

正常情况

行号	脚本	主栈 (左侧是栈底, 右侧是栈顶)	从栈 (左侧是栈底, 右侧是栈顶)	说明
1	Sig1	Sig1		第1个签名
2	Pk1	Sig1 Pk1		第1个公钥
3	OP_TRUE	Sig1 Pk1 TRUE		第1个条件有效
4	Sig2	Sig1 Pk1 TRUE Sig2		第2个签名
5	Pk2	Sig1 Pk1 TRUE Sig2 Pk2		第2个公钥
6	OP_TRUE	Sig1 Pk1 TRUE Sig2 Pk2 TRUE		第2个条件有效
7	0	Sig1 Pk1 TRUE Sig2 Pk2 TRUE 0		匹配成功的公钥数量, 初始值0
8	OP_TOALTSTACK	Sig1 Pk1 TRUE Sig2 Pk2 TRUE	0	将初始值0放入从栈
9	OP_IF	Sig1 Pk1 TRUE Sig2 Pk2	0	如果第2个条件为真, 执行行10到行17
10	OP_DUP	Sig1 Pk1 TRUE Sig2 Pk2 Pk2	0	复制栈顶Pk2
11	OP_HASH160	Sig1 Pk1 TRUE Sig2 Pk2 Pkh2	0	对复制的Pk计算hash160
12	dd2d89bb9f64cbdf4139ff0e23c4813124af85e6	Sig1 Pk1 TRUE Sig2 Pk2 Pkh2 Pkh2'	0	Pkh2应该等于Pkh2'
13	OP_EQUALVERIFY	Sig1 Pk1 TRUE Sig2 Pk2	0	比较Pkh2, 如果不等脚本异常结束
14	OP_CHECKSIGVERIFY	Sig1 Pk1 TRUE	0	检查Sig2是否可以用Pk2验证, 无法验证则异常结束
15	OP_FROMALTSTACK	Sig1 Pk1 TRUE 0		从栈数据移入主栈
16	OP_1ADD	Sig1 Pk1 TRUE 1		栈顶加1, 匹配成功的公钥数量变为1
17	OP_TOALTSTACK	Sig1 Pk1 TRUE	1	将1放入从栈
18	OP_ENDIF	Sig1 Pk1 TRUE	1	条件代码结束
19	OP_IF	Sig1 Pk1	1	如果第一个条件为真, 执行行20到行27
20	OP_DUP	Sig1 Pk1 Pk1	1	复制栈顶Pk1
21	OP_HASH160	Sig1 Pk1 Pkh1	1	对复制的Pk计算hash160
22	aef82c0ef3f0c1d867e12b64e9e8d2ebb983dc81	Sig1 Pk1 Pkh1 Pkh1'	1	Pkh1应该等于Pkh1'
23	OP_EQUALVERIFY	Sig1 Pk1	1	比较Pkh1, 如果不等脚本异常结束
24	OP_CHECKSIGVERIFY		1	检查Sig1是否可以用Pk1验证, 无法验证则异常结束
25	OP_FROMALTSTACK	1		从栈数据移入主栈
26	OP_1ADD	2		栈顶加1, 匹配成功的公钥数量变为2
27	OP_TOALTSTACK		2	将2放入从栈
28	OP_ENDIF		2	条件代码结束
29	OP_2	2	2	最少需要的公钥数量
30	OP_FROMALTSTACK	2 2		从栈数据移入主栈
31	<u>OP_GREATERTHANOREQUAL</u>	TRUE		最少需要的数量是否小于解锁的公钥数量 (这里有错误? 应该为OP_LESSTHANOREQUAL)

异常情况

行号	脚本	主栈 (左侧是栈底, 右侧是栈顶)	从栈 (左侧是栈底, 右侧是栈顶)	说明
1	0	0		未设置第1个签名和公钥
2	0	0 0		未设置第2个签名和公钥
3	0	0 0 0		匹配成功的公钥数量, 初始值0
4	OP_TOALTSTACK	0 0	0	将初始值0放入从栈
5	OP_IF			第2个公钥为假, 跳过行6到行14
6	OP_DUP			
7	OP_HASH160			
8	dd2d89bb9f64cbdf4139ff0e23c4813124af85e6			
9	OP_EQUALVERIFY			
10	OP_CHECKSIGVERIFY			
11	OP_FROMALTSTACK			
12	OP_1ADD			
13	OP_TOALTSTACK			
14	OP_ENDIF			
15	OP_IF	0	0	第1个公钥为假, 跳过行16到行24
16	OP_DUP			
17	OP_HASH160			
18	aef82c0ef3f0c1d867e12b64e9e8d2ebb983dc81			
19	OP_EQUALVERIFY			
20	OP_CHECKSIGVERIFY			
21	OP_FROMALTSTACK			
22	OP_1ADD			
23	OP_TOALTSTACK			
24	OP_ENDIF			
25	OP_2	2	0	最少需要的公钥数量
26	OP_FROMALTSTACK	2 0		从栈数据移入主栈
27	<u>OP_GREATERTHANOREQUAL</u>	TRUE		最少需要的数量是否小于解锁的公钥数量 (这里有错误? 应该为 OP_LESSTHANOREQUAL)