

Demystifying
Mastering Bitcoin
Chapter 4
by Applying Libbitcoin,
UNIX, and Python
Command Line Interfaces

Author: Scott Holben
Nov. 17th, 2018

Base 58

Decimal (Base10)	Hexadecimal (Base16)	Binary (Base2)
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

Base58

is used extensively by
Cryptocurrencies and
Comprised of this Character set:

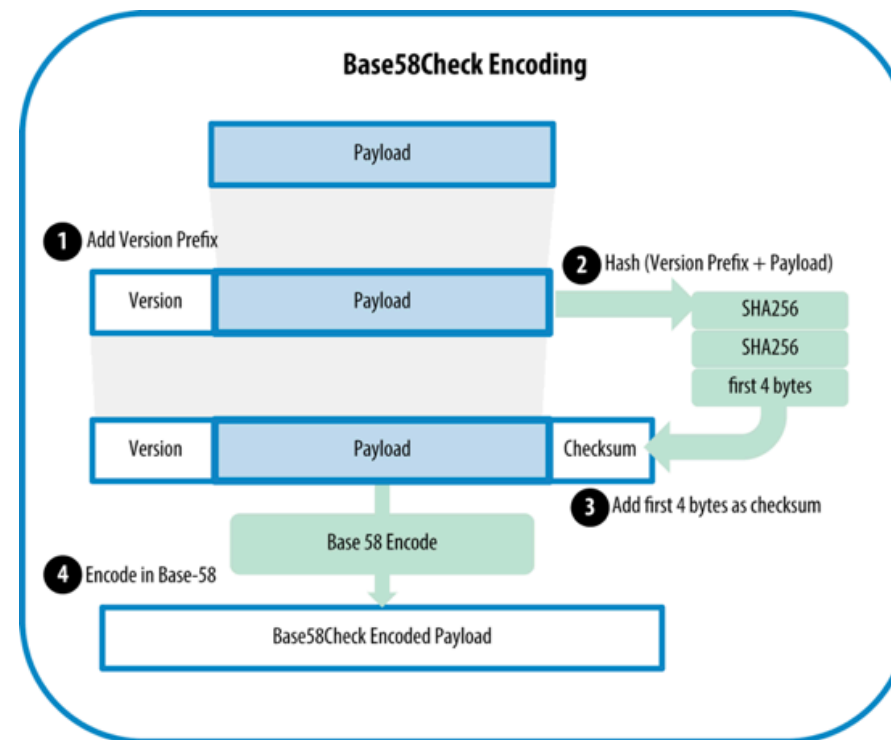
123456789
ABCDEFGHIJKLMNPQRSTUVWXYZ
abcdefghijklmnopqrstuvwxy

Is Missing: "0", "I", "O", "1"

$$10 + 26 + 26 - 4 = 58$$

Wallet Input Format (WIF) Private Key Encoding

<https://github.com/libbitcoin/libbitcoin-explorer/wiki> - reference for using the bx command line interface



```
% echo 1E99423A4ED27608A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDD | sed 's/^/80/' | bx sha256 | bx sha256 | cut -c 1-8  
c47e83ff
```

```
% echo 801E99423A4ED27608A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDDc47e83ff | bx base58-encode  
5J3mBbAH58CpQ3Y5RNJpUKPE62SQ5tfcvU2JpbnkeyhfsYB1Jcn
```

Or

```
% echo 1E99423A4ED27608A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDD | bx base58check-encode -v 128  
5J3mBbAH58CpQ3Y5RNJpUKPE62SQ5tfcvU2JpbnkeyhfsYB1Jcn
```

```
% echo 1E99423A4ED27608A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDD | sed 's/$/01/' | bx base58check-encode -v 128  
KxFC1jmwWCoACiCAWZ3eXa96mBM6tb3TYzGmf6YwgdGWZgawvrt
```

Elliptic Curve Math

$y^2 = x^3 + ax + b \pmod{p}$ per <http://www.secg.org/sec2-v2.pdf> page 9,
Weierstrass normal form for elliptic curves when $4a^3 + 27b^2 \neq 0$.

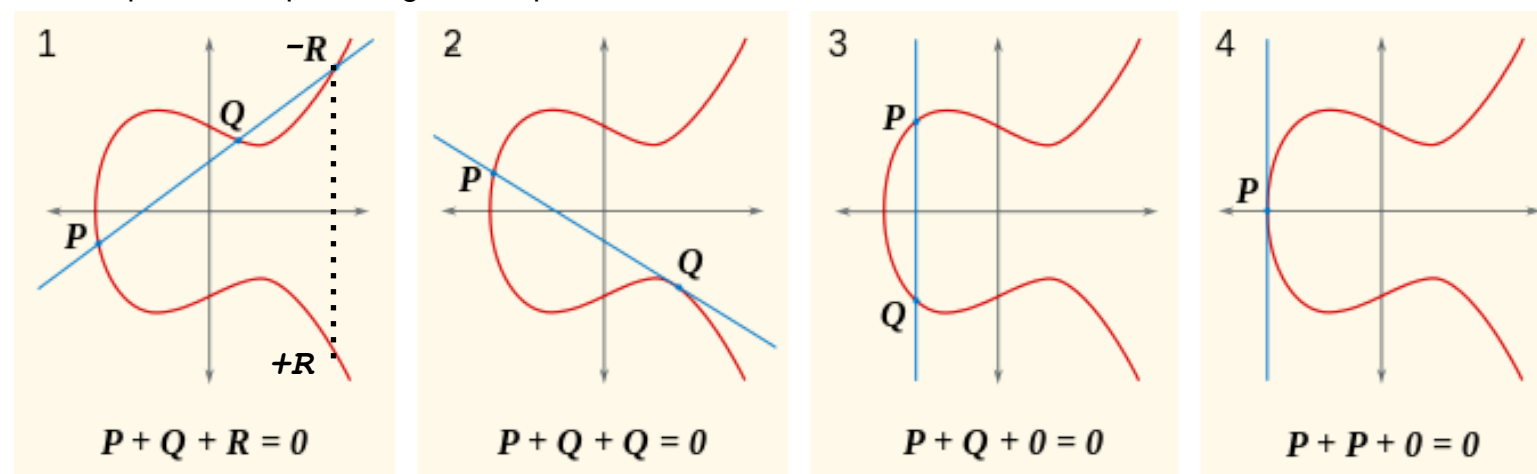
secp256k1: $a = 0$, $b = 7$, $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$ and p is a prime number

$G_x = 0x79BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798$

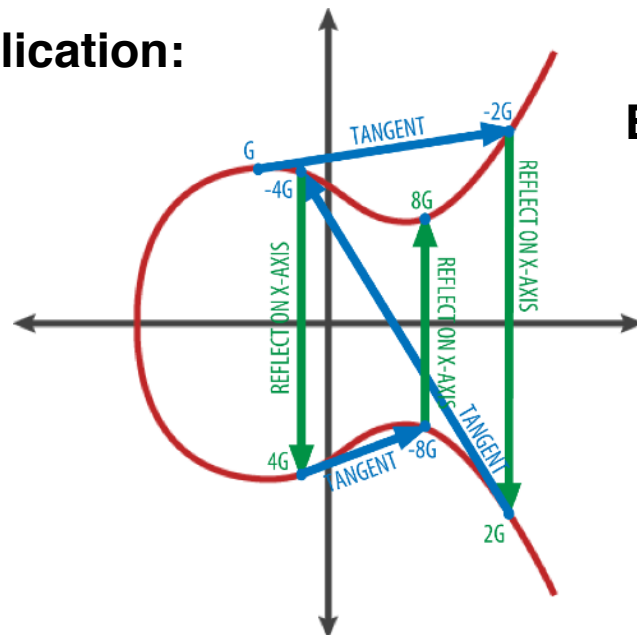
$G_y = 0x483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A68554199C47D08FFB10D4B8$

$n = \text{curve order} = 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEBAAEDCE6AF48A03BBFD25E8CD0364141$

Addition: source https://en.wikipedia.org/wiki/Elliptic_curve#



Multiplication:



Excellent Sources for Learning:

<http://andrea.corbellini.name/2015/05/30/elliptic-curve-cryptography-ecdh-and-ecdsa/>

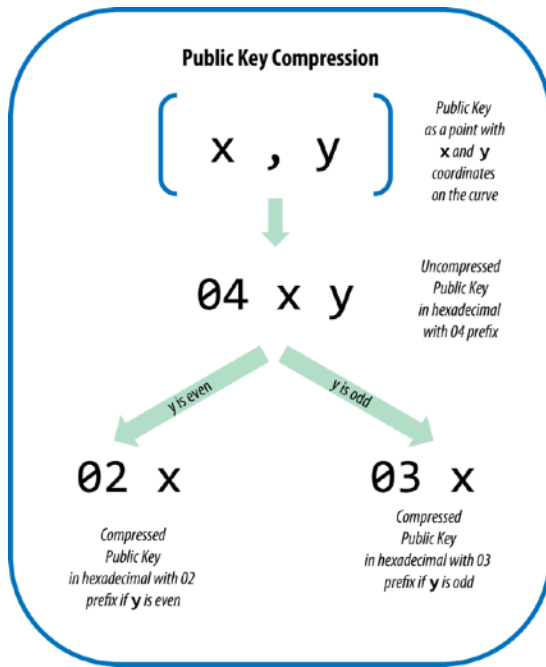
<https://cdn.rawgit.com/andreacorbellini/ecc/920b29a/interactive/real-add.html>

<https://cdn.rawgit.com/andreacorbellini/ecc/920b29a/interactive/real-mul.html>

<https://cdn.rawgit.com/andreacorbellini/ecc/920b29a/interactive/modk-add.html>

<https://cdn.rawgit.com/andreacorbellini/ecc/920b29a/interactive/modk-mul.html>

Point of Infinity for the secp256k1 Elliptic Curve



$$\mathbf{K} = \mathbf{k}^* \mathbf{G} = \mathbf{G}^* \mathbf{k}$$

- is scalar integer point multiplication defined by the Point of Infinity ($\mathbf{G}$), $\mathbf{K}$ is a public key (is a trap door function defined)
- An **uncompressed public key** is an $[x, y]$ pair with 04 prefix
- A **compressed public key** is an x coordinate with a 02 prefix ($+y$) or 03 prefix ($-y$)

where: **k** is the private key and must be an integer

k > 0 and

k < curve order (**n**) and n is prime

p > n

[illegible][illegible]

Point of Infinity in Base 10:

G = 0255066263022277343669578718895168534326250603453777594175500187360389116729240

G = 045506626302227734366957871889516853432625060345377759417550018736038911672924032670510020758816978083085130507043184471273380659243275938904335757337482424

Point of Infinity in Base 16: per <http://www.secg.org/sec2-v2.pdf> page 9

G = 0279BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798

G = 0479BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A68554199C47D08FFB10D4B8

[illegible][illegible]

secp256k1 Point of Infinity Integer Multiplication

$K = k \cdot G = G \cdot k$ (scalar point multiplication is an invertible trap door function)

```
1*G % bx ec-to-public 0000000000000000000000000000000000000000000000000000000000000001
0279be667ef9dcbbac55a06295ce870b07029bfcdb2dce28d959f2815b16f81798

2*G % bx ec-to-public 0000000000000000000000000000000000000000000000000000000000000002
02c6047f9441ed7d6d3045406e95c07cd85c778e4b8cef3ca7abac09b95c709ee5

3*G % bx ec-to-public 0000000000000000000000000000000000000000000000000000000000000003
02f9308a019258c31049344f85f89d5229b531c845836f99b08601f113bce036f9

4*G % bx ec-to-public 0000000000000000000000000000000000000000000000000000000000000004
02e493dbf1c10d80f3581e4904930b1404cc6c13900ee0758474fa94abe8c4cd13

8*G % bx ec-to-public 0000000000000000000000000000000000000000000000000000000000000008
022f01e5e15cca351daff3843fb70f3c2f0a1bdd05e5af888a67784ef3e10a2a01

1*G % bx ec-to-public -u 0000000000000000000000000000000000000000000000000000000000000001
0479be667ef9dcbbac55a06295ce870b07029bfcdb2dce28d959f2815b16f81798483ada7726a3c4655da4fbfc0e1108a8fd17b448a68554199c47d08ffb10d4b8

2*G % bx ec-to-public -u 0000000000000000000000000000000000000000000000000000000000000002
04c6047f9441ed7d6d3045406e95c07cd85c778e4b8cef3ca7abac09b95c709ee51ae168fea63dc339a3c58419466ceaeef7f632653266d0e1236431a950cfe52a

3*G % bx ec-to-public -u 0000000000000000000000000000000000000000000000000000000000000003
04f9308a019258c31049344f85f89d5229b531c845836f99b08601f113bce036f9388f7b0f632de8140fe337e62a37f3566500a99934c2231b6cb9fd7584b8e672

4*G % bx ec-to-public -u 0000000000000000000000000000000000000000000000000000000000000004
04e493dbf1c10d80f3581e4904930b1404cc6c13900ee0758474fa94abe8c4cd1351ed993ea0d455b75642e2098ea51448d967ae33bfbdfe40cfe97bdc47739922

8*G % bx ec-to-public -u 0000000000000000000000000000000000000000000000000000000000000008
042f01e5e15cca351daff3843fb70f3c2f0a1bdd05e5af888a67784ef3e10a2a015c4da8a741539949293d082a132d13b4c2e213d6ba5b7617b5da2cb76cbde904
```

Cyclic Ordinate “Normalization”

Enforcing secp256k1

0 < k1 < curve order

0 < k2 < curve order

0 < k1+ ... < curve order:

[illegible]

```
% bx ec-add-secrets FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEBAAEDCE6AF48A03BBFD25E8CD0364140
fffffffffffffffffffffffffffebaaedce6af48a03bbfd25e8cd0364140
```

```
% bx ec-add-secrets FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEBAAEDCE6AF48A03BBFD25E8CD0364141
Error: the argument ('FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEBAAEDCE6AF48A03BBFD25E8CD0364141') for option '--SECRET' is invalid
```

[illegible]

0 < k < curve order

$0 < k^* \dots < \text{curve order}:$

[illegible]

```
% bx ec-multiply-secrets FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEBAAEDCE6AF48A03BBFD25E8CD0364141
Error: the argument ('FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEBAAEDCE6AF48A03BBFD25E8CD0364141') for option '--SECRET' is invalid
```

```
% bx ec-multiply-secrets 79BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798
79BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798
8d31d7866c819d2d7d8ec9c3e9124631c0d5c4f5aa5c70e5142fd8a2bcc3fa5f
```

Public Key Calculations for secp256k1

Point of Infinity in Base 16 (G Spot on slide #4):

G = 0279BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798

G = 0479BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A68554199C47D08FFB10D4B8

k = 1E99423A4ED27608A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDD

K = **k*****G** = **G*****k**

```
% bx ec-multiply 0279BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798
1E99423A4ED27608A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDD
03f028892bad7ed57d2fb57bf33081d5cfcf6f9ed3d3d7f159c2e2fff579dc341a
```

```
% bx ec-multiply
0479BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A68554199C47D08FFB10D4B8
1E99423A4ED27608A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDD
04f028892bad7ed57d2fb57bf33081d5cfcf6f9ed3d3d7f159c2e2fff579dc341a07cf33da18bd734c600b96a72bbc4749d5141c90ec8ac328ae52ddfe2e505bdb
```

Or

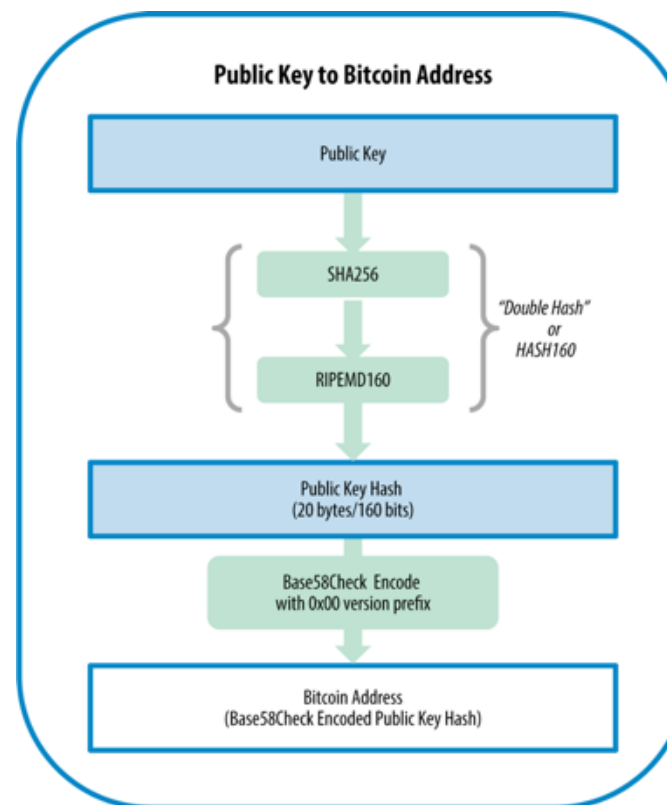
```
% bx ec-to-public -u 1E99423A4ED27608A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDD
03f028892bad7ed57d2fb57bf33081d5cfcf6f9ed3d3d7f159c2e2fff579dc341a
```

```
% bx ec-to-public -u 1E99423A4ED27608A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDD
04f028892bad7ed57d2fb57bf33081d5cfcf6f9ed3d3d7f159c2e2fff579dc341a07cf33da18bd734c600b96a72bbc4749d5141c90ec8ac328ae52ddfe2e505bdb
```

Bitcoin Address Calculation from Public Address

```
% bx ec-to-public 1E99423A4ED27608A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDD | bx sha256 | bx ripemd160 | bx base58check-encode -v 0  
1J7mdg5rbQyUHENYdx39WVWK7fsLpEoXZy
```

```
% bx ec-to-public -u 1E99423A4ED27608A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDD | bx sha256 | bx ripemd160 | bx base58check-encode -v 0  
1424C2F4bC9JidNjjTUZCbUxv6Sa1Mt62x
```



```
% bx ec-to-public 1E99423A4ED27608A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDD | bx ec-to-address -v 0  
1J7mdg5rbQyUHENYdx39WVWK7fsLpEoXZy
```

```
% bx ec-to-public -u 1E99423A4ED27608A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDD | bx ec-to-address -v 0  
1424C2F4bC9JidNjjTUZCbUxv6Sa1Mt62x
```

<https://www.blockchain.com/btc/address/1J7mdg5rbQyUHENYdx39WVWK7fsLpEoXZy>

<https://www.blockchain.com/btc/address/1424C2F4bC9JidNjjTUZCbUxv6Sa1Mt62x>

BIP 38 WIF Private Key AES Encryption - Roundtrip

```
% echo 5J3mBbAH58CpQ3Y5RNJpUKPE62SQ5tfcvU2JpbnkeyhfsYB1Jcn | bx base58check-decode  
wrapper  
{  
  checksum 4286807748  
  payload 1e99423a4ed27608a15a2616a2b0e9e52ced330ac530edcc32c8ffc6a526aedd  
  version 128  
}
```

```
% echo 5J3mBbAH58CpQ3Y5RNJpUKPE62SQ5tfcvU2JpbnkeyhfsYB1Jcn | bx base58check-decode | sed -n '/payload/ p' | sed 's/....payload.//'  
1e99423a4ed27608a15a2616a2b0e9e52ced330ac530edcc32c8ffc6a526aedd
```

```
% bx ec-to-ek -v 0 'MyTestPassphrase' 1e99423a4ed27608a15a2616a2b0e9e52ced330ac530edcc32c8ffc6a526aedd  
6PYJzKy76VEwRK87u9gx78w1FXGK7yRFbq13ZqjEpheRYfdHHwrvgRVCDd
```

```
% bx ek-to-ec 'MyTestPassphrase' 6PYJzKy76VEwRK87u9gx78w1FXGK7yRFbq13ZqjEpheRYfdHHwrvgRVCDd  
1e99423a4ed27608a15a2616a2b0e9e52ced330ac530edcc32c8ffc6a526aedd
```

```
% echo 1e99423a4ed27608a15a2616a2b0e9e52ced330ac530edcc32c8ffc6a526aedd | bx base58check-encode -v 128  
5J3mBbAH58CpQ3Y5RNJpUKPE62SQ5tfcvU2JpbnkeyhfsYB1Jcn
```

<https://github.com/cantonbecker/bitcoinpaperwallet> - Validate/Decrypt/Print

BIP 16 Pay to Script Hash (P2SH) Multisig Address

<https://github.com/bitcoin/bips/blob/master/bip-0016.mediawiki#520-byte-limitation>

“OP_2 <Pubkey1> <Pubkey2> <Pubkey3> <Pubkey4> OP_4 OP_CHECKMULTISIG”

From <https://en.bitcoin.it/wiki/Script>

0x52 = OP_2
0x54 = OP_4
0xae = OP_CHECKMULTISIG

P2SH address corresponding to a 2 of 4 multisig script for BTC:

```
% echo "2 [020ae29f86f404e4b302cfa17ff15d93149af6a54c80a4172d47e41f55f6a78d73]
[03664d528eb80096671ef9011c533ceb5df133238e3690d88f2960c786398b86b1] [029a449ea4a2155ea10002d704604bb3e8606631d35af20889a74b82b2dab572f6]
[0321602d78046d63256b1730b119blaca3428039f18fdb73ccf45ad3e148dd9b17] 4 checkmultisig" | bx script-encode
5221020ae29f86f404e4b302cfa17ff15d93149af6a54c80a4172d47e41f55f6a78d732103664d528eb80096671ef9011c533ceb5df133238e3690d88f2960c786398b86b121
029a449ea4a2155ea10002d704604bb3e8606631d35af20889a74b82b2dab572f6210321602d78046d63256b1730b119blaca3428039f18fdb73ccf45ad3e148dd9b1754ae
```

```
% echo "2 [020ae29f86f404e4b302cfa17ff15d93149af6a54c80a4172d47e41f55f6a78d73]
[03664d528eb80096671ef9011c533ceb5df133238e3690d88f2960c786398b86b1] [029a449ea4a2155ea10002d704604bb3e8606631d35af20889a74b82b2dab572f6]
[0321602d78046d63256b1730b119blaca3428039f18fdb73ccf45ad3e148dd9b17] 4 checkmultisig" | bx script-encode | bx sha256 | bx ripemd160 | bx
base58check-encode -v 5
3HMjXVGHwqqRTknhBGy7vEBFTGvDWzrQUW
```

```
% echo "2 [020ae29f86f404e4b302cfa17ff15d93149af6a54c80a4172d47e41f55f6a78d73]
[03664d528eb80096671ef9011c533ceb5df133238e3690d88f2960c786398b86b1] [029a449ea4a2155ea10002d704604bb3e8606631d35af20889a74b82b2dab572f6]
[0321602d78046d63256b1730b119blaca3428039f18fdb73ccf45ad3e148dd9b17] 4 checkmultisig" | bx script-to-address -v 5
3HMjXVGHwqqRTknhBGy7vEBFTGvDWzrQUW
```

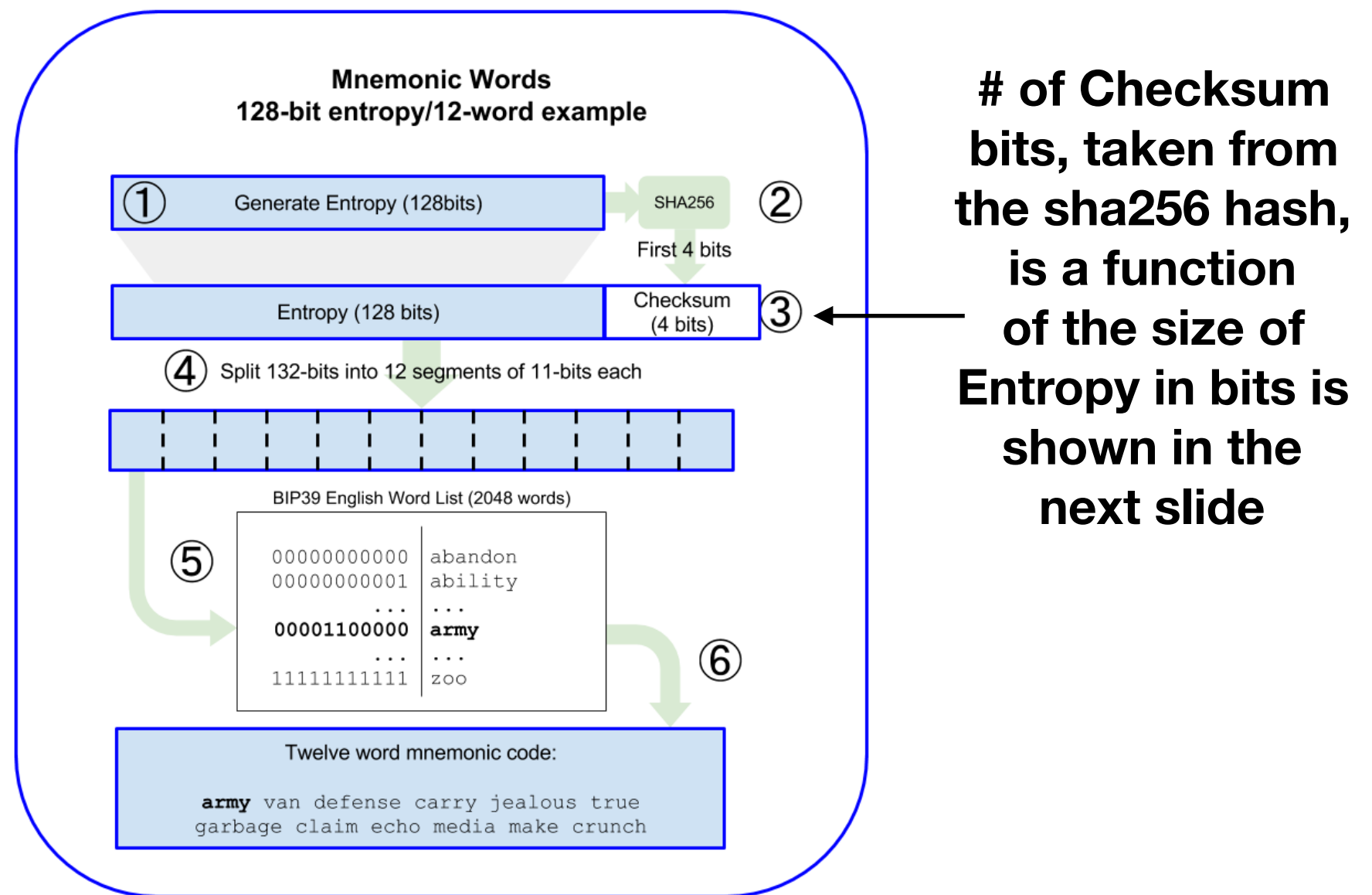
Demystifying
Mastering Bitcoin
Chapter 5
by Applying Libbitcoin,
UNIX, and Python
Command Line Interfaces

Author: Scott Holben
Nov. 8th, 2018

BIP 39

12 Word Example

HD wallet entropy seed is **0C1E24E5917779D297E14D45F14E1A1A**



<https://github.com/bitcoin/bips/blob/master/bip-0039/bip-0039-wordlists.md> supports 8 languages

BIP 39

Checksum Size

<https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki#generating-the-mnemonic>

ENT = entropy in bits

CS = checksum in bits

MS = mnemonic sentence length in words

ENT (1)	CS (3)	ENT+CS	MS
128	4	132	12
160	5	165	15
192	6	198	18
224	7	231	21
256	8	264	24

$$\text{CS} = \text{ENT}/32$$

$$\text{MS} = (\text{ENT} + \text{CS})/11$$

<https://github.com/bitcoin/bips/blob/master/bip-0039/bip-0039-wordlists.md> supports 8 languages

BIP 39 Example for Calculating 12 Words

```
% bx mnemonic-new 0C1E24E5917779D297E14D45F14E1A1A
army van defense carry jealous true garbage claim echo media make crunch
```

Or

```
% echo 0C1E24E5917779D297E14D45F14E1A1A | bx sha256
76e57a90f93135e97ce700a9e79196ba46315d65e696d0a4518270a8de3e80e4
```

```
% echo 0C1E24E5917779D297E14D45F14E1A1A | bx sha256 | cut -c 1-17
```

<https://github.com/bitcoin/bips/blob/master/bip-0039/english.txt>

0	C	1	E	2	4	E	5	9	1	7	7	7	9	D	2	9
0000	1100000	11110001001	00111001011	00100010111	01110111100	11101001010										
000001100000	011110001001	000111001011	000100010111	001110111100	011101001010											
0x060	0x789	0x1CB	0x117	0x3BC	0x74A											
96	1929	459	279	956	1866											
97	1930	460	280	957	1867											
army	van	defense	carry	jealous	true											

7	E	1	4	D	4	5	F	1	4	E	1	A	1	A	7
01011111100	00101001101	01000101111	10001010011	10000110100	00110100111										
001011111100	000101001101	001000101111	010001010011	010000110100	000110100111										
0x2FC	0x14D	0x22F	0x453	0x434	0x1A7										
764	333	559	1107	1076	423										
765	334	560	1108	1077	424										
gap	claim	echo	media	make	crunch										

Measuring Entropy for an ASCII String

<http://www.fourmilab.ch/random/>

```
% echo -n "This is a VERY poor low entropy brain wallet" | wc
      0      9    45
```

```
% echo -n "This is a VERY poor low entropy brain wallet" | ./ent
Entropy = 4.011204 bits per byte.
```

Optimum compression would reduce the size
of this 45 byte file by 49 percent.

Chi square distribution for 45 samples is 848.16, and randomly
would exceed this value less than 0.01 percent of the times.

Arithmetic mean value of data bytes is 92.4889 (127.5 = random).
Monte Carlo value for Pi is 4.000000000 (error 27.32 percent).
Serial correlation coefficient is -0.172575 (totally uncorrelated = 0.0).

