Script 言語のいろは

--- ビットバンク社 技術顧問 ジョナサン・アンダーウッド

概要

- ·Script言語の仕組み
- ・ビットコイン取引における Script
 - P2PK Script 基礎的な例をあげよう
 - •P2PKH Script 主流のビットコイン取引はこれ
 - •P2SH Script Scriptの逆襲
 - •Segregated Witness Scriptの救世主
- •OP CODE一覧と説明
- •ビットコインゲットクイズ!

Script 言語の 仕組み

Script 言語の仕組み

- ・スタック系の言語
- ・スタック整理コマンドと処理コマンド
- ・ALTSTACKについて
- •チューリング不完全



P2PK Script

問いかけ:

① PUSH_DATA(公開鍵) ② OP_CHECKSIG

回答:

① PUSH_DATA(電子署名)

	Stack	Operation
	PUSH_DATA_304402201c625c63c9de9d254664a72521dbbc9e026620d7fba4b84f63e5adde4 +	
[/'304402201c625c63c3de9d254664a72521dbbc9e026620d7fba4b84f63e5adde43ab119f022C	OP_CODESEPARATOR	
[**304402201c625c63c9de9d254664a72521dbbc9e026620d7fba4b84f63e5adde43ab119f022C	PUSH_DATA_044664c1cdbb7d05901ae6327a58a6ffc3dc480ef6d81b270654468d5ef1ac9fb	
[**@14402201c825c83c9de94254644a72521dbbc9e02662047fba4b84f63e5adde43ab119f022f [**044684c1cdbb7d05901ae8927a59a6ffc3dc490ef6d81b270854488d5ef1ac9fb1adb442945e	OP_CHECKSIG	
1	RESULT	

P2PKH Script

問いかけ:

①OP_DUP ②OP_HASH160 ③PUSH_DATA(公開鍵ハッシュ) ④OP_EQUALVERIFY ⑤OP_CHECKSIG

回答:

①PUSH_DATA(電子署名) ②PUSH_DATA(公開鍵)

St ack		Operation
	PUSH_DATA_30440220583265-4354847908683ae89cfefbf90255f39575a6474c2f01f23e8b8	
[**3044022058326b435d8d7908663ae89cfefbf90255f39575a6474c2f01f23e8b87b373e3022C	PUSH DATA 0319aeachfe647a116326a4624fae121b2ad7c19226aab92f93bd4163cc7cf2ea	
[**30440/22/058326b45548d7900863 se89cf ef bf 90255f 39575a6474c2f 01f 23e8b87b373e3022C [**03138aeacbfe647a116335a4824f se 121b2ad7c19238aa862f 83bd4f 83cc 7cf2ea2**]	OP_CODESEPARATOR	
["3044022058326b45568d7908663æ89cfefbf90255f39575a6474c2f01f23e8b67b373e9022C ["0313eaecbfe647a116325a4824fae121b2ad7c19225aab82f35bd4183cc7cf2ea2"]		
•	OP_DUP	
["3044022058326b455d8d7908863as86cf ef bf 90255f 38575ab474c2f01f 23e6b87b378c9022f "391 9aeachf e647a118326a462f ef ae [21b2ad7c18226asb82f 95bd 4180c.7cf 26ac2f" ["3019 3eaachf e647a118326a462f ar ae [21b2ad7c18226asb62f 95bd 4180c.7cf 26ac2f"]		
·	CP_HASH160	
["3044022058325642568047908693.ae99cf ef bf 90255f 39575a6474c2f 01f 23 e6867b373e3022C ["0319aeach fe647a118325a4824f ae 12162a47c19228aeb92f 93b44183cc7cf 2ee2"] ["6062f 933c98df b1b1844349381725424984f c471"]		
•	PUSH DATA e062f893c98dfb1b18443493d72b5424694fc471	
["30440]22(56326145540d7908663æ89cfefbf90255f33575a6474c2f01f23e6b87b373e3022("0313eaechfe647a116326a4624fae121b2adfc18226aab92f53bd4163cc7cf2ea2"] "6165f890369dfb1b18445393172562489464671"] "6165f899369461b181443493172562489464671"]		
•	OP_EQUALVERIFY	
[**3044022(58326)455486179(0683ae884cf ef bf 90255f 39575a6474c2f 01f 23 96867b373e3022ť [**0319aeachf e647a116326a45024f ae 121b2a47c18226aak62f 39bd 4165cc7cf2ea2**]		
4	OP_CHECKSIG	
	RESULT	

