上海交通大学
SHANGHAI JIAO TONG UNIVERSITY

第四次作业

李子龙
123033910195

2023 年 10 月 27 日

解 A = Alice (PK_1, SK_1), B = Bob (PK_2, SK_2), C = Carol (PK_3, SK_3), D = David (PK_4, SK_4), E = Eve (PK_5, SK_5)

TX_1 :

Input :

prev : $H(TX_0)$

n : 0

scriptSig :

`Sign(`SK_4, TX_0`)`

PK_4

Output :

$TXO[0]$:

value : 100

scriptPubKey :

`OP_DUP`

`OP_HASH160`

$H(PK_4)$

`OP_EQUALVERIFY`

`OP_CHECKSIG`

$TXO[1]$:

value : 100

scriptPubKey :

`OP_2`

$H(PK_1)$

$H(PK_2)$

$H(PK_3)$

`OP_3`

`OP_CHECKMULTISIG`

TX_2 :

Input :

prev : $H(TX_1)$

n : 1

scriptSig :

`OP_0`

`Sign(`SK_1, TX_1`)`

`Sign(`SK_2, TX_1`)`

Output :

$TXO[0]$:

value : 60

scriptPubKey :

`OP_DUP`

`OP_HASH160`

$H(PK_5)$

`OP_EQUALVERIFY`

`OP_CHECKSIG`

$TXO[1]$:

value : 40

scriptPubKey :

`OP_2`

$H(PK_1)$

$H(PK_2)$

$H(PK_3)$

`OP_3`

`OP_CHECKMULTISIG`

这里假设 TX_1 中 D 给 ABC 公司的 TXO 在 [1] 位置上；TX_2 中提供了 A 和 B 的签名，给 E 的 TXO 在 [0] 位置上。这里假设没有交易费。

其中 OP_CHECKMULTISIG 的前置参数是

OP_0 <Sig_1> ... <Sig_M> OP_M <PubKeyHash_1> ... <PubKeyHash_N> OP_N

只需要提供 N 个公钥对应的 M 个签名即可通过 OP_CHECKMULTISIG。OP_0 是占位符（无操作），OP_1 ～OP_16 输出对应数字。

参考文献：https://en.bitcoin.it/wiki/Script