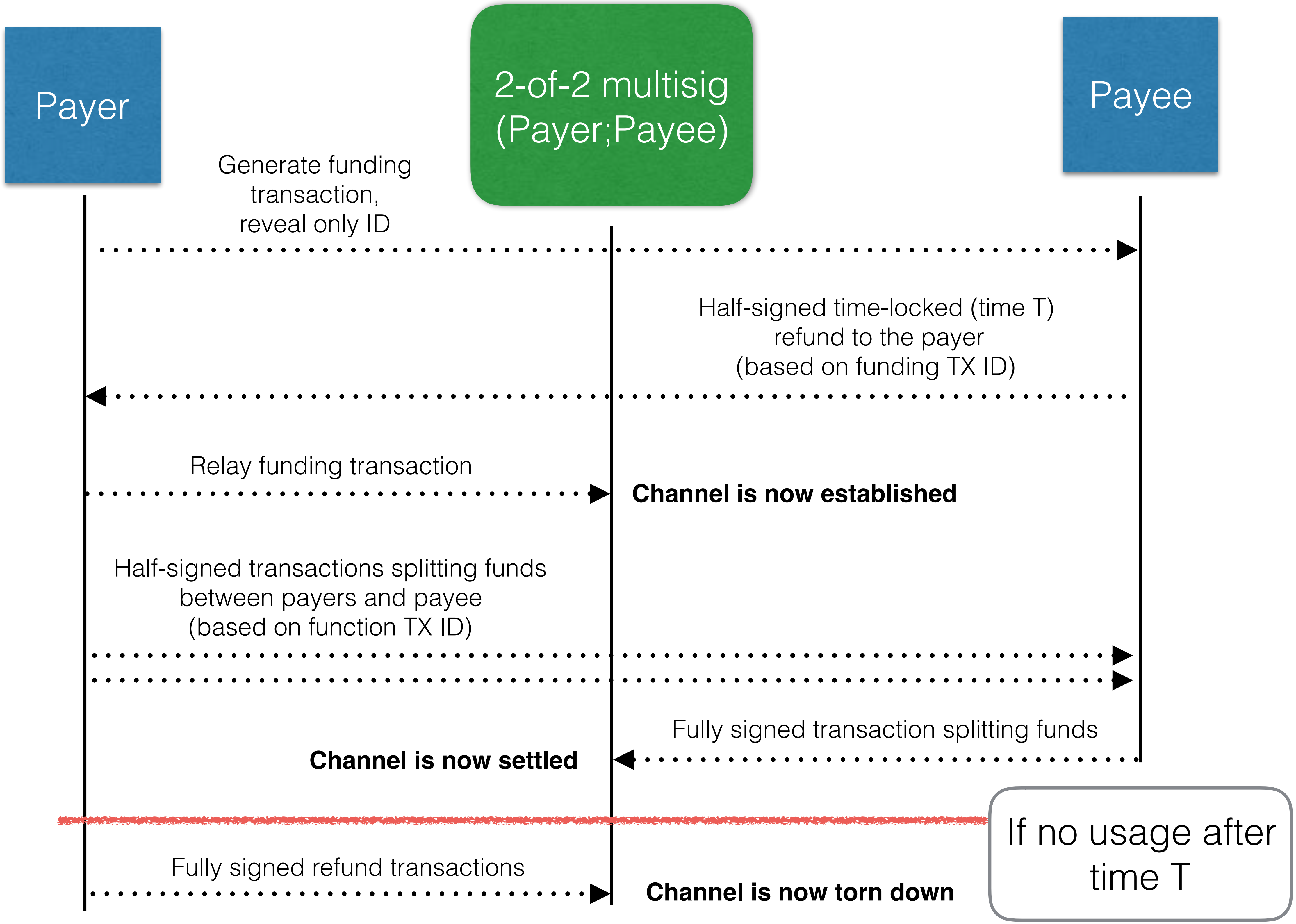
Many to many channels

Alexey Akhunov (ledgerwatch)

Payment channel - Bitcoin



Payer

2-of-2 multisig (Payer;Payee)

Payee

Generate funding transaction, reveal only ID

Half-signed time-locked (time T) refund to the payer (based on funding TX ID)

Relay funding transaction

Channel is now established

Half-signed transactions splitting funds between payers and payee (based on function TX ID)

