Bitcoin Script Analysis

Goals

- What scripts are being used the most?
- What interesting scripts are out there?
- How is script usage changing?
- How can we keep track of unusual scripts?

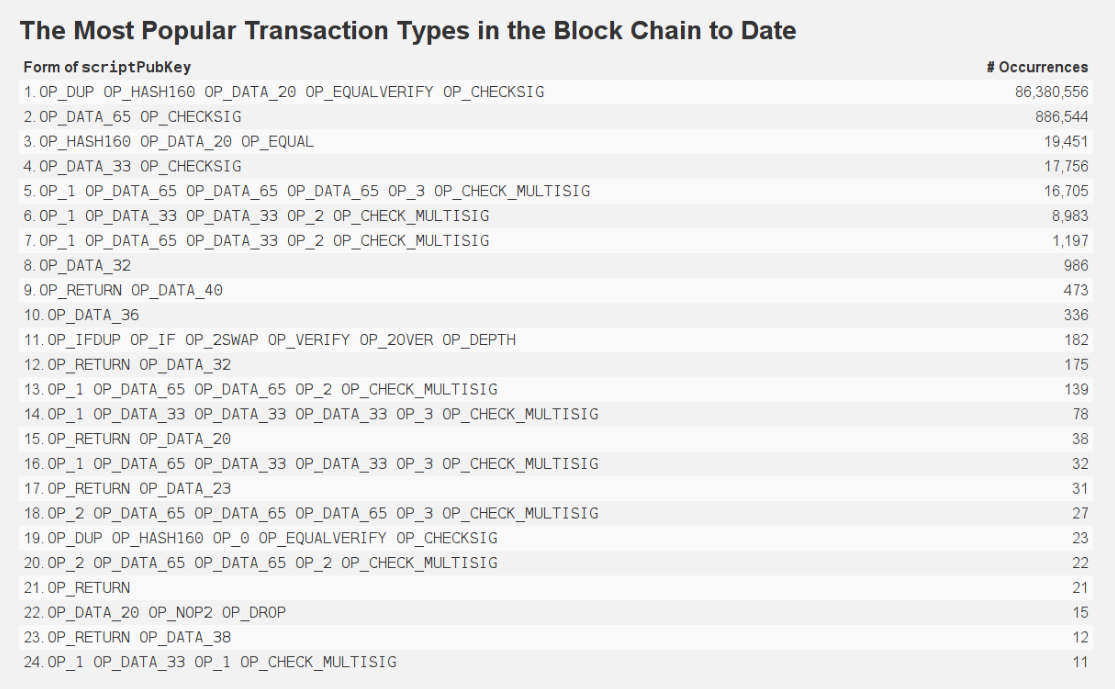
Inspiration

QuantaBytes: “A Survey of Bitcoin Transaction Types”

Includes first 290,000 blocks, up to about last april

Explains common types of transactions

Snapshot in time



The Most Popular Transaction Types in the Block Chain to Date

Form of scriptPubKey	# Occurrences
1. OP_DUP OP_HASH160 OP_DATA_20 OP_EQUALVERIFY OP_CHECKSIG	86,380,556
2. OP_DATA_65 OP_CHECKSIG	886,544
3. OP_HASH160 OP_DATA_20 OP_EQUAL	19,451
4. OP_DATA_33 OP_CHECKSIG	17,756
5. OP_1 OP_DATA_65 OP_DATA_65 OP_DATA_65 OP_3 OP_CHECK_MULTISIG	16,705
6. OP_1 OP_DATA_33 OP_DATA_33 OP_2 OP_CHECK_MULTISIG	8,983
7. OP_1 OP_DATA_65 OP_DATA_33 OP_2 OP_CHECK_MULTISIG	1,197
8. OP_DATA_32	986
9. OP_RETURN OP_DATA_40	473
10. OP_DATA_36	336
11. OP_IFDUP OP_IF OP_2SWAP OP_VERIFY OP_2OVER OP_DEPTH	182
12. OP_RETURN OP_DATA_32	175
13. OP_1 OP_DATA_65 OP_DATA_65 OP_2 OP_CHECK_MULTISIG	139
14. OP_1 OP_DATA_33 OP_DATA_33 OP_DATA_33 OP_3 OP_CHECK_MULTISIG	78
15. OP_RETURN OP_DATA_20	38
16. OP_1 OP_DATA_65 OP_DATA_33 OP_DATA_33 OP_3 OP_CHECK_MULTISIG	32
17. OP_RETURN OP_DATA_23	31
18. OP_2 OP_DATA_65 OP_DATA_65 OP_DATA_65 OP_3 OP_CHECK_MULTISIG	27
19. OP_DUP OP_HASH160 OP_0 OP_EQUALVERIFY OP_CHECKSIG	23
20. OP_2 OP_DATA_65 OP_DATA_65 OP_2 OP_CHECK_MULTISIG	22
21. OP_RETURN	21
22. OP_DATA_20 OP_NOP2 OP_DROP	15
23. OP_RETURN OP_DATA_38	12
24. OP_1 OP_DATA_33 OP_1 OP_CHECK_MULTISIG	11

