Tæknin á bak við Bitcoin

Hash function

=

```
79054025
255fb1a2
6e4bc422
aef54eb4
```

Blockchain

Block 1

This block:
839a8e6886
Previous block:
19d6689c08

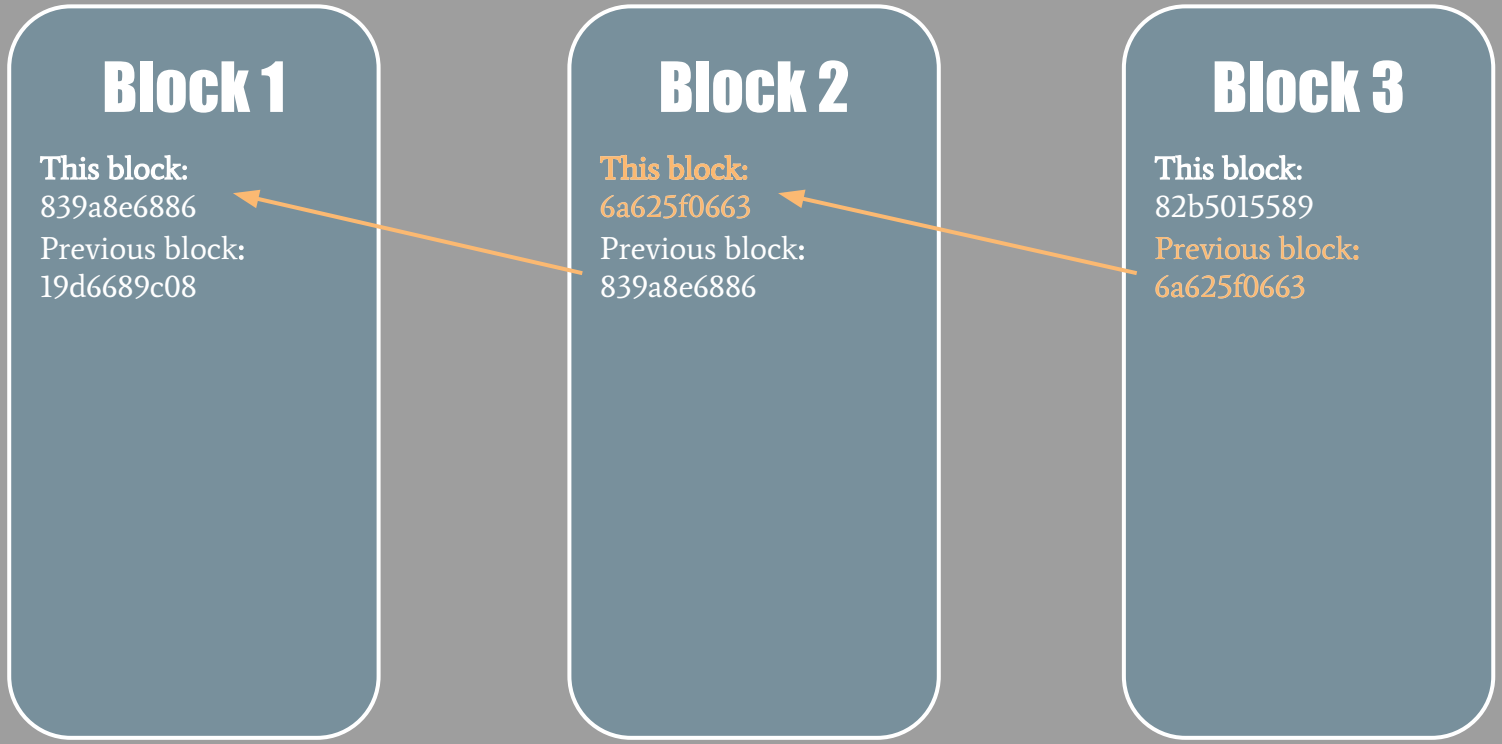
Block 2

This block:
6a625f0663
Previous block:
839a8e6886

