

باسمه تعالی



دانشگاه صنعتی شریف

دانشکده مهندسی برق

## درس مبانی تکنولوژی بلاکچین و رمزارزها

گزارش تمرین شماره سه

علی محرابیان 96102331

استاد: دکتر مداح علی

زمستان 1398



### سوال 1:

فایل داده شده deploy می کنیم.

```
18 // Function to recover the funds on the contract
19 function kill() public returns(string memory){
20     if (msg.sender == owner)
21         selfdestruct(owner);
22     return "Bye";
23 }
24 }
25
26 contract Greeter is Mortal {
27     /* Define variable greeting of the type string */
28     string greeting;
29
30     /* This runs when the contract is executed */
31     constructor(string memory _greeting) public {
32         greeting = _greeting;
33     }
34
35     /* Main function */
36     function greet() view external returns (string memory) {
37         return greeting;
38     }
39 }
```

### سوال 5:

با توجه به این که اولاً افراد می توانند ID های ناشناخته زیادی بسازند و بدون هیچ محدودیتی رای بدهند  
ثانیاً این که هنگامی که افراد رای می دهند، هیچ سازکاری برای تایید آن ها وجود ندارد. بنابراین در برابر  
Sybil attack آسیب پذیر است.



سوال 6:

پس از انجام مراحل، رای به صورت زیر است.

### Results

Candidate	Votes
0	3
1	1
2	2
3	4

Candidate ID  
3

Wallet Address  
0xd66a42cfbfbf9b5a735c200a897b9d474d1285664

Vote

Close