Project Deliverables

- Script
  - Database of unusual transactions
  - Report on most common transaction types
  - Track raw count and value transferred
  - Updates with new blocks on each run

Project Deliverables

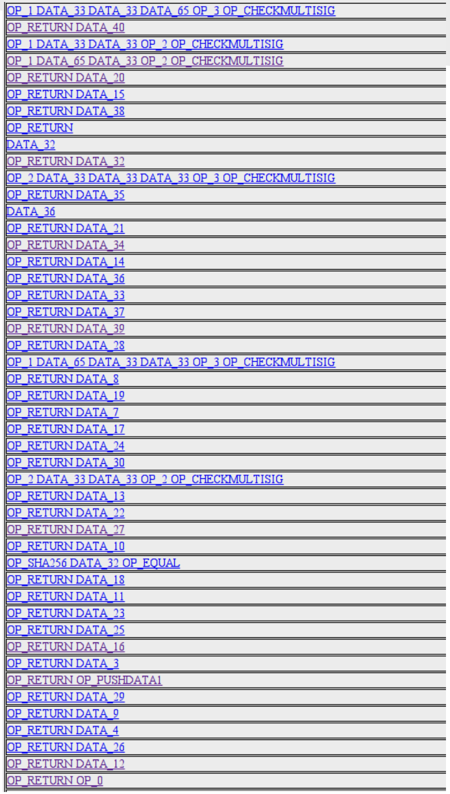
- Web Page
  - Provides view of data in database
  - Graph of most common unusual transactions
  - Links to Blockchain.info
  - configurable time range for data retrieval

Script Types

- Pay to public key transaction
- Pay to script hash transaction
- Mining rewards
- Multisignature transaction
- Data Storage
- Other