P2SH Script

(偽) 問いかけ:

①OP_HASH160 ②PUSH_DATA(redeemScriptハッシュ) ③OP_EQUAL 回答:

①PUSH_DATA() ... PUSH_DATA(redeemScript)

(真) 問いかけ:
redeemScriptハッシュをScriptとしてパースしたもの
回答:
その解答

	St ack	Operation
	PUSH_DATA_52210297ad3ee53d7ba40a227c1958609cca32197dd905092078c4f04847296bc	
[″52210297ad3ee53d7ba40a227c1958609cca32197dd905092078c4f04847298bce824e210355 ▶	OP_CODESEPARATOR	
7°52210297ad3ee53d7ba40a227c1958609cca32197dd905092078c4f04847298bce824e210355	OP_HASH160	
["09ff1296c1532bccb21e00bd77b0a315a6491700"]	PUSH DATA 09ff1296c1532bccb21e00bd77b0a315a6491700	
[*09ff1296c1532bccb21e00bd77b0a315a6491700*] *09ff1296c1532bccb21e00bd77b0a315a6491700**]	OP_EQUAL	
	RESULT	

Segregated Witness

ソフトフォークにできる理由がScriptの特性にある:

回答問いかけ

【空欄】 redeemscript v2.0

redeemscript v2.0の中身: PUSHDATA(Script ver. # + 元の問いかけ)

