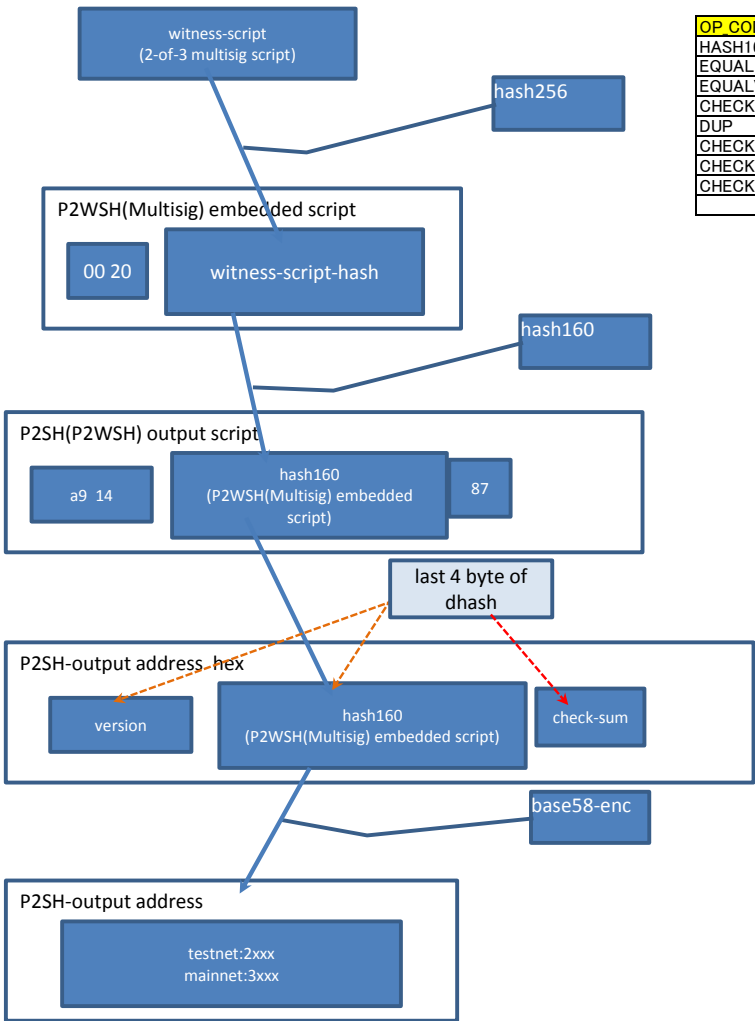


Sending to P2SH(P2WSH) Output

Pay-to-Witness-Script-Hash (P2WSH) address wrapped in a pay-to-script-hash address

Tx 構成	Script
Output Script	HASH160 [20-byte hash160(0 <sha256(witness program)>)] EQUAL



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

Redeem a P2SH(P2WSH) Output

Tx 構成	Script
Output Script	指定先送金アドレス
Input Script	[00 20 <32-byte sha256(witness script)>]
Script Code	witness script
Witness	[input script of witness script] [witness script]

No.	txinwitness構成	備考欄
1	Number of following witness elements for the first input	0x04
2	Leading zero for multisig input script	0x00
3	Length of 1st 71-byte signature	0x47/0x48
4	1st signature(DER signature + sighash marker)	sig1
5	Length of 2st 72-byte signature	0x47/0x48
6	2st signature(DER signature + sighash marker)	sig2
7	2-of-3 Multisig output script(witness script)	