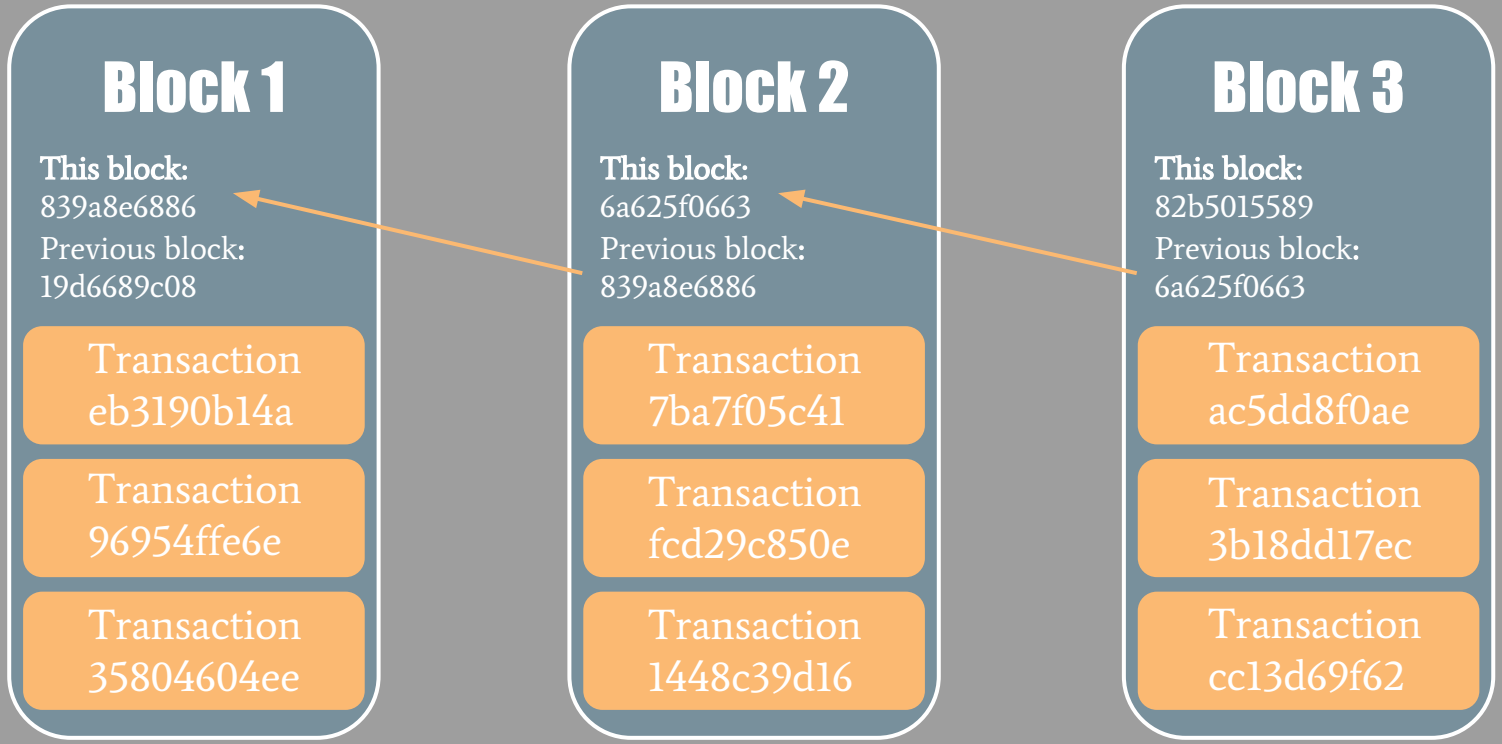
Block 3

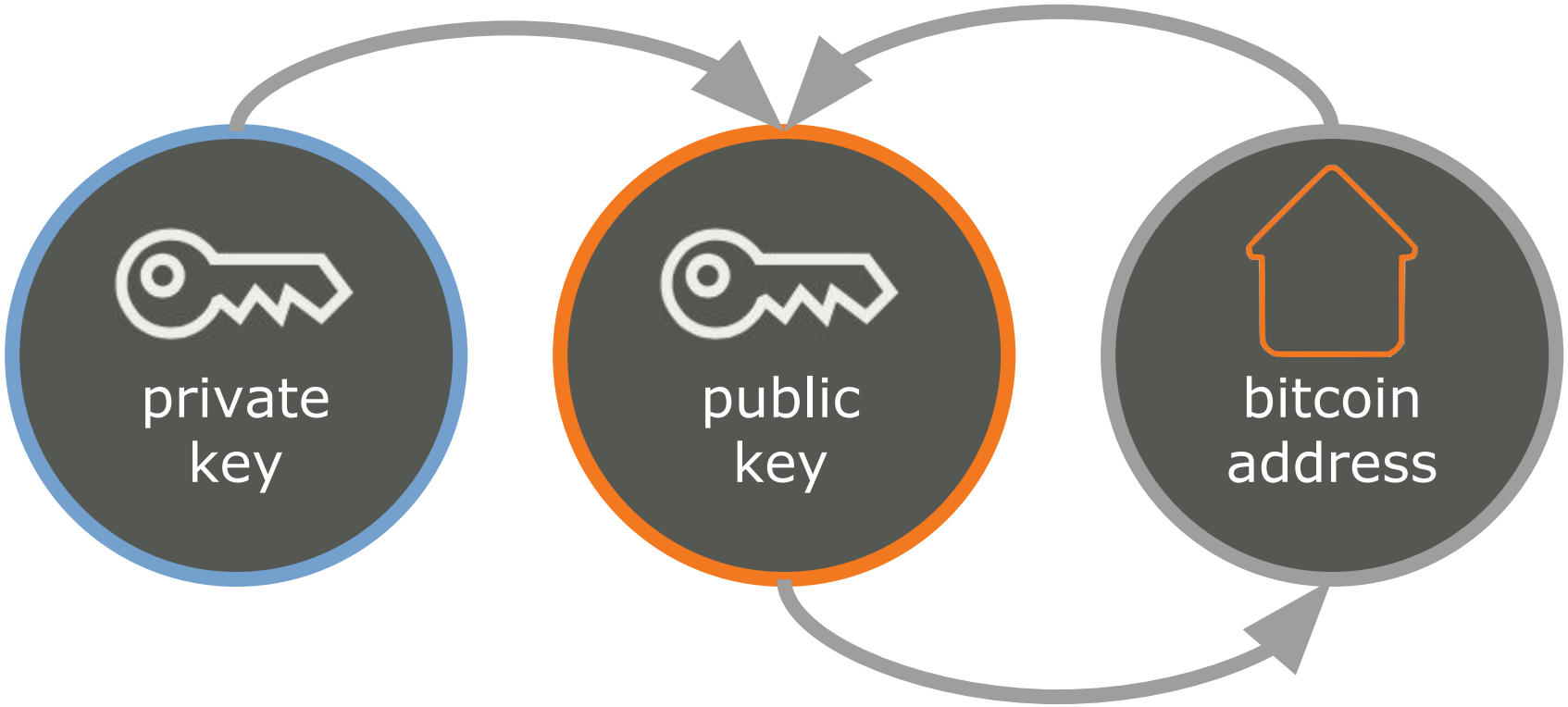
This block:
82b5015589
Previous block:
6a625f0663