これでScriptのコマンドが簡単にアップデートできるようになる

先日有効になったばかりのOP_CHECKLOCKTIMEVERIFYのような 醜いソフトフォークはOP CODE追加時に不要になった

OP CODE 一覧と 説明

OP CODE 一覧と説明

OP CODES

https://en.bitcoin.it/wiki/Script

```
//
                                                                                        push
                                                                                                                                                                                 value
OP FALSE:
                                   OP PUSHDATA1:
                                                                                     OP PUSHDATA4:
                   OP 0:
                                                            OP PUSHDATA2:
                                                                                                       78
                                                                                                               OP 1NEGATE:
                                                                                                                               79
                                                                                                                                     OP TRUE:
                                                                                                                                                         OP 1:
                                                                              77
                  OP 4:
                                    OP 5:
                                               85
                                                                                                               OP 9:
                                                                                                                                                    OP 11:
OP_3:
           83
                             84
                                                       OP 6:
                                                                          OP 7:
                                                                                            OP 8:
                                                                                                       88
                                                                                                                         89
                                                                                                                                 OP 10:
                                                                                                                                                                91
                                                                                                                                                                        OP 12:
                                                                                                                                                                                    92
                                                  OP 14:
OP_13:
                                                                              94
                                                                                                     OP 15:
                                                                                                                                 95
                                                                                                                                                        OP 16:
                                                                                                                                                                                    96
                                                                                                                                                                                control
OP IF:
               99
                            OP NOTIF:
                                               100
                                                            OP ELSE:
                                                                              103
                                                                                            OP ENDIF:
                                                                                                               104
                                                                                                                            OP VERIFY:
                                                                                                                                                105
                                                                                                                                                              OP RETURN:
                                                                                                                                                                                  106
                                                                                        stack
                                                                                                                                                                                   ops
                     OP FROMALTSTACK:
                                               OP 2DROP:
                                                           109 OP 2DUP: 110
                                                                                 OP 3DUP: 111 OP 20VER: 112
                                                                                                                   OP 2ROT: 113 OP 2SWAP:
                                                                                                                                                114 OP IFDUP: 115
OP TOALTSTACK: 107
                                                                                                                                                                                  116
                                                                                  OP PICK:
                                                                                                      OP ROLL:
OP DROP:
             117
                     OP DUP:
                                 118
                                         OP NIP:
                                                    119
                                                             OP OVER:
                                                                          120
                                                                                              121
                                                                                                                    122
                                                                                                                            OP ROT:
                                                                                                                                       123
                                                                                                                                                OP SWAP:
                                                                                                                                                                      OP TUCK:
                                                                                                                                                                                  125
                                                                                        splice
                                                                                                                                                                                   ops
OP SIZE:
                                                                                                                                                                                  130
                                                                                         bit
                                                                                                                                                                                  logic
OP EQUAL:
                                                           135
                                                                                                                 OP EQUALVERIFY:
                                                                                                                                                                                  136
//
                                                                                                                                                                               numeric
OP 1ADD:
              139
                       OP 1SUB:
                                     140
                                              OP NEGATE:
                                                                       OP ABS:
                                                                                             OP NOT:
                                                                                                          145
                                                                                                                   OP ONOTEQUAL:
                                                                                                                                      146
                                                                                                                                                OP ADD:
                                                                                                                                                             147
                                                                                                                                                                      OP SUB:
                                                                                                                                                                                  148
                                                              143
                                                                                    144
                                                         155
                                                                                               156
                                                                                                                                                       OP NUMNOTEQUAL:
OP BOOLAND:
                      154
                                    OP BOOLOR:
                                                                       OP NUMEQUAL:
                                                                                                             OP NUMEQUALVERIFY:
                                                                                                                                         157
                                                                                                                                                                                  158
OP LESSTHAN:
                 159
                         OP GREATERTHAN:
                                              160
                                                      OP LESSTHANOREQUAL:
                                                                                       OP GREATERTHANOREQUAL:
                                                                                                                   162
                                                                                                                                       163
                                                                                                                                               OP MAX:
                                                                                                                                                                                  165
                                                                              161
                                                                                                                           OP MIN:
                                                                                                                                                            164
                                                                                                                                                                    OP WITHIN:
                                                                                                                                                                                 crypto
OP RIPEMD160: 166 OP SHA1: 167 OP SHA256: 168 OP HASH160: 169 OP HASH256: 170 OP CODESEPARATOR: 171 OP CHECKSIG: 172 OP CHECKSIGVERIFY: 173 OP CHECKMULTISIG: 174 OP CHECKMULTISIGVERIFY: 175
                                                                                                                                                                               locktime
OP CHECKLOCKTIMEVERIFY: 177
```

ルール:

- ① 全てのクイズがP2SHのアドレスになりますので、ビットコインの回収はこちらで https://bip32jp.github.io/english/createp2sh.html
- ② 一番上の枠に出題を入力いただき、P2SHのアドレスを作成し、出題と同じか確認 フォーマット: 開発環境アドレス,本番アドレス
- ③ 同じアドレスであれば、回答は2つ目の枠で、送金先のビットコインアドレスは3つ目
- ④ エラーが返ってくる場合は殆ど回答が正しくないという意味なので、ご了承下さい
- ⑤ 回収できたら、即座に手挙げて下さい。
- ⑥ 先に例題をみんなでやります。

例題: 2MzuYNTgfcezpymFsHLGjsNPchnKXwNP7SK, 39MLJike1CVUmydKcCesFRQMVS7N8x5CNS

022d4549c2f5aca5697dc232390770a99d6ee6ee139fda0fa0412e77a7bcd4b3ee OP_CHECKSIGVERIFY

OP_5

OP_ADD

OP_8

OP_EQUAL

(署名用秘密鍵:

開発環境: cPvTKVTkYRRvaY6xnfpRv6EkNK5hdR5MPXvvvdMckb1DGZMxZWFc

番環境: KyZTraTu7MjfR6dhQG1JYmjgk5nHxxyfKVnTpCu7FUMD1pHb68YY)