Effective Entropy = 45 (bytes) x 4.011204 (bits/bytes)= 180.50418 bits

BIP 39 Pseudo Random Brain Wallet Examples

```
% echo -n "This is a VERY poor low entropy brain wallet" | bx base16-encode | bx sha256 | cut -c 1-8 | bx mnemonic-new  
health boil hotel
```

```
% echo -n "This is a VERY poor low entropy brain wallet" | bx base16-encode | bx sha256 | cut -c 1-32 | bx mnemonic-new  
health boil host ostrich fire spike body solar collect harvest catalog crystal
```

```
% echo -n "This is a VERY poor low entropy brain wallet" | bx base16-encode | bx sha256 | cut -c 1-40 | bx mnemonic-new  
health boil host ostrich fire spike body solar collect harvest catalog cup mix tattoo merge
```

```
% echo -n "This is a VERY poor low entropy brain wallet" | bx base16-encode | bx sha256 | cut -c 1-48 | bx mnemonic-new  
health boil host ostrich fire spike body solar collect harvest catalog cup mix tattoo market festival sudden please
```

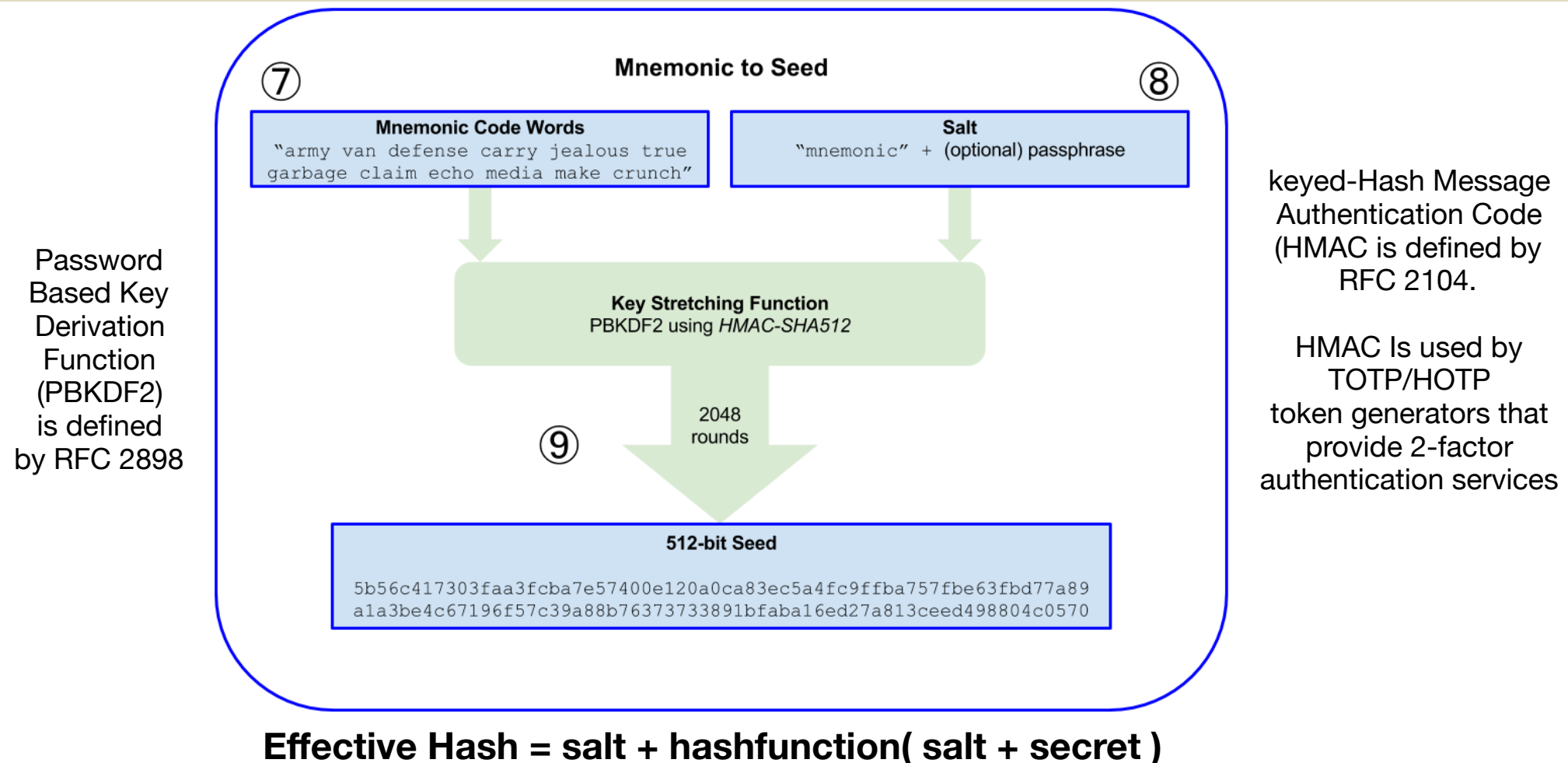
```
% echo -n "This is a VERY poor low entropy brain wallet" | bx base16-encode | bx sha256 | cut -c 1-56 | bx mnemonic-new  
health boil host ostrich fire spike body solar collect harvest catalog cup mix tattoo market festival sudden pony notable beach wreck
```

```
% echo -n "This is a VERY poor low entropy brain wallet" | bx base16-encode | bx sha256 | cut -c 1-64 | bx mnemonic-new  
health boil host ostrich fire spike body solar collect harvest catalog cup mix tattoo market festival sudden pony notable beach wide  
health original inform
```

```
% echo -n "This is a VERY poor low entropy brain wallet" | bx base16-encode | bx sha512 | bx sha256 | cut -c 1-64 | bx mnemonic-new  
saddle fork cheap uniform able amused lawsuit spoon lion surprise pony frozen palm hundred quality kite obvious invite alley salmon  
someone raven neutral team
```

BIP 39 Mnemonic to Seed

```
% echo "army van defense carry jealous true garbage claim echo media make crunch" | bx mnemonic-to-seed -p ""  
5b56c417303faa3fcba7e57400e120a0ca83ec5a4fc9ffba757fbe63fbd77a89a1a3be4c67196f57c39a88b76373733891bfaba16ed27a813ceed498804c0570
```



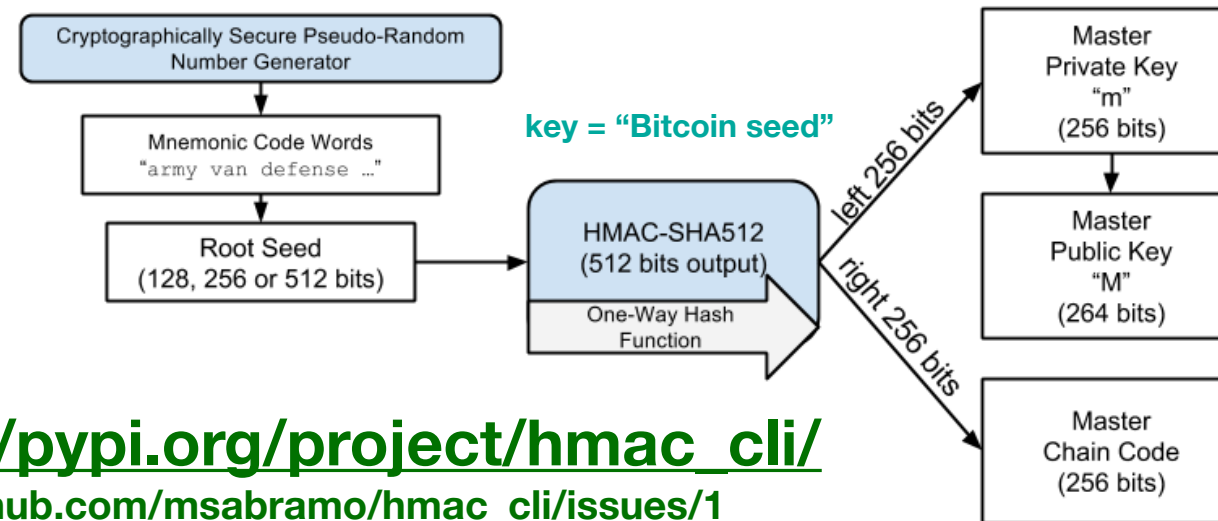
<https://pypi.org/project/stretch/>

`stretch->passlib.pbkdf2( secret, "mnemonic"+salt, rounds=2048, keylength=64, sha512 )`

<https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki#from-mnemonic-to-seed>

```
% stretch -f sha512 -r 2048 "army van defense carry jealous true garbage claim echo media make crunch" mnemonic | sed 's/^b.//' |  
sed 's/.$///' | bx base64-decode | bx base16-encode  
5b56c417303faa3fcba7e57400e120a0ca83ec5a4fc9ffba757fbe63fbd77a89a1a3be4c67196f57c39a88b76373733891bfaba16ed27a813ceed498804c0570
```

Calculating BIP 32/39 Extended Root Keys



https://pypi.org/project/hmac_cli/
https://github.com/msabramo/hmac_cli/issues/1

<https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki#master-key-generation> mentions "Bitcoin seed"

```
% echo "army van defense carry jealous true garbage claim echo media make crunch" | bx mnemonic-to-seed -p ""
5b56c417303faa3fcba7e57400e120a0ca83ec5a4fc9ffba757fbe63fbd77a89a1a3be4c67196f57c39a88b76373733891bfaba16ed27a813ceed498804c0570
```

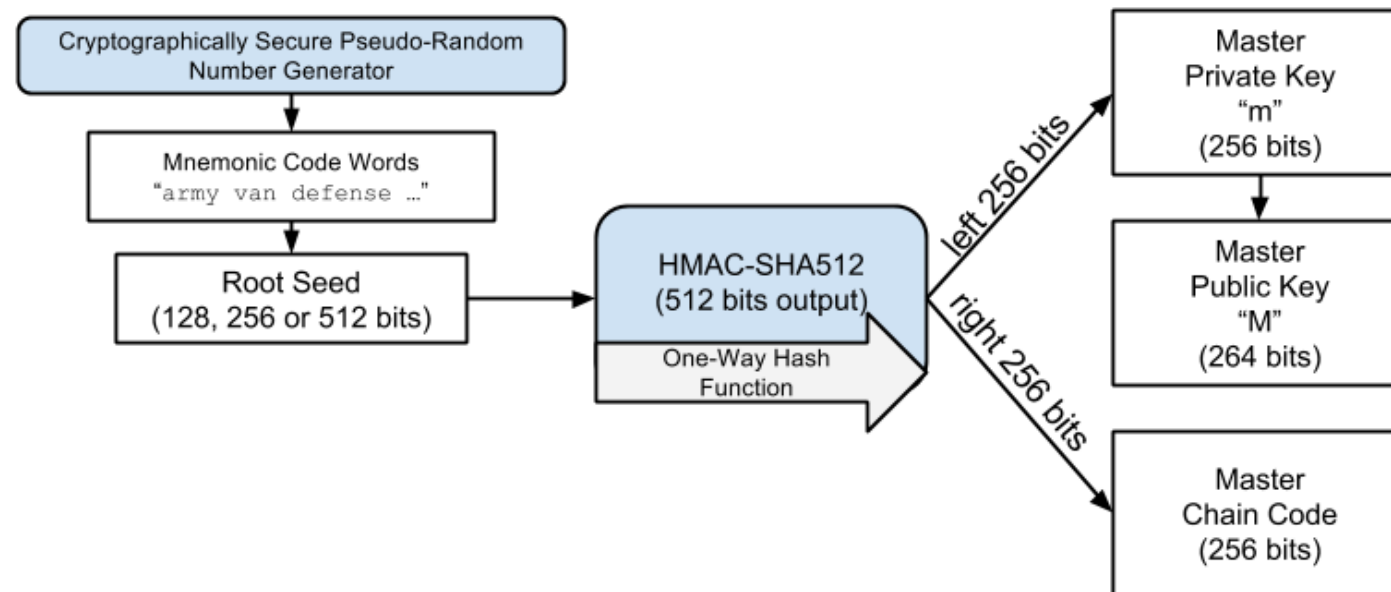
```
% echo 5b56c417303faa3fcba7e57400e120a0ca83ec5a4fc9ffba757fbe63fbd77a89a1a3be4c67196f57c39a88b76373733891bfaba16ed27a813ceed498804c0570
| bx base16-decode | hmac --algorithm sha512 --key "Bitcoin seed" -
b2a0d576b828b537688b561f2cfa8dac3602d54c62bde619ad5331e6c235ee26b70d675323c40ec461e0a6af603b1f135fb2af9ae753eef18922732a73b0f05
```

```
% echo 5b56c417303faa3fcba7e57400e120a0ca83ec5a4fc9ffba757fbe63fbd77a89a1a3be4c67196f57c39a88b76373733891bfaba16ed27a813ceed498804c0570
| bx base16-decode | hmac --algorithm sha512 --key "Bitcoin seed" - | cut -c 1-64
b2a0d576b828b537688b561f2cfa8dac3602d54c62bde619ad5331e6c235ee26 (Master Private Key)
```

```
% echo 5b56c417303faa3fcba7e57400e120a0ca83ec5a4fc9ffba757fbe63fbd77a89a1a3be4c67196f57c39a88b76373733891bfaba16ed27a813ceed498804c0570
| bx base16-decode | hmac --algorithm sha512 --key "Bitcoin seed" - | cut -c 1-64 | bx ec-to-public
03ca72b45eede592f059b7eaf3da13eb7d8d15aa472b6f79f74820bb22ff596186 (Master Public Key)
```

```
% echo 5b56c417303faa3fcba7e57400e120a0ca83ec5a4fc9ffba757fbe63fbd77a89a1a3be4c67196f57c39a88b76373733891bfaba16ed27a813ceed498804c0570
| bx base16-decode | hmac --algorithm sha512 --key "Bitcoin seed" - | cut -c 65-128
b70d675323c40ec461e0a6af603b1f135fb2af9ae753eef18922732a73b0f05 (Chain Code)
```

Calculating BIP 32/39 Extended Root Keys



Extended Private Key (**xprv**)
can also be Associated with
the Output of this Diagram

```
% echo "army van defense carry jealous true garbage claim echo media make crunch" | bx mnemonic-to-seed -p "" | bx hd-new -v 76066276
xprv9s21ZrQH143K3t4UZrNgeA3w861fwjYLaGwmPtQyPMmzshV2owVpfBSd2Q7YsHZ9j6i6ddYjb5PLtUdMzn8LhvuCVhGcQntq5rn7JVMqnie
```

```
% echo "army van defense carry jealous true garbage claim echo media make crunch" | bx mnemonic-to-seed -p "" | bx hd-new -v 76067358
xpub661MyMwAqRbcGN8wfsuhlHzfg7rAMCGBwVsNCGpawhJykVpBMUp5Cym6sbFpxThk8qA6Y5ffFq8oVvB9TSctTnVN1hazG7ht1ifM4ZgY5E9
```

EXT_PRIVATE_KEY prefix, responsible for **xprv** from <https://github.com/bitcoin/bitcoin/blob/master/src/chainparams.cpp#L133>,
i.e., 0x488ADE4 = **76066276**

EXT_PUBLIC_KEY prefix, responsible for **xpub** from <https://github.com/bitcoin/bitcoin/blob/master/src/chainparams.cpp#L132>,
i.e., 0x488B21E = **76067358**

```
% echo xprv9s21ZrQH143K3t4UZrNgeA3w861fwjYLaGwmPtQyPMmzshV2owVpfBSd2Q7YsHZ9j6i6ddYjb5PLtUdMzn8LhvuCVhGcQntq5rn7JVMqnie | bx hd-to-ec
b2a0d576b828b537688b561f2cfa8dac3602d54c62bde619ad5331e6c235ee26
```

```
% echo b2a0d576b828b537688b561f2cfa8dac3602d54c62bde619ad5331e6c235ee26 | bx ec-to-public
03ca72b45eede592f059b7eaf3da13eb7d8d15aa472b6f79f74820bb22ff596186
```

Serialization of a BIP 32 Extended Private Key

```
% echo "army van defense carry jealous true garbage claim echo media make crunch" | bx mnemonic-to-seed -p "" | bx hd-new -v 76066276  
xprv9s21ZrQH143K3t4UZrNgeA3w861fwjYLaGwmPtQyPMmzshV2owVpfBSd2Q7YsHZ9j6i6ddYjb5PLtUdMzn8LhvuCVhGcQntq5rn7JVMqnie  
  
% echo xprv9s21ZrQH143K3t4UZrNgeA3w861fwjYLaGwmPtQyPMmzshV2owVpfBSd2Q7YsHZ9j6i6ddYjb5PLtUdMzn8LhvuCVhGcQntq5rn7JVMqnie | bx base58check-  
decode  
wrapper  
{  
  checksum 1131671762  
  payload  
88ade400000000000000000000b70d675323c40ec461e0a6af603b1f135fb2af9ae753eeff18922732a73b0f0500b2a0d576b828b537688b561f2cfa8dac3602d54c62bde619ad  
5331e6c235ee26  
  version 4  
}  
  
% echo xprv9s21ZrQH143K3t4UZrNgeA3w861fwjYLaGwmPtQyPMmzshV2owVpfBSd2Q7YsHZ9j6i6ddYjb5PLtUdMzn8LhvuCVhGcQntq5rn7JVMqnie | bx base58-decode | cut -c 1-156  
0488ade400000000000000000000b70d675323c40ec461e0a6af603b1f135fb2af9ae753eeff18922732a73b0f0500b2a0d576b828b537688b561f2cfa8dac3602d54c62bde619ad5331e6c235ee26  
  
xprv      % echo xprv9s21ZrQH143K3t4UZrNgeA3w861fwjYLaGwmPtQyPMmzshV2owVpfBSd2Q7YsHZ9j6i6ddYjb5PLtUdMzn8LhvuCVhGcQntq5rn7JVMqnie | bx base58-decode | cut -c 1-8  
0488ade4  
  
Depth     % echo xprv9s21ZrQH143K3t4UZrNgeA3w861fwjYLaGwmPtQyPMmzshV2owVpfBSd2Q7YsHZ9j6i6ddYjb5PLtUdMzn8LhvuCVhGcQntq5rn7JVMqnie | bx base58-decode | cut -c 9-10  
00  
  
Parent  
Fingerprint % echo xprv9s21ZrQH143K3t4UZrNgeA3w861fwjYLaGwmPtQyPMmzshV2owVpfBSd2Q7YsHZ9j6i6ddYjb5PLtUdMzn8LhvuCVhGcQntq5rn7JVMqnie | bx base58-decode | cut -c 11-18  
00000000  
  
Child Index % echo xprv9s21ZrQH143K3t4UZrNgeA3w861fwjYLaGwmPtQyPMmzshV2owVpfBSd2Q7YsHZ9j6i6ddYjb5PLtUdMzn8LhvuCVhGcQntq5rn7JVMqnie | bx base58-decode | cut -c 19-26  
00000000  
  
Chain Code % echo xprv9s21ZrQH143K3t4UZrNgeA3w861fwjYLaGwmPtQyPMmzshV2owVpfBSd2Q7YsHZ9j6i6ddYjb5PLtUdMzn8LhvuCVhGcQntq5rn7JVMqnie | bx base58-decode | cut -c 27-90  
b70d675323c40ec461e0a6af603b1f135fb2af9ae753eeff18922732a73b0f05  
  
Private Key (secp256k1) % echo xprv9s21ZrQH143K3t4UZrNgeA3w861fwjYLaGwmPtQyPMmzshV2owVpfBSd2Q7YsHZ9j6i6ddYjb5PLtUdMzn8LhvuCVhGcQntq5rn7JVMqnie | bx base58-decode | cut -c 93-156  
b2a0d576b828b537688b561f2cfa8dac3602d54c62bde619ad5331e6c235ee26
```

Serialization a BIP 32 Extended Public Key

<https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki#serialization-format>
and contrast to results with <https://bip32jp.github.io/english/>

```
% echo xpub661MyMwAqRbcGN8wfsuh1Hzfg7rAMCGBwVsNCGpawhJykVpBMUp5Cym6sbFpxThk8qA6Y5ffFq8oVvB9TSctTnVN1hazG7ht1ifM4ZgY5E9 | bx base58-decode |  
cut -c 1-156  
0488b21e000000000000000000b70d675323c40ec461e0a6af603b1f135fb2af9ae753eeff18922732a73b0f0500b2a0d576b828b537688b561f2cfa8dac3602d54c62bde619  
ad5331e6c235ee26
```

```
xpub % echo xpub661MyMwAqRbcGN8wfsuh1Hzfg7rAMCGBwVsNCGpawhJykVpBMUp5Cym6sbFpxThk8qA6Y5ffFq8oVvB9TSctTnVN1hazG7ht1ifM4ZgY5E9 | bx base58-decode | cut -c 1-8  
0488b21e
```

```
Depth % echo xpub661MyMwAqRbcGN8wfsuh1Hzfg7rAMCGBwVsNCGpawhJykVpBMUp5Cym6sbFpxThk8qA6Y5ffFq8oVvB9TSctTnVN1hazG7ht1ifM4ZgY5E9 | bx base58-decode | cut -c 9-10  
00
```

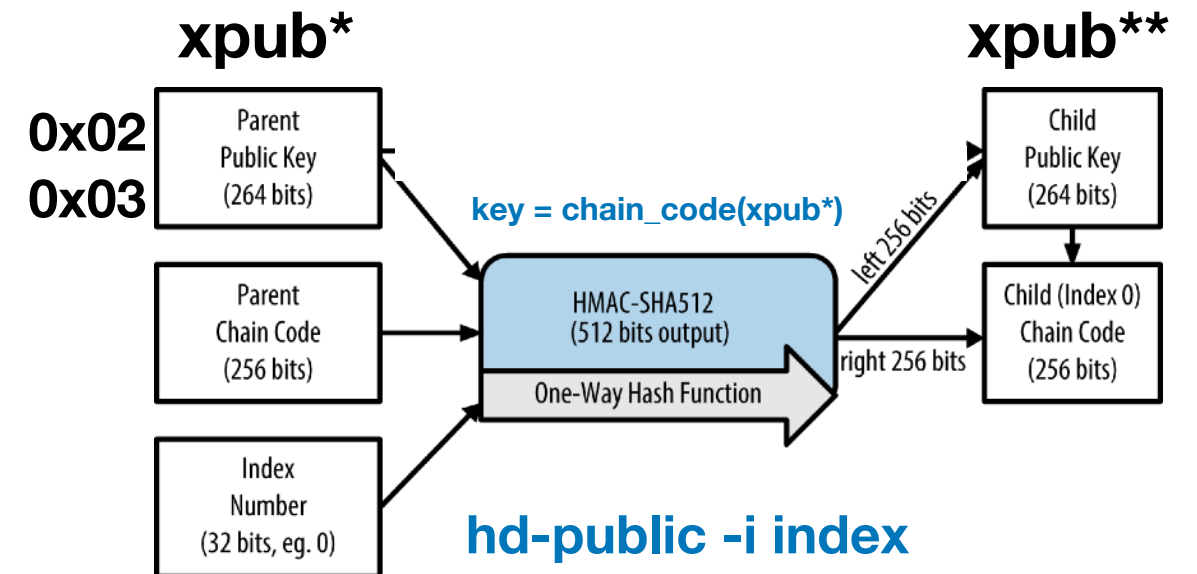
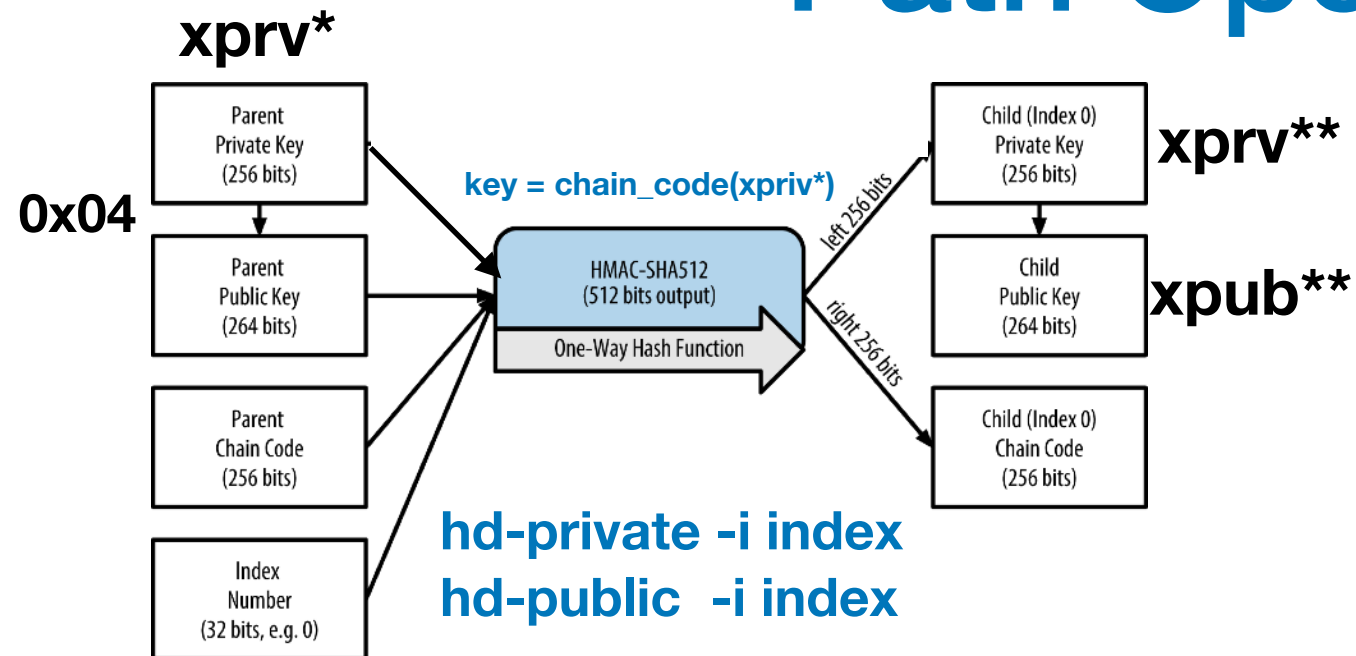
```
Parent Fingerprint echo xpub661MyMwAqRbcGN8wfsuh1Hzfg7rAMCGBwVsNCGpawhJykVpBMUp5Cym6sbFpxThk8qA6Y5ffFq8oVvB9TSctTnVN1hazG7ht1ifM4ZgY5E9 | bx base58-decode | cut -c 11-18  
00000000
```

```
Child Index % echo xpub661MyMwAqRbcGN8wfsuh1Hzfg7rAMCGBwVsNCGpawhJykVpBMUp5Cym6sbFpxThk8qA6Y5ffFq8oVvB9TSctTnVN1hazG7ht1ifM4ZgY5E9 | bx base58-decode | cut -c 19-26  
00000000
```

```
Chain Code % echo xpub661MyMwAqRbcGN8wfsuh1Hzfg7rAMCGBwVsNCGpawhJykVpBMUp5Cym6sbFpxThk8qA6Y5ffFq8oVvB9TSctTnVN1hazG7ht1ifM4ZgY5E9 | bx base58-decode | cut -c 27-90  
b70d675323c40ec461e0a6af603b1f135fb2af9ae753eeff18922732a73b0f05
```

```
Public Key (secp256k1) % echo xpub661MyMwAqRbcGN8wfsuh1Hzfg7rAMCGBwVsNCGpawhJykVpBMUp5Cym6sbFpxThk8qA6Y5ffFq8oVvB9TSctTnVN1hazG7ht1ifM4ZgY5E9 | bx base58-decode | cut -c 91-156  
00b2a0d576b828b537688b561f2cfa8dac3602d54c62bde619ad5331e6c235ee26
```

Hierarchical Deterministic (HD) BIP 32 Child Key Derivation (CKD) Path Operations



Notes:

1. $0 \leq \text{index} \leq 2^{32} - 1$ keys are soft
2. $0 \leq \text{index} \leq 2^{31} - 1$ keys are hardened
3. All private keys are by default uncompressed

<https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki#child-key-derivation-ckd-functions>

BTC BIP 32 CKD Path Examples

Using BIP 39 with a Passphrase

m/:

```
% echo "army van defense carry jealous true garbage claim echo media make crunch" | bx mnemonic-to-seed -p "ionized salt" | bx hd-new -v 76066276  
xprv9s21ZrQH143K3mYZUzu588D3wU6ZTgwikSf2o2nR5wRWcD7tp4xa76kM7678s8h4Az2WD2RP8VrTybpZ8XTnCBvJJcDez73hXQuFFTLovyb
```

m/0'/0'/0'/:

```
% echo "army van defense carry jealous true garbage claim echo media make crunch" | bx mnemonic-to-seed -p "ionized salt" | bx hd-new -v  
76066276 | bx hd-private -d -i 0 | bx hd-private -d -i 0 | bx hd-private -d -i 0  
xprv9yMDuLCasp9DyNhuFGr8rYzRgLEk4Phm5DBrQ2iYV1cXZpLCgs7g3kuPi2GDA2WU9SB37S4485UNHYvzh9LRxU1LhKNLMQXdk53bPYvCds
```

M/0'/0'/0'/:

```
% echo "army van defense carry jealous true garbage claim echo media make crunch" | bx mnemonic-to-seed -p "ionized salt" | bx hd-new -v  
76066276 | bx hd-private -d -i 0 | bx hd-private -d -i 0 | bx hd-public -d -i 0  
xpub6CLaJqjUiBhXBrnNMJP9DgwAEN5ETrRcSS7TCR8A3M9WScfMEQRvbZDsZHS671HfMeiKGYxqHnY8UHANPFRDmB8UWEyBKLj5Qe6aALDXPy5
```

m/44'/0'/0'/0/0 compressed WIF key:

```
% echo "army van defense carry jealous true garbage claim echo media make crunch" | bx mnemonic-to-seed -p "ionized salt" | bx hd-new -v  
76066276 | bx hd-private -d -i 44 | bx hd-private -d -i 0 | bx hd-private -d -i 0 | bx hd-private -i 0 | bx hd-private -i 0 | bx hd-to-ec  
| sed 's/$/01/' | bx base58check-encode -v 128  
L34uf7zEA3KX5LSQRKN9MWJjWJ4YLKzyRNm2P4jF4sgT9uegbPvW
```

M/44'/0'/0'/0/0 compressed address:

```
% echo "army van defense carry jealous true garbage claim echo media make crunch" | bx mnemonic-to-seed -p "ionized salt" | bx hd-new -v  
76066276 | bx hd-private -d -i 44 | bx hd-private -d -i 0 | bx hd-private -d -i 0 | bx hd-private -i 0 | bx hd-private -i 0 | bx hd-to-ec |  
bx ec-to-public | bx ec-to-address -v 0  
1BXst1jWfc517kFbwbAB1qdsYd6vaRzbah
```

```
% echo "army van defense carry jealous true garbage claim echo media make crunch" | bx mnemonic-to-seed -p "ionized salt" | bx hd-new -v  
76066276 | bx hd-private -d -i 44 | bx hd-private -d -i 0 | bx hd-public -d -i 0 | bx hd-public -i 0 | bx hd-public -i 0 | bx hd-to-ec |  
bx ec-to-address -v 0  
1BXst1jWfc517kFbwbAB1qdsYd6vaRzbah
```

BIP 44's Five BIP 32 Path Levels

<https://github.com/bitcoin/bips/blob/master/bip-0044.mediawiki#path-levels>

is what Trezor, Ledger, Keepkey, Jaxx, Coinomi and other products use.

```
m / purpose' / coin_type' / account' / change / address_index
M / purpose' / coin_type' / account' / change / address_index
```

purpose' = 44 (hardened/detached)

coin_type' integers (hardened/detached) are defined at <https://github.com/satoshilabs/slips/blob/master/slip-0044.md>

account' = 0, 1, 2... (hardened/detached)

change = 0 for visible addresses provided by wallet applications, 1 for internal hidden return change addresses

address_index = 0 to $2^{32}-1$ for non hardened keys, 0 to $2^{31}-1$ for hardened keys

<https://github.com/libbitcoin/libbitcoin/wiki/Altcoin-Version-Mappings#bip44-altcoin-version-mapping-table>

Columns 1 through 6 facilitate key and address synthesis for numerous coins types

Table below is an extracted subset

Coin	BIP 44 coin_type	main net version_WIF	main net version_p2pkh	main net version_psh	EXT_SECRET_KEY
BTC	0	128	0/('1')	5/('3')	76066276/('xprv')
LTC	2	176	48/('L')	5/('3')	76066276/('xprv')
DOGE	3	158	30/('D')	22/('9' 'A')	49988504/('dgpv')
DASH	5	204	76/('X')	16/('7')	50221772/('drkp')