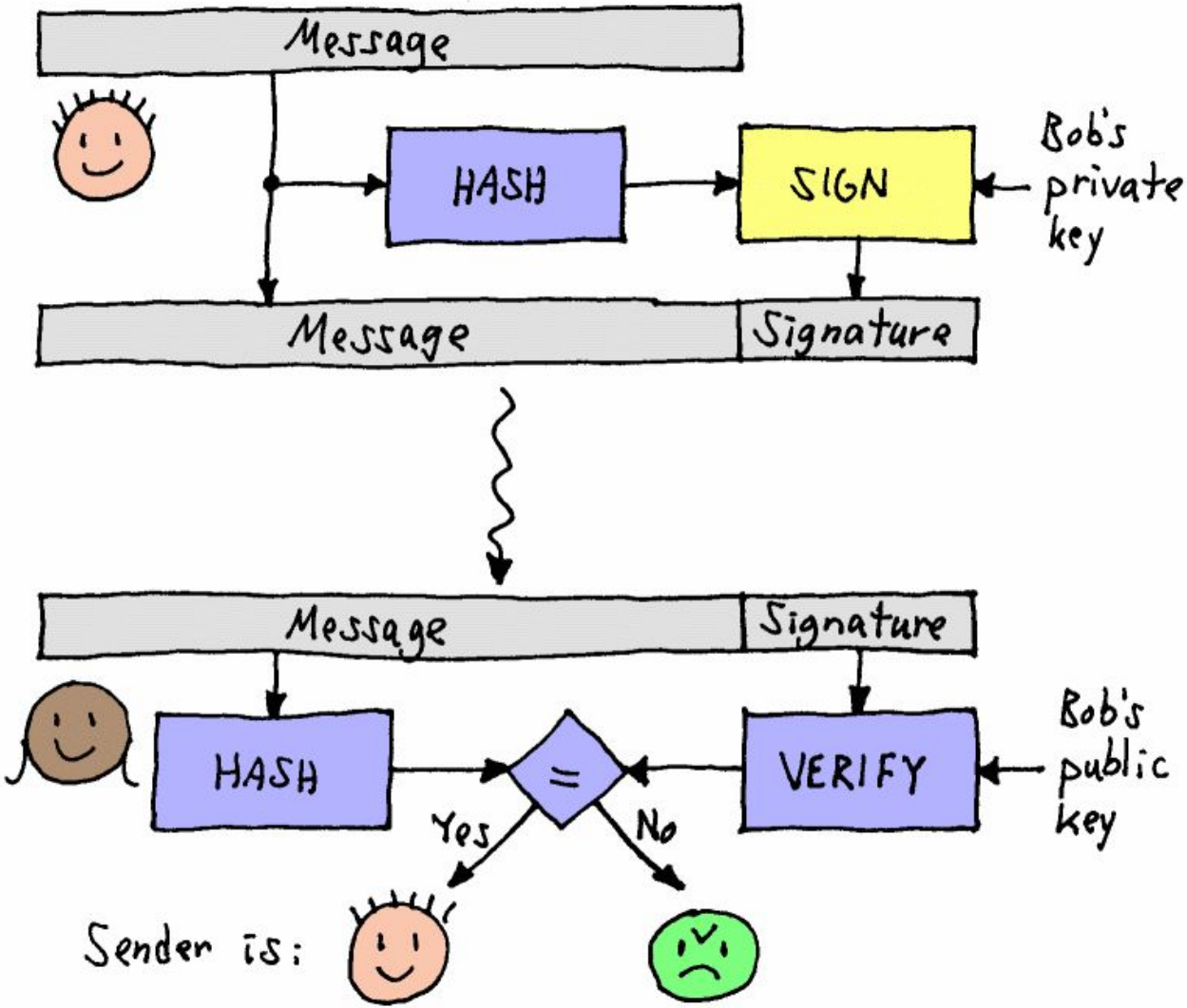
Blockchain


Block 1
This block:
839a8e6886
Previous block:
19d6689c08
Block 2
This block:
6a625f0663
Previous block:
839a8e6886
Block 3
This block:
82b5015589
Previous block:
6a625f0663

