0999 tex prufa

gaman

1. nóvember 2018

Efnisyfirlit

1 rex prufa lecture

1.1 ekkert

1.1.1 gaman

hallo

2 ReST table test

2.1 The assembler

where we see (from `https://en.bitcoin.it/wiki/Script`) the meaning of the sequence
`OP_DUP OP_HASH160 OP_EQUALVERY OP_CHECKSIG OP_EQUAL OP_VERIFY`
in the table in the handout.

2.1.1 Handout

code	dec	hex	Input	Output	Description
OP_DUP	118	0x76			Duplicates the top stack item.
OP_HASH160	169	0xa9	in	hash	The input is hashed twice: first with SHA-256 and then with RIPEMD-160.
OP_EQUALVERIFY	136	0x88	x1 x2	Nothing/fail	Same as OP_EQUAL, but runs OP_VERIFY afterward.
OP_CHECKSIG	172	0xac	sig pubkey	True / false	The entire transaction outputs, inputs, and script (from the most recently-executed OP_CODESEPARATOR to the end) are hashed. The signature used by OP_CHECKSIG must be a valid signature for this hash and public key. If it is, 1 is returned, 0 otherwise.
OP_EQUAL	135	0x87	x1 x2	True/false	Returns 1 if the inputs are exactly equal, 0 otherwise.
OP_VERIFY	105	0x69	True / false	Nothing/ / fail	Marks transaction as invalid if top stack value is not true. The top stack value is removed.
	20	0x14			push 20 bytes onto the stack the following 160 bit hash

code	dec	hex	Input	Output	Description