

# Bitcoin Script Stack Execution

## P2PKH: Pay-to-Public-Key-Hash

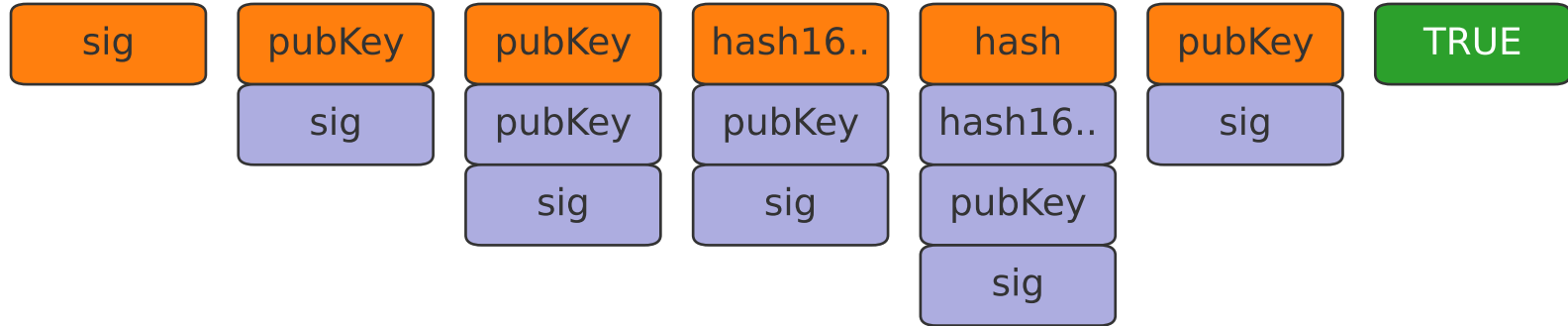
### ScriptSig (Unlocking)

<sig> <pubKey> OP\_DUP OP\_HASH160

### ScriptPubKey (Locking)

<hash> OP\_EQUALVERIFY OP\_CHECKSIG

1. Push <sig>
2. Push <pubKey>
3. OP\_DUP
4. OP\_HASH160
5. Push <hash>
6. OP\_EQUALVERIFY
7. OP\_CHECKSIG



Stack grows  
downward

**Stack = TRUE -> Valid!**