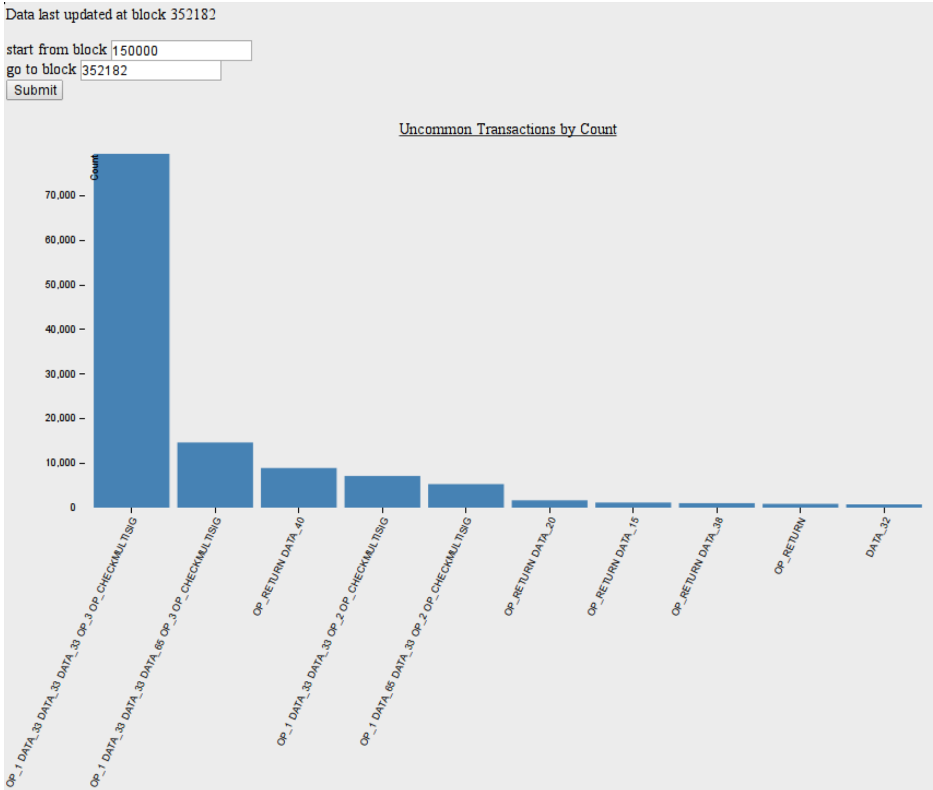
“Unusual” Scripts

- Multisignature Transactions
- Data Storage
- Malformed Scripts



OP_1 DATA_33 DATA_33 DATA_65 OP_3 OP_CHECKMULTISIG
OP_RETURN DATA_40
OP_1 DATA_33 DATA_33 OP_2 OP_CHECKMULTISIG
OP_1 DATA_65 DATA_33 OP_2 OP_CHECKMULTISIG
OP_RETURN DATA_20
OP_RETURN DATA_15
OP_RETURN DATA_38
OP_RETURN
DATA_32
OP_RETURN DATA_32
OP_2 DATA_33 DATA_33 DATA_33 OP_3 OP_CHECKMULTISIG
OP_RETURN DATA_35
DATA_36
OP_RETURN DATA_21
OP_RETURN DATA_34
OP_RETURN DATA_14
OP_RETURN DATA_36
OP_RETURN DATA_33
OP_RETURN DATA_37
OP_RETURN DATA_39
OP_RETURN DATA_28
OP_1 DATA_65 DATA_33 DATA_33 OP_3 OP_CHECKMULTISIG
OP_RETURN DATA_8
OP_RETURN DATA_19
OP_RETURN DATA_7
OP_RETURN DATA_17
OP_RETURN DATA_24
OP_RETURN DATA_30
OP_2 DATA_33 DATA_33 OP_2 OP_CHECKMULTISIG
OP_RETURN DATA_13
OP_RETURN DATA_22
OP_RETURN DATA_27
OP_RETURN DATA_10
OP_SHA256 DATA_32 OP_EQUAL
OP_RETURN DATA_18
OP_RETURN DATA_11
OP_RETURN DATA_23
OP_RETURN DATA_25
OP_RETURN DATA_16
OP_RETURN DATA_3
OP_RETURN OP_PUSHDATA1
OP_RETURN DATA_29
OP_RETURN DATA_9
OP_RETURN DATA_4
OP_RETURN DATA_26
OP_RETURN DATA_12
OP_RETURN OP_0