BIP 32/39/44 HD Wallet P2PKH

Key and Address Examples

m/44'/0'/0'/0/0 **BTC** compressed **WIF** key:

```
% echo "army van defense carry jealous true garbage claim echo media make crunch" | bx mnemonic-to-seed -p "ionized salt" | bx hd-new -v 76066276 | bx hd-private -d -i 44 | bx hd-private -d -i 0 | bx hd-private -d -i 0 | bx hd-private -i 0 | bx hd-private -i 0 | bx hd-to-ec | sed 's/$/01/' | bx base58check-encode -v 128  
L34uf7zEA3KX5LsQRKN9MWJjWJ4YLKzyRNm2P4jF4sgT9uegbPvW
```

M/44'/0'/0'/0/0 **BTC** compressed **address**:

```
% echo "army van defense carry jealous true garbage claim echo media make crunch" | bx mnemonic-to-seed -p "ionized salt" | bx hd-new -v 76066276 | bx hd-private -d -i 44 | bx hd-private -d -i 0 | bx hd-public -d -i 0 | bx hd-public -i 0 | bx hd-public -i 0 | bx hd-to-ec | bx ec-to-address -v 0  
1BXst1jWfc517kFbwbAB1qdsYd6vaRzbah
```

```
% echo "army van defense carry jealous true garbage claim echo media make crunch" | bx mnemonic-to-seed -p "ionized salt" | bx hd-new -v 76066276 | bx hd-private -d -i 44 | bx hd-private -d -i 0 | bx hd-public -d -i 0  
xpub6DA9JgkMA4PGUSDtwJ3WTiM9Ne6y2rKNX69H4m3SxM9tBbWp7YDabUfcHnswnU4P5wqXiyULxiCn6HYHRLAyQb8Dnj8oTgB45XbG9mPt6f
```

<https://www.blockchain.com/btc/xpub/xpub6DA9JgkMA4PGUSDtwJ3WTiM9Ne6y2rKNX69H4m3SxM9tBbWp7YDabUfcHnswnU4P5wqXiyULxiCn6HYHRLAyQb8Dnj8oTgB45XbG9mPt6f>

m/44'/5'/0'/0/0 **DASH** compressed **WIF** key:

```
% echo "army van defense carry jealous true garbage claim echo media make crunch" | bx mnemonic-to-seed -p "ionized salt" | bx hd-new -v 76066276 | bx hd-private -d -i 44 | bx hd-private -d -i 5 | bx hd-private -d -i 0 | bx hd-private -i 0 | bx hd-private -i 0 | bx hd-to-ec | sed 's/$/01/' | bx base58check-encode -v 204  
XH4znBdaCoJm7ZBK9ZV813eoB6seR7yw4wfeu9m8UyZbN6zh19Lw
```

M/44'/5'/0'/0/0 **DASH** compressed **address**:

```
% echo "army van defense carry jealous true garbage claim echo media make crunch" | bx mnemonic-to-seed -p "ionized salt" | bx hd-new -v 76066276 | bx hd-private -d -i 44 | bx hd-private -d -i 5 | bx hd-public -d -i 0 | bx hd-public -i 0 | bx hd-public -i 0 | bx hd-to-ec | bx ec-to-address -v 76  
XewKGCNVm4iPetF1SBsiwCdaFqxLpExFbc
```

Trezor: BIP 49

P2WPKH-nested-in-P2SH

<https://github.com/bitcoin/bips/blob/master/bip-0049.mediawiki#test-vectors> and version = 196

m/49'/0'/0'/0/0 BTC uncompressed private key:

```
% echo "army van defense carry jealous true garbage claim echo media make crunch" | bx mnemonic-to-seed -p "ionized salt" | bx hd-new -v 76066276 | bx hd-private -d -i 49 | bx hd-private -d -i 0 | bx hd-private -d -i 0 | bx hd-private -i 0 | bx hd-private -i 0 | bx hd-to-ec 134adb604a4055186a7c2dcad2e512d9c0b920fb045c873291968865eaf2ab74
```

M/49'/0'/0'/0/0 BTC P2WPKH-nested-in-P2SH address:

```
% echo "army van defense carry jealous true garbage claim echo media make crunch" | bx mnemonic-to-seed -p "ionized salt" | bx hd-new -v 76066276 | bx hd-private -d -i 49 | bx hd-private -d -i 0 | bx hd-private -d -i 0 | bx hd-private -i 0 | bx hd-private -i 0 | bx hd-to-ec | bx ec-to-public 02523d3f63f6e0a633355270d5661bd05e1dbf9f692db8791c0215ac2cb4ef2bb1
```

```
% echo "army van defense carry jealous true garbage claim echo media make crunch" | bx mnemonic-to-seed -p "ionized salt" | bx hd-new -v 76066276 | bx hd-private -d -i 49 | bx hd-private -d -i 0 | bx hd-private -d -i 0 | bx hd-private -i 0 | bx hd-private -i 0 | bx hd-to-ec | bx ec-to-public | bx bitcoin160 d5858d1e5e0f7f750d32cca66619f3385dc6c15b
```

```
% echo "0 [d5858d1e5e0f7f750d32cca66619f3385dc6c15b]" | bx script-encode 0014d5858d1e5e0f7f750d32cca66619f3385dc6c15b
```

```
% echo "0 [d5858d1e5e0f7f750d32cca66619f3385dc6c15b]" | bx script-encode | bx sha256 | bx ripemd160 | bx base58check-encode -v 5 382Db9auK4UrFCzWc15Tu8GGCv2RLfVkmC
```

```
% echo "0 [d5858d1e5e0f7f750d32cca66619f3385dc6c15b]" | bx script-encode | bx bitcoin160 | bx base58check-encode -v 5 382Db9auK4UrFCzWc15Tu8GGCv2RLfVkmC
```

```
% echo "0 [d5858d1e5e0f7f750d32cca66619f3385dc6c15b]" | bx script-to-address -v 5 382Db9auK4UrFCzWc15Tu8GGCv2RLfVkmC
```

Demystifying
Mastering Bitcoin
Chapter 6
by Applying Libbitcoin,
UNIX, and Python
Command Line Interfaces

Author: Scott Holben
Jan. 10th, 2019

Alice's Transaction to Bob's Cafe

Transaction Summary:

Alice sends Bob 0.015 BTC (1,500,000 Satoshis) to [1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA](#) (Bob's address to pay for coffee)

Alice's Change 0.08450 BTC (8,450,000 Satoshis) to [1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK](#) (Alice reuses her old address)

Mining Fee of 0.0005 BTC (50,000 Satoshis) to an implicit address

$$\begin{aligned}\text{Fees} &= \text{Sum(Inputs)} - \text{Sum(Outputs)} \\ &= 10,000,000 - (1,500,000 + 8,450,000) \\ &= 50,000\end{aligned}$$

Blockchain Explorer Details:

Monotonic Block Number for the Pertinent Transaction (Dated 2013-12-27 23:03:05)

<https://www.blockchain.com/btc/block-height/277316>

Block Referenced by Block ID:

<https://www.blockchain.com/btc/block/00000000000000001b6b9a13b095e96db41c4a928b97ef2d944a9b31b2cc7bdc4>

Transaction Referenced by Transaction ID:

<https://www.blockchain.com/btc/tx/0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2>

Alice's Transaction to Bob's Cafe

```
% bx fetch-tx -c ~/bitcoin-explorer/bx-mainnet-remote.cfg 0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2
transaction
{
  hash 0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2
  inputs
  {
    input
    {
      address_hash 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8
      previous_output
      {
        hash 7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18 Is a TX ID and Index for the UTXO funding the TX, references a specific P2PKH Encumbrance Script
        index 0
      }
      script "[3045022100884d142d86652a3f47ba4746ec719bbfb040a570b1deccbb6498c75c4ae24cb02204b9f039ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e381301] [0484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ade8416ab9fe423cc5412336376789d172787ec3457eee41c04f4938de5cc17b4a10fa336a8d752adf]" 1st # is a DER Signature, Second # is a public key
      sequence 4294967295
    }
  }
  lock_time 0
  outputs
  {
    output
    {
      address_hash ab68025513c3dbd2f7b92a94e0581f5d50f654e7
      script "dup hash160 [ab68025513c3dbd2f7b92a94e0581f5d50f654e7] equalverify checksig" Is an output P2PKH Encumbrance Script
      value 1500000
    }
    output
    {
      address_hash 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8
      script "dup hash160 [7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8] equalverify checksig" Is an output P2PKH Encumbrance Script
      value 8450000
    }
  }
  version 1
}
```

***Non-interactive* BX Commands**

Supporting Construction of Transactions

Creates a skeleton TX by specifying UTXO inputs, sets destination address and amounts, implicitly sets encumbrance scripts:

<https://github.com/libbitcoin/libbitcoin-explorer/wiki/bx-tx-encode>

Signs a specific TX parts; index is the specific UTXO index number; specific encumbrance script or redemption script is needed as input:

<https://github.com/libbitcoin/libbitcoin-explorer/wiki/bx-input-sign>

Updates a specific TX input with a signed UTXO; index is the skeleton's input number starting from zero:

<https://github.com/libbitcoin/libbitcoin-explorer/wiki/bx-input-set>

Cryptographically checks one or more portions of a TX by executing one or more times:

<https://github.com/libbitcoin/libbitcoin-explorer/wiki/bx-input-validate>

Analysis of Alice's Transaction to Bob's Cafe

```
% echo
0100000001186f9f998a5aa6f048e51dd8419a14d8a0f1a8a2836dd734d2804fe65fa35779000000008b483045022100884d142d86652a3f47ba4746ec719bbfbd040
a570b1deccbb6498c75c4ae24cb02204b9f039ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e381301410484ecc0d46f1918b30928fa0e4ed99f16
a0fb4fde0735e7ade8416ab9fe423cc5412336376789d172787ec3457eee41c04f4938de5cc17b4a10fa336a8d752adfffffffff0260e31600000000001976a914ab6
8025513c3dbd2f7b92a94e0581f5d50f654e788acd0ef8000000000001976a9147f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a888ac00000000 | bx sha256 |
bx sha256
f2c245c38672a5d8fba5a5caa44dcef277a52e916a0603272f91286f2b052706 (Needs to be Little Endian reversed to obtain TX ID Offline)
```

<http://learnmeabitcoin.com/tools/swapendian/?hexadecimal=f2c245c38672a5d8fba5a5caa44dcef277a52e916a0603272f91286f2b052706>

```
% echo
0100000001186f9f998a5aa6f048e51dd8419a14d8a0f1a8a2836dd734d2804fe65fa35779000000008b483045022100884d142d86652a3f47ba4746ec719bbfbd040
a570b1deccbb6498c75c4ae24cb02204b9f039ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e381301410484ecc0d46f1918b30928fa0e4ed99f16
a0fb4fde0735e7ade8416ab9fe423cc5412336376789d172787ec3457eee41c04f4938de5cc17b4a10fa336a8d752adfffffffff0260e31600000000001976a914ab6
8025513c3dbd2f7b92a94e0581f5d50f654e788acd0ef8000000000001976a9147f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a888ac00000000 | bx bitcoin256
0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2
```

```
% echo
0484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ade8416ab9fe423cc5412336376789d172787ec3457eee41c04f4938de5cc17b4a10fa336a8d752adf |
bx bitcoin160
7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8
```

```
% echo ab68025513c3dbd2f7b92a94e0581f5d50f654e7 | bx base58check-encode -v 0
1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA
```

```
% echo 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 | bx base58check-encode -v 0
1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK
```

```
% bx tx-encode -v 1 -i 7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18:0 -o 1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA:
1500000 -o 1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK:8450000 | bx input-set -i 0
"[3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6498c75c4ae24cb02204b9f039ff08df09cbe9f6addac960298cad530a863ea8f53982c0
9db8f6e381301]
[0484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ade8416ab9fe423cc5412336376789d172787ec3457eee41c04f4938de5cc17b4a10fa336a8d752adf]"
| bx bitcoin256
0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2
```

Viewing the Transaction Reconstructed Using BX

```
% bx tx-encode -v 1 -i 7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18:0 -o 1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA:1500000 -o
1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK:8450000 | bx input-set -i 0
"[3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6498c75c4ae24cb02204b9f039ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e381301
] [0484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ade8416ab9fe423cc5412336376789d172787ec3457eee41c04f4938de5cc17b4a10fa336a8d752adf]" | bx tx-
decode
transaction
{
  hash 0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2
  inputs
  {
    input
    {
      address_hash 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8
      previous_output
      {
        hash 7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18
        index 0
      }
      script
      "[3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6498c75c4ae24cb02204b9f039ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e381301
] [0484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ade8416ab9fe423cc5412336376789d172787ec3457eee41c04f4938de5cc17b4a10fa336a8d752adf]"
      sequence 4294967295
    }
  }
  lock_time 0
  outputs
  {
    output
    {
      address_hash ab68025513c3dbd2f7b92a94e0581f5d50f654e7
      script "dup hash160 [ab68025513c3dbd2f7b92a94e0581f5d50f654e7] equalverify checksig"
      value 1500000
    }
    output
    {
      address_hash 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8
      script "dup hash160 [7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8] equalverify checksig"
      value 8450000
    }
  }
  version 1
}
```

Analyzing a Raw Transaction

```
% echo
0100000001186f9f998a5aa6f048e51dd8419a14d8a0f1a8a2836dd734d2804fe65fa35779000000008b483045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6
498c75c4ae24cb02204b9f039ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e381301410484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ade8416ab9fe
423cc5412336376789d172787ec3457eee41c04f4938de5cc17b4a10fa336a8d752adfffffffff0260e31600000000001976a914ab68025513c3dbd2f7b92a94e0581f5d50f654e788
acd0ef80000000000001976a9147f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a888ac00000000 | bx tx-decode
transaction
{
  hash 0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2
  inputs
  {
    input
    {
      address_hash 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8
      previous_output
      {
        hash 7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18
        index 0
      }
      script
      "[3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6498c75c4ae24cb02204b9f039ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e381301
0484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ade8416ab9fe423cc5412336376789d172787ec3457eee41c04f4938de5cc17b4a10fa336a8d752adf]"
      sequence 4294967295
    }
  }
  lock_time 0
  outputs
  {
    output
    {
      address_hash ab68025513c3dbd2f7b92a94e0581f5d50f654e7
      script "dup hash160 [ab68025513c3dbd2f7b92a94e0581f5d50f654e7] equalverify checksig"
      value 150000
    }
    output
    {
      address_hash 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8
      script "dup hash160 [7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8] equalverify checksig"
      value 845000
    }
  }
  version 1
}
```

Distinguished Encoding Rules (DER)

DER-encoded Digital Signature:

```
3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6498c75c4ae24cb02204b9f039ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e381301
```

```
% echo -n 3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6498c75c4ae24cb02204b9f039ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e381301 | wc
0      1      144
```

```
% echo -n 00884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6498c75c4ae24cb | wc
0      1      66
```

```
% echo -n 4b9f039ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e3813 | wc
0      1      64
```

$66 + 64 + 7 \times 2 = 144$ (hex characters) = 72 (bytes)

- 0x30—indicating the start of a DER sequence
- 0x45—the length of the sequence (69 bytes)
- 0x02—an integer value follows
- 0x21—the length of the integer (33 bytes)
- R—00884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6498c75c4ae24cb
- 0x02—another integer follows
- 0x20—the length of the integer (32 bytes)
- S—4b9f039ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e3813
- SIGHASH suffix (0x01) indicating the type of hash used (SIGHASH_ALL)

SIGHASH Flag Meanings (Scope of signature is related to non-segwit transaction malleability)

SIGHASH Flags	Value	Description
ALL	0x01	Signature applies to all inputs and outputs
NONE	0x02	Signature applies to all inputs, none of the output
SINGLE	0x03	Signature applies to all inputs, but only the one output with the same index number as the signed input
ALL ANYONECANPAY	0x81	Signature applies to one input, and all outputs
NONE ANYONECANPAY	0x82	Signature applies to one input, none of the outputs
SINGLE ANYONECANPAY	0x83	Signature applies to one input, and the output with the same index number (Used by Coinjoin and to lower TX fees)

** Note that the **bx input-sign** command produces DER-encoded signatures and directly supports SIGHASH Flags above. We don't have Alice's private key so we can't reproduce the signature.

Confirming a Single Input Endorsement is Correct

<https://github.com/libbitcoin/libbitcoin-explorer/wiki/bx-input-validate>

or

```
% bx input-validate -h
```

```
Usage: bx input-validate [-h] [--config value] [--index value]
EC_PUBLIC_KEY CONTRACT ENDORSEMENT [TRANSACTION]
```

```
Info: Validate a transaction input endorsement.
```

```
Options (named):
```

```
-c [--config]      The path to the configuration settings file.
-h [--help]        Get a description and instructions for this command.
-i [--index]       The ordinal position of the input within the
                   transaction, defaults to 0.
```

```
Arguments (positional):
```

```
EC_PUBLIC_KEY      The Base16 EC public key to verify against.
CONTRACT           The previous output script used in signing. Multiple
                   tokens must be quoted.
ENDORSEMENT        The endorsement to validate.
TRANSACTION        The Base16 transaction. If not specified the
                   transaction is read from STDIN.
```

```
% echo
```

```
0100000001186f9f998a5aa6f048e51dd8419a14d8a0f1a8a2836dd734d2804fe65fa357790000000008b483045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccb
b6498c75c4ae24cb02204b9f039ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e381301410484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ade8416a
b9fe423cc5412336376789d172787ec3457eee41c04f4938de5cc17b4a10fa336a8d752adfffffffff0260e31600000000001976a914ab68025513c3dbd2f7b92a94e0581f5d50f6
54e788acd0ef80000000000001976a9147f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a888ac00000000 | bx input-validate -i 0
0484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ade8416ab9fe423cc5412336376789d172787ec3457eee41c04f4938de5cc17b4a10fa336a8d752adf "dup hash160
[7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8] equalverify checksig"
3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6498c75c4ae24cb02204b9f039ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e381301
The endorsement is valid.
```

* Note that the **SIGHASH Suffix** checking is implicit because it is included as part of the Dark Green DER signature/endorsement

If Alice used bx, She Could Validate the TX Online Before Sending the TX

<https://github.com/libbitcoin/libbitcoin-explorer/wiki/bx-validate-tx>

or

```
% bx validate-tx -h
```

```
Usage: bx validate-tx [-h] [--config value] [TRANSACTION]
```

```
Info: Determine if a transaction is valid for submission to the
blockchain. Requires a Libbitcoin server connection.
```

```
Options (named):
```

```
-c [--config]      The path to the configuration settings file.
-h [--help]       Get a description and instructions for this command.
```

```
Arguments (positional):
```

```
TRANSACTION       The Base16 transaction. If not specified the
                  transaction is read from STDIN.
```

```
% echo
```

```
0100000001186f9f998a5aa6f048e51dd8419a14d8a0f1a8a2836dd734d2804fe65fa35779000000008b483045022100884d142d86652a3f47ba4746ec719
bbfbd040a570b1deccbb6498c75c4ae24cb02204b9f039ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e381301410484ecc0d46f1918b3
0928fa0e4ed99f16a0fb4fde0735e7ade8416ab9fe423cc5412336376789d172787ec3457eee41c04f4938de5cc17b4a10fa336a8d752adfffffffff0260e
31600000000001976a914ab68025513c3dbd2f7b92a94e0581f5d50f654e788acd0ef8000000000001976a9147f9b1a7fb68d60c536c2fd8aeaa53a8f3cc0
25a888ac00000000 | bx validate-tx -c ~/Projects/bitcoin-explorer/bx-mainnet-remote.cfg
```

```
The transaction is valid.
```

```
matching transaction with unspent outputs
```

If Alice used bx, She Could Send the TX Online

<https://github.com/libbitcoin/libbitcoin-explorer/wiki/bx-send-tx>

or

```
% bx send-tx -h
```

```
Usage: bx send-tx [-h] [--config value] [TRANSACTION]
```

```
Info: Broadcast a transaction to the Bitcoin network via a Libbitcoin  
server.
```

```
Options (named):
```

```
-c [--config]      The path to the configuration settings file.  
-h [--help]       Get a description and instructions for this command.
```

```
Arguments (positional):
```

```
TRANSACTION       The Base16 transaction to send. If not specified the  
                  transaction is read from STDIN.
```

```
% echo
```

```
0100000001186f9f998a5aa6f048e51dd8419a14d8a0f1a8a2836dd734d2804fe65fa35779000000008b483045022100884d142d86652a3f47ba4746  
ec719bbfbd040a570b1deccbb6498c75c4ae24cb02204b9f039ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e381301410484ecc0  
d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ade8416ab9fe423cc5412336376789d172787ec3457eee41c04f4938de5cc17b4a10fa336a8d752a  
dfffffffff0260e31600000000001976a914ab68025513c3dbd2f7b92a94e0581f5d50f654e788acd0ef8000000000001976a9147f9b1a7fb68d60c5  
36c2fd8aeaa53a8f3cc025a888ac00000000 | bx send-tx -c ~/Projects/bitcoin-explorer/bx-mainnet-remote.cfg
```

```
Sent transaction.
```

```
matching transaction with unspent outputs
```

Watch TX Status Until Confirmed

```
% bx watch-address -c ~/Projects/bitcoin-explorer/bx-mainnet-remote.cfg 1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK
Watching address: 1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK...
1 277316 0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2
```

Other Useful Online Commands:

```
% bx fetch-balance -c ~/Projects/bitcoin-explorer/bx-mainnet-remote.cfg 1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK
balance
{
  address 1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK
  received 20330143
  spent 10000000
}
```

Contrast to: <https://www.blockchain.com/btc/address/1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK>

```
% bx fetch-utxo -c ~/Projects/bitcoin-explorer/bx-mainnet-remote.cfg 1 1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK
points
{
  point
  {
    hash ee5f17e9d821ca5d3ad7b221ba48820e8301a79e57a8660c7ac1b8db2b5c34bd
    index 1
    value 3020
  }
}
```

Check Transaction History for an Address

```
% bx fetch-history -c ~/Projects/bitcoin-explorer/bx-mainnet-remote.cfg 1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK
transfers
{
  transfer
  {
    received
    {
      hash b45a9cb4a1061b7c48752757c44c28575051366483c54c9934036130c4752289
      height 547522
      index 1
    }
    value 6236
  }
  transfer
  {
    received
    {
      hash ee5f17e9d821ca5d3ad7b221ba48820e8301a79e57a8660c7ac1b8db2b5c34bd
      height 515490
      index 1
    }
    value 3020
  }
  transfer
  {
    received
    {
      hash 1c65aea26b6cb5711ada1418b61465b0a7eec6c82dc499c91f99e3260e57b9a2
      height 430305
      index 0
    }
    value 10000
  }
  transfer
  {
    received
    {
      hash 0e07ec4be87cd9291cbcb3fec88c601a8ad6fd3d4341ed88376a8ccdb80c2305
      height 430305
      index 0
    }
    value 10000
  }
  transfer
  {
    received
    {
      hash d1a81e8555f11d5df3527338a11d37ba745cf7a300edff3e98d0387a0c47a6b8
      height 430296
      index 0
    }
    value 10000
  }
  transfer
  {
    received
    {
      hash 1f4c52db84b1021ee0300ebcd57b07b1b465744d29ac5b62b21c9d9f03d649d0
      height 429390
      index 0
    }
    value 11100
  }
  transfer
  {
    received
    {
      hash ddef943391fbeb63729b67a39db138e767162da8d1947f4030e8b35d6fdb7b41
      height 426852
      index 0
    }
    value 10000
  }
  transfer
  {
    received
    {
      hash 79acb2dab272e4c8f833a4655534edda326a8bad979cca8179090df99df61d3f
      height 346661
      index 1
    }
  }
}
```

Elliptic Curve Message Validation

Use Case: “Proof of Existence (PoE) of Cold Storage Keys without the Need to Thaw Keys”

Offline - Private Compressed DASH Key Synthesis:

```
% echo 0000111122223333444455556666777788889999aaaabbbbccccddddeeeeffff | sed 's/$/01/' | bx  
base58check-encode -v 204  
XBHdfdHC4YocfzyfuFRx3DxjmvFJmK3txDh3zXk29GxpMWaWfDKL
```

Offline - Public Compressed DASH P2PKH Address Synthesis:

```
% echo 0000111122223333444455556666777788889999aaaabbbbccccddddeeeeffff | bx ec-to-public | bx ec-to-  
address -v 76  
XyHHinPZB5Q4FC9jtbksaQBJmXq48gtVGB
```

Offline - Message is Developed or Provided to Private Key Holder:

```
% echo -n "Craig Wright is not the real Satoshi!" | bx message-sign  
XBHdfdHC4YocfzyfuFRx3DxjmvFJmK3txDh3zXk29GxpMWaWfDKL  
H4k3D8jR4efMsAjCs9K/Pt8GB64h83Z07jkV4mERvNUZaYKG2ggWGmfoiJJl1ELh/8j6RikruaVeLWmHdQgeZfU=
```

Online - Only a Candidate Message, Signature, and Address are Provided:

```
% echo -n "Craig Wright is not the real Satoshi!" | bx message-validate  
XyHHinPZB5Q4FC9jtbksaQBJmXq48gtVGB H4k3D8jR4efMsAjCs9K/Pt8GB64h83Z07jkV4mERvNUZaYKG2ggWGmfoiJJl1ELh/  
8j6RikruaVeLWmHdQgeZfU=  
The signature is valid.
```

```
% echo -n "Craig Wright is not the real Satoshi! " | bx message-validate  
XyHHinPZB5Q4FC9jtbksaQBJmXq48gtVGB H4k3D8jR4efMsAjCs9K/Pt8GB64h83Z07jkV4mERvNUZaYKG2ggWGmfoiJJl1ELh/  
8j6RikruaVeLWmHdQgeZfU=  
The signature is not valid.
```

Demystifying
Mastering Bitcoin
Chapter 7
by Applying Libbitcoin,
UNIX, and Python
Command Line Interfaces

Author: Scott Holben
Jan. 9th, 2019

Important Bitcoin Transaction Concepts

Source/Payee	Destination/Payer
Withdrawal	+ Deposit
Input Script	+ Output Script
Signed Contract	+ Encumbrance
Unlocking Script	+ Locking Script
Signature Script	+ Public Key Script
ScriptSig	+ ScriptPubKey
Witness	+ Witness Script
ENDORSEMENT Script	+ CONTRACT or PAYMENT Script

- Each Bitcoin Network transaction (**TX**) can have up to 256 inputs and 256 outputs & must be ***smaller than 100K bytes***
- Satoshi denominations are accounted for by the Bitcoin Network using Unsigned TX Outputs (**UTXO**) records
- Prior network payments to a user's wallet, held in committed UTXO records, can effectively be added together to meet enduser payment output needs by having a user's wallet compose a TX with multiple inputs
- Multiple transaction payments (e.g., company payroll) can be made with a single TX having multiple outputs
- To enable spending, each **UTXO** is uniquely specified by a **TX ID** and a **TX output index**, and has one associated **CONTRACT** that gets digitally signed and becomes part of a **ENDORSEMENT** that is integrated into a future TX
- Each ***signature script must be smaller than 1,650 bytes***
- Different signatures can be applied to each transaction's ENDORCEMENT an LOCKING SCRIPTs.
- For each node, **unconfirmed transaction** typically resides within each nodes **Mempool** until confirmed
- **Confirmed transactions** are added to a network's **Blockchain** and new UTXO are committed to a node's database until spent. After six confirmations, a transaction is considered **settled**.
- UTXOs are not partially spent. As part of confirming a TX, spent UTXOs are removed from each node's UTXO database, and one or more new UTXOs are typically added to the same database
- UTXOs can be dynamically audited by actively scanning the Bitcoin Blockchain per the networks **consensus rules**

Bitcoin Scripting

Opcodes and Patterns

Bitcoin Scripting Opcodes and Patterns:

P2PK (Pay to Public Key) - *deprecated*, many of Satoshi's 1 million BTC are of this type

P2SM (Pay to Standard Multisig) - *deprecated*

P2PKH (Pay to Public Key Hash) - addresses start with the number 1

P2SH (Pay to Script Hash) - BIPs 13 and 16, e.g. multisig addresses start with the number 3

OP_RETURN - used to store up to 80 bytes of information, can't be

OP_CHECKLOCKTIMEVERIFY (CLTV) - absolute transaction lock time

OP_CHECKSEQUENCEVERIFY (CSV) - relative transaction lock time

P2WPKH (Pay to Witness Public Key Hash) - BIP 141 and BIP 173, e.g. Bech 32

P2WSH (Pay to Witness Script Hash) - BIP 141 and BIP 173, e.g. Bech 32

P2SH(P2WPKH): P2WPKH-nested-in-P2SH - BIP 49

P2SH(P2WSH): P2WSH-nested-in-P2SH -

- <https://en.bitcoin.it/wiki/Script> concisely documents many commands and scripting patterns
- Opcodes are Hungarian Prefixed with the characters **OP_**, opcode patterns above start with **P2**
- All P2 patterns above have paired input scripts and output scripts
- **OP_RETURN** command has no associated output address that can later be spent
- With the exception of the **OP_RETURN**, each of the script types above have predefined locking script and address formats that a recipient's wallet can later process to spend
- After the introduction of **segwit**, output scripts have defined version numbers

P2PK(Pay to Public Key)

Deprecated

Template P2PK Scripts:

[Sig] + **[PubKey] OP_CHECKSIG**

[Sig(payer: TXID, TXO_index, P2PK_contract)] + **[PubKey(payee)] OP_CHECKSIG**

- Original Satoshi Bitcoin Transaction Type
- Vulnerable to future Quantum Computing Attacks

Examples:

Testnet Destination P2PK Address

```
% echo 043297c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269bffc3ceb4e786affac12e4b778480df72442f3b9564dd1cecb06717dc2a7a18d46be91e9a5 | bx  
base58check-encode -v 111  
5sxEnKYdGsgjREgiebB4JVJuxSksSXFZFavbVpp3g9V8LMhiPsnnGwEwXf7o6pthryieYuMB1P5rk9QUT4X2cBB3X9RLgKkS (95 characters)
```

[PubKey] OP_CHECKSIG:

```
% echo 5sxEnKYdGsgjREgiebB4JVJuxSksSXFZFavbVpp3g9V8LMhiPsnnGwEwXf7o6pthryieYuMB1P5rk9QUT4X2cBB3X9RLgKkS | bx base58check-decode  
wrapper  
{  
  checksum 2811515363  
  payload 043297c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269bffc3ceb4e786affac12e4b778480df72442f3b9564dd1cecb06717dc2a7a18d46be91e9a5  
  version 111  
}  
(created by wallet sending funds to another wallet)
```

```
% echo "[043297c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269bffc3ceb4e786affac12e4b778480df72442f3b9564dd1cecb06717dc2a7a18d46be91e9a5]  
checksum" | bx script-encode  
41043297c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269bffc3ceb4e786affac12e4b778480df72442f3b9564dd1cecb06717dc2a7a18d46be91e9a5ac
```

[sig]:

(synthesized from the application of **tx-encode** and **input-sign** commands)

```
% bx script-encode  
"[3045022100be19bbce24f35895a38c88a7dd60c5a96df6151ba19c1523fb8a34f3afd6cd3d0220667123fbe85e698c4a4d7d391c3c25bf8a52a17542178c996c6c9849ea58662d01  
]"  
483045022100be19bbce24f35895a38c88a7dd60c5a96df6151ba19c1523fb8a34f3afd6cd3d0220667123fbe85e698c4a4d7d391c3c25bf8a52  
a17542178c996c6c9849ea58662d01
```

