

Figure 1: Chain of transaction for Embodiment 1 example

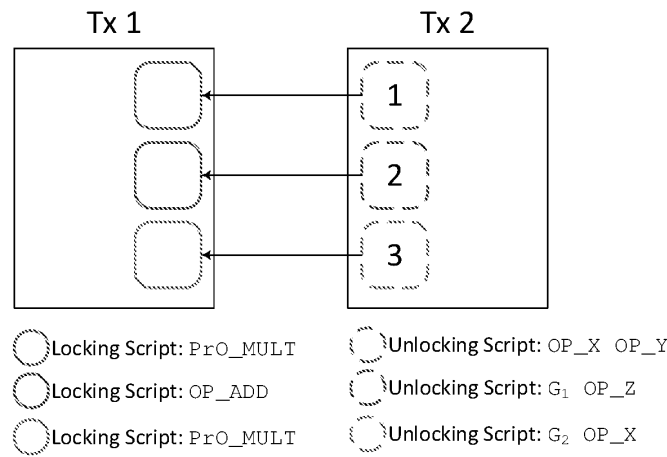


Figure 2: Transaction 1 Tx1 (embodiment 1)

Transaction 1	
01	Transaction-ID
Version Number	Version number
01	Number of inputs
Previous Tx	Prev Trans Output
00	Prev Trans Output index
Script length	Script length
<Alice's signature> <Alice's public key>	ScriptSig
SIGHASH_ALL	ScriptSig
Sequence number	Sequence number
03	Number of Outputs
Few satoshis	Output value
Output Script Length	Output script length
OP_HASH160 <hash160(redeem script 1)> OP_EQUAL	Output script
Few satoshis	Output value
Output Script Length	Output script length
OP_HASH160 <hash160(redeem script 2)> OP_EQUAL	Output script
Few satoshis	Output value
Output Script Length	Output script length
OP_HASH160 <hash160(redeem script 3)> OP_EQUAL	Output script
LockTime	LockTime

Pro_MULT OP_SWAP <Bob's public key> OP_CHECKSIG	Redeem script 1
OP_ADD OP_SWAP <Bob's public key> OP_CHECKSIG	Redeem script 2
Pro_MULT OP_SWAP <Bob's public key> OP_CHECKSIG	Redeem script 3

Figure 3: Transaction 2 Tx2 (embodiment 1)

Transaction 2	
02	Transaction-ID
Version Number	Version number
03	Number of inputs
01	Prev Trans Output
00	Prev Trans Output index
Script length	Script length
<Bob's signature> OP_X OP_Y <Redeem script 1>	ScriptSig
SIGHASH_NONE SIGHASH_ANYONECANPAY	ScriptSig
01	Prev Trans Output
01	Prev Trans Output index
Script length	Script length
<Bob's signature> G ₁ OP_Z <Redeem script 2>	ScriptSig
SIGHASH_NONE SIGHASH_ANYONECANPAY	ScriptSig
01	Prev Trans Output
02	Prev Trans Output index
Script length	Script length
<Bob's signature> G ₂ OP_X <Redeem script 3>	ScriptSig
SIGHASH_ALL	ScriptSig
Sequence number	Sequence number
01	Number of Outputs
Few satoshis	Output value
Output Script Length	Output script length
OP_DUP HASH160 <hash160(Bob's public key)> OP_EQUALVERIFY OP_CHECKSIG	Output script
LockTime	LockTime