Fully signed transaction splitting funds

Channel is now settled

If no usage after time T

Fully signed refund transactions

Channel is now torn down

Payment channel - Ethereum

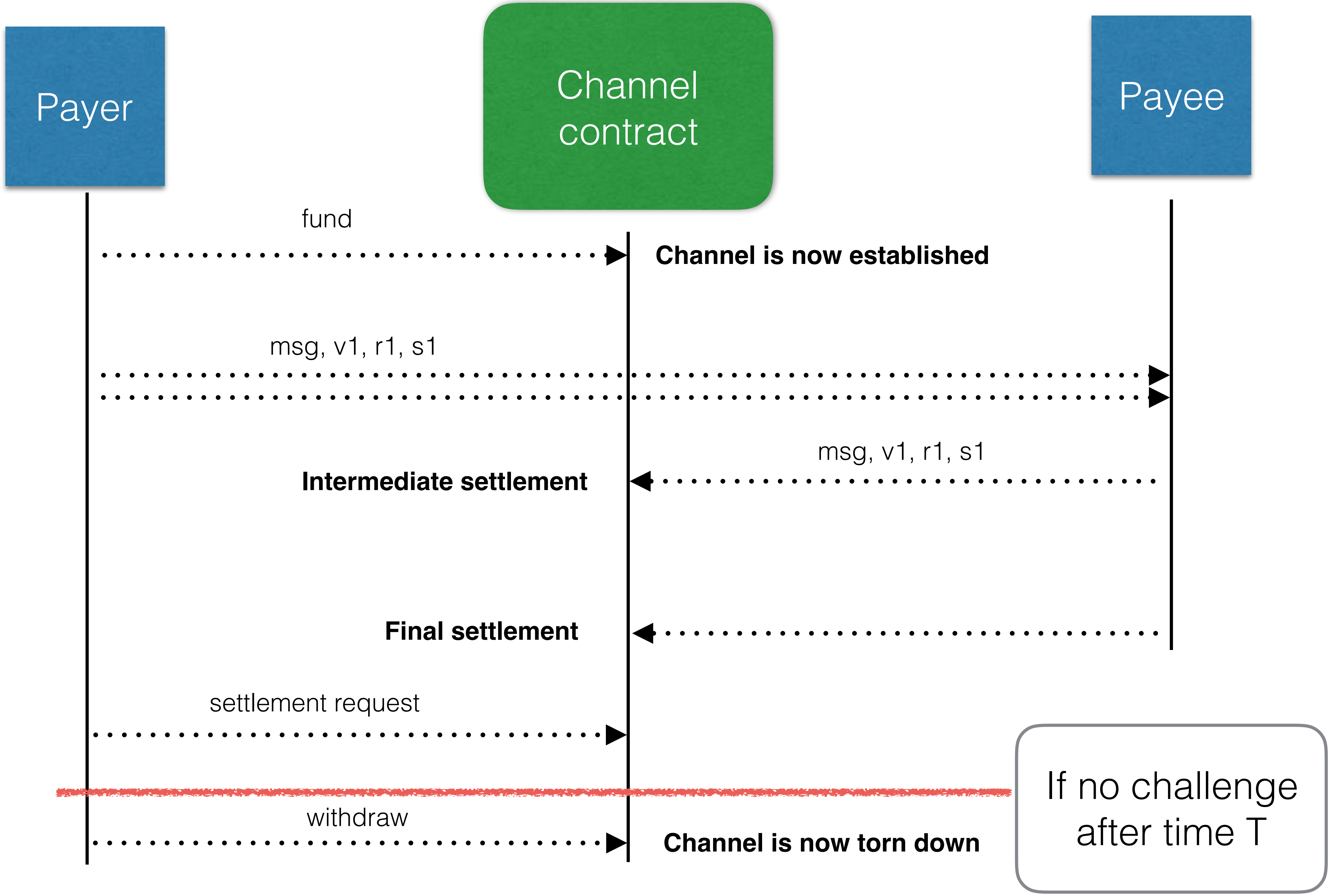
- There are no “half-signed” transactions in Ethereum

- Keeping signed transaction “off-chain” is not safe, sender can always rescind by re-using the nonce

- Solution - “synthetic multisig”