Bitcoin Stack Steps to Spend a P2PK Payment

Explicit Execution Script:

[Sig] [PubKey] OP_CHECKSIG

[Sig] = secp256k1_signature(MESSAGE, PrivKey)
MESSAGE = [PubKey]

Bitcoin LIFO Stack

Empty Stack

[Sig]

[Sig] [PubKey]

1

Script Execution Queue

[Sig] [PubKey] OP_CHECKSIG

[PubKey] OP_CHECKSIG

OP_CHECKSIG *(implicitly used MESSAGE above to complete operation)*

Empty Script

P2PKH

(Pay to Public Key Hash)

Template P2PKH Scripts:

[SigLockScript] [PubKey] + OP_DUP OP_HASH160 [HASH160(PubKey)] OP_EQUALVERIFY OP_CHECKSIG

**[SigLockScript(payer: TXID, TXO_index, P2PKH_CONTRACT)] [PubKey(payer)]
+ OP_DUP OP_HASH160 [HASH160(PubKey(payee))] OP_EQUALVERIFY OP_CHECKSIG**

- Currently the most common Bitcoin Transaction Type
- Considered by some to be less vulnerable to future **Quantum Computing** attacks

Examples:

Testnet Destination P2PKH Address

```
% echo 8acdcaaf8fea863f0d5a7b770c330cf6f899fdb | bx base58check-encode -v 111  
mtAt5BpwY36j7nNhwaFBD35ZqtbiD6Z1W6
```

OP_DUP OP_HASH160 [HASH160(PubKey)] OP_EQUALVERIFY OP_CHECKSIG:

```
% echo mtAt5BpwY36j7nNhwaFBD35ZqtbiD6Z1W6 | bx base58check-decode  
wrapper  
{  
  checksum 2804423364  
  payload 8acdcaaf8fea863f0d5a7b770c330cf6f899fdb  
  version 111  
}
```

```
% echo "dup hash160 [8acdcaaf8fea863f0d5a7b770c330cf6f899fdb] equalverify checksig" | bx script-encode  
76a9148acdcaaf8fea863f0d5a7b770c330cf6f899fdb88ac
```

[SigLockScript] [PubKey]:

```
[3045022100bd333685ccb3c7ff6751050bc5cc0d64b63d0a711105daf315700145015d224502206d9f408d6fa7612ac0872f82d7786786ba513bc45d00048980d2fec335ba597401]  
[033297c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269bffc3ceb4e]
```

```
% echo  
"[304402202c3a685e40e98df65fc45a3f504e4e4c4c00b4be56e2bba6ca9ae1e009a1180602205659957b593ff724fa69fab99729aa5981f5d86029b4198c61351735bad805f601]  
[033297c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269bffc3ceb4e]" | bx script-encode  
47304402202c3a685e40e98df65fc45a3f504e4e4c4c00b4be56e2bba6ca9ae1e009a1180602205659957b593ff724fa69fab99729aa5981f5d86029b4198c61351735bad805f60121033  
297c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269bffc3ceb4e
```

Bitcoin Stack Steps to Spend a P2PKH Payment

Explicit Execution Script:

[SigLockScript] [PubKey] OP_DUP OP_HASH160 [HASH160(PubKey)] OP_EQUALVERIFY OP_CHECKSIG

LockScript = "OP_DUP OP_HASH160 [HASH160(PubKey)] OP_EQUALVERIFY OP_CHECKSIG"

MESSAGE = [{LockScript}]

Bitcoin LIFO Stack

Empty Stack

[SigLockScript]

[SigLockScript] [PubKey]

[SigLockScript] [PubKey] [PubKey]

[SigLockScript] [PubKey] [HASH160(PubKey)]

[SigLockScript] [PubKey] [HASH160(PubKey)] [HASH160(PubKey)]

[SigLockScript] [PubKey] *(implicitly used MESSAGE above to complete operation)* OP_CHECKSIG

1

Script Execution Queue

[SigLockScript] [PubKey] OP_DUP OP_HASH160 [HASH160(PubKey)]
OP_EQUALVERIFY OP_CHECKSIG

[PubKey] OP_DUP OP_HASH160 [HASH160(PubKey)] OP_EQUALVERIFY
OP_CHECKSIG

OP_DUP OP_HASH160 [HASH160(PubKey)] OP_EQUALVERIFY
OP_CHECKSIG

OP_HASH160 [HASH160(PubKey)] OP_EQUALVERIFY OP_CHECKSIG

[HASH160(PubKey)] OP_EQUALVERIFY OP_CHECKSIG

OP_EQUALVERIFY OP_CHECKSIG

OP_CHECKSIG

Empty Script

P2SM

(Pay to Standard MultiSig)

Deprecated

Template P2MS Scripts:

OP_0 [Sig1] [Sig2] + OP_2 [PubKey1] [PubKey2] [PubKey3] OP_3 OP_CHECKMULTISIG
OP_0 [Sig1] [Sig3] + OP_2 [PubKey1] [PubKey2] [PubKey3] OP_3 OP_CHECKMULTISIG
OP_0 [Sig2] [Sig3] + OP_2 [PubKey1] [PubKey2] [PubKey3] OP_3 OP_CHECKMULTISIG

- Only guaranteed to work for up to 3 keys
- Puts an onus on sender to pay more mining fees
- Has wallet coordination issues to receive multiple addresses to successfully send payments
- Not backwardly compatible with wallets that could only send single signature payments
- Was not widely implemented

P2SH - BIP 16

(Pay to Script Hash)

Single Signature P2SH Scripts:

```
RedeemScript = "[PubKey] OP_CHECKSIG"  
{RedeemScript} = script-encode( "[PubKey] OP_CHECKSIG" )  
[SigRedeemScript] [{RedeemScript}] + OP_HASH160 [HASH160(RedeemScript)] OP_EQUAL
```

Acceptable 2 of 4 Multi Signature P2SH Scripts:

```
RedeemScript = "OP_2 [PubKey1] [PubKey2] [PubKey3] [Pubkey4] OP_4 OP_CHECKMULTISIG"
```

```
OP_0 [Sig1] [Sig2] [{RedeemScript}] + OP_HASH160 [HASH160(RedeemScript)] OP_EQUAL  
OP_0 [Sig1] [Sig3] [{RedeemScript}] + OP_HASH160 [HASH160(RedeemScript)] OP_EQUAL  
OP_0 [Sig1] [Sig4] [{RedeemScript}] + OP_HASH160 [HASH160(RedeemScript)] OP_EQUAL  
OP_0 [Sig2] [Sig3] [{RedeemScript}] + OP_HASH160 [HASH160(RedeemScript)] OP_EQUAL  
OP_0 [Sig2] [Sig4] [{RedeemScript}] + OP_HASH160 [HASH160(RedeemScript)] OP_EQUAL  
OP_0 [Sig3] [Sig4] [{RedeemScript}] + OP_HASH160 [HASH160(RedeemScript)] OP_EQUAL
```

- **P2SH** address formats are backwardly compatible with **P2PKH** wallet address formats
- P2SH Redeem Scripts can support up to 15 compressed multisig keys
- **P2SH Redeem Scripts** are general purpose, and can be used for applications other than P2SH-based **multisig**
- Hash160(**RedeemScript**) provides greater blockchain privacy until an Endorsement is posted
- ASCII RedeemScripts are **script-encoded** before being placed into a **SignatureScript**
- Multisig RedeemScript will become deprecated when Schnorr Signatures are deployed
- Maximum Redeem Script size of 520 bytes, called Serialized Script in BIP 16
- Maximum script size of 10,000 bytes
- *Appears to have an implicit OP_DUP for the RedeemScript in the ScriptSig and performs a script-decode for leftmost copy*

P2SH (continued)

Related Examples:

Testnet Destination P2SH Address

```
% echo "2 [020ae29f86f404e4b302cfa17ff15d93149af6a54c80a4172d47e41f55f6a78d73]
[03664d528eb80096671ef9011c533ceb5df133238e3690d88f2960c786398b86b1] [029a449ea4a2155ea10002d704604bb3e8606631d35af20889a74b82b2dab572f6]
[0321602d78046d63256b1730b119b1aca3428039f18fdb73ccf45ad3e148dd9b17] 4 checkmultisig" | bx script-encode | bx sha256 | bx ripemd160 | bx
base58check-encode -v 196
2N8uwbECKZJLmfYRErQazYBAWfd8PJ66rAN
```

```
% echo "2 [020ae29f86f404e4b302cfa17ff15d93149af6a54c80a4172d47e41f55f6a78d73]
[03664d528eb80096671ef9011c533ceb5df133238e3690d88f2960c786398b86b1] [029a449ea4a2155ea10002d704604bb3e8606631d35af20889a74b82b2dab572f6]
[0321602d78046d63256b1730b119b1aca3428039f18fdb73ccf45ad3e148dd9b17] 4 checkmultisig" | bx script-to-address -v 196
2N8uwbECKZJLmfYRErQazYBAWfd8PJ66rAN
```

Evidence Multisig Funds were Successfully Spent:

```
% bx fetch-balance 2N8uwbECKZJLmfYRErQazYBAWfd8PJ66rAN
balance
{
  address 2N8uwbECKZJLmfYRErQazYBAWfd8PJ66rAN
  received 500000000
  spent 500000000
}
```

OP_HASH160 [HASH160(RedeemScript)] OP_EQUAL:

```
% echo 2N8uwbECKZJLmfYRErQazYBAWfd8PJ66rAN | bx base58check-decode
wrapper
{
  checksum 3150497462
  payload abdc6bdb3646d67f6117047bba7a419f1bf3578
  version 196
}
```

```
% echo "hash160 [abdc6bdb3646d67f6117047bba7a419f1bf3578] equal" | bx script-encode
a914abdc6bdb3646d67f6117047bba7a419f1bf357887
```

P2SH (continued)

OP_0 [Sig1] [Sig2] [script-encode(“OP_2 [PubKey1] [PubKey2] [PubKey3] [Pubkey4] OP_4 OP_CHECKMULTISIG”)]

Sig1:

```
[ 3045022100a5bc2cecbf9aa3ae4caaabe3c18c6cca9803729078947a4ab1bca348afed58c5022020c68d5e49ef19b97bb445d268b14c5c5cb08f7e4215e15984238f44b9eab37e01 ]
```

Sig2:

```
[ 304402204a2480da8c35625e51583694f7d8d5911cc51ecdc9419e0ac7230ff71f2a56a902206ccb631e1063c1865dc98e8f9aa2889c1323da6ec845037964ab7c9e72e5734201 ]
```

script-encode(“OP_2 [PubKey1] [PubKey2] [PubKey3] [Pubkey4] OP_4 OP_CHECKMULTISIG”):

```
% echo "2 [020ae29f86f404e4b302cfa17ff15d93149af6a54c80a4172d47e41f55f6a78d73]
[03664d528eb80096671ef9011c533ceb5df133238e3690d88f2960c786398b86b1]
[029a449ea4a2155ea10002d704604bb3e8606631d35af20889a74b82b2dab572f6]
[0321602d78046d63256b1730b119b1aca3428039f18fdb73ccf45ad3e148dd9b17] 4 checkmultisig" | bx script-encode
5221020ae29f86f404e4b302cfa17ff15d93149af6a54c80a4172d47e41f55f6a78d732103664d528eb80096671ef9011c533ceb5df133238e3690d88f2960c786398b86b121029a449ea4a2155ea10002d704604bb3e8606631d35af20889a74b82b2dab572f6210321602d78046d63256b1730b119b1aca3428039f18fdb73ccf45ad3e148dd9b1754ae
```

OP_0 [Sig1] [Sig2] [script-encode(“OP_2 [PubKey1] [PubKey2] [PubKey3] [Pubkey4] OP_4 OP_CHECKMULTISIG”)]:

```
"zero
[ 3045022100a5bc2cecbf9aa3ae4caaabe3c18c6cca9803729078947a4ab1bca348afed58c5022020c68d5e49ef19b97bb445d268b14c5c5cb08f7e4215e15984238f44b9eab37e01 ]
[ 304402204a2480da8c35625e51583694f7d8d5911cc51ecdc9419e0ac7230ff71f2a56a902206ccb631e1063c1865dc98e8f9aa2889c1323da6ec845037964ab7c9e72e5734201 ]
[ 5221020ae29f86f404e4b302cfa17ff15d93149af6a54c80a4172d47e41f55f6a78d732103664d528eb80096671ef9011c533ceb5df133238e3690d88f2960c786398b86b121029a449ea4a2155ea10002d704604bb3e8606631d35af20889a74b82b2dab572f6210321602d78046d63256b1730b119b1aca3428039f18fdb73ccf45ad3e148dd9b1754ae ] " | bx script-encode
```

```
00483045022100a5bc2cecbf9aa3ae4caaabe3c18c6cca9803729078947a4ab1bca348afed58c5022020c68d5e49ef19b97bb445d268b14c5c5cb08f7e4215e15984238f44b9eab37e0147304402204a2480da8c35625e51583694f7d8d5911cc51ecdc9419e0ac7230ff71f2a56a902206ccb631e1063c1865dc98e8f9aa2889c1323da6ec845037964ab7c9e72e57342014c8b5221020ae29f86f404e4b302cfa17ff15d93149af6a54c80a4172d47e41f55f6a78d732103664d528eb80096671ef9011c533ceb5df133238e3690d88f2960c786398b86b121029a449ea4a2155ea10002d704604bb3e8606631d35af20889a74b82b2dab572f6210321602d78046d63256b1730b119b1aca3428039f18fdb73ccf45ad3e148dd9b1754ae
```

Bitcoin Stack Steps to Spend a P2SH Payment

Explicit Execution Script:

[SigRedeemScript] [{RedeemScript}] OP_HASH160 [HASH160(RedeemScript)] OP_EQUAL

Implicit Execution Script:

[SigRedeemScript] [PubKey] OP_CHECKSIG [{RedeemScript}] OP_HASH160 [bitcoin160({RedeemScript})] OP_EQUAL

RedeemScript = “[PubKey] OP_CHECKSIG”,
MESSAGE = [{RedeemScript}]

Bitcoin LIFO Stack

Empty Stack

[SigRedeemScript]

[SigRedeemScript] [PubKey]

[SigRedeemScript] [PubKey] OP_CHECKSIG

[SigRedeemScript] [PubKey] OP_CHECKSIG [{RedeemScript}]

[SigRedeemScript] [PubKey] OP_CHECKSIG [bitcoin160({RedeemScript})]

[SigRedeemScript] [PubKey] OP_CHECKSIG [bitcoin160({RedeemScript})] [bitcoin160({RedeemScript})] OP_EQUAL

[SigRedeemScript] [PubKey] OP_CHECKSIG 1

[SigRedeemScript] [PubKey] OP_CHECKSIG (implicitly used MESSAGE above to complete operation)

1

Script Execution Queue

[SigRedeemScript] [PubKey] OP_CHECKSIG [{RedeemScript}]
OP_HASH160 [bitcoin160({RedeemScript})] OP_EQUAL

[PubKey] OP_CHECKSIG [{RedeemScript}]
OP_HASH160 [bitcoin160({RedeemScript})] OP_EQUAL

OP_CHECKSIG [{RedeemScript}]
OP_HASH160 [bitcoin160({RedeemScript})] OP_EQUAL

[{RedeemScript}]
OP_HASH160 [bitcoin160({RedeemScript})] OP_EQUAL

OP_HASH160 [bitcoin160({RedeemScript})]
OP_EQUAL

[bitcoin160({RedeemScript})] OP_EQUAL

Empty Script

Empty Script

Empty Script

OP_RETURN

Template OP_RETURN Script:

OP_RETURN [ENCODED_DATA]

- Has no payment **Address** and associated **Endorsement** Script, all endorsements fail
- Satoshi output value should always be zero, thus not impacting **UTXO Databases**
- **IsStandard()** function confirms a TX has no more than one OP_RETURN
- Bitcoin version 0.10+ stores up to 80 bytes of information
 - Notaries apply to archive electronic document signatures, e.g. Tierion
 - Used to color coins (shares, voting, dividends, collectables), e.g. Counterparty, Open Assets
 - Applied for completing a Diffie-Hellman key exchange for stealth transactions

Examples:

Encoding Data

```
% echo "Happy 77th Birthday Silver Fox" | bx base16-encode  
486170707920373774682042697274686461792053696c76657220466f780a
```

OP_RETURN [ENCODED_DATA]

```
% echo "return [486170707920373774682042697274686461792053696c76657220466f780a]" | bx script-encode  
6a1f486170707920373774682042697274686461792053696c76657220466f780a
```

Important Concept About Transaction Balances

Insensitive To Base58check Encoding Version Numbers

```
% echo "2 [020ae29f86f404e4b302cfa17ff15d93149af6a54c80a4172d47e41f55f6a78d73]
[03664d528eb80096671ef9011c533ceb5df133238e3690d88f2960c786398b86b1] [029a449ea4a2155ea10002d704604bb3e8606631d35af20889a74b82b2dab572f6]
[0321602d78046d63256b1730b119b1aca3428039f18fdb73ccf45ad3e148dd9b17] 4 checkmultisig" | bx script-encode | bx bitcoin160
abdc6bdb3646d67f6117047bba7a419f1bf3578
```

```
% echo "2 [020ae29f86f404e4b302cfa17ff15d93149af6a54c80a4172d47e41f55f6a78d73]
[03664d528eb80096671ef9011c533ceb5df133238e3690d88f2960c786398b86b1] [029a449ea4a2155ea10002d704604bb3e8606631d35af20889a74b82b2dab572f6]
[0321602d78046d63256b1730b119b1aca3428039f18fdb73ccf45ad3e148dd9b17] 4 checkmultisig" | bx script-to-address -v 196
2N8uwbECKZJLmfYRErQazYBAWfd8PJ66rAN
```

```
% echo abdc6bdb3646d67f6117047bba7a419f1bf3578 | bx base58check-encode -v 5
3HMjXVGHwqqRTknhBGy7vEBFTGvDWzrQUW
```

```
% echo 2N8uwbECKZJLmfYRErQazYBAWfd8PJ66rAN | bx base58check-decode
wrapper
{
  checksum 3150497462
  payload abdc6bdb3646d67f6117047bba7a419f1bf3578
  version 196
}
```

```
% echo 3HMjXVGHwqqRTknhBGy7vEBFTGvDWzrQUW | bx base58check-decode
wrapper
{
  checksum 1335154895
  payload abdc6bdb3646d67f6117047bba7a419f1bf3578
  version 5
}
```

```
bx fetch-balance 2N8uwbECKZJLmfYRErQazYBAWfd8PJ66rAN
balance
{
  address 2N8uwbECKZJLmfYRErQazYBAWfd8PJ66rAN
  received 500000000
  spent 500000000
}
```

OP_RETURN

Real Example #1

Testnet Transaction Synthesis

Example was Tested:

- Single input **P2PKH** UTXO is unlocked with a signature (44.00000000 TEST)
- Two P2PKH and multisig P2SH locking scripts are implicitly created based upon initial destination addresses
 - Output **P2PKH** locking script remains the same as the input (43.99900000 TEST after confirmed)
 - Output **P2SH** locking script was edited to become a **OP_RETURN**
- Transaction must be signed again after manual edits

Testnet P2PKH Address Synthesis

```
% echo "00112233445566778899aabbccddeeffffeeddccbbaa99887766554433221100" | bx ec-new
3db377a7cc2cc64920b95d2f8594e63b12c0ab7747c0a655536ddf45e86b2788
```

```
% echo 033297c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269bffc3ceb4e | bx bitcoin160
d46ef5fd67873ccbe43cd71ac55c4c3b335213e5
```

```
% echo 033297c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269bffc3ceb4e | bx ec-to-address -v 111
mztCURLXppqDsUnk4XtebZAkq8sr93etgs (Already has 44 TEST)
```

UTXO(s) Exist, but need to locate

```
% bx fetch-balance mztCURLXppqDsUnk4XtebZAkq8sr93etgs
balance
{
  address mztCURLXppqDsUnk4XtebZAkq8sr93etgs
  received 13700000000
  spent 9300000000 ( 137-93 = 44 )
}
```

Testnet P2SH Multisig Address Synthesis (BIP 13)

```
% echo "2 [020ae29f86f404e4b302cfa17ff15d93149af6a54c80a4172d47e41f55f6a78d73]
[03664d528eb80096671ef9011c533ceb5df133238e3690d88f2960c786398b86b1] [029a449ea4a2155ea10002d704604bb3e8606631d35af20889a74b82b2dab572f6]
[0321602d78046d63256b1730b119b1aca3428039f18fdb73ccf45ad3e148dd9b17] 4 checkmultisig" | bx script-to-address -v 196
2N8uwbeCKZJLmfYRErQazYBAWfd8PJ66rAN
```

Identify TX ID to Locate UTXO

```
% bx fetch-history mztCURLXppqDsUnk4XtebZAkq8sr93etgs
transfers
{
  transfer
  {
    received
    {
      hash 354b1eda7d1929a5105d0f16bbce76ec76c48097f79a6d6ae7e6ee67aff0c4cf
      height 509580
      index 1
    }
    value 4400000000
  }
  transfer
  {
    received
    {
      hash 8c294512c98c463f0d4fb2476e8e517549ce1219c71b0eb0c79f632ed446fb5b
      height 505549
      index 0
    }
    spent
    {
      hash 354b1eda7d1929a5105d0f16bbce76ec76c48097f79a6d6ae7e6ee67aff0c4cf
      height 509580
      index 0
    }
    value 4900100000
  }
}
```

Locate UTXO Index and PubKey Script within TX

```
% bx fetch-tx 354b1eda7d1929a5105d0f16bbce76ec76c48097f79a6d6ae7e6ee67aff0c4cf
transaction
{
  hash 354b1eda7d1929a5105d0f16bbce76ec76c48097f79a6d6ae7e6ee67aff0c4cf
  inputs
  {
    input
    {
      address_hash d46ef5fd67873ccbe43cd71ac55c4c3b335213e5
      previous_output
      {
        hash 8c294512c98c463f0d4fb2476e8e517549ce1219c71b0eb0c79f632ed446fb5b
        index 0
      }
      script
      "[3045022100be19bbce24f35895a38c88a7dd60c5a96df6151ba19c1523fb8a34f3afd6cd3d0220667123fbe85e698c4a4d7d391c3c25bf8a52a17542178c996c6c9849ea58662d01] [033297c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269bffc3ceb4e]"
      sequence 4294967295
    }
  }
  lock_time 0
  outputs
  {
    output
    {
      address_hash abdc6bdb3646d67f6117047bba7a419f1bf3578
      script "hash160 [abdc6bdb3646d67f6117047bba7a419f1bf3578] equal"
      value 500000000
    }
    output
    {
      address_hash d46ef5fd67873ccbe43cd71ac55c4c3b335213e5
      script "dup hash160 [d46ef5fd67873ccbe43cd71ac55c4c3b335213e5] equalverify checksig"
      value 4400000000
    }
  }
  version 1
}
```

Note the **UTXO index** is **1** because the TX output of interest is the 2nd one

Construct Skeleton TX

```
% bx tx-encode -v 1 -i 354b1eda7d1929a5105d0f16bbce76ec76c48097f79a6d6ae7e6ee67aff0c4cf:1 -o mztCURLXppqDsUnk4XtebZAkq8sr93etgs:4399900000 -o 2N8uwbECKZJLmfYRErQazYBAWfd8PJ66rAN:0 0100000001cfc4f0af67eee6e76a6d9af79780c476ec76cebb160f5d10a529197ddale4b3501000000000ffffffff0260254106010000001976a914d46ef5fd67873ccbe43cd71ac55c4c3b335213e588ac000000000000000017a914abdc6bdb3646d67f6117047bba7a419f1bf35788700000000
```

```
% bx tx-encode -v 1 -i 354b1eda7d1929a5105d0f16bbce76ec76c48097f79a6d6ae7e6ee67aff0c4cf:1 -o mztCURLXppqDsUnk4XtebZAkq8sr93etgs:4399900000 -o 2N8uwbECKZJLmfYRErQazYBAWfd8PJ66rAN:0 | bx tx-decode
```

```
transaction
{
  hash 098d68844dd03f38aeb1a8aa4fd86d4a5028ca668363e08f6bae57641027e20f
  inputs
  {
    input
    {
      previous_output
      {
        hash 354b1eda7d1929a5105d0f16bbce76ec76c48097f79a6d6ae7e6ee67aff0c4cf
        index 1
      }
      script ""
      sequence 4294967295
    }
  }
  lock_time 0
  outputs
  {
    output
    {
      address_hash d46ef5fd67873ccbe43cd71ac55c4c3b335213e5
      script "dup hash160 [d46ef5fd67873ccbe43cd71ac55c4c3b335213e5] equalverify checksig"
      value 4399900000
    }
    output
    {
      address_hash abdc6bdb3646d67f6117047bba7a419f1bf3578
      script "hash160 [abdc6bdb3646d67f6117047bba7a419f1bf3578] equal"
      value 0
    }
  }
  version 1
}
```

Note the
ENDORSEMENT Script
is undefined

Copy Contract, Sign Contract, Set Endorsement Script, and Validate

```
% echo
0100000001cfc4f0af67eee6e76a6d9af79780c476ec76cebb160f5d10a529197dda1e4b350100000000ffffffff0260254106010000001976a91
4d46ef5fd67873ccbe43cd71ac55c4c3b335213e588ac000000000000000017a914abdc6bdb3646d67f6117047bba7a419f1bf35788700000000
| bx input-sign -i 0 3db377a7cc2cc64920b95d2f8594e63b12c0ab7747c0a655536ddf45e86b2788 "dup hash160
[d46ef5fd67873ccbe43cd71ac55c4c3b335213e5] equalverify checksig"
304402202c3a685e40e98df65fc45a3f504e4e4c4c00b4be56e2bba6ca9ae1e009a1180602205659957b593ff724fa69fab99729aa5981f5d8602
9b4198c61351735bad805f601
```

Form of Endorsement Script is a function of Contract Type

```
% echo
0100000001cfc4f0af67eee6e76a6d9af79780c476ec76cebb160f5d10a529197dda1e4b350100000000ffffffff0260254106010000001976a91
4d46ef5fd67873ccbe43cd71ac55c4c3b335213e588ac000000000000000017a914abdc6bdb3646d67f6117047bba7a419f1bf35788700000000
| bx input-set -i 0
"[304402202c3a685e40e98df65fc45a3f504e4e4c4c00b4be56e2bba6ca9ae1e009a1180602205659957b593ff724fa69fab99729aa5981f5d86
029b4198c61351735bad805f601] [03297c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269bffc3ceb4e]"
0100000001cfc4f0af67eee6e76a6d9af79780c476ec76cebb160f5d10a529197dda1e4b350100000006a47304402202c3a685e40e98df65fc45a3
f504e4e4c4c00b4be56e2bba6ca9ae1e009a1180602205659957b593ff724fa69fab99729aa5981f5d86029b4198c61351735bad805f601210332
97c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269bffc3ceb4efffffffffff0260254106010000001976a914d46ef5fd67873ccbe43cd
71ac55c4c3b335213e588ac000000000000000017a914abdc6bdb3646d67f6117047bba7a419f1bf35788700000000
```

```
% echo
0100000001cfc4f0af67eee6e76a6d9af79780c476ec76cebb160f5d10a529197dda1e4b350100000006a47304402202c3a685e40e98df65fc45a3
f504e4e4c4c00b4be56e2bba6ca9ae1e009a1180602205659957b593ff724fa69fab99729aa5981f5d86029b4198c61351735bad805f601210332
97c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269bffc3ceb4efffffffffff0260254106010000001976a914d46ef5fd67873ccbe43cd
71ac55c4c3b335213e588ac000000000000000017a914abdc6bdb3646d67f6117047bba7a419f1bf35788700000000 | bx input-validate -
i 0 03297c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269bffc3ceb4e "dup hash160
[d46ef5fd67873ccbe43cd71ac55c4c3b335213e5] equalverify checksig"
304402202c3a685e40e98df65fc45a3f504e4e4c4c00b4be56e2bba6ca9ae1e009a1180602205659957b593ff724fa69fab99729aa5981f5d8602
9b4198c61351735bad805f601
The endorsement is valid.
```

Notice the New Signature Script

```
% echo
0100000001cfc4f0af67eee6e76a6d9af79780c476ec76cebb160f5d10a529197dda1e4b35010000006a47304402202c3a685e40e98df65fc45a3f504e4e4c4c00b4be56e2bba6ca9a
ele009a1180602205659957b593ff724fa69fab99729aa5981f5d86029b4198c61351735bad805f60121033297c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269bffc3c
eb4effffffff0260254106010000001976a914d46ef5fd67873ccbe43cd71ac55c4c3b335213e588ac000000000000000017a914abdc6bdb3646d67f6117047bbea7a419f1bf357887
00000000 | bx tx-decode
transaction
{
  hash 80eecb43742ab119a30121c8bf733fbb9bd4de95bcd50d35d1e33d6a328d6a90
  inputs
  {
    input
    {
      address_hash d46ef5fd67873ccbe43cd71ac55c4c3b335213e5
      previous_output
      {
        hash 354b1eda7d1929a5105d0f16bbce76ec76c48097f79a6d6ae7e6ee67aff0c4cf
        index 1
      }
      script
      "[304402202c3a685e40e98df65fc45a3f504e4e4c4c00b4be56e2bba6ca9ae1e009a1180602205659957b593ff724fa69fab99729aa5981f5d86029b4198c61351735bad805f601]
[033297c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269bffc3ceb4e]"
      sequence 4294967295
    }
  }
  lock_time 0
  outputs
  {
    output
    {
      address_hash d46ef5fd67873ccbe43cd71ac55c4c3b335213e5
      script "dup hash160 [d46ef5fd67873ccbe43cd71ac55c4c3b335213e5] equalverify checksig"
      value 4399900000
    }
    output
    {
      address_hash abdc6bdb3646d67f6117047bbea7a419f1bf3578
      script "hash160 [abdc6bdb3646d67f6117047bbea7a419f1bf3578] equal"
      value 0
    }
  }
  version 1
}
```

Manual Editing Of Raw TX to Include OP_RETURN

See: <https://en.bitcoin.it/wiki/Transaction> and <https://en.bitcoin.it/wiki/Script>

```
0100000001cfc4f0af67eee6e76a6d9af79780c476ec76cebb160f5d10a529197dda1e4b35010000006a47304402202c
3a685e40e98df65fc45a3f504e4e4c4c00b4be56e2bba6ca9ae1e009a1180602205659957b593ff724fa69fab99729aa
5981f5d86029b4198c61351735bad805f60121033297c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269bf
fc3ceb4effffffff0260254106010000001976a914d46ef5fd67873ccbe43cd71ac55c4c3b335213e588ac0000000000
00000017a914abdc6bdb3646d67f6117047bbea7a419f1bf35788700000000
```

```
% echo 76a914d46ef5fd67873ccbe43cd71ac55c4c3b335213e5 | bx script-decode
dup hash160 [d46ef5fd67873ccbe43cd71ac55c4c3b335213e5]
```

```
% echo a914abdc6bdb3646d67f6117047bbea7a419f1bf357887 | bx script-decode
hash160 [abdc6bdb3646d67f6117047bbea7a419f1bf3578] equal
```

```
% echo "Happy 77th Birthday Silver Fox" | bx base16-encode
486170707920373774682042697274686461792053696c76657220466f780a
```

```
% echo "return [486170707920373774682042697274686461792053696c76657220466f780a]" | bx script-
encode
6a1f486170707920373774682042697274686461792053696c76657220466f780a
```

```
0100000001cfc4f0af67eee6e76a6d9af79780c476ec76cebb160f5d10a529197dda1e4b35010000006a47304402202c
3a685e40e98df65fc45a3f504e4e4c4c00b4be56e2bba6ca9ae1e009a1180602205659957b593ff724fa69fab99729aa
5981f5d86029b4198c61351735bad805f60121033297c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269bf
fc3ceb4effffffff0260254106010000001976a914d46ef5fd67873ccbe43cd71ac55c4c3b335213e588ac0000000000
000000216a1f486170707920373774682042697274686461792053696c76657220466f780a00000000
```