Multisignature Scripts



Data last updated at block 352182

start from block 150000
go to block 352182

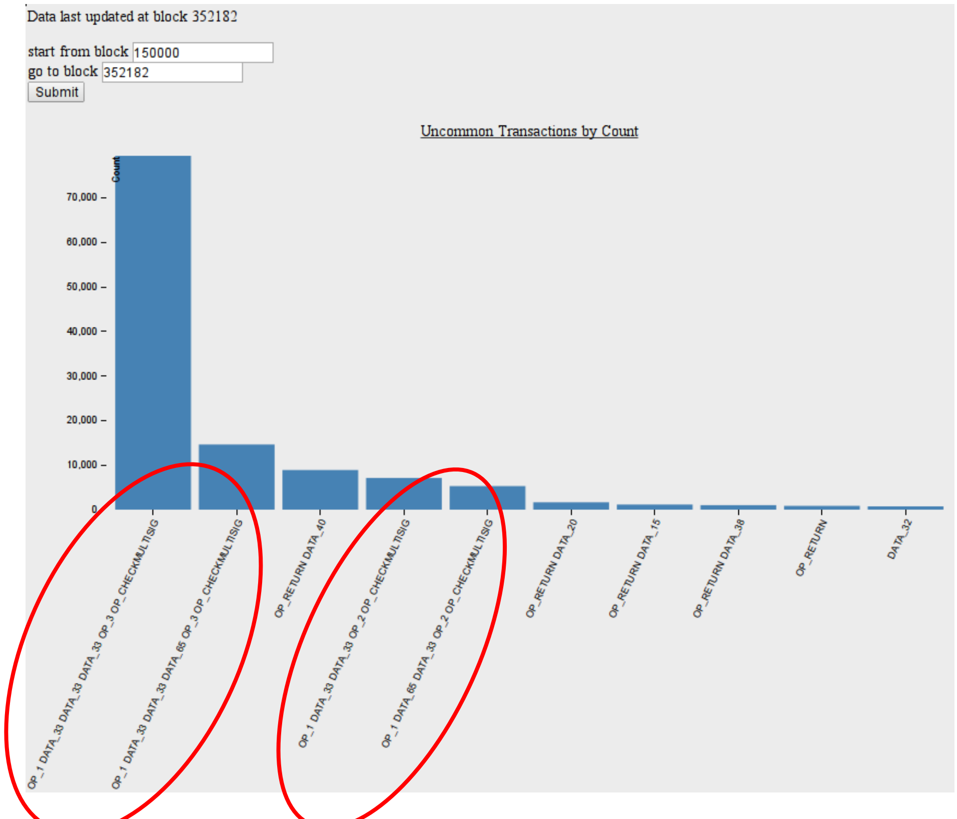
Submit
Uncommon Transactions by Count
Count
70,000
60,000
50,000
40,000
30,000
20,000
10,000
0
OP_1 DATA_33 DATA_33 DATA_33 OP_3 OP_CHECKMULTISIG
OP_1 DATA_33 DATA_33 DATA_65 OP_3 OP_CHECKMULTISIG
OP_RETURN DATA_40
OP_1 DATA_33 DATA_33 OP_2 OP_CHECKMULTISIG
OP_1 DATA_65 DATA_33 OP_2 OP_CHECKMULTISIG
OP_RETURN DATA_20
OP_RETURN DATA_15
OP_RETURN DATA_38
OP_RETURN
DATA_32

Multisig popularity has **boomed**

About **5x** as many now as last year

Total number of transactions roughly doubled

Multisignature Scripts



Data last updated at block 352182

start from block 150000

go to block 352182

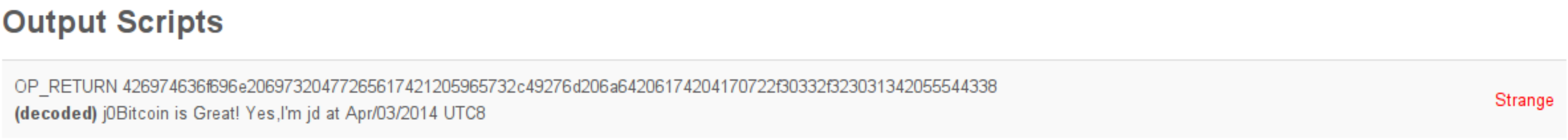
Submit
Uncommon Transactions by Count
Count
70,000
60,000
50,000
40,000
30,000
20,000
10,000
0
OP_1 DATA_33 DATA_33 DATA_33 OP_3 OP_CHECKMULTISIG
OP_1 DATA_33 DATA_33 DATA_65 OP_3 OP_CHECKMULTISIG
OP_RETURN DATA_40
OP_1 DATA_33 DATA_33 OP_2 OP_CHECKMULTISIG
OP_1 DATA_65 DATA_33 OP_2 OP_CHECKMULTISIG
OP_RETURN DATA_20
OP_RETURN DATA_15
OP_RETURN DATA_38
OP_RETURN
DATA_32