Figure 4: Chain of transactions according to embodiment 2

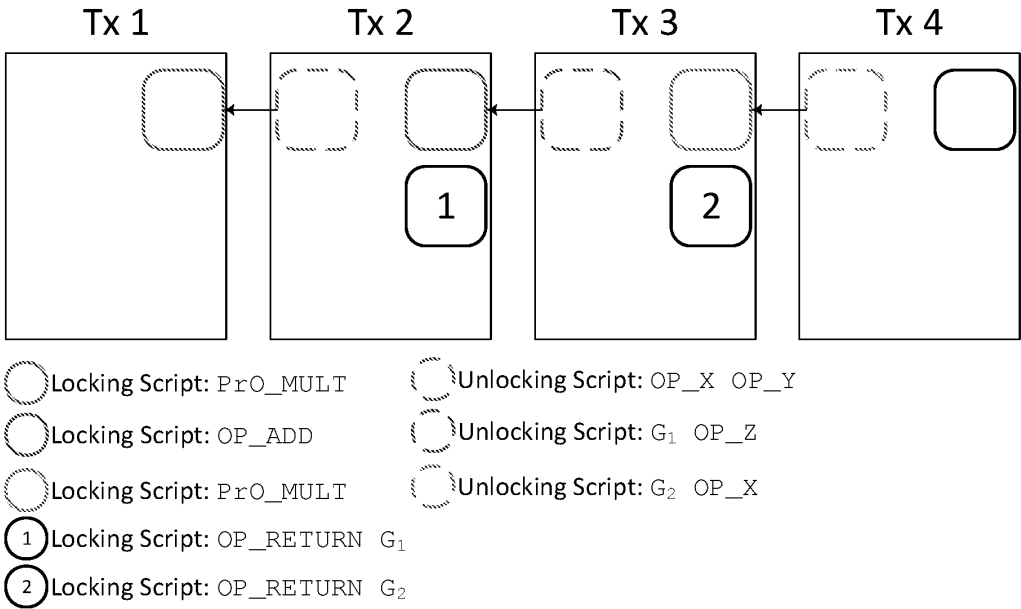


Figure 5: Transaction 1 of embodiment 2

Transaction 1	
01	Transaction-ID
Version Number	Version number
01	Number of inputs
Previous Tx	Prev Trans Output
00	Prev Trans Output index
Script length	Script length
<Alice's signature> <Alice's public key>	ScriptSig
SIGHASH_ALL	ScriptSig
Sequence number	Sequence number
01	Number of Outputs
4BTC	Output value
Output Script Length	Output script length
OP_HASH160 <hash160(redeem script 1)> OP_EQUAL	Output script
LockTime	LockTime

Figure 6: Transaction 2 of embodiment 2

Transaction 2	
02	Transaction-ID
Version Number	Version number
01	Number of inputs
01	Prev Trans Output
00	Prev Trans Output index
Script length	Script length
<Bob's signature> OP_X OP_Y <Redeem script 1>	ScriptSig
SIGHASH_ALL	ScriptSig
Sequence number	Sequence number
02	Number of Outputs
3BTC	Output value
Output Script Length	Output script length
OP_HASH160 <hash160(redeem script 2)> OP_EQUAL	Output script
0.98BTC	Output value
Output Script Length	Output script length
OP_RETURN G ₁	Output script
LockTime	LockTime

Figure 7: Transaction 3 of embodiment 2

Transaction 3	
03	Transaction-ID
Version Number	Version number
01	Number of inputs
02	Prev Trans Output
00	Prev Trans Output index
Script length	Script length
<Bob's signature> G ₁ OP_Z <Redeem script 2>	ScriptSig
SIGHASH_ALL	ScriptSig
Sequence number	Sequence number
02	Number of Outputs
2BTC	Output value
Output Script Length	Output script length
OP_HASH160 <hash160(redeem script 3)> OP_EQUAL	Output script
0.98BTC	Output value
Output Script Length	Output script length
OP_RETURN G ₂	Output script
LockTime	LockTime

Figure 8: Transaction 4 of embodiment 2

Transaction 4	
04	Transaction-ID
Version Number	Version number
01	Number of inputs
03	Prev Trans Output
00	Prev Trans Output index
Script length	Script length
<Bob's signature> G ₂ OP_X <Redeem script 3>	ScriptSig
SIGHASH_ALL	ScriptSig
Sequence number	Sequence number
01	Number of Outputs
1.08BTC	Output value
Output Script Length	Output script length
OP_DUP HASH160 <hash160(Bob's public key)> OP_EQUALVERIFY OP_CHECKSIG	Output script
LockTime	LockTime