Feedback that the Manual Edit is Good

```
% echo
0100000001cfc4f0af67eee6e76a6d9af79780c476ec76cebb160f5d10a529197dda1e4b35010000006a47304402202c3a685e40e98df65fc45a3f504e4e4c4c00b4be56e2bba6ca9ae
1e009a1180602205659957b593ff724fa69fab99729aa5981f5d86029b4198c61351735bad805f60121033297c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269bffc3ceb
4effffffff0260254106010000001976a914d46ef5fd67873ccbe43cd71ac55c4c3b335213e588ac0000000000000000216a1f486170707920373774682042697274686461792053696
c76657220466f780a00000000
| bx tx-decode
transaction
{
  hash 9b4ff8d9045456d50d542599f801020a5e7c19e012bd77b2d3136184491b5e6f
  inputs
  {
    input
    {
      address_hash d46ef5fd67873ccbe43cd71ac55c4c3b335213e5
      previous_output
      {
        hash 354b1eda7d1929a5105d0f16bbce76ec76c48097f79a6d6ae7e6ee67aff0c4cf
        index 1
      }
      script
      "[304402202c3a685e40e98df65fc45a3f504e4e4c4c00b4be56e2bba6ca9ae1e009a1180602205659957b593ff724fa69fab99729aa5981f5d86029b4198c61351735bad805f601]
[033297c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269bffc3ceb4e]"
      sequence 4294967295
    }
  }
  lock_time 0
  outputs
  {
    output
    {
      address_hash d46ef5fd67873ccbe43cd71ac55c4c3b335213e5
      script "dup hash160 [d46ef5fd67873ccbe43cd71ac55c4c3b335213e5] equalverify checksig"
      value 4399900000
    }
    output
    {
      script "return [486170707920373774682042697274686461792053696c76657220466f780a]"
      value 0
    }
  }
  version 1
}
```

sign-input again, set-input, input-validate

```
% echo
0100000001cfc4f0af67eee6e76a6d9af79780c476ec76cebb160f5d10a529197dda1e4b35010000006a47304402202c3a685e40e98df65fc45a3f504e4e4c4c00b4be56e2bba6c
a9ae1e009a1180602205659957b593ff724fa69fab99729aa5981f5d86029b4198c61351735bad805f60121033297c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269
bffc3ceb4effffffffff0260254106010000001976a914d46ef5fd67873ccbe43cd71ac55c4c3b335213e588ac0000000000000000216a1f486170707920373774682042697274686
461792053696c76657220466f780a00000000 | bx input-validate -i 0 033297c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269bffc3ceb4e "dup hash160
[d46ef5fd67873ccbe43cd71ac55c4c3b335213e5] equalverify checksig"
304402202c3a685e40e98df65fc45a3f504e4e4c4c00b4be56e2bba6ca9ae1e009a1180602205659957b593ff724fa69fab99729aa5981f5d86029b4198c61351735bad805f601
The endorsement is not valid.
```

```
% echo
0100000001cfc4f0af67eee6e76a6d9af79780c476ec76cebb160f5d10a529197dda1e4b35010000006a47304402202c3a685e40e98df65fc45a3f504e4e4c4c00b4be56e2bba6c
a9ae1e009a1180602205659957b593ff724fa69fab99729aa5981f5d86029b4198c61351735bad805f60121033297c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269
bffc3ceb4effffffffff0260254106010000001976a914d46ef5fd67873ccbe43cd71ac55c4c3b335213e588ac0000000000000000216a1f486170707920373774682042697274686
461792053696c76657220466f780a00000000 | bx input-sign -i 0 3db377a7cc2cc64920b95d2f8594e63b12c0ab7747c0a655536ddf45e86b2788 "dup hash160
[d46ef5fd67873ccbe43cd71ac55c4c3b335213e5] equalverify checksig"
3044022001d50b67bf020de1a22f808098ef467bc643217a5fee430e63c2f8d5a85894a0022047df7c0d15ddd2fa45e4068ca94ce8087bb260ac2bf33e6264a4d4f12251ce0b01
```

```
% echo
0100000001cfc4f0af67eee6e76a6d9af79780c476ec76cebb160f5d10a529197dda1e4b35010000006a47304402202c3a685e40e98df65fc45a3f504e4e4c4c00b4be56e2bba6c
a9ae1e009a1180602205659957b593ff724fa69fab99729aa5981f5d86029b4198c61351735bad805f60121033297c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269
bffc3ceb4effffffffff0260254106010000001976a914d46ef5fd67873ccbe43cd71ac55c4c3b335213e588ac0000000000000000216a1f486170707920373774682042697274686
461792053696c76657220466f780a00000000 | bx input-set -i 0
"[3044022001d50b67bf020de1a22f808098ef467bc643217a5fee430e63c2f8d5a85894a0022047df7c0d15ddd2fa45e4068ca94ce8087bb260ac2bf33e6264a4d4f12251ce0b01]
[033297c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269bffc3ceb4e]"
0100000001cfc4f0af67eee6e76a6d9af79780c476ec76cebb160f5d10a529197dda1e4b35010000006a473044022001d50b67bf020de1a22f808098ef467bc643217a5fee430e6
3c2f8d5a85894a0022047df7c0d15ddd2fa45e4068ca94ce8087bb260ac2bf33e6264a4d4f12251ce0b0121033297c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269
bffc3ceb4effffffffff0260254106010000001976a914d46ef5fd67873ccbe43cd71ac55c4c3b335213e588ac0000000000000000216a1f486170707920373774682042697274686
461792053696c76657220466f780a00000000
```

```
% echo
0100000001cfc4f0af67eee6e76a6d9af79780c476ec76cebb160f5d10a529197dda1e4b35010000006a473044022001d50b67bf020de1a22f808098ef467bc643217a5fee430e6
3c2f8d5a85894a0022047df7c0d15ddd2fa45e4068ca94ce8087bb260ac2bf33e6264a4d4f12251ce0b0121033297c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269
bffc3ceb4effffffffff0260254106010000001976a914d46ef5fd67873ccbe43cd71ac55c4c3b335213e588ac0000000000000000216a1f486170707920373774682042697274686
461792053696c76657220466f780a00000000 | bx input-validate -i 0 033297c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269bffc3ceb4e "dup hash160
[d46ef5fd67873ccbe43cd71ac55c4c3b335213e5] equalverify checksig"
3044022001d50b67bf020de1a22f808098ef467bc643217a5fee430e63c2f8d5a85894a0022047df7c0d15ddd2fa45e4068ca94ce8087bb260ac2bf33e6264a4d4f12251ce0b01
The endorsement is valid.
```

Compute TXID, Send, Watch, Balance

```
% echo
0100000001cfc4f0af67eee6e76a6d9af79780c476ec76cebb160f5d10a529197dda1e4b35010000006a473044022001d50b67bf020de1a22f808098ef467bc643217a5fee430e63c2f8d5a85894a0022047df7c0d15ddd2fa45e4068ca94ce8087bb260ac2bf33e6264a4d4f12251ce0b0121033297c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269bffc3ceb4effffffffff0260254106010000001976a914d46ef5fd67873ccbe43cd71ac55c4c3b335213e588ac00000000000000000216a1f486170707920373774682042697274686461792053696c76657220466f780a00000000 | bx bitcoin256
a041f7d7139debf75ade2d8ea7f7d22e88acfa9f6a4b08b8b5625dc0779af198
```

```
% bx send-tx
0100000001cfc4f0af67eee6e76a6d9af79780c476ec76cebb160f5d10a529197dda1e4b35010000006a473044022001d50b67bf020de1a22f808098ef467bc643217a5fee430e63c2f8d5a85894a0022047df7c0d15ddd2fa45e4068ca94ce8087bb260ac2bf33e6264a4d4f12251ce0b0121033297c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269bffc3ceb4effffffffff0260254106010000001976a914d46ef5fd67873ccbe43cd71ac55c4c3b335213e588ac00000000000000000216a1f486170707920373774682042697274686461792053696c76657220466f780a00000000
Sent transaction at 2015-Aug-09 23:32:09.
```

```
% bx watch-address mztCURLXppqDsUnk4XtebZAkq8sr93etgs
Watching address: mztCURLXppqDsUnk4XtebZAkq8sr93etgs...
```

```
% bx fetch-balance mztCURLXppqDsUnk4XtebZAkq8sr93etgs
balance
{
  address mztCURLXppqDsUnk4XtebZAkq8sr93etgs
  confirmed 4399900000
  received 13700000000
  unspent 4399900000
}
```

Address History After Blockchain Commitment

```
% bx fetch-history mztCURLXppqDsUnk4XtebZAkq8sr93etgs
transfers
{
  transfer
  {
    received
    {
      hash a041f7d7139debf75ade2d8ea7f7d22e88acfa9f6a4b08b8b5625dc0779af198
      height 529179
      index 0
    }
    value 4399900000
  }
  transfer
  {
    received
    {
      hash 354b1eda7d1929a5105d0f16bbce76ec76c48097f79a6d6ae7e6ee67aff0c4cf
      height 509580
      index 1
    }
    spent
    {
      hash a041f7d7139debf75ade2d8ea7f7d22e88acfa9f6a4b08b8b5625dc0779af198
      height 529179
      index 0
    }
    value 4400000000
  }
  transfer
  {
    received
    {
      hash 8c294512c98c463f0d4fb2476e8e517549ce1219c71b0eb0c79f632ed446fb5b
      height 505549
      index 0
    }
    spent
    {
      hash 354b1eda7d1929a5105d0f16bbce76ec76c48097f79a6d6ae7e6ee67aff0c4cf
      height 509580
      index 0
    }
    value 4900100000
  }
}
```

Block Details for Mined TX

```
% bx fetch-header -t 529179
```

```
header
```

```
{
```

```
bits 439544256
```

```
hash 000000000001aab176ad30b6aef36ff1b1c2445cf4a8799e6cf43f8d1e18515
```

```
merkle_tree_hash 25567e8b4dd7ad4198598528c53f631bbaaf70c05faa444a6ddeb9b3c941b8aa
```

```
nonce 1410842890
```

```
previous_block_hash 00000000086135e25d5b6e3a5c594a22fca08c5cafe7ff8430318ea96bc05ec
```

```
time_stamp 1439184912
```

```
version 3
```

```
}
```

```
% bx fetch-header -s 000000000001aab176ad30b6aef36ff1b1c2445cf4a8799e6cf43f8d1e18515
```

```
header
```

```
{
```

```
bits 439544256
```

```
hash 000000000001aab176ad30b6aef36ff1b1c2445cf4a8799e6cf43f8d1e18515
```

```
merkle_tree_hash 25567e8b4dd7ad4198598528c53f631bbaaf70c05faa444a6ddeb9b3c941b8aa
```

```
nonce 1410842890
```

```
previous_block_hash 00000000086135e25d5b6e3a5c594a22fca08c5cafe7ff8430318ea96bc05ec
```

```
time_stamp 1439184912
```

```
version 3
```

```
}
```

This Fetched TX Should Look Familiar

```
% bx fetch-tx a041f7d7139debf75ade2d8ea7f7d22e88acfa9f6a4b08b8b5625dc0779af198
transaction
{
  hash a041f7d7139debf75ade2d8ea7f7d22e88acfa9f6a4b08b8b5625dc0779af198
  inputs
  {
    input
    {
      address_hash d46ef5fd67873ccbe43cd71ac55c4c3b335213e5
      previous_output
      {
        hash 354b1eda7d1929a5105d0f16bbce76ec76c48097f79a6d6ae7e6ee67aff0c4cf
        index 1
      }
      script
      "[3044022001d50b67bf020de1a22f808098ef467bc643217a5fee430e63c2f8d5a85894a0022047df7c0d15ddd2fa45e4068ca94ce8087bb260ac2bf33e6264a4d4f12251ce0b01] [033297c7e4f78310e53d9c732374267b4deeb30b532bda0947e5269bffc3ceb4e]"
      sequence 4294967295
    }
  }
  lock_time 0
  outputs
  {
    output
    {
      address_hash d46ef5fd67873ccbe43cd71ac55c4c3b335213e5
      script "dup hash160 [d46ef5fd67873ccbe43cd71ac55c4c3b335213e5] equalverify checksig"
      value 4399900000
    }
    output
    {
      script "return [486170707920373774682042697274686461792053696c76657220466f780a]"
      value 0
    }
  }
  version 1
}
```

Simpler Approach to Create the Same OP_RETURN TX in One Slide

```
% echo 3db377a7cc2cc64920b95d2f8594e63b12c0ab7747c0a655536ddf45e86b2788 | bx ec-to-public  
033297c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269bffc3ceb4e
```

```
% echo "Happy 77th Birthday Silver Fox" | bx base16-encode  
486170707920373774682042697274686461792053696c76657220466f780a
```

```
% echo "return [486170707920373774682042697274686461792053696c76657220466f780a]" | bx script-encode  
6a1f486170707920373774682042697274686461792053696c76657220466f780a
```

```
% bx tx-encode -v 1 -i 354b1eda7d1929a5105d0f16bbce76ec76c48097f79a6d6ae7e6ee67aff0c4cf:1 -o  
mztCURLXppqDsUnk4XtebZAkq8sr93etgs:4399900000 -o 6a1f486170707920373774682042697274686461792053696c76657220466f780a:  
0  
0100000001cfc4f0af67eee6e76a6d9af79780c476ec76cebb160f5d10a529197dda1e4b350100000000ffffffff0260254106010000001976a9  
14d46ef5fd67873ccbe43cd71ac55c4c3b335213e588ac0000000000000000216a1f486170707920373774682042697274686461792053696c76  
657220466f780a00000000
```

```
% bx tx-encode -v 1 -i 354b1eda7d1929a5105d0f16bbce76ec76c48097f79a6d6ae7e6ee67aff0c4cf:1 -o  
mztCURLXppqDsUnk4XtebZAkq8sr93etgs:4399900000 -o 6a1f486170707920373774682042697274686461792053696c76657220466f780a:  
0 | bx input-sign -i 0 3db377a7cc2cc64920b95d2f8594e63b12c0ab7747c0a655536ddf45e86b2788 "dup hash160  
[d46ef5fd67873ccbe43cd71ac55c4c3b335213e5] equalverify checksig"  
3044022001d50b67bf020de1a22f808098ef467bc643217a5fee430e63c2f8d5a85894a0022047df7c0d15ddd2fa45e4068ca94ce8087bb260ac  
2bf33e6264a4d4f12251ce0b01
```

```
% bx tx-encode -v 1 -i 354b1eda7d1929a5105d0f16bbce76ec76c48097f79a6d6ae7e6ee67aff0c4cf:1 -o  
mztCURLXppqDsUnk4XtebZAkq8sr93etgs:4399900000 -o 6a1f486170707920373774682042697274686461792053696c76657220466f780a:  
0 | bx input-set -i 0  
"[3044022001d50b67bf020de1a22f808098ef467bc643217a5fee430e63c2f8d5a85894a0022047df7c0d15ddd2fa45e4068ca94ce8087bb260  
ac2bf33e6264a4d4f12251ce0b01] [033297c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269bffc3ceb4e]"  
0100000001cfc4f0af67eee6e76a6d9af79780c476ec76cebb160f5d10a529197dda1e4b350100000006a473044022001d50b67bf020de1a22f80  
8098ef467bc643217a5fee430e63c2f8d5a85894a0022047df7c0d15ddd2fa45e4068ca94ce8087bb260ac2bf33e6264a4d4f12251ce0b012103  
3297c7e4f78310e53d9c732374267b4deeeb30b532bda0947e5269bffc3ceb4effffffffff0260254106010000001976a914d46ef5fd67873ccbe4  
3cd71ac55c4c3b335213e588ac00000000000000000216a1f486170707920373774682042697274686461792053696c76657220466f780a000000  
00
```

Transactions with Locktimes

Bitcoin LockTime Mechanisms

LockTimes in a Nutshell

LockTime Mechanisms	<i>Absolute Timelock</i>	<i>Relative Timelock</i>
<i>Transaction Level</i>	nLockTime	nSequence
<i>UTXO Level (or Script Level)</i>	CheckLockTimeVerify (CLTV)	CheckSequenceVerify (CSV)

Source: <https://medium.com/@RobinHung/bitcoin-timelocks-in-a-nutshell-4c95aafc7a59>

Using bx tx-encode to Set nLocktime and nSequence

```
% bx tx-encode -v 2 -l 2148930648 -i 354b1eda7d1929a5105d0f16bbce76ec76c48097f79a6d6ae7e6ee67aff0c4cf:1:506 -o mztCURLXppqDsUnk4XtebZAkq8sr93etgs:4399900000 -o 2N8uwbECKZJLmfYRErQazYBAWfd8PJ66rAN:0 | bx tx-decode transaction
```

```
{
  hash d081b36ea8c93440144552d020fa296792f2851af7b8126e6a21871c49e318c8
  inputs
  {
    input
    {
      previous_output
      {
        hash 354b1eda7d1929a5105d0f16bbce76ec76c48097f79a6d6ae7e6ee67aff0c4cf
        index 1
      }
      script ""
      sequence 506
    }
  }
  lock_time 2148930648
  outputs
  {
    output
    {
      address_hash d46ef5fd67873ccbe43cd71ac55c4c3b335213e5
      script "dup hash160 [d46ef5fd67873ccbe43cd71ac55c4c3b335213e5] equalverify checksig"
      value 4399900000
    }
    output
    {
      address_hash abdc6bdb3646d67f6117047bba7a419f1bf3578
      script "hash160 [abdc6bdb3646d67f6117047bba7a419f1bf3578] equal"
      value 0
    }
  }
  version 2
}
```

Then wait 506 blocks ($506 \times 512 / 3600 \approx 72$ Hrs.) before redeeming

Don't route/forward/broadcast TX until Block 1447000 is mined
(per next slide, absolute block # 1447000 = 0x80161458)

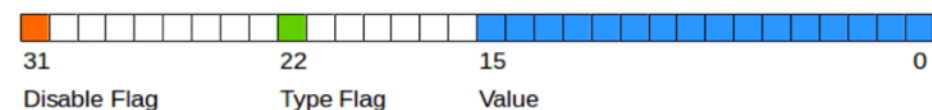
Transaction-Level nLockTime and nSequence Input Value Semantics

- **nLockTime** (absolute time) is the block number or timestamp at which this transaction will be propagated to remote **mempools** for mining. Was originally a 32bit unsigned integer. See the Table below from https://en.bitcoin.it/wiki/Protocol_documentation#tx concerning value semantics.

Value	Description
0	Not locked
< 500000000	Block number at which this transaction is unlocked
>= 500000000	UNIX timestamp at which this transaction is unlocked

UNIX Time started 1 January 1970,
and ends 19 January 2038 UTC

- **nSequence** (relative UTXO time) was repurposed to prevent mining of a transaction until a certain age of the spent output measured in blocks or timespan is reached
 - **Pre BIP 68** Consensus Rules:
 - Was a 32 bit unsigned integer that used as a transaction script version number defined by the sender for each locking script. Intended for transactions in mempool when information is updated to block inclusion
 - **Post BIP 68** Consensus Rules:
 - **Disable Flag** bit (1<<31) is set, locktime is **absolute**
 - **Disable Flag** bit (1<<31) is unset, locktime is **relative**
 - **Type Flag** bit (1<<22) is unset, **units are in number of blocks**
 - **Type Flag** bit (1<<22) is set, **units are in seconds** in multiples of 512 seconds unlike **nLockTime**
 - **Relative offsets** are specified by the least significant bits bitmask **0x0000FFFF**, up to ~388 days to ~455 days of offsets
- **BIP 125** “Opt-In Replace By Fee (**RBF**)” logic is for nodes recognizing a TX with an unfinalized nSequence versions is to replace a TX versions already residing in mempools, but not yet mined. This useful to reprioritize the mining of related TXs when the collective Bitcoin Network mempool is congested and confirmation times are taking hours or even days. **BIP 125** & **BIP 68** can co-exist.
- With bitcoin-explorer (bx), an undefined **sequence** (nSequence) defaults to **0xFFFFFFFF** (4,294,967,295), signaling a finalized locking script version. This sets the default lock time to be **absolute**, and forces **nLockTime to be 0**. This behavior will cause CHECKLOCKTIMEVERIFY (CLTV) to always fail.



Absolute Locktime

nLocktime and BIP 65 CLTV

(OP_CHECKLOCKTIMEVERIFY)

Use Case: Predated Personal Check (Absolute Time)

Template P2SH-CLTV Scripts:

[Sig] [PubKey]

[locktime] OP_CHECKLOCKTIMEVERIFY OP_DROP OP_DUP OP_HASH160 [HASH160(PubKey)] OP_EQUALVERIFY OP_CHECKSIG

- One value **nLocktime** applies to all TX inputs
- With no CLTV context, **nLocktime** is associated with transaction-level node propagation behaviors
- **CLTV** opcode should be nested inside a standard **P2SH** payment address to be **IsStandard**
- **CLTV locktime** is absolute lock time measured by block number or UNIX time
- nLocktime and CLTV lock time units (Block or UNIX time) **MUST** match
- Each UTXO locking script can have a unique CLTV locktime
- CLTV locktimes complements nLocktime by restricting when a specific UTXO can be spent by a future transaction with its input nLocktime set to a value greater than or equal to a newly created transaction endorsement(s) of CLTV UTXO(s). An encumbrance script's CLTV expiration time must be set to be less than or equal to a newly created spending transaction's nLocktime
- **nLocktime** and CLTV locktime units (Block or UNIX Time) **MUST** match. Additionally for time to be absolute, **nSequence** value must be set to be **greater than 2^{31}**
- Smart Contract scripts utilizing CLTV will tend to utilize decision flow control; IF, ELSE, ENDIF
- Types of Bitcoin Time: Block Height, Block Time (a block's UNIX timestamp), **Median-Time-Passed (MTP)**. As a counter measure to miners lying about a block's time (when block mining seignorage fees are less substantial), MTP is applied when BIP 65 (CLTV) and BIP 112 (CSV) needs time denoted in UNIX Time. MTP (BIP-113) is the median time for a moving 11 block window used instead of a block's affixed timestamp.

Relative Locktime

BIP 68 **nSequence** and BIP112 **CSV** (OP_CHECKSEQUENCEVERIFY)

Use Case: **Predated Personal Check (Relative Time)**

Template P2SH-CSV Scripts:

[sig] [pubKey] +
[locktime] OP_CHECKSEQUENCEVERIFY OP_DROP OP_DUP OP_HASH160 [HASH160(PubKey)] OP_EQUALVERIFY OP_CHECKSIG

- CSV Proof-of-Publication (**PoP**) enables escrow, payment channels, Hashed TimeLock Contracts (**HTLC**) for cross chain atomic swaps, and bi-direction payment channels used by the Lightning Network (**LN**)
- Each TX input can have its own unique **nSequence**
- **CSV** opcode should be nested inside a **P2SH** payment address to be **IsStandard**
- **BIP 68 nSequence** plays a consensus-based role is analogous to **nLockTime**, but at the input endorsement script-level instead of at the input transaction-level
- **CSV locktime** (measured in block height or UNIX time) are relative to specific mined UTXO events, opposed to specific mined block number or absolute time. A relative locktime clock doesn't start counting until the TX output containing a CSV locking script becomes a UTXO
- **nSequence** and CSV locktime units (Block or UNIX Time) **MUST** match. Additionally for time to be relative, **nSequence** value must be set to be **less than** 2^{31}
- Purpose of **CSV (BIP 112)** is analogous to **CLTV (BIP 65)** for each encumbrance script, but requires the **transaction version number to be 2 or greater** (BIP 112)
- Smart Contract scripts utilizing CSV will tend to utilize decision flow control; IF, ELSE, ENDIF
- Types of Bitcoin Time: Block Height, Block Time (a block's UNIX timestamp), **Median-Time-Passed (MTP)**. As a counter measure to miners lying about a block's time (when block mining seignorage fees are less substantial), MTP is applied when BIP 65 (CLTV) and BIP 112 (CSV) needs time denoted in UNIX Time. MTP (BIP-113) is the median time for a moving 11 block window used instead of a block's affixed timestamp.

Real Example #2

Testnet Transaction Synthesis

One Testnet Input:

- **P2PKH**

Four Testnet Outputs:

1. **P2PKH,**
2. **P2SH (not multisig),**
3. **CSV-P2PKH,**
4. **P2SH(P2WPKH)**

Bitcoin Stack Steps to Spend a P2PKH Payment

Explicit Execution Script:

[SigLockScript] [PubKey] OP_DUP OP_HASH160 [HASH160(PubKey)] OP_EQUALVERIFY OP_CHECKSIG

LockScript = "OP_DUP OP_HASH160 [HASH160(PubKey)] OP_EQUALVERIFY OP_CHECKSIG"

MESSAGE = [{LockScript}]

Bitcoin LIFO Stack

Empty Stack

[SigLockScript]

[SigLockScript] [PubKey]

[SigLockScript] [PubKey] [PubKey]

[SigLockScript] [PubKey] [HASH160(PubKey)]

[SigLockScript] [PubKey] [HASH160(PubKey)] [HASH160(PubKey)]

[SigLockScript] [PubKey] *(implicitly used MESSAGE above to complete operation)* OP_CHECKSIG

1

Script Execution Queue

[SigLockScript] [PubKey] OP_DUP OP_HASH160 [HASH160(PubKey)]
OP_EQUALVERIFY OP_CHECKSIG

[PubKey] OP_DUP OP_HASH160 [HASH160(PubKey)] OP_EQUALVERIFY
OP_CHECKSIG

OP_DUP OP_HASH160 [HASH160(PubKey)] OP_EQUALVERIFY
OP_CHECKSIG

OP_HASH160 [HASH160(PubKey)] OP_EQUALVERIFY OP_CHECKSIG

[HASH160(PubKey)] OP_EQUALVERIFY OP_CHECKSIG

OP_EQUALVERIFY OP_CHECKSIG

OP_CHECKSIG

Empty Script

Bitcoin Stack Steps to Spend a P2SH Payment

Explicit Execution Script:

[SigRedeemScript] [{RedeemScript}] OP_HASH160 [HASH160(RedeemScript)] OP_EQUAL

Implicit Execution Script:

[SigRedeemScript] [PubKey] OP_CHECKSIG [{RedeemScript}] OP_HASH160 [bitcoin160({RedeemScript})] OP_EQUAL
RedeemScript = “[PubKey] OP_CHECKSIG”,
MESSAGE = [{RedeemScript}]

Bitcoin LIFO Stack

Empty Stack

[SigRedeemScript]

[SigRedeemScript] [PubKey]

[SigRedeemScript] [PubKey] OP_CHECKSIG

[SigRedeemScript] [PubKey] OP_CHECKSIG [{RedeemScript}]

[SigRedeemScript] [PubKey] OP_CHECKSIG [bitcoin160({RedeemScript})]

[SigRedeemScript] [PubKey] OP_CHECKSIG [bitcoin160({RedeemScript})] [bitcoin160({RedeemScript})] OP_EQUAL

[SigRedeemScript] [PubKey] OP_CHECKSIG 1

[SigRedeemScript] [PubKey] OP_CHECKSIG (implicitly used MESSAGE above to complete operation)

1

Script Execution Queue

[SigRedeemScript] [PubKey] OP_CHECKSIG [{RedeemScript}]
OP_HASH160 [bitcoin160({RedeemScript})] OP_EQUAL

[PubKey] OP_CHECKSIG [{RedeemScript}]
OP_HASH160 [bitcoin160({RedeemScript})] OP_EQUAL

OP_CHECKSIG [{RedeemScript}]
OP_HASH160 [bitcoin160({RedeemScript})] OP_EQUAL

[{RedeemScript}]
OP_HASH160 [bitcoin160({RedeemScript})] OP_EQUAL

OP_HASH160 [bitcoin160({RedeemScript})]
OP_EQUAL

[bitcoin160({RedeemScript})] OP_EQUAL

Empty Script

Empty Script

Empty Script

Bitcoin Stack Steps to Spend a P2SH(CSV-P2PK) Payment

Explicit Execution Script:

[SigRedeemScript] [{RedeemScript}] OP_HASH160 [HASH160({RedeemScript})] OP_EQUAL

Implicit Execution Script:

[SigRedeemScript] [bitcoin160({CSV-P2PK})] OP_CHECKSIG [{RedeemScript}] OP_HASH160 [bitcoin160({RedeemScript})] OP_EQUAL

CSV-P2PK = "[0040000f] checksequenceverify drop [PubKey]",

RedeemScript = "[bitcoin160({CSV-P2PK})] OP_CHECKSIG",

MESSAGE = [{RedeemScript}]

** Insights above gleaned from a careful examination of <https://github.com/bitcoin/bips/blob/master/bip-0016.mediawiki#specification> and generalization of "Spending a P2SH Payment"; operation {} = bx script-encode();

Bitcoin LIFO Stack

Empty Stack

[SigRedeemScript]

[SigRedeemScript] [bitcoin160({CSV-P2PK})]

[SigRedeemScript] [bitcoin160({CSV-P2PK})] OP_CHECKSIG

[SigRedeemScript] [bitcoin160({CSV-P2PK})] OP_CHECKSIG [{RedeemScript}]

[SigRedeemScript] [bitcoin160({CSV-P2PK})] OP_CHECKSIG [bitcoin160({RedeemScript})]

[SigRedeemScript] [bitcoin160({CSV-P2PK})] OP_CHECKSIG [bitcoin160({RedeemScript})] [bitcoin160({RedeemScript})]

[SigRedeemScript] [bitcoin160({CSV-P2PK})] OP_CHECKSIG 1

[SigRedeemScript] [bitcoin160({CSV-P2PK})] OP_CHECKSIG (implicitly used MESSAGE above to complete operation)

1

Script Execution Queue

[SigRedeemScript] [bitcoin160({CSV-P2PK})] OP_CHECKSIG [{RedeemScript}]
OP_HASH160 [bitcoin160({RedeemScript})] OP_EQUAL

[bitcoin160({CSV-P2PK})] OP_CHECKSIG [{RedeemScript}]
OP_HASH160 [bitcoin160({RedeemScript})] OP_EQUAL

OP_CHECKSIG [{RedeemScript}]
OP_HASH160 [bitcoin160({RedeemScript})] OP_EQUAL

[{RedeemScript}]
OP_HASH160 [bitcoin160({RedeemScript})] OP_EQUAL

OP_HASH160 [bitcoin160({RedeemScript})] OP_EQUAL

[bitcoin160({RedeemScript})] OP_EQUAL

OP_EQUAL

Empty Script

Empty Script

Empty Script

Example #2 - Input UTXO to Fund Transaction

Testnet HASH160(Public Key):

```
% echo eb0df72d458a700e19199394ae209898ca06f31f4094c9eedd9f56074ced95a1 | bx ec-to-public | bx bitcoin160
4809949b267446c532024d13211a6e6e71ee1937
```

