تمرین عملی سوم درس بلاک چین

زانا رحمانی- ۹۵۱۰۵۵۸۴

سوال ۴)

contract hash: 0xc79eb7014cf5b5ce5cf313329ceeb7b05b3b7a69e416206dd38fc5c67b132622

add book 1: 0xa710a27d5a59eda307006778062a8d4635cd97ed888038adcb00694d827a9342

add book 2: *0xf4a29cedd2c9e2fcd45e326d79b9b18b299e30f173156098a61cf4b3f64fdca1*

سوال ۵)

قسمت اول : برای شمارش آرای افراد از متغییری به اسم count استفاده می‌کنیم که نوع آن uint8 است، یعنی متغییری ۸ بیتی است و حداکثر می‌تواند ۲۵۵ رای حساب کند و اگر آرا از آن بیشتر شود تعداد آرا صفر می‌شود.

قسمت دوم : برای جلوگیری از attack reentrancy باید قبل از صدا زدن تابع خارجی ابتدا موجودی را کم کنیم و بعد از آن تابع خارجی را صدا بزنیم.
وقتی که در یک تابع، تابعی از یک قرارداد هوشمند دیگر را فراخوانی می‌کنیم جریان اجرای تابع اول تغییر می‌کند و می‌توان مجددا آن تابع را قبل از تمام شدن کارش دوباره صدا زد و مثلا در تابع withdraw می‌توان چندین بار پول را خارج کرد و فقط یک تابع burn اجرا شود. برای جلوگیری از این مشکل کافی‌ست ابتدا موجودی را کاهش دهیم و بعد از آن انتقال را انجام بدهیم، به صورت زیر:

```
_burn(msg.sender, amount);
recipient.transfer(amount);
```

منبع : https://consensys.github.io/smart-contract-best-practices/known_attacks/