Blockchain


Block 1
This block:
839a8e6886
Previous block:
19d6689c08
Transaction
eb3190b14a
Transaction
96954ffe6e
Transaction
35804604ee
Block 2
This block:
6a625f0663
Previous block:
839a8e6886
Transaction
7ba7f05c41
Transaction
fcd29c850e
Transaction
1448c39d16
Block 3
This block:
82b5015589
Previous block:
6a625f0663
Transaction
ac5dd8f0ae
Transaction
3b18dd17ec
Transaction
cc13d69f62


private
key
public
key
bitcoin
address


Message
HASH
SIGN
Bob's private key
Message
Signature
Message
Signature
HASH
=
VERIFY
Bob's public key
Yes
No
Sender is:

Wallet

Address 1	
Debit	Credit
200	
	50
	100
	50

Address 2	
Debit	Credit
100	
	100
	0

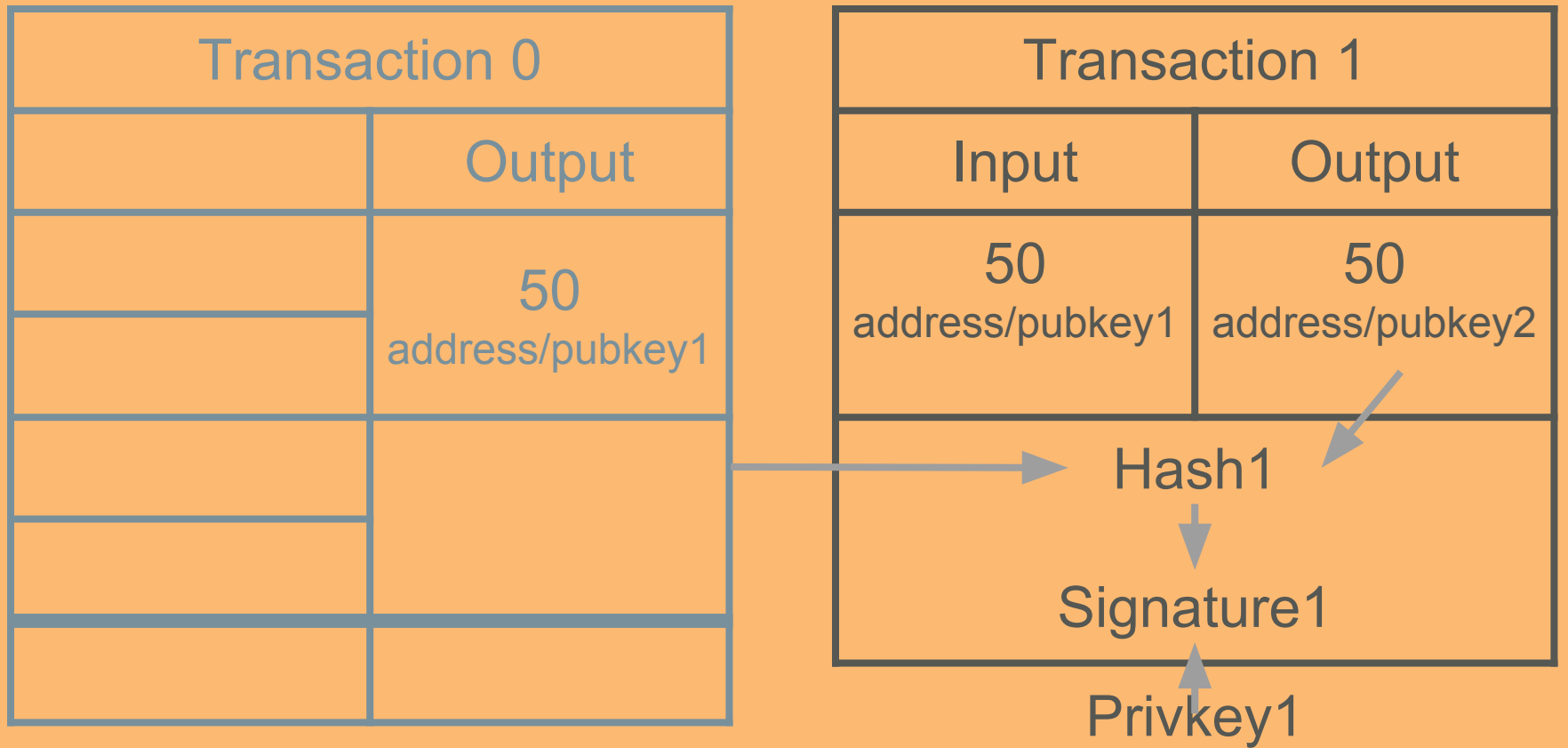
Address 3	
Debit	Credit
300	
	120
	80
	200

