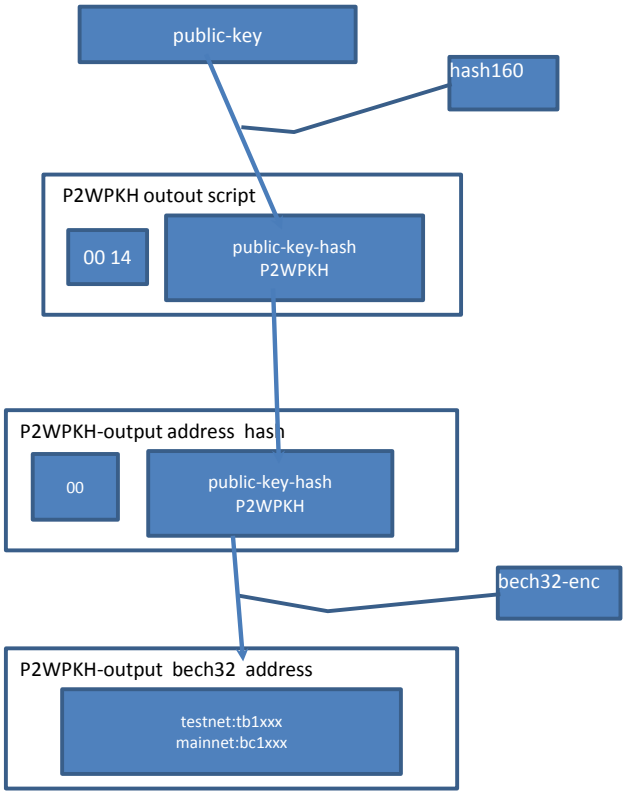
Sending to a native P2WPKH Output

witness_v0_keyhash

Tx 構成	Script
Output Script	00 [20-byte hash160(public key)]



OP_CODE	HEX
HASH160	a9
EQUAL	87
EQUALVERIFY	88
CHECKSIG	ac
DUP	76
CHECKSIGVERIFY	ad
CHECKMULTISIG	ae
CHECKMULTISIGVERIFY	af

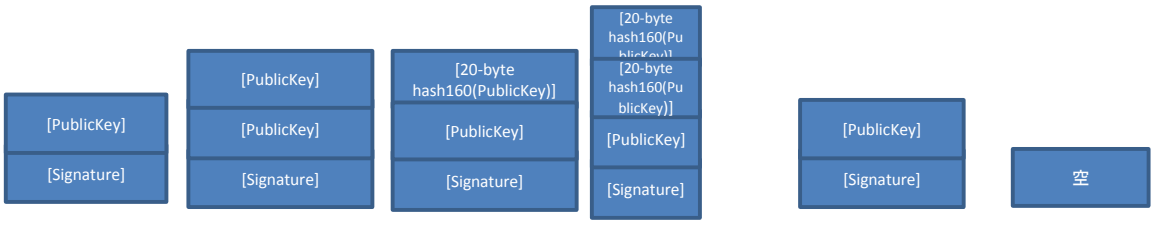
Redeem a native P2WPKH output

Tx 構成	Script
Output Script	指定先送金アドレス
Input Script	"空"
Script Code	DUP HASH160 [20-byte hash160(Public Key)] EQUALVERIFY CHECKSIG
Witness	[Signature] [Public Key]

hash160(Input Script) = previous P2SH-output script

[Signature] [PublicKey] DUP HASH160 [20-byte hash160(PublicKey)] EQUALVERIFY CHECKSIG

スクリプトの検証順番は左から右へ行う



A segwit address[6] is a Bech32 encoding of	
hrp	The human-readable part "bc" for mainnet, and "tb" for testnet
separator	1
data	a list of integers representing the characters after conversion using the table above
Checksum	The last six characters of the data part form a checksum and contain no information

No.	Witness	構成
1	02	witness構成数
2	47	length [DER signature + sighash marker]
3	witness data	[DER signature + sighash marker]
4	21	length [public key]
5	public key data	[public key]