Testnet P2PKH Address:

```
% echo eb0df72d458a700e19199394ae209898ca06f31f4094c9eedd9f56074ced95a1 | bx ec-to-public | bx ec-to-address -v 111
mn5rRXhVEqV6tboNXmpg62xUcnxLGV8Dhe
```

```
% echo mn5rRXhVEqV6tboNXmpg62xUcnxLGV8Dhe | bx base58check-decode
wrapper
{
  checksum 1566033198
  payload 4809949b267446c532024d13211a6e6e71ee1937
  version 111
}
```

```
% echo "dup hash160 [4809949b267446c532024d13211a6e6e71ee1937] equalverify checksig" | bx script-encode
76a9144809949b267446c532024d13211a6e6e71ee193788ac
```

Locate UTXO TX ID, and TX Output Index:

```
% bx fetch-utxo 1 mn5rRXhVEqV6tboNXmpg62xUcnxLGV8Dhe
points
{
  point
  {
    hash 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9
    index 0
    value 125000000
  }
}
```

Find Block Height:

```
% bx fetch-tx-index 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9
metadata
{
  hash 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9
  height 509649
  index 7
}
```

Example #2 - Obtaining Input UTXO Locking Script (needed for signing later)

Associated Private key (previous slide) = **eb0df72d458a700e19199394ae209898ca06f31f4094c9eedd9f56074ced95a1**

```
% bx fetch-tx 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9
transaction
{
  hash 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9
  inputs
  {
    input
    {
      address_hash abdc6bdb3646d67f6117047bba7a419f1bf3578
      previous_output
      {
        hash 354bleda7d1929a5105d0f16bbce76ec76c48097f79a6d6ae7e6ee67aff0c4cf
        index 0
      }
      script "zero [3045022100a5bc2cecbf9aa3ae4caaabe3c18c6cca9803729078947a4ab1bca348afed58c5022020c68d5e49ef19b97bb445d268b14c5c5cb08f7e4215e15984238f44b9eab37e01]
[304402204a2480da8c35625e1583694f7d8d5911cc51ecd9419e0ac7230ff71f2a56a902206ccb631e1063c1865dc98e8f9aa2889c1323da6ec845037964ab7c9e72e5734201]
[5221020ae29f86f404e4b302cfa17ff15d93149af6a54c80a4172d47e41f55f6a78d732103664d528eb80096671ef9011c533ceb5df133238e3690d88f2960c786398b86b121029a449ea4a2155ea10002d704604bb3e8606631d35af20889a74b82b2dab572f6210321602d78046d63256b1730b119b1aca3428039f
18fdb73ccf45ad3e148dd9b1754ae]"
      sequence 4294967295
    }
  }
  lock_time 0
  outputs
  {
    output
    {
      address_hash 4809949b267446c532024d13211a6e6e71ee1937
      script "dup hash160 [4809949b267446c532024d13211a6e6e71ee1937] equalverify checksig"
      value 125000000
    }
    output
    {
      address_hash fe58762223ae84731709aa7a3cb6cc8859b252c7
      script "dup hash160 [fe58762223ae84731709aa7a3cb6cc8859b252c7] equalverify checksig"
      value 125000000
    }
    output
    {
      address_hash f03b4896fa7a608b3518d78354fdb078107aafd2
      script "dup hash160 [f03b4896fa7a608b3518d78354fdb078107aafd2] equalverify checksig"
      value 125000000
    }
    output
    {
      address_hash 708ce93ea17534e1c144a59c7886adfc75a5743f
      script "dup hash160 [708ce93ea17534e1c144a59c7886adfc75a5743f] equalverify checksig"
      value 125000000
    }
  }
  version 1
}
```

Example #2 - Synthesizing TX Outputs

P2PKH, Single Signature P2SH, CSV-P2PKH, and P2SH(P2WPKH)

Sharing a common Private Key

```
% echo 824844a7964a56dfe3c1b44d66b11728657061807a59cdabf41635c88ca01f5d | bx ec-to-public (Payer does not typically have these these keys!)
02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b
```

```
% echo 02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b | bx bitcoin160
2a773c929b7932fa781b0d1154accaacc565935e
```

Testnet P2PKH Address, Locking Script and Signature Script Form:

```
% echo 2a773c929b7932fa781b0d1154accaacc565935e | bx base58check-encode -v 111
mjPVWpH6EKes6SibsK6rtUWyg1x24whE7f
```

Locking Script: `"dup hash160 [2a773c929b7932fa781b0d1154accaacc565935e] equalverify checksig"`

Signature Script Form:

`"[ENDORSEMENT_of_Locking_Script] [02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b]"`

Testnet Single Signature P2SH Address, Locking Script, and Signature Script Form:

```
% echo "[02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b] checksig" | bx script-encode
2102e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3bac
```

```
% echo "[02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b] checksig" | bx script-to-address -v 196
2N9SdyRjbWH7yRVpya1XwbvZeDcEKwJjFxA
```

```
% echo 2N9SdyRjbWH7yRVpya1XwbvZeDcEKwJjFxA | bx base58check-decode
wrapper
{
  checksum 3614735338
  payload b1aa9c27c00578216d62947e289a57b9466a29f7
  version 196
}
```

Locking Script: `"hash160 [b1aa9c27c00578216d62947e289a57b9466a29f7] equal"`

Redemption Script: `"[02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b] checksig"`

Signature Script Form:

`"[ENDORSEMENT_of_Redemption_Script] [2102e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3bac]"`

Example #2 - Synthesizing TX Outputs

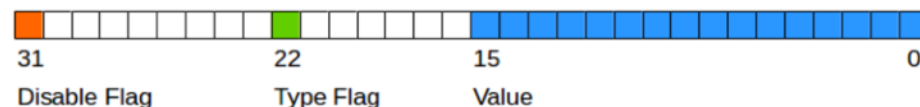
P2PKH, Single Signature P2SH, CSV-P2PKH, and P2SH(P2WPKH)

Sharing a common Private Key

```
% echo 824844a7964a56dfe3c1b44d66b11728657061807a59cdabf41635c88ca01f5d | bx ec-to-public
02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b
```

```
% echo 824844a7964a56dfe3c1b44d66b11728657061807a59cdabf41635c88ca01f5d | bx ec-to-public | bx bitcoin160
2a773c929b7932fa781b0d1154accaacc565935e
```

Testnet CSV-P2PKH **Locking Script**, and **Signature Script** :



0x0040000f specifies a relative locktime is set to **-128 minutes** (15*512/60)

```
% echo "[0040000f] checksequenceverify drop dup hash160 [2a773c929b7932fa781b0d1154accaacc565935e] equalverify
checksig" | bx script-encode
040040000fb27576a9142a773c929b7932fa781b0d1154accaacc565935e88ac
```

Signature Script Form:

```
"[ENDORSEMENT] [02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b]"
```

Testnet BIP 49 P2SH(P2WPKH) **Public Key**, **Address**, and **Signature Script** minus Witness:

```
% echo "0 [2a773c929b7932fa781b0d1154accaacc565935e]" | bx script-encode
00142a773c929b7932fa781b0d1154accaacc565935e
```

```
% echo "0 [2a773c929b7932fa781b0d1154accaacc565935e]" | bx script-encode | bx bitcoin160
aefc3905c26f851f8c319b0050d493fbc3e83a18
```

```
% echo aefc3905c26f851f8c319b0050d493fbc3e83a18 | bx base58check-encode -v 196
2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR
```

Locking Script: "hash160 [aefc3905c26f851f8c319b0050d493fbc3e83a18] equal"

Signature Script: "[00142a773c929b7932fa781b0d1154accaacc565935e]"

Synthesizing an Associated Skeleton Transaction

Mining Fee = **125,000,000** - **30,000,000** - **20,000,000** - **24,998,000** - **50,000,000** = **2,000 Satoshis**

```
% bx tx-encode -v 2 -i 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9:0 -o mjPVWpH6EKES6SibsK6rtUWyg1x24whE7f:30000000 -o 2N9SdyRjbWH7yRVpya1XwbvZeDcEKwJjFxA:20000000 -o 040040000fb27576a9142a773c929b7932fa781b0d1154accaacc565935e88ac:24998000 -o 2N9CTiQVprfyEiXvAV9f7Gzgf4ZpCTpu7sR:50000000 | bx tx-decode
transaction
{
  hash ebdac4deebbe961c44b05e2067bd8febecda6da5bb88752935747182d3548e95
  inputs
  {
    input
    {
      previous_output
      {
        hash 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9
        index 0
      }
      script ""
      sequence 4294967295
    }
  }
  lock_time 0
  outputs
  {
    output
    {
      address_hash 2a773c929b7932fa781b0d1154accaacc565935e
      script "dup hash160 [2a773c929b7932fa781b0d1154accaacc565935e] equalverify checksig"
      value 30000000
    }
    output
    {
      address_hash blaa9c27c00578216d62947e289a57b9466a29f7
      script "hash160 [blaa9c27c00578216d62947e289a57b9466a29f7] equal"
      value 20000000
    }
    output
    {
      script "[0040000f] checksequenceverify drop dup hash160 [2a773c929b7932fa781b0d1154accaacc565935e] equalverify checksig"
      value 24998000
    }
    output
    {
      address_hash aefc3905c26f851f8c319b0050d493fbc3e83a18
      script "hash160 [aefc3905c26f851f8c319b0050d493fbc3e83a18] equal"
      value 50000000
    }
  }
  version 2
}
```

Input Signature **script** is Undefined

Unspecified **sequence** defaults to 0xFFFFFFFF = **4,294,967,295**

Endorse UTXO's Contract, Set Signature Script, Validate

```
Input keys for input TX_ID:UTXO_index == 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9:0
Used to spend this P2PKH Contract
"dup hash160 [4809949b267446c532024d13211a6e6e71ee1937] equalverify checksig"
```

```
% echo eb0df72d458a700e19199394ae209898ca06f31f4094c9eedd9f56074ced95a1 | bx ec-to-public
020ae29f86f404e4b302cfa17ff15d93149af6a54c80a4172d47e41f55f6a78d73
```

```
% echo 020ae29f86f404e4b302cfa17ff15d93149af6a54c80a4172d47e41f55f6a78d73 | bx bitcoin160
4809949b267446c532024d13211a6e6e71ee1937
```

The **Endorsement** for input index 0 is the Signature of the **Encumbrance Script** for TX_ID:UTXO_index above

```
% bx tx-encode -v 2 -i 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9:0 -o mjPVWpH6EKES6SibsK6rtUWyg1x24whE7f:30000000 -o
2N9SdyRjbWH7yRVpya1XwbvZeDcEKwJjFxA:20000000 -o 040040000fb27576a9142a773c929b7932fa781b0d1154accaacc565935e88ac:24998000 -o
2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR:50000000 | bx input-sign -i 0 eb0df72d458a700e19199394ae209898ca06f31f4094c9eedd9f56074ced95a1 "dup
hash160 [4809949b267446c532024d13211a6e6e71ee1937] equalverify checksig"
3045022100f9fcd99a430645a03273bd73b81f2f2aadb6aab3917afdea8984ec1afbc56afd02201ea19cea6a428c0d1c00c4b44dee78fc8f7e9ec21e68aa201245e7dea34fbf1001
```

Create the signed TX:

```
% bx tx-encode -v 2 -i 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9:0 -o mjPVWpH6EKES6SibsK6rtUWyg1x24whE7f:30000000 -o
2N9SdyRjbWH7yRVpya1XwbvZeDcEKwJjFxA:20000000 -o 040040000fb27576a9142a773c929b7932fa781b0d1154accaacc565935e88ac:24998000 -o
2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR:50000000 | bx input-set -i 0
"[3045022100f9fcd99a430645a03273bd73b81f2f2aadb6aab3917afdea8984ec1afbc56afd02201ea19cea6a428c0d1c00c4b44dee78fc8f7e9ec21e68aa201245e7dea34fbf10
01] [020ae29f86f404e4b302cfa17ff15d93149af6a54c80a4172d47e41f55f6a78d73]"
0200000001d93dc14d376cd4799c5331699c14f1df1d027fbbb33e4e849824f00046a57530000000006b483045022100f9fcd99a430645a03273bd73b81f2f2aadb6aab3917afdea
8984ec1afbc56afd02201ea19cea6a428c0d1c00c4b44dee78fc8f7e9ec21e68aa201245e7dea34fbf100121020ae29f86f404e4b302cfa17ff15d93149af6a54c80a4172d47e41f
55f6a78d73ffffffff0480c3c901000000001976a9142a773c929b7932fa781b0d1154accaacc565935e88ac002d31010000000017a914b1aa9c27c00578216d62947e289a57b946
6a29f78770707d01000000002004004000fb27576a9142a773c929b7932fa781b0d1154accaacc565935e88ac80f0fa020000000017a914aefc3905c26f851f8c319b0050d493fb
c3e83a188700000000
```

Validate TX input:

```
% bx tx-encode -v 2 -i 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9:0 -o mjPVWpH6EKES6SibsK6rtUWyg1x24whE7f:30000000 -o
2N9SdyRjbWH7yRVpya1XwbvZeDcEKwJjFxA:20000000 -o 040040000fb27576a9142a773c929b7932fa781b0d1154accaacc565935e88ac:24998000 -o
2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR:50000000 | bx input-set -i 0
"[3045022100f9fcd99a430645a03273bd73b81f2f2aadb6aab3917afdea8984ec1afbc56afd02201ea19cea6a428c0d1c00c4b44dee78fc8f7e9ec21e68aa201245e7dea34fbf10
01] [020ae29f86f404e4b302cfa17ff15d93149af6a54c80a4172d47e41f55f6a78d73]" | bx input-validate -i 0
020ae29f86f404e4b302cfa17ff15d93149af6a54c80a4172d47e41f55f6a78d73 "dup hash160 [4809949b267446c532024d13211a6e6e71ee1937] equalverify checksig"
3045022100f9fcd99a430645a03273bd73b81f2f2aadb6aab3917afdea8984ec1afbc56afd02201ea19cea6a428c0d1c00c4b44dee78fc8f7e9ec21e68aa201245e7dea34fbf1001
The endorsement is valid.
```

Fully Formed Transaction

tx-decode Output

```
% bx tx-encode -v 2 -i 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9:0 -o mjPVWpH6EKES6SibsK6rtUWyglx24whE7f:30000000 -o 2N9SdyRjbWH7yRVpyalXwbvZeDcEKwJjFxA:20000000 -o 040040000fb27576a9142a773c929b7932fa781b0d1154accaacc565935e88ac:24998000 -o 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR:50000000
| bx input-set -i 0 "[3045022100f9fcd99a430645a03273bd73b81f2f2aadb6aab3917afdea8984ec1afbc56afd02201ea19cea6a428c0d1c00c4b44dee78fc8f7e9ec21e68aa201245e7dea34fbf1001]
[020ae29f86f404e4b302cfa17ff15d93149af6a54c80a4172d47e41f55f6a78d73]" | bx tx-decode
transaction
{
  hash e1b429277d53c6aec0850875ad37a93e4cf877826857d09c4deeb983c2770b71
  inputs
  {
    input
    {
      address_hash 4809949b267446c532024d13211a6e6e71ee1937
      previous_output
      {
        hash 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9
        index 0
      }
      script "[3045022100f9fcd99a430645a03273bd73b81f2f2aadb6aab3917afdea8984ec1afbc56afd02201ea19cea6a428c0d1c00c4b44dee78fc8f7e9ec21e68aa201245e7dea34fbf1001]
[020ae29f86f404e4b302cfa17ff15d93149af6a54c80a4172d47e41f55f6a78d73]"
      sequence 4294967295
    }
  }
  lock_time 0
  outputs
  {
    output
    {
      address_hash 2a773c929b7932fa781b0d1154accaacc565935e
      script "dup hash160 [2a773c929b7932fa781b0d1154accaacc565935e] equalverify checksig"
      value 30000000
    }
    output
    {
      address_hash b1aa9c27c00578216d62947e289a57b9466a29f7
      script "hash160 [b1aa9c27c00578216d62947e289a57b9466a29f7] equal"
      value 20000000
    }
    output
    {
      script "[0040000f] checksequenceverify drop dup hash160 [2a773c929b7932fa781b0d1154accaacc565935e] equalverify checksig"
      value 24998000
    }
    output
    {
      address_hash aefc3905c26f851f8c319b0050d493fbc3e83a18
      script "hash160 [aefc3905c26f851f8c319b0050d493fbc3e83a18] equal"
      value 50000000
    }
  }
  version 2
}
```

Examine TX Size, Validate TX, Send TX

```
% bx tx-encode -v 2 -i 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9:0 -o mjPVWpH6EKES6SibsK6rtUWyg1x24whE7f:30000000 -o 2N9SdyRjbWH7yRVpya1XwbvZeDcEKwJjFxA:20000000 -o 040040000fb27576a9142a773c929b7932fa781b0d1154accaacc565935e88ac:24998000 -o 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR:50000000 | bx input-set -i 0 "[3045022100f9fcd99a430645a03273bd73b81f2f2aadb6aab3917afdea8984ec1afbc56afd02201ea19cea6a428c0d1c00c4b44dee78fc8f7e9ec21e68aa201245e7dea34fbf1001] [020ae29f86f404e4b302cfa17ff15d93149af6a54c80a4172d47e41f55f6a78d73]" 0200000001d93dc14d376cd4799c5331699c14f1df1d027fbbb33e4e849824f00046a57530000000006b483045022100f9fcd99a430645a03273bd73b81f2f2aadb6aab3917afdea8984ec1afbc56afd02201ea19cea6a428c0d1c00c4b44dee78fc8f7e9ec21e68aa201245e7dea34fbf100121020ae29f86f404e4b302cfa17ff15d93149af6a54c80a4172d47e41f55f6a78d73fffffffff0480c3c901000000001976a9142a773c929b7932fa781b0d1154accaacc565935e88ac002d3101000000017a914b1aa9c27c00578216d62947e289a57b9466a29f78770707d010000000020040040000fb27576a9142a773c929b7932fa781b0d1154accaacc565935e88ac80f0fa020000000017a914aefc3905c26f851f8c319b0050d493fbc3e83a188700000000
```

```
% echo -n 0200000001d93dc14d376cd4799c5331699c14f1df1d027fbbb33e4e849824f00046a57530000000006b483045022100f9fcd99a430645a03273bd73b81f2f2aadb6aab3917afdea8984ec1afbc56afd02201ea19cea6a428c0d1c00c4b44dee78fc8f7e9ec21e68aa201245e7dea34fbf100121020ae29f86f404e4b302cfa17ff15d93149af6a54c80a4172d47e41f55f6a78d73fffffffff0480c3c901000000001976a9142a773c929b7932fa781b0d1154accaacc565935e88ac002d3101000000017a914b1aa9c27c00578216d62947e289a57b9466a29f78770707d010000000020040040000fb27576a9142a773c929b7932fa781b0d1154accaacc565935e88ac80f0fa020000000017a914aefc3905c26f851f8c319b0050d493fbc3e83a188700000000 | wc 0 1 594 (TX -s 297 bytes in size)
```

```
% bx tx-encode -v 2 -i 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9:0 -o mjPVWpH6EKES6SibsK6rtUWyg1x24whE7f:30000000 -o 2N9SdyRjbWH7yRVpya1XwbvZeDcEKwJjFxA:20000000 -o 040040000fb27576a9142a773c929b7932fa781b0d1154accaacc565935e88ac:24998000 -o 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR:50000000 | bx input-set -i 0 "[3045022100f9fcd99a430645a03273bd73b81f2f2aadb6aab3917afdea8984ec1afbc56afd02201ea19cea6a428c0d1c00c4b44dee78fc8f7e9ec21e68aa201245e7dea34fbf1001] [020ae29f86f404e4b302cfa17ff15d93149af6a54c80a4172d47e41f55f6a78d73]" | bx validate-tx The transaction is valid.
```

```
% bx tx-encode -v 2 -i 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9:0 -o mjPVWpH6EKES6SibsK6rtUWyg1x24whE7f:30000000 -o 2N9SdyRjbWH7yRVpya1XwbvZeDcEKwJjFxA:20000000 -o 040040000fb27576a9142a773c929b7932fa781b0d1154accaacc565935e88ac:24998000 -o 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR:50000000 | bx input-set -i 0 "[3045022100f9fcd99a430645a03273bd73b81f2f2aadb6aab3917afdea8984ec1afbc56afd02201ea19cea6a428c0d1c00c4b44dee78fc8f7e9ec21e68aa201245e7dea34fbf1001] [020ae29f86f404e4b302cfa17ff15d93149af6a54c80a4172d47e41f55f6a78d73]" | bx send-tx Sent transaction.
```

Fetch TX Details from tBTC Network after 1 Confirmation

```
% bx fetch-tx e1b429277d53c6aec0850875ad37a93e4cf877826857d09c4deeb983c2770b71
transaction
{
  hash e1b429277d53c6aec0850875ad37a93e4cf877826857d09c4deeb983c2770b71
  inputs
  {
    input
    {
      address_hash 4809949b267446c532024d13211a6e6e71ee1937
      previous_output
      {
        hash 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9
        index 0
      }
      script "[3045022100f9fcd99a430645a03273bd73b81f2f2aadb6aab3917afdea8984ec1afbc56afd02201ea19cea6a428c0dlc00c4b44dee78fc8f7e9ec21e68aa201245e7dea34fbf1001]
[020ae29f86f404e4b302cfa17ff15d93149af6a54c80a4172d47e41f55f6a78d73]"
      sequence 4294967295
    }
  }
  lock_time 0
  outputs
  {
    output
    {
      address_hash 2a773c929b7932fa781b0d1154accaacc565935e
      script "dup hash160 [2a773c929b7932fa781b0d1154accaacc565935e] equalverify checksig"
      value 30000000
    }
    output
    {
      address_hash blaa9c27c00578216d62947e289a57b9466a29f7
      script "hash160 [blaa9c27c00578216d62947e289a57b9466a29f7] equal"
      value 20000000
    }
    output
    {
      script "[0040000f] checksequenceverify drop dup hash160 [2a773c929b7932fa781b0d1154accaacc565935e] equalverify checksig"
      value 24998000
    }
    output
    {
      address_hash aefc3905c26f851f8c319b0050d493fbc3e83a18
      script "hash160 [aefc3905c26f851f8c319b0050d493fbc3e83a18] equal"
      value 50000000
    }
  }
  version 2
}
```

Using bx to Spend 1st UTXO as P2PKH Payment for a TX Input

TX_ID = **e1b429277d53c6aec0850875ad37a93e4cf877826857d09c4deeb983c2770b71**, index = 0

```
% echo 824844a7964a56dfe3c1b44d66b11728657061807a59cdabf41635c88ca01f5d | bx ec-to-public  
02e18f47b78730f788b726c46459fdc29b57fd6d437b69587ale59efa343c46a3b
```

```
% echo 02e18f47b78730f788b726c46459fdc29b57fd6d437b69587ale59efa343c46a3b | bx bitcoin160  
2a773c929b7932fa781b0d1154accaacc565935e
```

```
% echo 2a773c929b7932fa781b0d1154accaacc565935e | bx base58check-encode -v 111  
mjPVWpH6EKES6SibsK6rtUWyg1x24whE7f
```

Locking Script: "dup hash160 [2a773c929b7932fa781b0d1154accaacc565935e] equalverify checksig"

```
% bx tx-encode -v 1 -i e1b429277d53c6aec0850875ad37a93e4cf877826857d09c4deeb983c2770b71:0 -o 2N9e4AjRbiQyvuu3QMhCahQEDijjavfmET3:29999000  
010000001710b77c283b9ee4d9cd057688277f84c3ea937ad750885c0aec6537d2729b4e1000000000ffffffffff0198bfc9010000000017a914b3d361e8a80c49dd0c9a5d6e40c561  
1f35a3cade8700000000
```

```
% bx tx-encode -v 1 -i e1b429277d53c6aec0850875ad37a93e4cf877826857d09c4deeb983c2770b71:0 -o 2N9e4AjRbiQyvuu3QMhCahQEDijjavfmET3:29999000 | bx  
input-sign -i 0 824844a7964a56dfe3c1b44d66b11728657061807a59cdabf41635c88ca01f5d "dup hash160 [2a773c929b7932fa781b0d1154accaacc565935e]  
equalverify checksig"  
3044022033bae81f2ccece7048c738630b5c93c268e9d26fd0ac3d8ed96b4cbadc2de7eb0220040d7c2d9744c6ac773eb38d93af56046f463cc22bab2f495e046757d7abc2d601
```

```
% bx tx-encode -v 1 -i e1b429277d53c6aec0850875ad37a93e4cf877826857d09c4deeb983c2770b71:0 -o 2N9e4AjRbiQyvuu3QMhCahQEDijjavfmET3:29999000 | bx  
input-set -i 0  
"3044022033bae81f2ccece7048c738630b5c93c268e9d26fd0ac3d8ed96b4cbadc2de7eb0220040d7c2d9744c6ac773eb38d93af56046f463cc22bab2f495e046757d7abc2d601"  
[02e18f47b78730f788b726c46459fdc29b57fd6d437b69587ale59efa343c46a3b]"  
010000001710b77c283b9ee4d9cd057688277f84c3ea937ad750885c0aec6537d2729b4e10000000006a473044022033bae81f2ccece7048c738630b5c93c268e9d26fd0ac3d8ed96b  
4cbadc2de7eb0220040d7c2d9744c6ac773eb38d93af56046f463cc22bab2f495e046757d7abc2d6012102e18f47b78730f788b726c46459fdc29b57fd6d437b69587ale59efa343c4  
6a3bffffffff0198bfc9010000000017a914b3d361e8a80c49dd0c9a5d6e40c5611f35a3cade8700000000
```

```
% bx tx-encode -v 1 -i e1b429277d53c6aec0850875ad37a93e4cf877826857d09c4deeb983c2770b71:0 -o 2N9e4AjRbiQyvuu3QMhCahQEDijjavfmET3:29999000 | bx  
input-set -i 0  
"3044022033bae81f2ccece7048c738630b5c93c268e9d26fd0ac3d8ed96b4cbadc2de7eb0220040d7c2d9744c6ac773eb38d93af56046f463cc22bab2f495e046757d7abc2d601"  
[02e18f47b78730f788b726c46459fdc29b57fd6d437b69587ale59efa343c46a3b]" | bx input-validate  
02e18f47b78730f788b726c46459fdc29b57fd6d437b69587ale59efa343c46a3b "dup hash160 [2a773c929b7932fa781b0d1154accaacc565935e] equalverify checksig"  
3044022033bae81f2ccece7048c738630b5c93c268e9d26fd0ac3d8ed96b4cbadc2de7eb0220040d7c2d9744c6ac773eb38d93af56046f463cc22bab2f495e046757d7abc2d601  
The endorsement is valid.
```

```
% bx tx-encode -v 1 -i e1b429277d53c6aec0850875ad37a93e4cf877826857d09c4deeb983c2770b71:0 -o 2N9e4AjRbiQyvuu3QMhCahQEDijjavfmET3:29999000 | bx  
input-set -i 0  
"3044022033bae81f2ccece7048c738630b5c93c268e9d26fd0ac3d8ed96b4cbadc2de7eb0220040d7c2d9744c6ac773eb38d93af56046f463cc22bab2f495e046757d7abc2d601"  
[02e18f47b78730f788b726c46459fdc29b57fd6d437b69587ale59efa343c46a3b]" | bx validate-tx  
The transaction is valid.
```

Using bx to Spend 2nd UTXO as P2SH Payment for a TX Input

TX_ID = **e1b429277d53c6aec0850875ad37a93e4cf877826857d09c4deeb983c2770b71**, index = 1

```
% echo 824844a7964a56dfe3c1b44d66b11728657061807a59cdabf41635c88ca01f5d | bx ec-to-public  
02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b
```

```
% echo "[02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b] checksig" | bx script-encode (per BIP 16)  
2102e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3bac
```

```
% echo 2102e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3bac | bx bitcoin160  
b1aa9c27c00578216d62947e289a57b9466a29f7
```

```
% echo b1aa9c27c00578216d62947e289a57b9466a29f7 | bx base58check-encode -v 196  
2N9SdyRjbWH7yRVpya1XwbvZeDcEKwJjFxA
```

Locking Script: "**hash160 [b1aa9c27c00578216d62947e289a57b9466a29f7] equal**"

Redemption Script: "**[02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b] checksig**"

```
% bx tx-encode -v 1 -i e1b429277d53c6aec0850875ad37a93e4cf877826857d09c4deeb983c2770b71:1 -o 2N9e4AjRbiQyvuu3QMhCahQEDijjavfmET3:19999000  
0100000001710b77c283b9ee4d9cd057688277f84c3ea937ad750885c0aec6537d2729b4e10100000000ffffffffff01182931010000000017a914b3d361e8a80c49dd0c9a5d6e40c5611f35a3  
cade8700000000
```

```
% bx tx-encode -v 1 -i e1b429277d53c6aec0850875ad37a93e4cf877826857d09c4deeb983c2770b71:1 -o 2N9e4AjRbiQyvuu3QMhCahQEDijjavfmET3:19999000 | bx input-  
sign -i 0 824844a7964a56dfe3c1b44d66b11728657061807a59cdabf41635c88ca01f5d "[02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b]  
checksig"  
3045022100beee6efa17a4998a642fef2c255341280f4e067841f5e07cae817bb052c162700220287fb3196068394fe23639fc9b62652d6d8f6bac35ef13e99d6bc9faec0a401e01
```

```
% bx tx-encode -v 1 -i e1b429277d53c6aec0850875ad37a93e4cf877826857d09c4deeb983c2770b71:1 -o 2N9e4AjRbiQyvuu3QMhCahQEDijjavfmET3:19999000 | bx input-set  
-i 0 "[3045022100beee6efa17a4998a642fef2c255341280f4e067841f5e07cae817bb052c162700220287fb3196068394fe23639fc9b62652d6d8f6bac35ef13e99d6bc9faec0a401e01]  
[2102e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3bac]"  
0100000001710b77c283b9ee4d9cd057688277f84c3ea937ad750885c0aec6537d2729b4e1010000006d483045022100beee6efa17a4998a642fef2c255341280f4e067841f5e07cae817bb0  
52c162700220287fb3196068394fe23639fc9b62652d6d8f6bac35ef13e99d6bc9faec0a401e01232102e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3bacff  
ffffff01182931010000000017a914b3d361e8a80c49dd0c9a5d6e40c5611f35a3cade8700000000
```

```
% bx tx-encode -v 1 -i e1b429277d53c6aec0850875ad37a93e4cf877826857d09c4deeb983c2770b71:1 -o 2N9e4AjRbiQyvuu3QMhCahQEDijjavfmET3:19999000 | bx input-set  
-i 0 "[3045022100beee6efa17a4998a642fef2c255341280f4e067841f5e07cae817bb052c162700220287fb3196068394fe23639fc9b62652d6d8f6bac35ef13e99d6bc9faec0a401e01]  
[2102e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3bac]" | bx input-validate  
02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b "[02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b] checksig"  
3045022100beee6efa17a4998a642fef2c255341280f4e067841f5e07cae817bb052c162700220287fb3196068394fe23639fc9b62652d6d8f6bac35ef13e99d6bc9faec0a401e01  
The endorsement is valid.
```

```
% bx tx-encode -v 1 -i e1b429277d53c6aec0850875ad37a93e4cf877826857d09c4deeb983c2770b71:1 -o 2N9e4AjRbiQyvuu3QMhCahQEDijjavfmET3:19999000 | bx input-set  
-i 0 "[3045022100beee6efa17a4998a642fef2c255341280f4e067841f5e07cae817bb052c162700220287fb3196068394fe23639fc9b62652d6d8f6bac35ef13e99d6bc9faec0a401e01]  
[2102e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3bac]" | bx validate-tx  
The transaction is valid.
```