Transactions

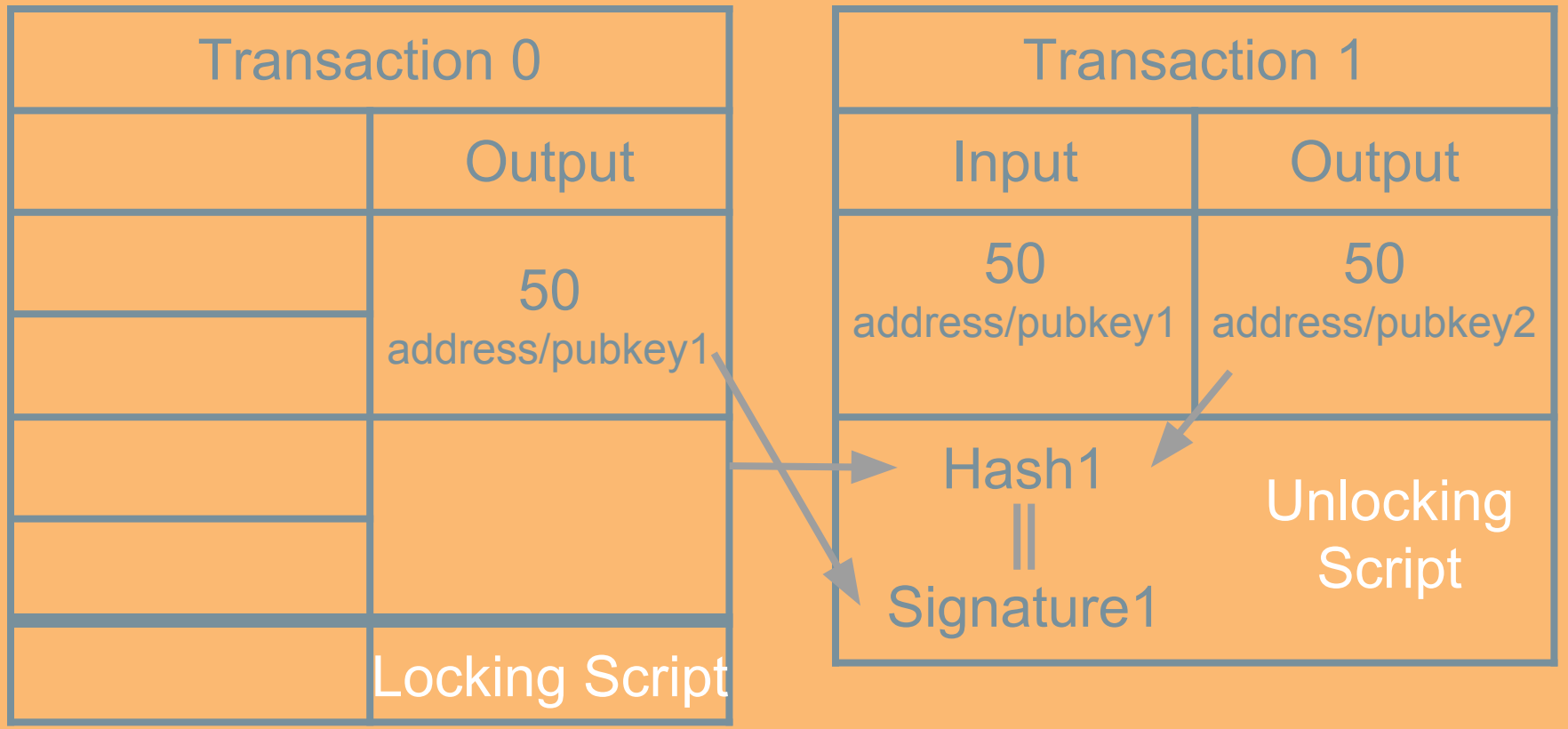
Transaction 0	
Input	Output
10	50 address/pubkey1
20	
30	20
10	
70	70

