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

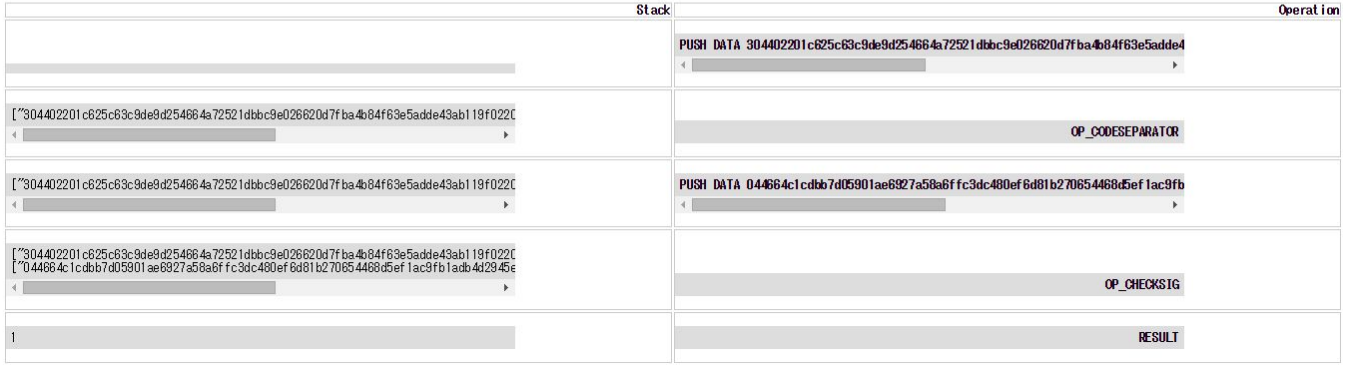
・チューリング不完全

ビットコイン取引におけるScript

P2PK Script

問いかけ:
① PUSH_DATA(公開鍵) ② OP_CHECKSIG

回答:
① PUSH_DATA(電子署名)

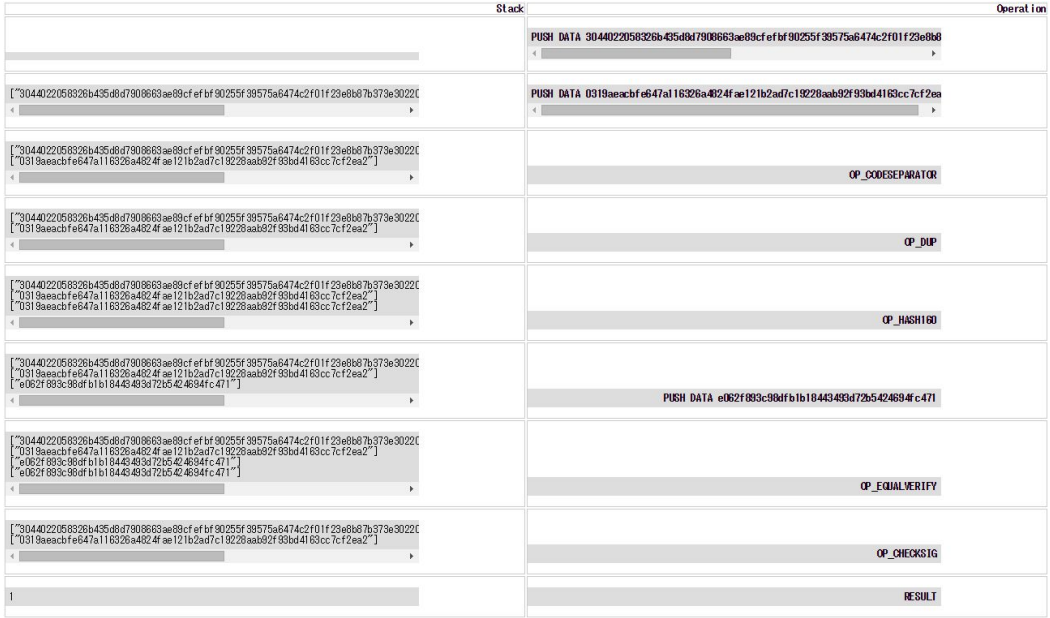


注:https://webbtc.com/script/ 例: https://blockchain.info/tx-index/232448

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)



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

Stack	Operation
	PUSH DATA 52210297ad3ee53d7ba40a227c1958609cca32197dd905092078c4f04847296bc
["52210297ad3ee53d7ba40a227c1958609cca32197dd905092078c4f04847296bce824e21035	OP_CODESEPARATOR
["52210297ad3ee53d7ba40a227c1958609cca32197dd905092078c4f04847296bce824e21035	OP_HASH160
["09ff1296c1532bccb21e00bd77b0a315a6491700"]	PUSH DATA 09ff1296c1532bccb21e00bd77b0a315a6491700
["09ff1296c1532bccb21e00bd77b0a315a6491700"] ["09ff1296c1532bccb21e00bd77b0a315a6491700"]	OP_EQUAL
1	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 CODES

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

// push value
OP_FALSE: 0 OP_0: 0 OP_PUSHDATA1: 76 OP_PUSHDATA2: 77 OP_PUSHDATA4: 78 OP_1NEGATE: 79 OP_TRUE: 81 OP_1: 81 OP_2: 82
OP_3: 83 OP_4: 84 OP_5: 85 OP_6: 86 OP_7: 87 OP_8: 88 OP_9: 89 OP_10: 90 OP_11: 91 OP_12: 92
OP_13: 93 OP_14: 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_TOALTSTACK: 107 OP_FROMALTSTACK: 108 OP_2DROP: 109 OP_2DUP: 110 OP_3DUP: 111 OP_2OVER: 112 OP_2ROT: 113 OP_2SWAP: 114 OP_IFDUP: 115 OP_DEPTH: 116
OP_DROP: 117 OP_DUP: 118 OP_NIP: 119 OP_OVER: 120 OP_PICK: 121 OP_ROLL: 122 OP_ROT: 123 OP_SWAP: 124 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: 143 OP_ABS: 144 OP_NOT: 145 OP_0NOTEQUAL: 146 OP_ADD: 147 OP_SUB: 148
OP_BOOLAND: 154 OP_BOOLOR: 155 OP_NUMEQUAL: 156 OP_NUMEQUALVERIFY: 157 OP_NUMNOTEQUAL: 158
OP_LESSTHAN: 159 OP_GREATERTHAN: 160 OP_LESSTHANOREQUAL: 161 OP_GREATERTHANOREQUAL: 162 OP_MIN: 163 OP_MAX: 164 OP_WITHIN: 165

// 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

ビットコインクイズ

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
本番環境: 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_EQUAL
OP_SWAP　OP_ROT
OP_ADD　OP_9
OP_EQUAL　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
6fe28c0ab6f1b372c1a6a246ae63f74f931e8365e15a089c68d6190000000000
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。