WIP - A Failed Try at Using bx to Spend Non-Standard 3rd UTXO CSV-P2PKH Payment for a TX Input

TX_ID = e1b429277d53c6aec0850875ad37a93e4cf877826857d09c4deeb983c2770b71, index = 2

```
% echo 824844a7964a56dfe3c1b44d66b11728657061807a59cdabf41635c88ca01f5d | bx ec-to-public
02e18f47b78730f788b726c46459fdc29b57fd6d437b69587ale59efa343c46a3b

% echo 824844a7964a56dfe3c1b44d66b11728657061807a59cdabf41635c88ca01f5d | bx ec-to-public | bx bitcoin160
2a773c929b7932fa781b0d1154accaacc565935e

% echo "[0040000f] checksequenceverify drop dup hash160 [2a773c929b7932fa781b0d1154accaacc565935e] equalverify checksig" | bx script-encode
040040000fb27576a9142a773c929b7932fa781b0d1154accaacc565935e88ac

little_endian( 0x004000f ) = 0x0f000400 = 251,659,264

base16( 4194319 ) = 0x0040000f

% bx tx-encode -v 2 -i e1b429277d53c6aec0850875ad37a93e4cf877826857d09c4deeb983c2770b71:2:194319 -o 2N9e4AjRBiQyvuu3QMhCahQEDijjavfmET3:24997000
0200000001710b77c283b9ee4d9cd057688277f84c3ea937ad750885c0aec6537d2729b4e102000000000ff7020001886c7d010000000017a914b3d361e8a80c49dd0c9a5d6e40c5611f3
5a3cade8700000000

% bx tx-encode -v 2 -i e1b429277d53c6aec0850875ad37a93e4cf877826857d09c4deeb983c2770b71:2:194319 -o 2N9e4AjRBiQyvuu3QMhCahQEDijjavfmET3:24997000 | bx
input-sign -i 0 824844a7964a56dfe3c1b44d66b11728657061807a59cdabf41635c88ca01f5d "[0040000f] checksequenceverify drop dup hash160
[2a773c929b7932fa781b0d1154accaacc565935e] equalverify checksig"
3045022100a7108d2e1fe9c3ecf770269416b5857c9151604eeec111d2b67cdf0b91be3c1a02206b596a9f9ba9aa273592e4736b43758097a653484ed49affa5ed24ff23b725f501

% bx tx-encode -v 2 -i e1b429277d53c6aec0850875ad37a93e4cf877826857d09c4deeb983c2770b71:2:194319 -o 2N9e4AjRBiQyvuu3QMhCahQEDijjavfmET3:24997000 | bx
input-set -i 0
"[3045022100a7108d2e1fe9c3ecf770269416b5857c9151604eeec111d2b67cdf0b91be3c1a02206b596a9f9ba9aa273592e4736b43758097a653484ed49affa5ed24ff23b725f501]
[040040000fb27576a9142a773c929b7932fa781b0d1154accaacc565935e88ac]"
0200000001710b77c283b9ee4d9cd057688277f84c3ea937ad750885c0aec6537d2729b4e1020000006a483045022100a7108d2e1fe9c3ecf770269416b5857c9151604eeec111d2b67cd
f0b91be3c1a02206b596a9f9ba9aa273592e4736b43758097a653484ed49affa5ed24ff23b725f50120040040000fb27576a9142a773c929b7932fa781b0d1154accaacc565935e88ac0f
f7020001886c7d010000000017a914b3d361e8a80c49dd0c9a5d6e40c5611f35a3cade8700000000

% bx tx-encode -v 2 -i e1b429277d53c6aec0850875ad37a93e4cf877826857d09c4deeb983c2770b71:2:194319 -o 2N9e4AjRBiQyvuu3QMhCahQEDijjavfmET3:24997000 | bx
input-set -i 0
"[3045022100a7108d2e1fe9c3ecf770269416b5857c9151604eeec111d2b67cdf0b91be3c1a02206b596a9f9ba9aa273592e4736b43758097a653484ed49affa5ed24ff23b725f501]
[02e18f47b78730f788b726c46459fdc29b57fd6d437b69587ale59efa343c46a3b]" | bx input-validate -i 0
02e18f47b78730f788b726c46459fdc29b57fd6d437b69587ale59efa343c46a3b "[0040000f] checksequenceverify drop dup hash160
[2a773c929b7932fa781b0d1154accaacc565935e] equalverify checksig"
3045022100a7108d2e1fe9c3ecf770269416b5857c9151604eeec111d2b67cdf0b91be3c1a02206b596a9f9ba9aa273592e4736b43758097a653484ed49affa5ed24ff23b725f501
The endorsement is valid.

% bx tx-encode -v 2 -i e1b429277d53c6aec0850875ad37a93e4cf877826857d09c4deeb983c2770b71:2:194319 -o 2N9e4AjRBiQyvuu3QMhCahQEDijjavfmET3:24997000 | bx
input-set -i 0
"[3045022100a7108d2e1fe9c3ecf770269416b5857c9151604eeec111d2b67cdf0b91be3c1a02206b596a9f9ba9aa273592e4736b43758097a653484ed49affa5ed24ff23b725f501]
[040040000fb27576a9142a773c929b7932fa781b0d1154accaacc565935e88ac]" | bx validate-tx
transaction currently locked
```

Ledger Nano S Spending of the 4th UTXO P2SH(P2WPKH) Payment Was Monitored Using bx

```
% bx fetch-balance 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR
balance
{
  address 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR
  received 50000000
  spent 0
}
```

```
% bx watch-address 2N2XqNprbWQ7DC2gMa9Tp4fxVbDcejY1jMP
Watching address: 2N2XqNprbWQ7DC2gMa9Tp4fxVbDcejY1jMP...
```

Ledger Nano S used here to send funds from 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR to 2N2XqNprbWQ7DC2gMa9Tp4fxVbDcejY1jMP

```
% bx watch-address 2N2XqNprbWQ7DC2gMa9Tp4fxVbDcejY1jMP
Watching address: 2N2XqNprbWQ7DC2gMa9Tp4fxVbDcejY1jMP...
1 1449826 412370ff1c2c60350b7ce8cec593af233f3375ed239cec633b90ffd737dd2595
```

```
% bx fetch-history 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR
transfers
{
  transfer
  {
    received
    {
      hash e1b429277d53c6aec0850875ad37a93e4cf877826857d09c4deeb983c2770b71
      height 1449825
      index 3
    }
    spent
    {
      hash 412370ff1c2c60350b7ce8cec593af233f3375ed239cec633b90ffd737dd2595
      height 1449826
      index 0
    }
    value 50000000
  }
}
```

Using a Ledger Nano S to Spend 4th UTXO P2SH(P2WPKH) Payment as a TX Input

TX_ID = **e1b429277d53c6aec0850875ad37a93e4cf877826857d09c4deeb983c2770b71**, index = 3

and Analyze Transaction with bx

```
% bx fetch-tx 412370ff1c2c60350b7ce8cec593af233f3375ed239cec633b90ffd737dd2595
transaction
{
  hash 412370ff1c2c60350b7ce8cec593af233f3375ed239cec633b90ffd737dd2595
  inputs
  {
    input
    {
      address_hash aefc3905c26f851f8c319b0050d493fbc3e83a18
      previous_output
      {
        hash e1b429277d53c6aec0850875ad37a93e4cf877826857d09c4deeb983c2770b71
        index 3
      }
      script [00142a773c929b7932fa781b0d1154accaacc565935e]
      sequence 16777215
    }
  }
  lock_time 0
  outputs
  {
    output
    {
      address_hash 65dd5412422ade598846433fc2d43d32539135f1
      script "hash160 [65dd5412422ade598846433fc2d43d32539135f1] equal"
      value 20000000
    }
    output
    {
      address_hash b3d361e8a80c49dd0c9a5d6e40c5611f35a3cade
      script "hash160 [b3d361e8a80c49dd0c9a5d6e40c5611f35a3cade] equal"
      value 29998048
    }
  }
  version 1
}
```

```
% echo 65dd5412422ade598846433fc2d43d32539135f1 | bx base58check-encode -v 196
2N2XqNprbWQ7DC2gMa9Tp4fxVbDcejY1jMP
```

```
% bx fetch-balance 2N2XqNprbWQ7DC2gMa9Tp4fxVbDcejY1jMP
balance
{
  address 2N2XqNprbWQ7DC2gMa9Tp4fxVbDcejY1jMP
  received 20000000
  spent 0
}
```

```
% echo b3d361e8a80c49dd0c9a5d6e40c5611f35a3cade | bx base58check-encode -v 196
2N9e4AjRBiQyvuu3QMhCahQEDijjavfmET3
```

```
% bx fetch-balance 2N9e4AjRBiQyvuu3QMhCahQEDijjavfmET3
balance
{
  address 2N9e4AjRBiQyvuu3QMhCahQEDijjavfmET3
  received 29998048
  spent 0
}
```

Explicitly defined destination address
that originated from a Ledger Nano S
that was manually input into
Ledger Nano S to send funds to itself

Implicitly defined internal HD wallet
return address used to receive remainder
of funds not spent after mining fees are paid

Using bx to Construct the Same 4th UTXO P2SH(P2WPKH) Payment as the

(TX_ID = **e1b429277d53c6aec0850875ad37a93e4cf877826857d09c4deeb983c2770b71**, index = 3)

Non-Witness **TX** Section of a Ledger Nano S

```
% bx tx-encode -v 1 -i e1b429277d53c6aec0850875ad37a93e4cf877826857d09c4deeb983c2770b71:3:16777215 -o  
2N2XqNprbWQ7DC2gMa9Tp4fxVbDcejY1jMP:20000000 -o 2N9e4AjRBiQyvuu3QMhCahQEDijjavfmET3:29998048 | bx input-set -i 0  
"[00142a773c929b7932fa781b0d1154accaacc565935e]"  
0100000001710b77c283b9ee4d9cd057688277f84c3ea937ad750885c0aec6537d2729b4e103000000171600142a773c929b7932fa781b0d1154acca  
acc565935effffff0002002d31010000000017a91465dd5412422ade598846433fc2d43d32539135f187e0bbc9010000000017a914b3d361e8a80c49  
dd0c9a5d6e40c5611f35a3cade8700000000
```

```
% bx tx-encode -v 1 -i e1b429277d53c6aec0850875ad37a93e4cf877826857d09c4deeb983c2770b71:3:16777215 -o  
2N2XqNprbWQ7DC2gMa9Tp4fxVbDcejY1jMP:20000000 -o 2N9e4AjRBiQyvuu3QMhCahQEDijjavfmET3:29998048 | bx input-set -i 0  
"[00142a773c929b7932fa781b0d1154accaacc565935e]" | bx bitcoin256  
412370ff1c2c60350b7ce8cec593af233f3375ed239cec633b90ffd737dd2595
```

Contrast results to:

```
% bx tx-encode -v 1 -i e1b429277d53c6aec0850875ad37a93e4cf877826857d09c4deeb983c2770b71:3:16777215 -o  
2N2XqNprbWQ7DC2gMa9Tp4fxVbDcejY1jMP:20000000 -o 2N9e4AjRBiQyvuu3QMhCahQEDijjavfmET3:29998048 | bx input-set -i 0  
"[00142a773c929b7932fa781b0d1154accaacc565935e]" | bx sha256 | bx sha256  
9525dd37d7ff903b63ec9c23ed75333f23af93c5cee87c0b35602c1cff702341
```

2nd Try, Sending a Payment a
P2SH(CSV-P2PK) Timelock UTXO and a
Ledger Nano S P2SH(P2WPKH) UTXO

Bitcoin Stack Steps to Spend a P2SH(CSV-P2PK) Payment

Explicit Execution Script:

[SigRedeemScript] [{RedeemScript}] OP_HASH160 [HASH160({RedeemScript})] OP_EQUAL

Implicit Execution Script:

[SigRedeemScript] [bitcoin160({CSV-P2PK})] OP_CHECKSIG [{RedeemScript}] OP_HASH160 [bitcoin160({RedeemScript})] OP_EQUAL

CSV-P2PK = "[0040000f] checksequenceverify drop [PubKey]",

RedeemScript = "[bitcoin160({CSV-P2PK})] OP_CHECKSIG",

MESSAGE = [{RedeemScript}]

** Insights above gleaned from a careful examination of <https://github.com/bitcoin/bips/blob/master/bip-0016.mediawiki#specification> and generalization of "Spending a P2SH Payment"; operation {} = bx script-encode();

Bitcoin LIFO Stack

Empty Stack

[SigRedeemScript]

[SigRedeemScript] [bitcoin160({CSV-P2PK})]

[SigRedeemScript] [bitcoin160({CSV-P2PK})] OP_CHECKSIG

[SigRedeemScript] [bitcoin160({CSV-P2PK})] OP_CHECKSIG [{RedeemScript}]

[SigRedeemScript] [bitcoin160({CSV-P2PK})] OP_CHECKSIG [bitcoin160({RedeemScript})]

[SigRedeemScript] [bitcoin160({CSV-P2PK})] OP_CHECKSIG [bitcoin160({RedeemScript})] [bitcoin160({RedeemScript})]

[SigRedeemScript] [bitcoin160({CSV-P2PK})] OP_CHECKSIG 1

[SigRedeemScript] [bitcoin160({CSV-P2PK})] OP_CHECKSIG (implicitly used MESSAGE above to complete operation)

1

Script Execution Queue

[SigRedeemScript] [bitcoin160({CSV-P2PK})] OP_CHECKSIG [{RedeemScript}]
OP_HASH160 [bitcoin160({RedeemScript})] OP_EQUAL

[bitcoin160({CSV-P2PK})] OP_CHECKSIG [{RedeemScript}]
OP_HASH160 [bitcoin160({RedeemScript})] OP_EQUAL

OP_CHECKSIG [{RedeemScript}]
OP_HASH160 [bitcoin160({RedeemScript})] OP_EQUAL

[{RedeemScript}]
OP_HASH160 [bitcoin160({RedeemScript})] OP_EQUAL

OP_HASH160 [bitcoin160({RedeemScript})] OP_EQUAL

[bitcoin160({RedeemScript})] OP_EQUAL

OP_EQUAL

Empty Script

Empty Script

Empty Script

Second Try at Composing a CheckSequenceVerify Payment Script, but IsStandard This Time

Basic TX inputs Information:

```
% echo 857608a143454263ccb0b6b4a482887d6a8add1f266f2023649d8a7657a05df | bx ec-to-public
03664d528eb80096671ef9011c533ceb5df133238e3690d88f2960c786398b86b1

% echo 857608a143454263ccb0b6b4a482887d6a8add1f266f2023649d8a7657a05df | bx ec-to-public | bx ec-to-address -v 111
n4houBuVDFxbg4Z1k2WUiqFWH5yC2YSH8B

% bx fetch-balance n4houBuVDFxbg4Z1k2WUiqFWH5yC2YSH8B
balance
{
  address n4houBuVDFxbg4Z1k2WUiqFWH5yC2YSH8B
  received 125000000
  spent 0
}

% echo 857608a143454263ccb0b6b4a482887d6a8add1f266f2023649d8a7657a05df | bx ec-to-public | bx bitcoin160
fe58762223ae84731709aa7a3cb6cc8859b252c7

tx = 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9, index = 1
```

Basic P2SH(CSV-P2PK) TX Output Information:

```
echo 824844a7964a56dfe3c1b44d66b11728657061807a59cdabf41635c88ca01f5d | bx ec-to-public (Payer does not typically
02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b have these these keys!)
```

CSV-P2PK = "[0040000f] checksequenceverify drop [PubKey]",
RedeemScript = "[bitcoin160([CSV-P2PK])] OP_CHECKSIG",

```
% echo "[0040000f] checksequenceverify drop [02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b]" | bx script-encode | bx bitcoin160
e3826cfda3e5233e946a8abc52ddae7d704815f5
```

RedeemScript = "[e3826cfda3e5233e946a8abc52ddae7d704815f5] checksig"

```
% echo "[e3826cfda3e5233e946a8abc52ddae7d704815f5] checksig" | bx script-encode
14e3826cfda3e5233e946a8abc52ddae7d704815f5ac
```

[SigRedeemScript] [RedeemScript] OP_HASH160 [HASH160([RedeemScript])] OP_EQUAL

```
% echo "[e3826cfda3e5233e946a8abc52ddae7d704815f5] checksig" | bx script-encode | bx bitcoin160
312d616b4c1529d55094f8aff9e935573021fa02 = HASH160(RedeemScript)
```

```
% echo "[e3826cfda3e5233e946a8abc52ddae7d704815f5] checksig" | bx script-to-address -v 196
2MwjFTn95iM2PmmlpUyi8hBzP6pLQio8NbZ
```

Fund Bitcoin-Explorer (bx) P2SH(CSV-P2PK) Address and Ledger Nano S P2SH(P2WPKH) Address Payment

```
% bx tx-encode -v 1 -i 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9:1 -o 2MwjFTn95iM2Pmm1pUyi8hBzP6pLQio8Nbz:10000 -o 2N9e4AjRBiQyvuu3QMhCahQEDijjavfmET3:124989000 0100000001d93dc14d376cd4799c5331699c14f1df1d027fbbb33e4e849824f00046a575300100000000fffffffff021027000000000000017a914312d616b4c1529d55094f8aff9e935573021fa0287482e73070000000017a914b3d361e8a80c49dd0c9a5d6e40c5611f35a3cade8700000000
```

```
% bx tx-encode -v 1 -i 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c/9d46c374dc13dd9:1 -o 2MwjFTn95iM2PmmlpUyi8hBzP6pLQio8Nbz:10000 -o 2N9e4AjRBiQyvuu3QMhCahQEDijjavfMET3:124989000 | bx input-sign -i 0 857608a143454263ccb0b6b4a482887d6a8add1f266f2023649d8a7657a05df "dup hash160 [fe58762223ae84731709aa7a3cb6cc8859b252c7] equalverify checksig" 3043021f3b5ad89e732b868edbc04f4b105079a0bed0906bb539a2e25210c2f2325f2502207126f43cb1c98f69b0159e1252d62081796e04a5bc97cfd5d7e2c8e5418ed94401
```

```
% bx tx-encode -v 1 -i 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9:1 -o 2MwjFTn95iM2Pmm1pUyi8hBzP6pLQio8Nbz:10000 -o
2N9e4AjRBiQyvuu3QMhCahQEDijjavfmET3:124989000 | bx input-set -i 0
"[3043021f3b5ad89e732b868edbc04f4b105079a0bed0906bb539a2e25210c2f2325f2502207126f43cb1c98f69b0159e1252d62081796e04a5bc97cfd5d7e2c8e5418ed94401]
[03664d528eb80096671ef9011c533ceb5df133238e3690d88f2960c786398b86b1]"
0100000001d93dc14d376cd4799c5331699c14f1df1d027fbbb33e4e849824f00046a5753001000000069463043021f3b5ad89e732b868edbc04f4b105079a0bed0906bb539a2e25
210c2f2325f2502207126f43cb1c98f69b0159e1252d62081796e04a5bc97cfd5d7e2c8e5418ed944012103664d528eb80096671ef9011c533ceb5df133238e3690d88f2960c786
398b86b1fffffffff021027000000000000017a914312d616b4c1529d55094f8aff9e935573021fa0287482e730700000000017a914b3d361e8a80c49dd0c9a5d6e40c5611f35a3cad
e8700000000
```

```

% bx tx-encode -v 1 -i 3075a54600f02498844e3eb3b7f021ddff1149c6931539c79d46c374dc13dd9:1 -o 2MwjFTn95iM2PmmlpUyi8hBzP6pLQio8NbZ:10000 -o
2N9e4AjRBiQyvuu3QMhCahQEDijjavfmET3:124989000 | bx input-set -i 0
"[3043021f3b5ad89e732b868edbc04f4b105079a0bed0906bb539a2e25210c2f2325f2502207126f43cb1c98f69b0159e1252d62081796e04a5bc97cfd5d7e2c8e5418ed94401]
[03664d528eb80096671ef9011c533ceb5df133238e3690d88f2960c786398b86b1]" | bx input-validate
03664d528eb80096671ef9011c533ceb5df133238e3690d88f2960c786398b86b1 "dup hash160 [fe58762223ae84731709aa7a3cb6cc8859b252c7] equalverify
checksig"
3043021f3b5ad89e732b868edbc04f4b105079a0bed0906bb539a2e25210c2f2325f2502207126f43cb1c98f69b0159e1252d62081796e04a5bc97cfd5d7e2c8e5418ed94401

```

```
% bx tx-encode -v 1 -i 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9:1 -o 2MwjFTn95iM2PmmlpUyi8hBzP6pLQio8NbZ:10000 -o 2N9e4AjRBiQyvuu3QMhCahQEDijjavfmET3:124989000 | bx input-set -i 0 [3043021f3b5ad89e732b868edbc04f4b105079a0bed0906bb539a2e25210c2f2325f2502207126f43cb1c98f69b0159e1252d62081796e04a5bc97cfd5d7e2c8e5418ed94401] [03664d528eb80096671ef9011c533ceb5df133238e3690d88f2960c786398b86b1]" | bx validate-tx
```

```
% bx tx-encode -v 1 -i 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9:1 -o 2MwjFTn95iM2PmmlpUyi8hBzP6pLQio8NbZ:10000 -o 2N9e4AjRBIQyvuu3QMhCahQEDijjavfmET3:124989000 | bx input-set -i 0 [3043021f3b5ad89e732b868edbc04f4b105079a0bed0906bb539a2e25210c2f2325f2502207126f43cb1c98f69b0159e1252d62081796e04a5bc97cfd5d7e2c8e5418ed94401] [03664d528eb80096671ef9011c533ceb5df133238e3690d88f2960c786398b86b1]" | bx send-tx
```

```
% bx watch-address 2MwjFTn95iM2Pmm1pUyi8hBzP6pLQio8NbZ
Watching address: 2MwjFTn95iM2Pmm1pUyi8hBzP6pLQio8NbZ...
1 1450689 9adfee2ceec089c52c450b3f33147b45eedcfd27ca48c638a1191bbe9466196
```

Spend P2SH(CSV-P2PK) Payment Using bx

```
% echo 824844a7964a56dfe3c1b44d66b11728657061807a59cdabf41635c88ca01f5d | bx ec-to-public  
02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b
```

```
base10( 0x0040000f ) = 4194319
```

```
% bx fetch-balance 2MwjFTn95iM2PmmlpUyi8hBzP6pLQio8Nbz  
balance  
{  
  address 2MwjFTn95iM2PmmlpUyi8hBzP6pLQio8Nbz  
  received 10000  
  spent 0  
}
```

```
% bx tx-encode -v 2 -i 9adfeea2ceec089c52c450b3f33147b45eedcfd27ca48c638a1191bbe9466196:0:4194319 -o 2N9e4AjRbiQyvuu3QMhCahQEDijjavfmET3:10000  
0200000001966146e9bb91118a638ca47cd2cfed5eb44731f3b350c4529c08eccea2eedf9a0000000000f00400001102700000000000017a914b3d361e8a80c49dd0c9a5d6e40c5611f35a3cade8700000000
```

```
% bx tx-encode -v 2 -i 9adfeea2ceec089c52c450b3f33147b45eedcfd27ca48c638a1191bbe9466196:0:4194319 -o 2N9e4AjRbiQyvuu3QMhCahQEDijjavfmET3:10000 | bx input-  
sign -i 0 824844a7964a56dfe3c1b44d66b11728657061807a59cdabf41635c88ca01f5d "[e3826cfda3e5233e946a8abc52ddae7d704815f5] checksig"  
30440220256996a816448204d1bc2ca905fe7f9bbfec2bcc60b0d66956534bbb7881b61502207bd0d7268c979836fc34b8872377f6b096fe0c20078ac858f827b8f0ee14318701
```

```
% bx tx-encode -v 2 -i 9adfeea2ceec089c52c450b3f33147b45eedcfd27ca48c638a1191bbe9466196:0:4194319 -o 2N9e4AjRbiQyvuu3QMhCahQEDijjavfmET3:10000 | bx input-  
set -i 0 "[30440220256996a816448204d1bc2ca905fe7f9bbfec2bcc60b0d66956534bbb7881b61502207bd0d7268c979836fc34b8872377f6b096fe0c20078ac858f827b8f0ee14318701]  
[14e3826cfda3e5233e946a8abc52ddae7d704815f5ac]"  
0200000001966146e9bb91118a638ca47cd2cfed5eb44731f3b350c4529c08eccea2eedf9a000000005f4730440220256996a816448204d1bc2ca905fe7f9bbfec2bcc60b0d66956534bbb7881  
b61502207bd0d7268c979836fc34b8872377f6b096fe0c20078ac858f827b8f0ee143187011614e3826cfda3e5233e946a8abc52ddae7d704815f5ac0f00400001102700000000000017a914b3  
d361e8a80c49dd0c9a5d6e40c5611f35a3cade8700000000
```

```
% bx tx-encode -v 2 -i 9adfeea2ceec089c52c450b3f33147b45eedcfd27ca48c638a1191bbe9466196:0:4194319 -o 2N9e4AjRbiQyvuu3QMhCahQEDijjavfmET3:10000 | bx input-  
set -i 0 "[30440220256996a816448204d1bc2ca905fe7f9bbfec2bcc60b0d66956534bbb7881b61502207bd0d7268c979836fc34b8872377f6b096fe0c20078ac858f827b8f0ee14318701]  
[14e3826cfda3e5233e946a8abc52ddae7d704815f5ac]" | bx input-validate -i 0 02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b  
"[e3826cfda3e5233e946a8abc52ddae7d704815f5] checksig"  
30440220256996a816448204d1bc2ca905fe7f9bbfec2bcc60b0d66956534bbb7881b61502207bd0d7268c979836fc34b8872377f6b096fe0c20078ac858f827b8f0ee14318701  
The endorsement is valid.
```

```
% bx tx-encode -v 2 -i 9adfeea2ceec089c52c450b3f33147b45eedcfd27ca48c638a1191bbe9466196:0:4194319 -o 2N9e4AjRbiQyvuu3QMhCahQEDijjavfmET3:10000 | bx input-  
set -i 0 "[30440220256996a816448204d1bc2ca905fe7f9bbfec2bcc60b0d66956534bbb7881b61502207bd0d7268c979836fc34b8872377f6b096fe0c20078ac858f827b8f0ee14318701]  
[14e3826cfda3e5233e946a8abc52ddae7d704815f5ac]" | bx validate-tx  
transaction currently locked
```

```
% bx fetch-height  
1450689
```

Increasing Mining Fees to Spend P2SH(CSV-P2PK) Payment Using bx

```
% bx fetch-height  
1450737
```

```
% bx tx-encode -v 2 -i 9adfeea2ceec089c52c450b3f33147b45eedcfd27ca48c638a1191bbe9466196:0:4194319 -o  
2N9e4AjRBiQyvuu3QMhCahQEDijjavfmET3:10000 | bx input-set -i 0  
"[30440220256996a816448204d1bc2ca905fe7f9bbfec2bcc60b0d66956534bbb7881b61502207bd0d7268c979836fc34b8872377f6b096fe0c20078ac858f827b8f0ee14318  
701] [14e3826cfda3e5233e946a8abc52ddae7d704815f5ac]" | bx validate-tx  
insufficient transaction fee
```

```
% bx tx-encode -v 2 -i 9adfeea2ceec089c52c450b3f33147b45eedcfd27ca48c638a1191bbe9466196:0:4194319 -o 2N9e4AjRBiQyvuu3QMhCahQEDijjavfmET3:5000  
| bx input-sign -i 0 824844a7964a56dfe3c1b44d66b11728657061807a59cdabf41635c88ca01f5d "[e3826cfda3e5233e946a8abc52ddae7d704815f5] checksig"  
3045022100859bf5813cc0b5ede7b96d6d4fe2354d6351357648e63ffb7b675da3dae122f502203a9f9cfb3fcce3cab537336bf27e671b75f4ec25084a6967702c377ab6e19a8  
b01
```

```
% bx tx-encode -v 2 -i 9adfeea2ceec089c52c450b3f33147b45eedcfd27ca48c638a1191bbe9466196:0:4194319 -o 2N9e4AjRBiQyvuu3QMhCahQEDijjavfmET3:5000  
| bx input-set -i 0  
"[3045022100859bf5813cc0b5ede7b96d6d4fe2354d6351357648e63ffb7b675da3dae122f502203a9f9cfb3fcce3cab537336bf27e671b75f4ec25084a6967702c377ab6e19  
a8b01] [02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b]"  
0200000001966146e9bb91118a638ca47cd2cfed5eb44731f3b350c4529c08eccea2eedf9a000000006b483045022100859bf5813cc0b5ede7b96d6d4fe2354d6351357648e63  
ffb7b675da3dae122f502203a9f9cfb3fcce3cab537336bf27e671b75f4ec25084a6967702c377ab6e19a8b012102e18f47b78730f788b726c46459fdc29b57fd6d437b69587a  
1e59efa343c46a3b0f00400001881300000000000017a914b3d361e8a80c49dd0c9a5d6e40c5611f35a3cade8700000000
```

```
% bx tx-encode -v 2 -i 9adfeea2ceec089c52c450b3f33147b45eedcfd27ca48c638a1191bbe9466196:0:4194319 -o 2N9e4AjRBiQyvuu3QMhCahQEDijjavfmET3:5000  
| bx input-set -i 0  
"[3045022100859bf5813cc0b5ede7b96d6d4fe2354d6351357648e63ffb7b675da3dae122f502203a9f9cfb3fcce3cab537336bf27e671b75f4ec25084a6967702c377ab6e19  
a8b01] [02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b]" | bx input-validate  
02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b "[e3826cfda3e5233e946a8abc52ddae7d704815f5] checksig"  
3045022100859bf5813cc0b5ede7b96d6d4fe2354d6351357648e63ffb7b675da3dae122f502203a9f9cfb3fcce3cab537336bf27e671b75f4ec25084a6967702c377ab6e19a8  
b01  
The endorsement is valid.
```

```
% bx tx-encode -v 2 -i 9adfeea2ceec089c52c450b3f33147b45eedcfd27ca48c638a1191bbe9466196:0:4194319 -o 2N9e4AjRBiQyvuu3QMhCahQEDijjavfmET3:5000  
| bx input-set -i 0  
"[3045022100859bf5813cc0b5ede7b96d6d4fe2354d6351357648e63ffb7b675da3dae122f502203a9f9cfb3fcce3cab537336bf27e671b75f4ec25084a6967702c377ab6e19  
a8b01] [02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b]" | bx validate-tx  
stack false
```

**3rd Try, Sending a Payment to
Ledger Nano S P2SH(P2WPKH) UTXO,
CSV-P2PKH UTXO and
P2SH(CSV-P2PK) UTXO
Using Little-Endian Encoding for Locktime**