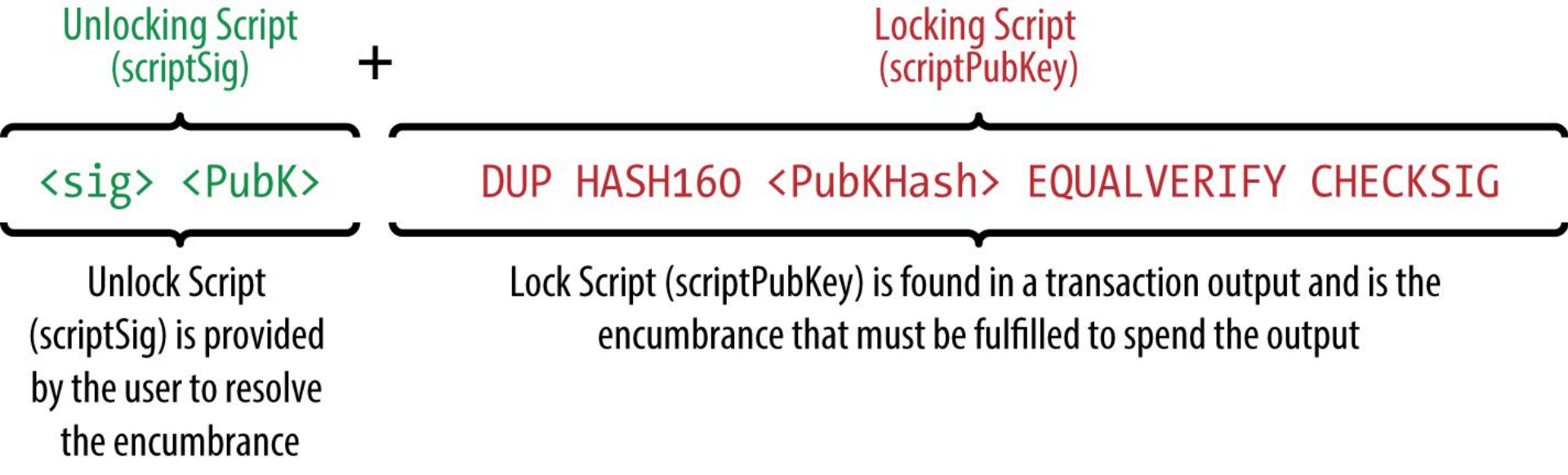
Transaction 1	
Input	Output
50 address/pubkey1	50 address/pubkey2
50	50

Sign Transaction



Verify Transaction




Unlocking Script
(scriptSig)
+
Locking Script
(scriptPubKey)
<sig> <PubK>
DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG
Unlock Script (scriptSig) is provided by the user to resolve the encumbrance
Lock Script (scriptPubKey) is found in a transaction output and is the encumbrance that must be fulfilled to spend the output

Script

Opcode	Description
OP_ADD	a + b
OP_IF	If the top stack value is not 0, the statements are executed. The top stack value is removed
OP_HASH256	The input is hashed two times with SHA-256.

Script Example

- Locking Script: (empty)
  Unlocking Script: OP_TRUE

  Anyone can spend

- <K1> <K2> <K3> 2 OP_CHECKMULTISIGVERIFY
  Unlocking Script: 2 <S1> <S3>

  Two out of three must agree