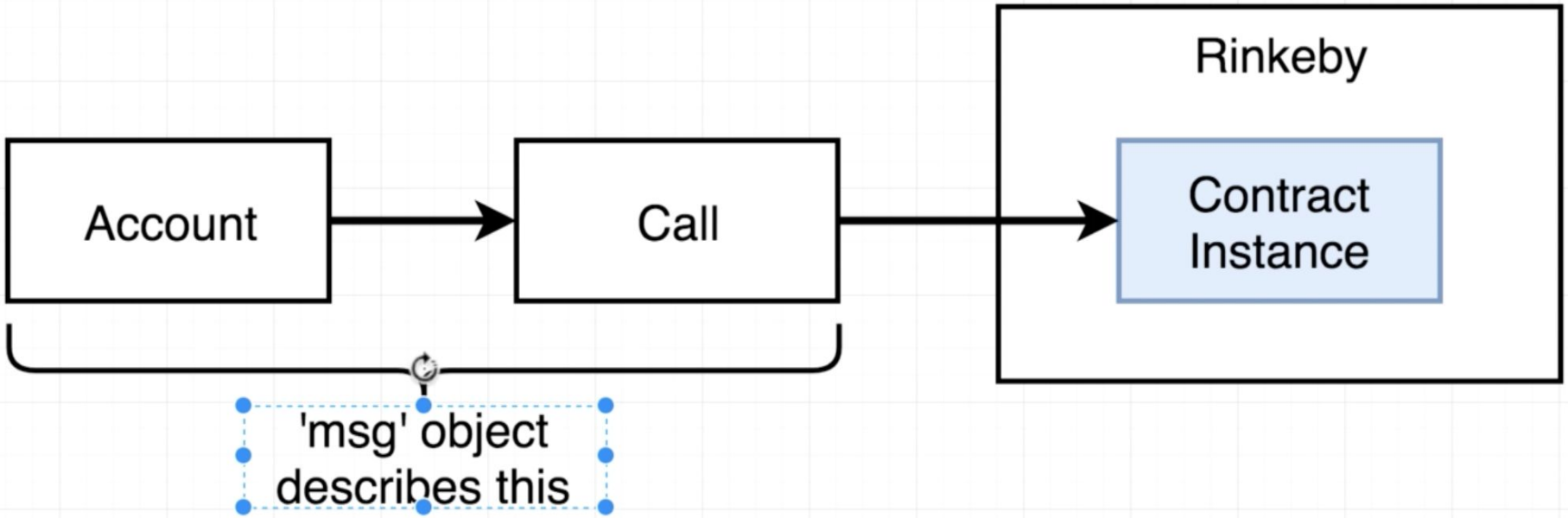
Name	Purpose
enter	Enters a player into the lottery
pickWinner	Randomly picks a winner and sends them the prize pool


Common Function Types
Can only use one per function
They mean the same thing
public
Anyone can call this function
private
Only this contract can call this function.
view
This function returns data and does *not* modify the contract's data
constant
This function returns data and does *not* modify the contract's data
pure
Function will not modify or even *read* the contract's data
payable
When someone call this function they might send ether along

Basic Types		
Name	Notes	Examples
string	Sequence of characters	"Hi there!" "Chocolate"
bool	Boolean value	true false
int	Integer, positive or negative. Has no decimal	0 -30000 59158
uint	'Unsigned' integer, positive number. Has no decimal	0 30000 999910
fixed/ufixed	'Fixed' point number. Number with a decimal after it	20.001 -42.4242 3.14
address	Has methods tied to it for sending money	0x18bae199c8dbae199c8d

Integer Ranges		
Name	Lower Bound	Upper Bound
int8	-128	127
int16	-32,768	32,767
int32	-2,147,483,648	2,147,483,647
...	...	...
int256	Really, really negative	Really, really big

