Bitcoin Transactions and Lightning Network

Kwinten De Backer

August 5, 2018

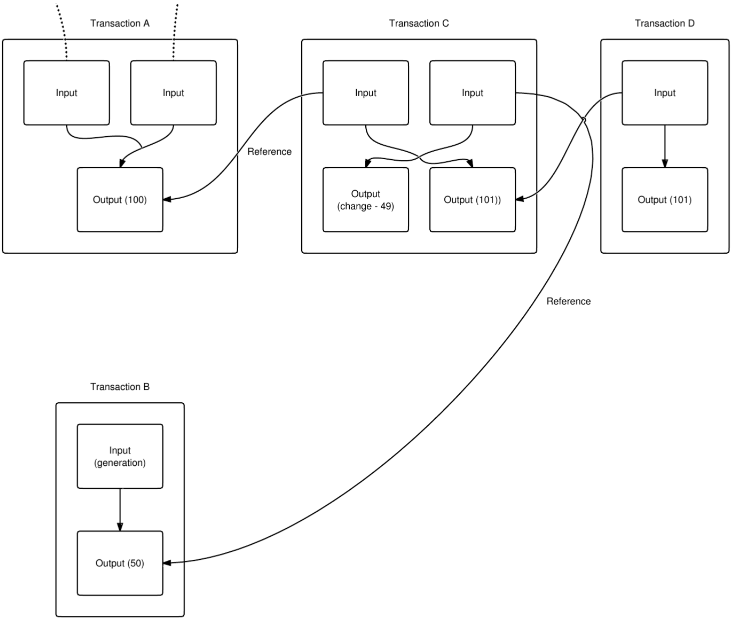
Overview

1. Bitcoin Transactions
2. The double spending problem
3. Problems with scalability
4. The Lightning Network
5. The real mindblowing stuff

General format of a Bitcoin transaction

- Number of inputs
- List of outputs
- Number of outputs
- List of outputs
- LockTime

General format of a Bitcoin transaction



Inputs

Inputs are references to **outputs** of previous transactions.
scriptSig is the first part of the script

```
Input:
Previous tx: f5d8ee39a430901c91a5917b9f2
dc19d6d1a0e9cea205b009ca73dd04470b9a6
Index: 0
scriptSig: 304502206e21798a42fae0e854281a
bd38bacd1aeed3ee3738d9e1446618c4571d10

90db022100e2ac980643b0b82c0
e88ffdfec6b64e3e6ba35e7ba5fdd7d5d6cc8d25c6b241501
```

Outputs

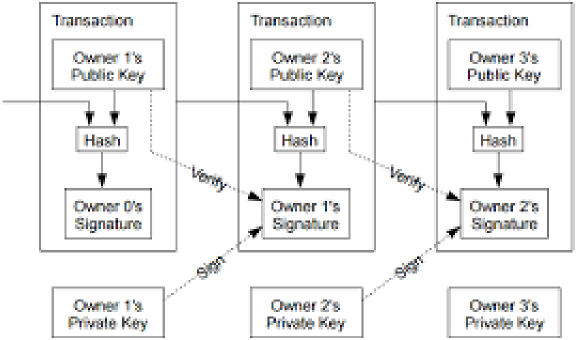
The total value of outputs must be less than the total value of the referenced outputs in the input part.
scriptPubKey is the second part of the script.

```
Output:
Value: 5000000000
scriptPubKey: OP_DUP OP_HASH160
 404371705fa9bd789a2fcd52
d2c580b65d35549d
OP EQUALVERIFY OP CHECKSIG
```

Verification

Bitcoin uses a *Forth*-like scripting language to check if a transaction is authorised. The parts in *scriptSig* and *scriptPubkey* are concatenated, pushed on a stack one by one and if the result is *true*, the transaction is valid.

What does it mean to own Bitcoin?



Pay to public key hash

Stack	Script	Description
sig pubKey	OP DUP OP HASH160 pubKeyHash OPEQUALVERIFY OP CHECKSIG	Constants are added to the stack.
sig pubKey pubKey	OP HASH160 pubKeyHash OP EQUALVERIFY OP CHECKSIG	Top stack item is duplicated.
sig pubKey pubHashA	pubKeyHash OP EQUALVERIFY OP CHECKSIG	Top stack item is hashed.
sig pubKey pubHashA pubKeyHash	OP EQUALVERIFY OP CHECKSIG	Constant added.
sig pubKey	OP CHECKSIG	Equality is checked between the top two stack items.
true	Empty.	Signature is checked for top two stack items.

Pay to script hash

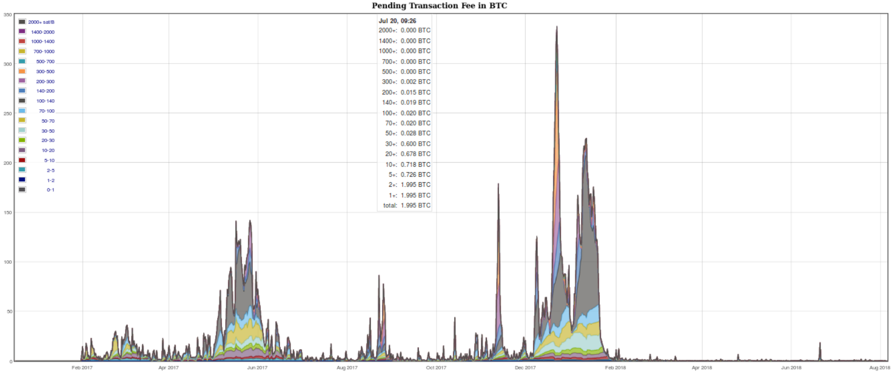
Created to move the responsability for supplying the conditions to redeem a transaction from the sender to the receiver. Makes funding a scripted transaction identical to funding a regular one.

```
scriptPubKey: OP_HASH160 <scriptHash> OP_EQUAL
scriptSig: ..signatures... <serialized script>
```

Mining (short)

Transactions need to be included in a block by a miner to be considered valid, to protect against double spendings. The more blocks are added on top of the block with the transaction, the more unlikely it is to be reversed. After 6 confirmations (1 hour), the transaction can safely be regarded as final.

Transaction fees



Blockspace and decentralization

All of the properties Bitcoin has, it has because of it's decentralization. It is absolutely vital that the cost of running a node which validates all rules independently is kept as low as possible.

- Size of the Blockchain is already around 200 GB
- Upload is around 200 GB/month, unmetered connection necessary.
- Need to keep up with a new block every 10 minutes.

Lightning on a conceptual level

Payment channels

Payment channel network (naive)

Payment channel network (better)

Lightning problems and solutions

Cross chain atomic swaps

Submarine swaps

Oracles

Channel Factories

References

John Smith (2012)
Title of the publication
Journal Name 12(3), 45 – 678.

The End