Multisig popularity has **boomed**

About **5x** as many now as last year

Total number of transactions roughly doubled

Data Storage

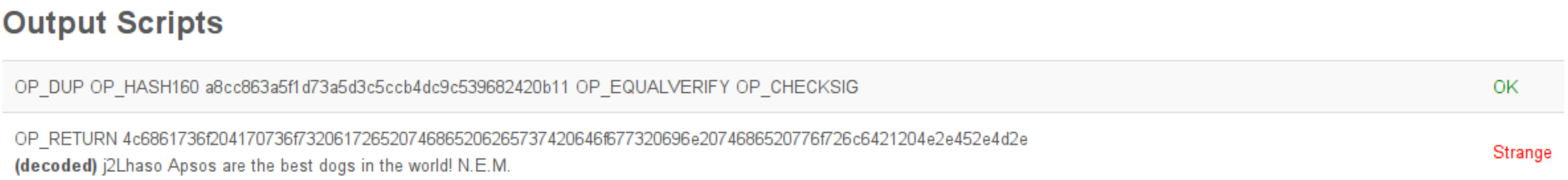


Output Scripts

OP_RETURN 426974636f696e2069732047726561742120596573 2c49276d206a64206174204170722f30332f3230313420555443 38

(decoded) j0Bitcoin is Great! Yes,I'm jd at Apr/03/2014 UTC8

Strange



Output Scripts

OP_DUP OP_HASH160 a8cc863a5f1d73a5d3c5ccb4dc9c539682420b11 OP_EQUALVERIFY OP_CHECKSIG

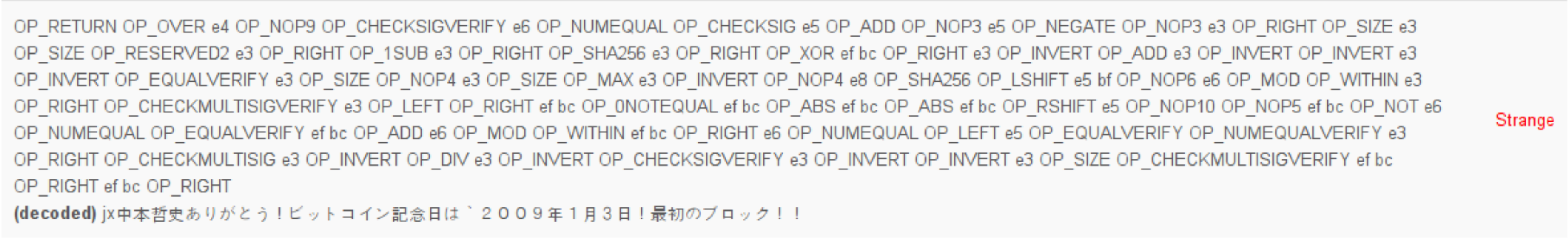
OK

OP_RETURN 4c6861736f204170736f7320617265207468652062657374 20646f677320696e20746865 20776f726c6421204e2e452e4d2e

(decoded) j2Lhaso Apsos are the best dogs in the world! N.E.M.