Bitcoin Stack Steps to Spend a P2PKH Payment

Explicit Execution Script:

[SigLockScript] [PubKey] OP_DUP OP_HASH160 [HASH160(PubKey)] OP_EQUALVERIFY OP_CHECKSIG

LockScript = "OP_DUP OP_HASH160 [HASH160(PubKey)] OP_EQUALVERIFY OP_CHECKSIG"

MESSAGE = [{LockScript}]

** operation {} = script-encode(); OP_HASH160 = bitcoin160()

Bitcoin LIFO Stack

Empty Stack

[SigLockScript]

[SigLockScript] [PubKey]

[SigLockScript] [PubKey] [PubKey]

[SigLockScript] [PubKey] [HASH160(PubKey)]

[SigLockScript] [PubKey] [HASH160(PubKey)] [HASH160(PubKey)]

[SigLockScript] [PubKey] *(implicitly used MESSAGE above to complete operation)*

1

Script Execution Queue

[SigLockScript] [PubKey] OP_DUP OP_HASH160 [HASH160(PubKey)]
OP_EQUALVERIFY OP_CHECKSIG

[PubKey] OP_DUP OP_HASH160 [HASH160(PubKey)] OP_EQUALVERIFY
OP_CHECKSIG

OP_DUP OP_HASH160 [HASH160(PubKey)] OP_EQUALVERIFY
OP_CHECKSIG

OP_HASH160 [HASH160(PubKey)] OP_EQUALVERIFY OP_CHECKSIG

[HASH160(PubKey)] OP_EQUALVERIFY OP_CHECKSIG

OP_EQUALVERIFY OP_CHECKSIG

OP_CHECKSIG

Empty Script

Bitcoin Stack Steps to Spend a P2SH(CSV-P2PK) Payment

Explicit Execution Script:

[SigRedeemScript] [{RedeemScript}] OP_HASH160 [HASH160({RedeemScript})] OP_EQUAL

Implicit Execution Script:

[SigRedeemScript] [bitcoin160({CSV-P2PK})] OP_CHECKSIG [{RedeemScript}] OP_HASH160 [bitcoin160({RedeemScript})] OP_EQUAL

CSV-P2PK = "[0f004000] checksequenceverify drop [PubKey]", to_little_endian(0x0040000f) = 0x0f004000

RedeemScript = "[bitcoin160({CSV-P2PK})] OP_CHECKSIG",

MESSAGE = [{RedeemScript}]

** Insights above gleaned from a careful examination of <https://github.com/bitcoin/bips/blob/master/bip-0016.mediawiki#specification> and generalization of “Spending a P2SH Payment”; operation {} = script-encode(); OP_HASH160 = bitcoin160()

Bitcoin LIFO Stack

Empty Stack

[SigRedeemScript]

[SigRedeemScript] [bitcoin160({CSV-P2PK})]

[SigRedeemScript] [bitcoin160({CSV-P2PK})] OP_CHECKSIG

[SigRedeemScript] [bitcoin160({CSV-P2PK})] OP_CHECKSIG [{RedeemScript}]

[SigRedeemScript] [bitcoin160({CSV-P2PK})] OP_CHECKSIG [bitcoin160({RedeemScript})]

[SigRedeemScript] [bitcoin160({CSV-P2PK})] OP_CHECKSIG [bitcoin160({RedeemScript})] [bitcoin160({RedeemScript})] OP_EQUAL

[SigRedeemScript] [bitcoin160({CSV-P2PK})] OP_CHECKSIG 1

[SigRedeemScript] [bitcoin160({CSV-P2PK})] OP_CHECKSIG (implicitly used MESSAGE above to complete operation)

1

Script Execution Queue

[SigRedeemScript] [bitcoin160({CSV-P2PK})] OP_CHECKSIG [{RedeemScript}]
OP_HASH160 [bitcoin160({RedeemScript})] OP_EQUAL

[bitcoin160({CSV-P2PK})] OP_CHECKSIG [{RedeemScript}]
OP_HASH160 [bitcoin160({RedeemScript})] OP_EQUAL

OP_CHECKSIG [{RedeemScript}]
OP_HASH160 [bitcoin160({RedeemScript})] OP_EQUAL

[{RedeemScript}]
OP_HASH160 [bitcoin160({RedeemScript})] OP_EQUAL

OP_HASH160 [bitcoin160({RedeemScript})] OP_EQUAL

[bitcoin160({RedeemScript})] OP_EQUAL

OP_EQUAL

Empty Script

Empty Script

Empty Script

Third Try at Composing CheckSequenceVerify Payment Scripts in a TX with 1 Input and 3 Outputs using Little Endian Encoding of Locktime

Testnet TX One and Only Input Information:

```
% echo 31a05e454abf3180e738724bbb00512cc82ald2c699c4674efe0c2fd1e5b0f74 | bx ec-to-public
029a449ea4a2155ea10002d704604bb3e8606631d35af20889a74b82b2dab572f6

% echo 029a449ea4a2155ea10002d704604bb3e8606631d35af20889a74b82b2dab572f6 | bx bitcoin160
f03b4896fa7a608b3518d78354fdb078107aafd2

% echo 31a05e454abf3180e738724bbb00512cc82ald2c699c4674efe0c2fd1e5b0f74 | bx ec-to-public | bx ec-to-address -v 111
n3RBVBnp5zPczs2zyTHiL3rKXu4dlnbqC1

% bx fetch-balance n3RBVBnp5zPczs2zyTHiL3rKXu4dlnbqC1
balance
{
  address n3RBVBnp5zPczs2zyTHiL3rKXu4dlnbqC1
  received 125000000
  spent 0
}

% echo 31a05e454abf3180e738724bbb00512cc82ald2c699c4674efe0c2fd1e5b0f74 | bx ec-to-public | bx bitcoin160
f03b4896fa7a608b3518d78354fdb078107aafd2

tx = 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9, index = 2
```

Locking Script: "dup hash160 [f03b4896fa7a608b3518d78354fdb078107aafd2] equalverify checksig"

Signature Script Form:

"[ENDORSEMENT_of_Locking_Script] [029a449ea4a2155ea10002d704604bb3e8606631d35af20889a74b82b2dab572f6]"

Testnet TX 1st Output BIP 49 P2SH(P2WPKH) Address, Locking Script, and Signature Script minus Witness:

```
% echo 824844a7964a56dfe3c1b44d66b11728657061807a59cdabf41635c88ca01f5d | bx ec-to-public
02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b

% echo 824844a7964a56dfe3c1b44d66b11728657061807a59cdabf41635c88ca01f5d | bx ec-to-public | bx bitcoin160
2a773c929b7932fa781b0d1154accaacc565935e

% echo "0 [2a773c929b7932fa781b0d1154accaacc565935e]" | bx script-encode
00142a773c929b7932fa781b0d1154accaacc565935e

% echo "0 [2a773c929b7932fa781b0d1154accaacc565935e]" | bx script-encode | bx bitcoin160
aefc3905c26f851f8c319b0050d493fbc3e83a18

% echo aefc3905c26f851f8c319b0050d493fbc3e83a18 | bx base58check-encode -v 196
2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR
```

Locking Script: "hash160 [aefc3905c26f851f8c319b0050d493fbc3e83a18] equal"

Signature Script: "[00142a773c929b7932fa781b0d1154accaacc565935e]"

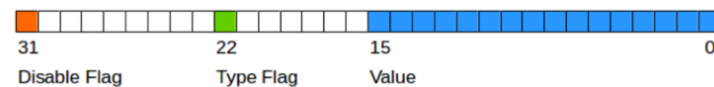
Third Try at Composing CheckSequenceVerify Payment Scripts in a TX with 1 Input and 3 Outputs using Little Endian Encoding of Locktime

```
% echo 824844a7964a56dfe3c1b44d66b11728657061807a59cdabf41635c88ca01f5d | bx ec-to-public
02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b (or mjPVWpH6EKES6SibsK6rtUWyglx24whE7f with version = 111)

% echo 824844a7964a56dfe3c1b44d66b11728657061807a59cdabf41635c88ca01f5d | bx ec-to-public | bx bitcoin160
2a773c929b7932fa781b0d1154accaacc565935e
```

Testnet TX 2nd Output CSV-P2PKH Locking Script, and Signature Script:

[ENDORSEMENT_of_Locking_Script] [PubKey] + dup hash160 [PubKey] equalverify checksig



0x0040000f specifies a relative locktime is set to -128 minutes (15*512/60)
to_little_endian(0x0040000f) = 0x0f004000

```
% echo "[0f004000] checksequenceverify drop dup hash160 [2a773c929b7932fa781b0d1154accaacc565935e] equalverify checksig" | bx script-encode
040f004000b27576a9142a773c929b7932fa781b0d1154accaacc565935e88ac
```

Signature Script Form:

"[ENDORSEMENT_of_Locking_Script] [02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b]"

Testnet TX 3rd Output P2SH(CSV-P2PK) Locking Script, Address, Redeem Script, and Signature Script :

CSV-P2PK = "[0f004000] checksequenceverify drop [PubKey]"
RedeemScript = "[bitcoin160({CSV-P2PK})] OP_CHECKSIG"
[SigRedeemScript] [[RedeemScript]] + OP_HASH160 [HASH160({RedeemScript})] OP_EQUAL

```
% echo "[0f004000] checksequenceverify drop [02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b]" | bx script-encode | bx bitcoin160
b45b290c69821f32c5f0949447e0b4768d95d433
```

RedeemScript = "[b45b290c69821f32c5f0949447e0b4768d95d433] checksig"

```
% echo "[b45b290c69821f32c5f0949447e0b4768d95d433] checksig" | bx script-encode
14b45b290c69821f32c5f0949447e0b4768d95d433ac
```

```
% echo "[b45b290c69821f32c5f0949447e0b4768d95d433] checksig" | bx script-encode | bx bitcoin160
50e64fef0162ebbf24576563351c20e5b9b891b4
```

```
% echo "[b45b290c69821f32c5f0949447e0b4768d95d433] checksig" | bx script-encode | bx bitcoin160 | bx base58check-encode -v 196
2Mzcyx1GT2T1Bt9tnbYCdHsub1aj8csBVku
```

Signature Script Form:

"[ENDORSEMENT_of_Redeem_Script] [b45b290c69821f32c5f0949447e0b4768d95d433]"

Third Try at Composing CheckSequenceVerify Payment Scripts in a TX with 1 Input and 3 Outputs using Little Endian Encoding of Locktime

```
% bx tx-encode -v 2 -i 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9:2 -o 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR:124900000 -o 040f004000b27576a9142a773c929b7932fa781b0d1154accaacc565935e88ac:49000 -o 2MzcyxlGT2TlBt9tnbYCdHsub1aj8csBVku:49000 [redacted] 0200000001d93dc14d376cd4799c5331699c14f1df1d027fbbb33e4e849824f00046a5753002000000000fffffffff03a0d271070000000017a914aefc3905c26f851f8c319b0050d493fbc3e83a188768bf00000000000020040f004000b27576a9142a773c929b7932fa781b0d1154accaacc565935e88ac68bf00000000000017a91450e64fef0162ebbf24576563351c20e5b9b891b48700000000
```

```
% bx tx-encode -v 2 -i 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9:2 -o 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR:124900000 -o 040f004000b27576a9142a773c929b7932fa781b0d1154accaacc565935e88ac:49000 -o 2MzcyxlGT2TlBt9tnbYCdHsub1aj8csBVku:49000 | bx input-sign -i 0 [redacted] 31a05e454abf3180e738724bbb00512cc82ald2c699c4674efe0c2fd1e5b0f74 "dup hash160 [f03b4896fa7a608b3518d78354fdb078107aafd2] equalverify checksig" [redacted] 3043022039alf0c165ad476dca6e64362fa31da3ed119e3a6b00a17846069d56a4283756021f4777558d4eb39f5d50a8491f96c055cfd49d01bc9760394cb7c89694a7203001
```

```
% bx tx-encode -v 2 -i 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9:2 -o 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR:124900000 -o 040f004000b27576a9142a773c929b7932fa781b0d1154accaacc565935e88ac:49000 -o 2MzcyxlGT2TlBt9tnbYCdHsub1aj8csBVku:49000 | bx input-set -i 0 [redacted] "[3043022039alf0c165ad476dca6e64362fa31da3ed119e3a6b00a17846069d56a4283756021f4777558d4eb39f5d50a8491f96c055cfd49d01bc9760394cb7c89694a7203001] [029a449ea4a2155ea10002d704604bb3e8606631d35af20889a74b82b2dab572f6]" [redacted] 0200000001d93dc14d376cd4799c5331699c14f1df1d027fbbb33e4e849824f00046a575300200000069463043022039alf0c165ad476dca6e64362fa31da3ed119e3a6b00a17846069d56a4283756021f4777558d4eb39f5d50a8491f96c055cfd49d01bc9760394cb7c89694a720300121029a449ea4a2155ea10002d704604bb3e8606631d35af20889a74b82b2dab572f6fffffffff03a0d271070000000017a914aefc3905c26f851f8c319b0050d493fbc3e83a188768bf00000000000020040f004000b27576a9142a773c929b7932fa781b0d1154accaacc565935e88ac68bf00000000000017a91450e64fef0162ebbf24576563351c20e5b9b891b48700000000
```

```
% bx tx-encode -v 2 -i 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9:2 -o 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR:124900000 -o 040f004000b27576a9142a773c929b7932fa781b0d1154accaacc565935e88ac:49000 -o 2MzcyxlGT2TlBt9tnbYCdHsub1aj8csBVku:49000 | bx input-set -i 0 [redacted] "[3043022039alf0c165ad476dca6e64362fa31da3ed119e3a6b00a17846069d56a4283756021f4777558d4eb39f5d50a8491f96c055cfd49d01bc9760394cb7c89694a7203001] [029a449ea4a2155ea10002d704604bb3e8606631d35af20889a74b82b2dab572f6]" | bx input-validate -i 0 [redacted] 029a449ea4a2155ea10002d704604bb3e8606631d35af20889a74b82b2dab572f6 "dup hash160 [f03b4896fa7a608b3518d78354fdb078107aafd2] equalverify checksig" [redacted] 3043022039alf0c165ad476dca6e64362fa31da3ed119e3a6b00a17846069d56a4283756021f4777558d4eb39f5d50a8491f96c055cfd49d01bc9760394cb7c89694a7203001 The endorsement is valid.
```

```
% bx tx-encode -v 2 -i 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9:2 -o 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR:124900000 -o 040f004000b27576a9142a773c929b7932fa781b0d1154accaacc565935e88ac:49000 -o 2MzcyxlGT2TlBt9tnbYCdHsub1aj8csBVku:49000 | bx input-set -i 0 [redacted] "[3043022039alf0c165ad476dca6e64362fa31da3ed119e3a6b00a17846069d56a4283756021f4777558d4eb39f5d50a8491f96c055cfd49d01bc9760394cb7c89694a7203001] [029a449ea4a2155ea10002d704604bb3e8606631d35af20889a74b82b2dab572f6]" | bx validate-tx [redacted] The transaction is valid.
```

Double Check TX Before Sending

```
% bx tx-encode -v 2 -i 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9:2 -o 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR:124900000 -o
040f004000b27576a9142a773c929b7932fa781b0d1154accaacc565935e88ac:49000 -o 2Mzcyx1GT2T1Bt9tnbYCdHsub1aj8csBVku:49000 | bx input-set -i 0
"[3043022039a1f0c165ad476dca6e64362fa31da3ed119e3a6b00a17846069d56a4283756021f4777558d4eb39f5d50a8491f96c055cfd49d01bc9760394cb7c89694a7203001]
[029a449ea4a2155ea10002d704604bb3e8606631d35af20889a74b82b2dab572f6]" | bx tx-decode
transaction
{
  hash 4c52f6c486b7e3372d0dc900aa041fcb0c390c89539a4af1ee9b55e9b78fd759
  inputs
  {
    input
    {
      address_hash f03b4896fa7a608b3518d78354fdb078107aafd2
      previous_output
      {
        hash 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9
        index 2
      }
      script "[3043022039a1f0c165ad476dca6e64362fa31da3ed119e3a6b00a17846069d56a4283756021f4777558d4eb39f5d50a8491f96c055cfd49d01bc9760394cb7c89694a7203001]
[029a449ea4a2155ea10002d704604bb3e8606631d35af20889a74b82b2dab572f6]"
      sequence 4294967295
    }
  }
  lock_time 0
  outputs
  {
    output
    {
      address_hash aefc3905c26f851f8c319b0050d493fbc3e83a18
      script "hash160 [aefc3905c26f851f8c319b0050d493fbc3e83a18] equal"
      value 124900000
    }
    output
    {
      script "[0f004000] checksequenceverify drop dup hash160 [2a773c929b7932fa781b0d1154accaacc565935e] equalverify checksig"
      value 49000
    }
    output
    {
      address_hash 50e64fef0162ebbf24576563351c20e5b9b891b4
      script "hash160 [50e64fef0162ebbf24576563351c20e5b9b891b4] equal"
      value 49000
    }
  }
  version 2
}
```

Compute TX ID, Send, Watch

```
encode -v 2 -i 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9:2 -o 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR:124900000 -o 040f004000b27576a9142a773c929b7932fa781b0d1154accaacc565935e88ac:49000 -o 2Mzcyx1GT2T1Bt9tnbYCdHsub1aj8csBVku:49000 | bx input-set -i 0 "[3043022039a1f0c165ad476dca6e64362fa31da3ed119e3a6b00a17846069d56a4283756021f4777558d4eb39f5d50a8491f96c055cfd49d01bc9760394cb7c89694a7203001] [029a449ea4a2155ea10002d704604bb3e8606631d35af20889a74b82b2dab572f6]" | bx bitcoin256 4c52f6c486b7e3372d0dc900aa041fcb0c390c89539a4af1ee9b55e9b78fd759
```

```
% bx tx-encode -v 2 -i 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9:2 -o 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR:124900000 -o 040f004000b27576a9142a773c929b7932fa781b0d1154accaacc565935e88ac:49000 -o 2Mzcyx1GT2T1Bt9tnbYCdHsub1aj8csBVku:49000 | bx input-set -i 0 "[3043022039a1f0c165ad476dca6e64362fa31da3ed119e3a6b00a17846069d56a4283756021f4777558d4eb39f5d50a8491f96c055cfd49d01bc9760394cb7c89694a7203001] [029a449ea4a2155ea10002d704604bb3e8606631d35af20889a74b82b2dab572f6]" | bx send-tx
```

```
% bx fetch-balance 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR
balance
{
  address 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR
  received 50000000
  spent 50000000
}
```

```
% bx watch-address 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR
Watching address: 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR...
1 1451593 4c52f6c486b7e3372d0dc900aa041fcb0c390c89539a4af1ee9b55e9b78fd759
```

```
% bx fetch-balance 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR
balance
{
  address 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR
  received 174900000
  spent 50000000
}
```

See Permanent TX Record

```
% bx fetch-tx 4c52f6c486b7e3372d0dc900aa041fcb0c390c89539a4af1ee9b55e9b78fd759
transaction
{
  hash 4c52f6c486b7e3372d0dc900aa041fcb0c390c89539a4af1ee9b55e9b78fd759
  inputs
  {
    input
    {
      address_hash f03b4896fa7a608b3518d78354fdb078107aafd2
      previous_output
      {
        hash 3075a54600f02498844e3eb3bb7f021ddff1149c6931539c79d46c374dc13dd9
        index 2
      }
      script
      "[3043022039a1f0c165ad476dca6e64362fa31da3ed119e3a6b00a17846069d56a4283756021f4777558d4eb39f5d50a8491f96c055cfd49d01bc9760394cb7c89694a7203001]
[029a449ea4a2155ea10002d704604bb3e8606631d35af20889a74b82b2dab572f6]"
      sequence 4294967295
    }
  }
  lock_time 0
  outputs
  {
    output
    {
      address_hash aefc3905c26f851f8c319b0050d493fbc3e83a18
      script "hash160 [aefc3905c26f851f8c319b0050d493fbc3e83a18] equal"
      value 124900000
    }
    output
    {
      script "[0f004000] checksequenceverify drop dup hash160 [2a773c929b7932fa781b0dl154accaacc565935e] equalverify checksig"
      value 49000
    }
    output
    {
      address_hash 50e64fef0162ebbf24576563351c20e5b9b891b4
      script "hash160 [50e64fef0162ebbf24576563351c20e5b9b891b4] equal"
      value 49000
    }
  }
  version 2
}
```

Spend 2nd UTXO

Non-Standard

CSV-P2PKH Payment

```
to_decimal( 0x0040000f ) = 4194319
to_decimal( 0x0F004000 ) = 251674624
```

```
% bx tx-encode -v 2 -i 4c52f6c486b7e3372d0dc900aa041fcb0c390c89539a4af1ee9b55e9b78fd759:1:4194319 -o 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR:47000
020000000159d78fb7e9559beef14a9a53890c390ccb1f04aa00c90d2d37e3b786c4f6524c0100000000f0040000198b70000000000017a914aefc3905c26f851f8c319b0050d493fbc3e83a188700000000
```

```
% bx tx-encode -v 2 -i 4c52f6c486b7e3372d0dc900aa041fcb0c390c89539a4af1ee9b55e9b78fd759:1:4194319 -o 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR:47000 | bx input-sign -i 0
824844a7964a56dfe3c1b44d66b11728657061807a59cdabf41635c88ca01f5d "[0f004000] checksequenceverify drop dup hash160 [2a773c929b7932fa781b0d1154accaacc565935e]
equalverify checksig"
304402205b939e9e9a4560373b51415ee9b9a2f58ae35e4509f6852f905664f2d815cc78022079414c816c303fcb35dc61938ced6e50f6ec16bff1a7b8e6ffcbc12dfc255a601
```

```
% bx tx-encode -v 2 -i 4c52f6c486b7e3372d0dc900aa041fcb0c390c89539a4af1ee9b55e9b78fd759:1:4194319 -o 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR:47000 | bx input-set -i 0
"[304402205b939e9e9a4560373b51415ee9b9a2f58ae35e4509f6852f905664f2d815cc78022079414c816c303fcb35dc61938ced6e50f6ec16bff1a7b8e6ffcbc12dfc255a601]
[02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b]"
020000000159d78fb7e9559beef14a9a53890c390ccb1f04aa00c90d2d37e3b786c4f6524c010000006a47304402205b939e9e9a4560373b51415ee9b9a2f58ae35e4509f6852f905664f2d815cc78022079414
c816c303fcb35dc61938ced6e50f6ec16bff1a7b8e6ffcbc12dfc255a6012102e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b0f0040000198b700000000000017a914aefc39
05c26f851f8c319b0050d493fbc3e83a188700000000
```

```
% bx tx-encode -v 2 -i 4c52f6c486b7e3372d0dc900aa041fcb0c390c89539a4af1ee9b55e9b78fd759:1:4194319 -o 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR:47000 | bx input-set -i 0
"[304402205b939e9e9a4560373b51415ee9b9a2f58ae35e4509f6852f905664f2d815cc78022079414c816c303fcb35dc61938ced6e50f6ec16bff1a7b8e6ffcbc12dfc255a601]
[02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b]" | bx input-validate -i 0 02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b
"[0f004000] checksequenceverify drop dup hash160 [2a773c929b7932fa781b0d1154accaacc565935e] equalverify checksig"
304402205b939e9e9a4560373b51415ee9b9a2f58ae35e4509f6852f905664f2d815cc78022079414c816c303fcb35dc61938ced6e50f6ec16bff1a7b8e6ffcbc12dfc255a601
The endorsement is valid.
```

```
% bx tx-encode -v 2 -i 4c52f6c486b7e3372d0dc900aa041fcb0c390c89539a4af1ee9b55e9b78fd759:1:4194319 -o 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR:47000 | bx input-set -i 0
"[304402205b939e9e9a4560373b51415ee9b9a2f58ae35e4509f6852f905664f2d815cc78022079414c816c303fcb35dc61938ced6e50f6ec16bff1a7b8e6ffcbc12dfc255a601]
[02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b]" | bx validate-tx
transaction currently locked
```

```
% bx fetch-height
1451593
```

```
% bx tx-encode -v 2 -i 4c52f6c486b7e3372d0dc900aa041fcb0c390c89539a4af1ee9b55e9b78fd759:1:4194319 -o 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR:47000 | bx input-set -i 0
"[304402205b939e9e9a4560373b51415ee9b9a2f58ae35e4509f6852f905664f2d815cc78022079414c816c303fcb35dc61938ced6e50f6ec16bff1a7b8e6ffcbc12dfc255a601]
[02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b]" | bx validate-tx
The transaction is valid.
```

```
% bx tx-encode -v 2 -i 4c52f6c486b7e3372d0dc900aa041fcb0c390c89539a4af1ee9b55e9b78fd759:1:4194319 -o 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR:47000 | bx input-set -i 0
"[304402205b939e9e9a4560373b51415ee9b9a2f58ae35e4509f6852f905664f2d815cc78022079414c816c303fcb35dc61938ced6e50f6ec16bff1a7b8e6ffcbc12dfc255a601]
[02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b]" | bx send-tx
```

```
% bx watch-address 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR
Watching address: 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR...
```

Spend 2nd UTXO

Non-Standard

CSV-P2PKH Payment (Continued)

```
% bx tx-encode -v 2 -i 4c52f6c486b7e3372d0dc900aa041fcb0c390c89539a4af1ee9b55e9b78fd759:1:4194319 -o 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR:47000  
| bx input-set -i 0  
"[304402205b939e9e9a4560373b51415ee9b9a2f58ae35e4509f6852f905664f2d815cc78022079414c816c303fcb35dc61938ced6e50f6ec16bff1a7b8e6ffcbc12dfc255a60  
1] [02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b]" | bx bitcoin256  
7fba79ad9511a0f27863b712d186c297843cb182569db0aded5d34ff1ca28809
```

```
% bx fetch-tx 7fba79ad9511a0f27863b712d186c297843cb182569db0aded5d34ff1ca28809  
transaction  
{  
  hash 7fba79ad9511a0f27863b712d186c297843cb182569db0aded5d34ff1ca28809  
  inputs  
  {  
    input  
    {  
      address_hash 2a773c929b7932fa781b0d1154accaacc565935e  
      previous_output  
      {  
        hash 4c52f6c486b7e3372d0dc900aa041fcb0c390c89539a4af1ee9b55e9b78fd759  
        index 1  
      }  
      script  
      "[304402205b939e9e9a4560373b51415ee9b9a2f58ae35e4509f6852f905664f2d815cc78022079414c816c303fcb35dc61938ced6e50f6ec16bff1a7b8e6ffcbc12dfc255a60  
1] [02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b]"  
      sequence 4194319  
    }  
  }  
  lock_time 0  
  outputs  
  {  
    output  
    {  
      address_hash aefc3905c26f851f8c319b0050d493fbc3e83a18  
      script "hash160 [aefc3905c26f851f8c319b0050d493fbc3e83a18] equal"  
      value 47000  
    }  
  }  
  version 2  
}
```

Spend 3rd UTXO

Standard

P2SH(CSV-P2PK) Payment

```
to_decimal( 0x0040000f ) = 4194319
to_decimal( 0x0F004000 ) = 251674624
```

```
% bx tx-encode -v 2 -i 4c52f6c486b7e3372d0dc900aa041fcb0c390c89539a4aflee9b55e9b78fd759:2:4194319 -o 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR:47000
020000000159d78fb7e9559beef14a9a53890c390ccb1f04aa00c90d2d37e3b786c4f6524c02000000000f0040000198b700000000000017a914aefc3905c26f851f8c319b0050d
493fbc3e83a1887000000000
```

```
% bx tx-encode -v 2 -i 4c52f6c486b7e3372d0dc900aa041fcb0c390c89539a4aflee9b55e9b78fd759:2:4194319 -o 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR:47000
| bx input-sign -i 0 824844a7964a56dfe3c1b44d66b11728657061807a59cdabf41635c88ca01f5d "[b45b290c69821f32c5f0949447e0b4768d95d433] checksig"
3044022045804ec838eaa445578803df51282394d20451df2692942872680026e27dae1302204f8df0a7382e67c2b03d616c173e2a52968446fbcf8690c7a1lee55cb2e3905801
```

```
% bx tx-encode -v 2 -i 4c52f6c486b7e3372d0dc900aa041fcb0c390c89539a4aflee9b55e9b78fd759:2:4194319 -o 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR:47000
| bx input-set -i 0
"[3044022045804ec838eaa445578803df51282394d20451df2692942872680026e27dae1302204f8df0a7382e67c2b03d616c173e2a52968446fbcf8690c7a1lee55cb2e390580
1] [b45b290c69821f32c5f0949447e0b4768d95d433]"
020000000159d78fb7e9559beef14a9a53890c390ccb1f04aa00c90d2d37e3b786c4f6524c020000005d473044022045804ec838eaa445578803df51282394d20451df269294287
2680026e27dae1302204f8df0a7382e67c2b03d616c173e2a52968446fbcf8690c7a1lee55cb2e390580114b45b290c69821f32c5f0949447e0b4768d95d4330f0040000198b700
000000000017a914aefc3905c26f851f8c319b0050d493fbc3e83a1887000000000
```

```
% bx tx-encode -v 2 -i 4c52f6c486b7e3372d0dc900aa041fcb0c390c89539a4aflee9b55e9b78fd759:2:4194319 -o 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR:47000
| bx input-set -i 0
"[3044022045804ec838eaa445578803df51282394d20451df2692942872680026e27dae1302204f8df0a7382e67c2b03d616c173e2a52968446fbcf8690c7a1lee55cb2e390580
1] [b45b290c69821f32c5f0949447e0b4768d95d433]" | bx input-validate -i 0 02e18f47b78730f788b726c46459fdc29b57fd6d437b69587a1e59efa343c46a3b
"[b45b290c69821f32c5f0949447e0b4768d95d433] checksig"
3044022045804ec838eaa445578803df51282394d20451df2692942872680026e27dae1302204f8df0a7382e67c2b03d616c173e2a52968446fbcf8690c7a1lee55cb2e3905801
The endorsement is valid.
```

```
% bx tx-encode -v 2 -i 4c52f6c486b7e3372d0dc900aa041fcb0c390c89539a4aflee9b55e9b78fd759:2:4194319 -o 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR:47000
| bx input-set -i 0
"[3044022045804ec838eaa445578803df51282394d20451df2692942872680026e27dae1302204f8df0a7382e67c2b03d616c173e2a52968446fbcf8690c7a1lee55cb2e390580
1] [b45b290c69821f32c5f0949447e0b4768d95d433]" | bx validate-tx
```

```
% bx tx-encode -v 2 -i 4c52f6c486b7e3372d0dc900aa041fcb0c390c89539a4aflee9b55e9b78fd759:2:4194319 -o 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR:47000
| bx input-set -i 0
"[3044022045804ec838eaa445578803df51282394d20451df2692942872680026e27dae1302204f8df0a7382e67c2b03d616c173e2a52968446fbcf8690c7a1lee55cb2e390580
1] [b45b290c69821f32c5f0949447e0b4768d95d433]" | bx send-tx
```

```
% bx watch-address 2N9CTiQVprfyEiXvAV9f7GzgF4ZpCTpu7sR
```

```
% bx fetch-tx TD_ID3
```

- <https://stedolan.github.io/jq/manual/#Invokingjq>