

P2SH Multisig



address

inizia con 3 in mainnet
inizia con 2 regtest/testnet
Il redeem script influenza l'output dell'address

multisig

2-3

necessarie due firme verificabili su 3 chiavi pubbliche

un address Multisig necessita quindi di generare 3 address distinti

OP_CHECKMULTISIG BUG

Effettua un pop in più

Si usa un elemento NULLDUMMY

OP_0

se si utilizza un altro valore la transazione non è standard



redeem script

custom script

sono le condizioni necessarie per sbloccare la UTXO

inserito nello scriptSig

multisig



dimensione fissa

20 bytes

Ripemd160

output 160 bit

160/8=20 byte

SHA256 e RIPEMD160 del redeem script



redeem script hash

L'hash viene effettuato solo se si firma la transazione

inserito nella UTXO



scriptPubKey

OP_HASH160 redeem_script_hash
OP_EQUAL

OP_HASH160 farà l'hash del redeem script durante lo stack

OP_EQUAL verifica i due hash



custom script

Nostra responsabilità

non possiamo firmare con bitcoin-cli

bitcoin-cli firma solo le transazioni standard

non viene riconosciuta



firmare manualmente



varInt

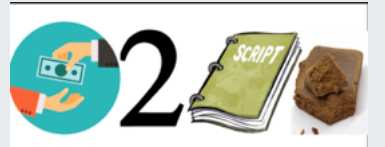
Se un valore super 0xFD (253 bytes - 506 caratteri esadecimali)



ottimizzare spazio

viene messo un prefisso secondo delle regole

le informazioni sono in little endian



Pay to Script Hash

BIP0016

address prefix

mainnet

05

address inizio con 3

testnet

C4

address inizio con 2

ScriptPubKey

OP_HASH160 [20-byte-hash-value] OP_EQUAL

ScriptSig

...signatures... {serialized script}

Il mittente non crea lo script



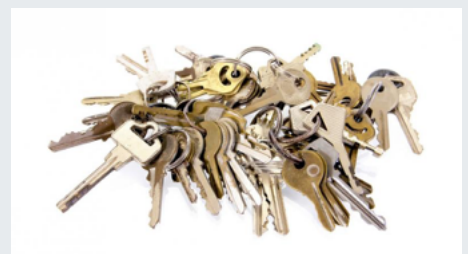
transazione più leggera

hash del redeem script



meno fees

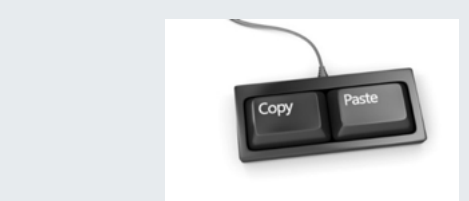
custom script



multisig +15 chiave (P2MS 3 chiavi)

Vantaggi

Stack



Lo stack è come se venisse duplicato

prima si verifica l'hash del redeem script con il redeem script stesso

Deserializzazione del redeem script

chi non ha aggiornato al BIP0016 la verifica si ferma qui



verifica delle firme (se presente)

verifica custom script (se presente)

chi non ha aggiornato

verifica solamente l'hash del redeem script

"/P2SH/"

inserito nella coinbase

Creare un address Multisignature

createmultisig

addmultisigaddress

viene aggiunto al wallet del nodo

agevola il recupero degli elementi UTXO