合約地址：0xCe67Dae630f4Db3e15bb46A82713E00F41E5E0d3

一、用enum定義各種STATUS：
0 -->活動進行中(InProgress)
1 -->計算贏家中(CalculatingWinner)
2 -->活動結束/未開始(EndOrNotStarted)

```
// (V)定義enum
enum STATUS {
    InProgress, //進行中
    CalculatingWinner, //計算贏家
    EndOrNotStarted    //結束，未開始
}
```

另外，將一開始的狀態設為未開始(EndNotStarted)，並設定owner

```
constructor() public {
    status = STATUS.EndOrNotStarted;
    _owner = msg.sender;
}
```

二、function startLottery()
1.用 onlyOwner這個modifier，在執行前先檢查是否是合約持有者操作
2.之後require檢查是否從狀態關閉，之後狀態開啟且設定入場費

```
function startLottery() public onlyOwner{
    require(status == STATUS.EndOrNotStarted ,"Start failed.");
    status = STATUS.InProgress;
    entranceFee = 0.00001 ether;
}
```

補：onlyOwner

```
modifier onlyOwner(){
    require(msg.sender == _owner, "Permission denied.");
    _;//回到function繼續執行
}
```

三、function enter()
1.require檢查狀態是否活動進行中且msg.value的籌碼大於入場費
2.把msg.sender push到players裡面

```
function enter() payable public {
    require(status == STATUS.InProgress ,"It hasn't started.");
    require(msg.value >= 0.00001 ether ,"The value need to be bigger than the entranceFee.");
    players.push(msg.sender);
}
```

四、function endLottery()

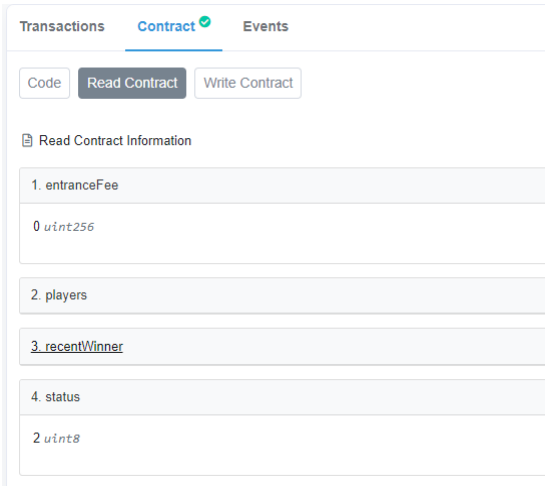
1. 一樣用 onlyOwner這個modifier，在執行前先檢查是否是合約持有者操作
2. require檢查狀態是否活動進行中且players[ ]裡的人數大於0
3. 開始計算winner（並設定成CalculatingWinner的狀態）：用加密雜湊演算法
4. 設定winner到recentWinner，用transfer把所有籌碼轉移給recentWinner
5. delete 清空players[ ]，但狀態設成EndOrNotStarted

```
function endLottery() public onlyOwner{
    require(status == STATUS.InProgress ,"It's not currently in progress.");
    require( players.length > 0 ,"There is currently no player in the pool.");
    status = STATUS.CalculatingWinner;

    uint256 indexOfWinner = uint256(
            keccak256(
                abi.encodePacked(msg.sender, block.difficulty, block.timestamp)
            )
    ) % players.length;
    recentWinner = players[indexOfWinner];
    payable(recentWinner).transfer(address(this).balance);
    delete players;
    status = STATUS.EndOrNotStarted;
}
```

執行結果：

一開始，狀態為2(未開始)



活動開始後，狀態為0(進行中)，並且入場費下限為0.00001 ether

Read Contract Information

1. entranceFee

10000000000000 *uint256*

2. players

3. recentWinner

4. status

0 *uint8*

輸入籌碼後，可以再players查詢位址

結束活動後，狀態為2(已結束)，且players已清空，recentwinner也已登記並獲得獎金