باسمه تعالی

دانشگاه صنعتی شریف

دانشکده مهندسی برق

مبانی رمز ارزها و بلاکچین

گزارش تمرین شماره دو

علی محرابیان96102331

استاد: دکتر مداح علی

زمستان1398

سوال3:

در قسمت اول از OP_IF استفاده می کنیم.ابتدا به کمک OP_DEPTH،تعداد کلید های ورودی را می سنجیم.اگر برابر با 3 بود،شرط اول IF ارضا شده و کلید عطا و فراز چک می شود.در غیر این صورت در ELSE،یک کلید از بین عطا و فراز و دو کلید از بین 3 سهام دار دیگر چک می شود.ترتیب قرار گرفتن کلیدها مهم است.

نکته مهمی که در OP_CHECKMULTISIG وجود دارد،این است که هنگام خواندن stack،با فرض این که m از n کلید نیاز است،m+n+2+1 خانه فراخوانده می شود.یعنی یک خانه بیشتر از چیزی که انتظار داریم. بنابراین هنگام verify کردن،با دستور OP_0،یک خانه اضافه می کنیم.چیزی شبیه به شکل زیر:

3
<Public Key Charlie>
<Public Key Bob>
<Public Key Alice>
2
<Signature Charlie>
<Signature Bob>
0

در قسمت بعدی هم،پس از سنجیدن تعداد کلید های ورودی و اختلاف آن از 3،ابتدا امضای 3 سهامدار چک می شود و سپس در آخر،امضای عطا یا فراز چک می شود.لازم به ذکر است برای این سوال،برای کلید عطا،از my_public_key استفاده کردیم.

سوال4:

در این فسمت از CLTV استفاده می کنیم.خروجی تراکنش تا هنگامی که زمان موردنظر نرسیده است،قابل مصرف نیست.از دستور OP_CHECKLOCKTIMEVERIFY استفاده می کنیم.اگر زمان زیر 500M باشد،بلاک مدنظر را نشان می دهد و اگر زمان بالاتر از 500M باشد،تاریخ مشخصی را نشان می دهد.از سایت Unixtimestamp.com برای تعیین زمان استفاده کردیم.تراکنش برای قسمت b،confirm نشد و فقط تراکنش قسمت a را آوردیم.

برای قسمت happybirth day،فایل مورد نظر را نوشته وبه کمک تابع hash که در تمرین قبلی ساختیم،از Hash فایل برای ساختن آدرس استفاده می کنیم.سپس مقداری کوین به آدرس ساخته شده می فرستیم.بنابراین فایل در blockchain قابل دسترس است.

سوال 5:

ایده این سوال نیز شبیه قسمت دوم سوال قبل است.از فایل hex. ساخته شده،به کمک hash آن،آدرس فایل را ساخته و مقداری کوین به آن می فرستیم.

در این قسمت باید از merkle tree استفاده کنیم و به root آن برسیم.بنابراین از کدی که در تمرین قبلی زدیم، استفاده می کنیم.با گرفتن فایل های ورودی و تعداد آن ها،درخت مورد نظر ساخته می شود و بعدا می توانیم اثبات کنیم که آیا فایلی در بین فایل های اولیه بوده است یا خیر.

سوال 6:

خواسته های سوال را به کمک OP_IF عملی می کنیم.اگر شرط if درست بود،در ابتدا HASH160 مقدار X ورودی با secret مقایسه می شود که اگر درست باشد،امضای نفر دوم با public_key او مقایسه شده و verify می شود.اگر شرط if درست نبود،به امضای هردو نفر نیاز است.بنابراین از CHECKMULTISIG استفاده می کنیم.حواسمان هست که در این حالت،OP_0 به ابتدای script اضافه شود.

در حالت اول که alice_redeems برابر با false باشد،خروجی به صورت زیر است.

```
Alice swap tx (BTC) created successfully!
Bob swap tx (BCY) created successfully!
Bob return coins (BCY) tx created successfully!
Alice return coins tx (BTC) created successfully!
```

و در حالتی که alice_redeems برابر با true باشد،خروجی به صورت زیر است.

```
Alice swap tx (BTC) created successfully!
Bob swap tx (BCY) created successfully!
Alice redeem from swap tx (BCY) created successfully!
Bob redeem from swap tx (BTC) created successfully!
```