第1問: 2MyDa63t2Jc7s6hnMTMdzQANmToqCFxT1gw, 37fN2Jwzh9cWtv9onE27nDPWFTd2UpH8Nw

022d4549c2f5aca5697dc232390770a99d6ee6ee139fda0fa0412e77a7bcd4b3ee

OP_CHECKSIGVERIFY

OP_8

OP SUB

OP 14

OP ADD

OP 16

OP_EQUAL

(署名用秘密鍵:

開発環境: cPvTKVTkYRRvaY6xnfpRv6EkNK5hdR5MPXvvvdMckb1DGZMxZWFc

本番環境: KyZTraTu7MjfR6dhQG1JYmjgk5nHxxyfKVnTpCu7FUMD1pHb68YY)

第2問: 2N4zWqUA8FGozyriGPURCe9BJJdwwdV4nzv, 3DSJmjE6dpJen55iiLoL2CC36HjmqvLxLc

022d4549c2f5aca5697dc232390770a99d6ee6ee139fda0fa0412e77a7bcd4b3ee

OP_CHECKSIGVERIFY

OP_IF

OP TRUE

OP_ELSE

OP_RETURN

OP_ENDIF

(署名用秘密鍵:

開発環境: cPvTKVTkYRRvaY6xnfpRv6EkNK5hdR5MPXvvvdMckb1DGZMxZWFc

本番環境: KyZTraTu7MjfR6dhQG1JYmjgk5nHxxyfKVnTpCu7FUMD1pHb68YY)

第3問: 2Mz1vb1aYn1WMsQbkTXqsbZAqp81xUTWYWi, 38TiXGeXAZ11fcyCnQDzycBabmonkMBK7y

022d4549c2f5aca5697dc232390770a99d6ee6ee139fda0fa0412e77a7bcd4b3ee OP CHECKSIGVERIFY OP 3DUP OP ADD OP 12 OP EOUAL OP SWAP OP ROT OP ADD OP 9 OP EOUAL OP 2SWAP OP ADD OP 7 OP EQUAL OP BOOLAND OP BOOLAND

(署名用秘密鍵:

開発環境: cPvTKVTkYRRvaY6xnfpRv6EkNK5hdR5MPXvvvdMckb1DGZMxZWFc本番環境: KyZTraTu7MjfR6dhQG1JYmjgk5nHxxyfKVnTpCu7FUMD1pHb68YY)

第4問: 2NBLeNoFWU2ESCFBYdj7MoszGw9zorrQGXg, 3KnSK4KUrZj5zTYzxbVVBw11ione6uvhFp

022d4549c2f5aca5697dc232390770a99d6ee6ee139fda0fa0412e77a7bcd4b3ee OP CHECKSIGVERIFY

OP HASH160

08f79eecd1dcff6810a5105f8d3d3df971131a48

OP_EQUAL

(署名用秘密鍵:

開発環境: cPvTKVTkYRRvaY6xnfpRv6EkNK5hdR5MPXvvvdMckb1DGZMxZWFc本番環境: KyZTraTu7MjfR6dhQG1JYmjgk5nHxxyfKVnTpCu7FUMD1pHb68YY)

第5問: 2N5WoqAzHr2cVYPsuRfkuU1LojgmonhLRHu, 3DxbmS4GEa79LcFMkY92r4MYXLZdyMPw7v

022d4549c2f5aca5697dc232390770a99d6ee6ee139fda0fa0412e77a7bcd4b3ee OP_CHECKSIGVERIFY OP_HASH256 6fe28c0ab6f1b372c1a6a246ae63f74f931e8365e15a089c68d619000000000 OP_EQUAL

(署名用秘密鍵:

開発環境: cPvTKVTkYRRvaY6xnfpRv6EkNK5hdR5MPXvvvdMckb1DGZMxZWFc本番環境: KyZTraTu7MjfR6dhQG1JYmjgk5nHxxyfKVnTpCu7FUMD1pHb68YY)

ヒント: 比べるデータの中に 0がたくさん付いていること

ヒント: (ノーコメント) https://bip32jp.github.io/english/blockheader.html

御清聴ありがとうございました。