Strange

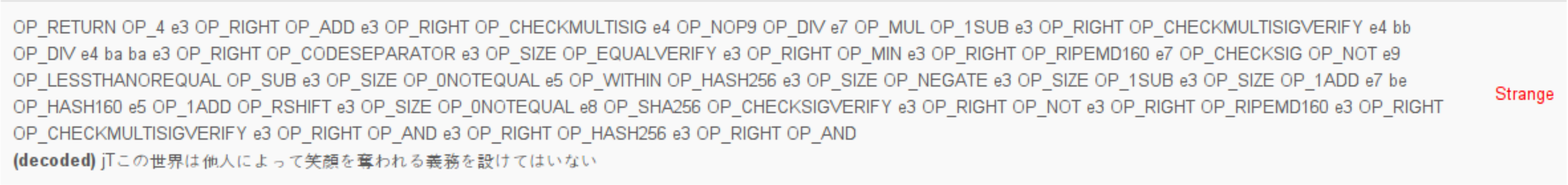
Data Storage



```
OP_RETURN OP_OVER e4 OP_NOP9 OP_CHECKSIGVERIFY e6 OP_NUMEQUAL OP_CHECKSIG e5 OP_ADD OP_NOP3 e5 OP_NEGATE OP_NOP3 e3 OP_RIGHT OP_SIZE e3
OP_SIZE OP_RESERVED2 e3 OP_RIGHT OP_1SUB e3 OP_RIGHT OP_SHA256 e3 OP_RIGHT OP_XOR ef bc OP_RIGHT e3 OP_INVERT OP_ADD e3 OP_INVERT OP_INVERT e3
OP_INVERT OP_EQUALVERIFY e3 OP_SIZE OP_NOP4 e3 OP_SIZE OP_MAX e3 OP_INVERT OP_NOP4 e8 OP_SHA256 OP_LSHIFT e5 bf OP_NOP6 e6 OP_MOD OP_WITHIN e3
OP_RIGHT OP_CHECKMULTISIGVERIFY e3 OP_LEFT OP_RIGHT ef bc OP_0NOTEQUAL ef bc OP_ABS ef bc OP_ABS ef bc OP_RSHIFT e5 OP_NOP10 OP_NOP5 ef bc OP_NOT e6
OP_NUMEQUAL OP_EQUALVERIFY ef bc OP_ADD e6 OP_MOD OP_WITHIN ef bc OP_RIGHT e6 OP_NUMEQUAL OP_LEFT e5 OP_EQUALVERIFY OP_NUMEQUALVERIFY e3
OP_RIGHT OP_CHECKMULTISIG e3 OP_INVERT OP_DIV e3 OP_INVERT OP_CHECKSIGVERIFY e3 OP_INVERT OP_INVERT e3 OP_SIZE OP_CHECKMULTISIGVERIFY ef bc
OP_RIGHT ef bc OP_RIGHT
```

(decoded) jx中本哲史ありがとう！ビットコイン記念日は｀２００９年１月３日！最初のブロック！！

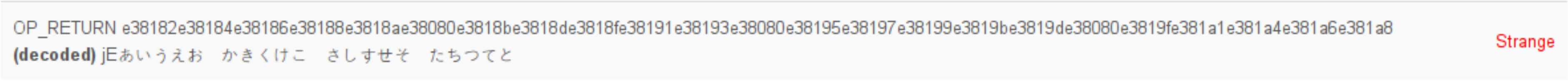
Strange



```
OP_RETURN OP_4 e3 OP_RIGHT OP_ADD e3 OP_RIGHT OP_CHECKMULTISIG e4 OP_NOP9 OP_DIV e7 OP_MUL OP_1SUB e3 OP_RIGHT OP_CHECKMULTISIGVERIFY e4 bb
OP_DIV e4 ba ba e3 OP_RIGHT OP_CODESEPARATOR e3 OP_SIZE OP_EQUALVERIFY e3 OP_RIGHT OP_MIN e3 OP_RIGHT OP_RIPEMD160 e7 OP_CHECKSIG OP_NOT e9
OP_LESSTHANOREQUAL OP_SUB e3 OP_SIZE OP_0NOTEQUAL e5 OP_WITHIN OP_HASH256 e3 OP_SIZE OP_NEGATE e3 OP_SIZE OP_1SUB e3 OP_SIZE OP_1ADD e7 be
OP_HASH160 e5 OP_1ADD OP_RSHIFT e3 OP_SIZE OP_0NOTEQUAL e8 OP_SHA256 OP_CHECKSIGVERIFY e3 OP_RIGHT OP_NOT e3 OP_RIGHT OP_RIPEMD160 e3 OP_RIGHT
OP_CHECKMULTISIGVERIFY e3 OP_RIGHT OP_AND e3 OP_RIGHT OP_HASH256 e3 OP_RIGHT OP_AND
```

(decoded) jTこの世界は他人によって笑顔を奪われる義務を設けてはいない

Strange



```
OP_RETURN e38182e38184e38186e38188e3818ae38080e3818be3818de3818fe38191e38193e38080e38195e38197e38199e3819be3819de38080e3819fe381a1e381a4e381a6e381a8
```

(decoded) jEあいうえお　かきくけこ　さしすせそ　たちつてと

Strange

Questions?