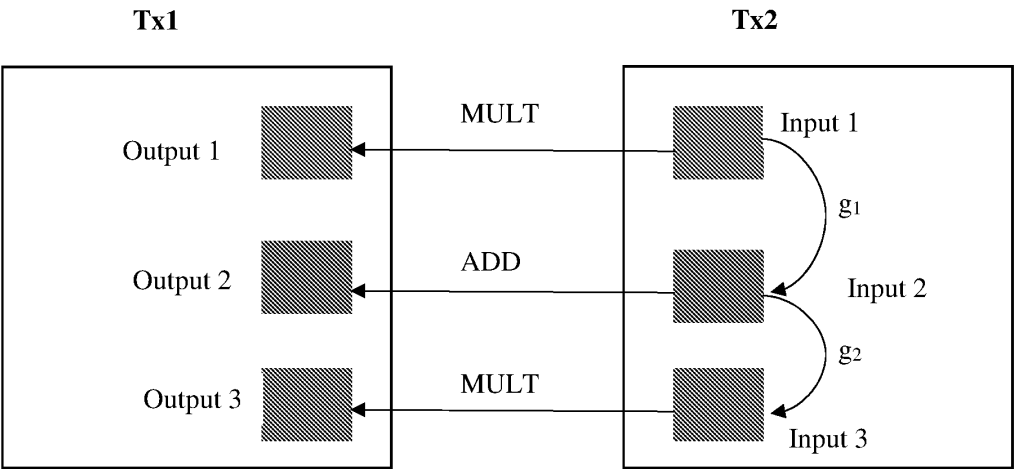
Figure 9a – Illustration of Embodiment 1 example

Locking Script: $f : x,y,z \rightarrow (x \cdot y + z) \cdot x$

$$g_1(x,y) = x \cdot y$$
$$g_2(g_1,z) = g_1 + z$$
$$f(g_2, x) = g_2 \cdot x$$

1st Unlocking Script: OP_X OP_Y

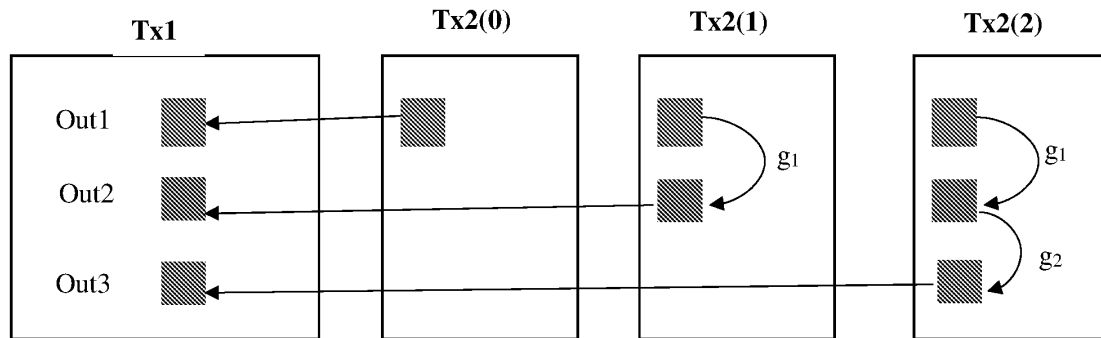
2nd Unlocking Script: g₁ OP_Z



Locking scripts incorporate functionality:

- Multiplication (MULT)
- Addition (ADD)
- Multiplication (MULT)

Figure 9b – Further Illustration of Embodiment 1 example



Phase 0: Prepare initial version of Tx2 – we will call this Tx2(0) in figure above; unlocking script of input 1 in Tx2(0) presents the arguments (OP_X and OP_Y) to the locking script of Output 1 in Tx1;
 validate Tx2(0) – produces a result g_1 which is left on the stack;

Phase 1: Update Tx2 to include input 2 (we will call this updated version Tx2(1);
 validate Tx2(1) using results g_1 produced by output 1 in phase 0

Phase 2: Update Tx2 to include input 3 (we will call this updated version Tx2(2);
 validate Tx2(2) using results g_1 and g_2

Phase 3: Submit Tx(2) to the blockchain

Figure 10 – Accessing the stack