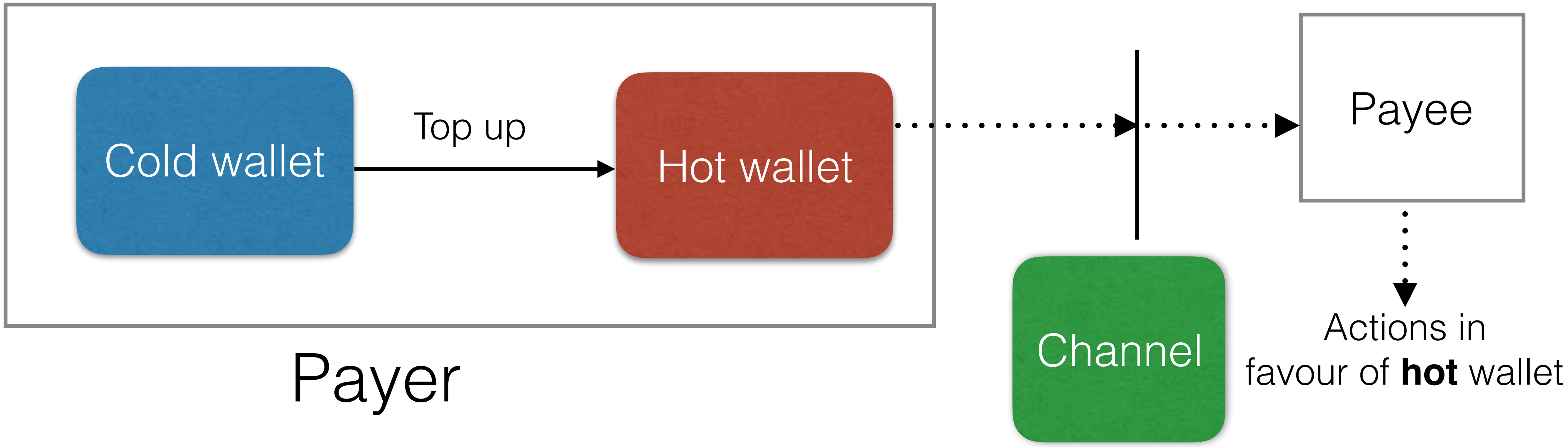
```
address payer;
address payee;

function settle(bytes32 msg, bytes32 hash, uint8 v, bytes32 r, bytes32 s) {
  require(sha3(msg) == hash);
  require(ecrecover(hash, v, r, s) == payer && msg.sender == payee);
  // Parse “msg” and split the funding deposit between payer and payee
}
```

Payment channel - Ethereum



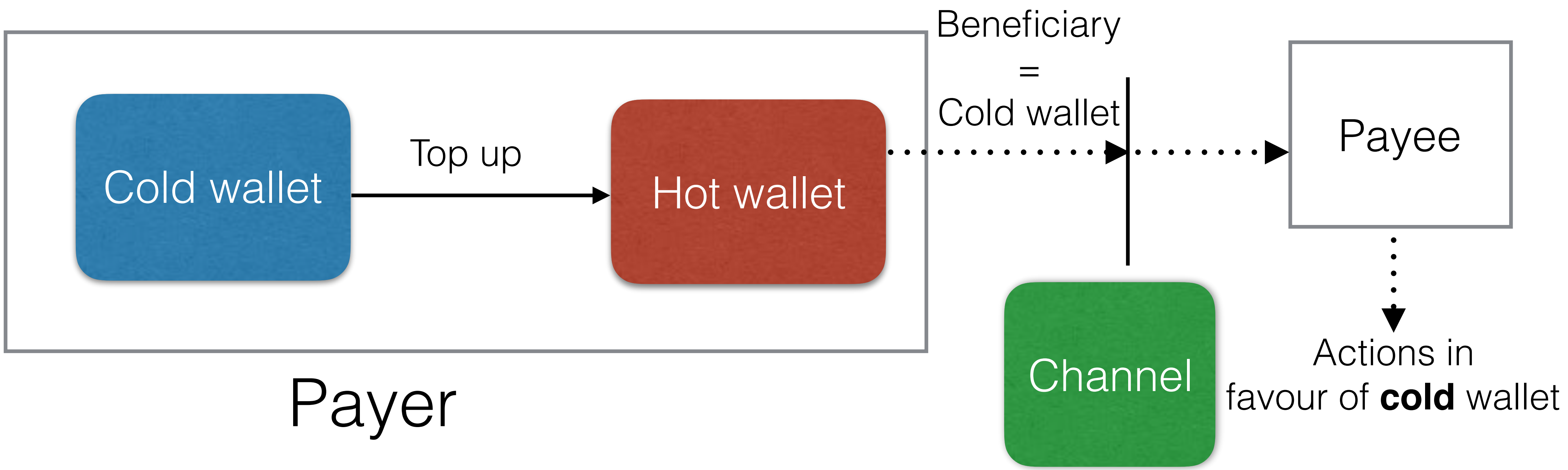
Downsides of the channels

- Established channel lock up payer's funds, once per payee
- Each channel requires at least 2 on-chain transactions
- Channel relies on an online (hot) wallet with access to private key