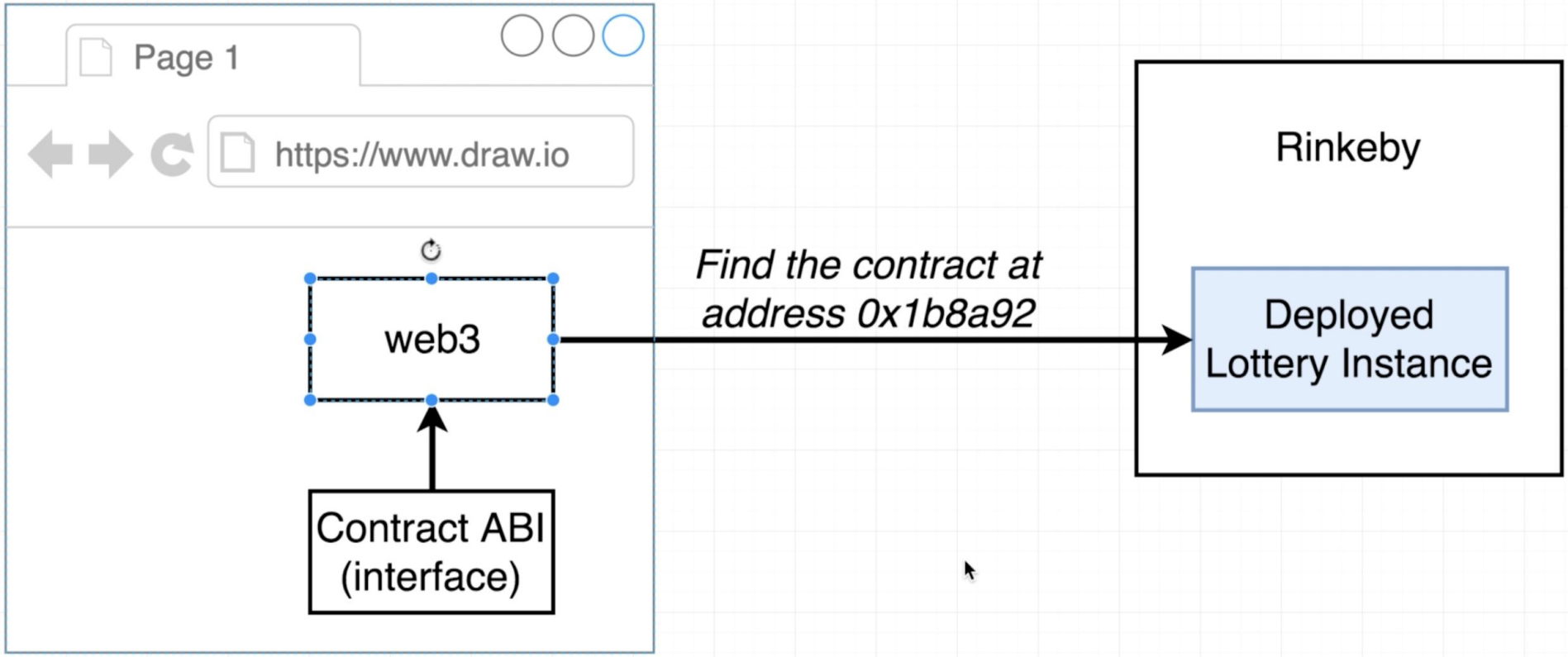
int == int256

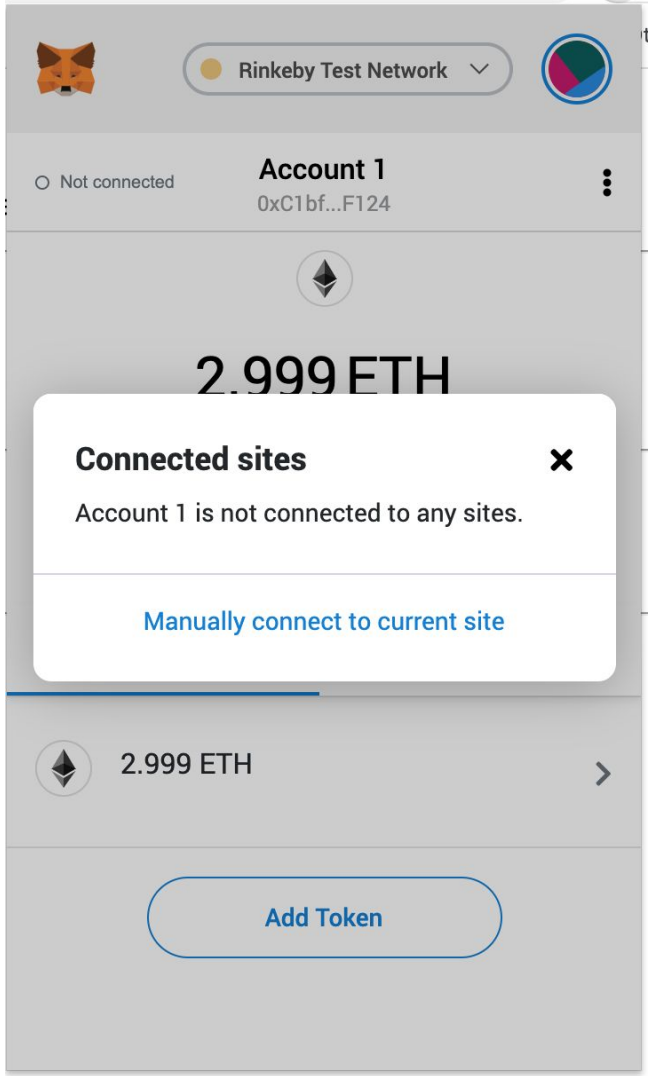

Rinkeby
Account
Call
Contract
Instance
'msg' object
describes this

The 'msg' Global Variable	
Property Name	Property Name
msg.data	'Data' field from the call or transaction that invoked the current function
msg.gas	Amount of gas the current function invocation has available
msg.sender	Address of the account that started the current function invocation
msg.value	Amount of ether (in wei) that was sent along with the function invocation

Reference Types		
Name	**Notes**	**Examples**
fixed array	Array that contains a *single type* of element. Has an unchanging length	`int[3] --> [1, 2, 3]` `bool[2] --> [true, false]`
dynamic array	Array that contains a *single type* of element. Can change in size over time	`int[] --> [1,2,3]` `bool[] --> [true, false]`
mapping	Collection of key value pairs. Think of Javascript objects, Ruby hashes, or Python dictionary. All keys must be of the same type, and all values must be of the same type	`mapping(string => string)` `mapping(int => bool)`
struct	Collection of key value pairs that can have different types.	`struct Car { string make; string model; uint value; }`

```
pragma solidity ^0.4.17;

contract Lottery {
    address public manager;
    address[] public players;

    function Lottery() public {
        manager = msg.sender;
    }

    function enter() public payable {
        require(msg.value > .01 ether);

        players.push(msg.sender);
    }

    function random() private view returns (uint) {
        return uint(keccak256(block.difficulty, now, players));
    }

    function pickWinner() public restricted {
        uint index = random() % players.length;
        players[index].transfer(this.balance);
        players = new address[](0);
    }

    modifier restricted() {
        require(msg.sender == manager);
        _;
    }

    function getPlayers() public view returns (address[]) {
        return players;
    }
}
```


Page 1
https://www.draw.io
web3
Contract ABI
(interface)
Find the contract at
address 0x1b8a92
Rinkeby
Deployed
Lottery Instance


Rinkeby Test Network
Not connected
Account 1
0xC1bf...F124
2.999 ETH
Connected sites
Account 1 is not connected to any sites.
Manually connect to current site
2.999 ETH
Add Token

Reference

https://www.udemy.com/course/ethereum-and-solidity-the-complete-developers-guide/learn/lecture/9020602#overview

https://solidity.readthedocs.io/