Hot wallet problem - two possible solutions

- Channel to have an extra attribute - beneficiary address



Hot wallet problem - two possible solutions

- Cold wallet used to pre-generate cheque book of granular payments

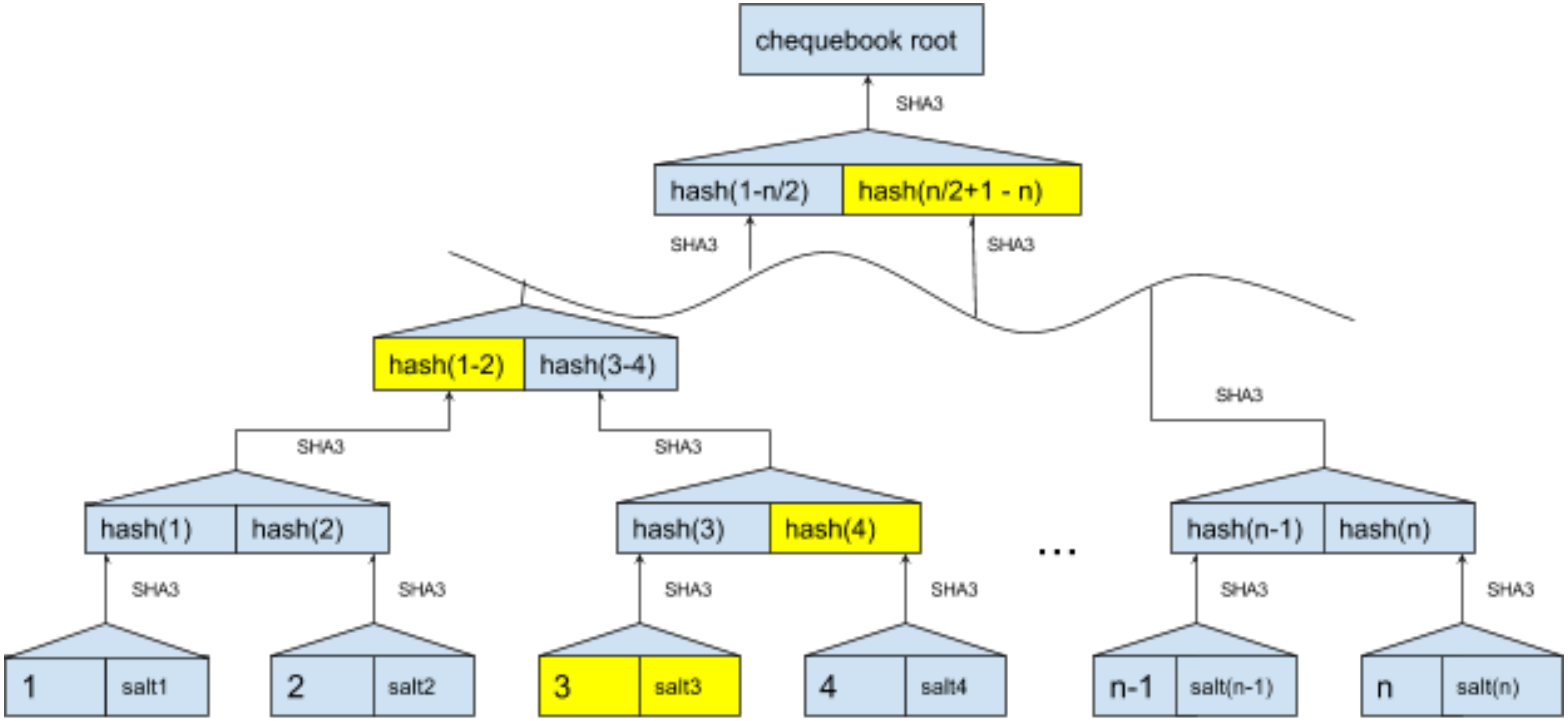
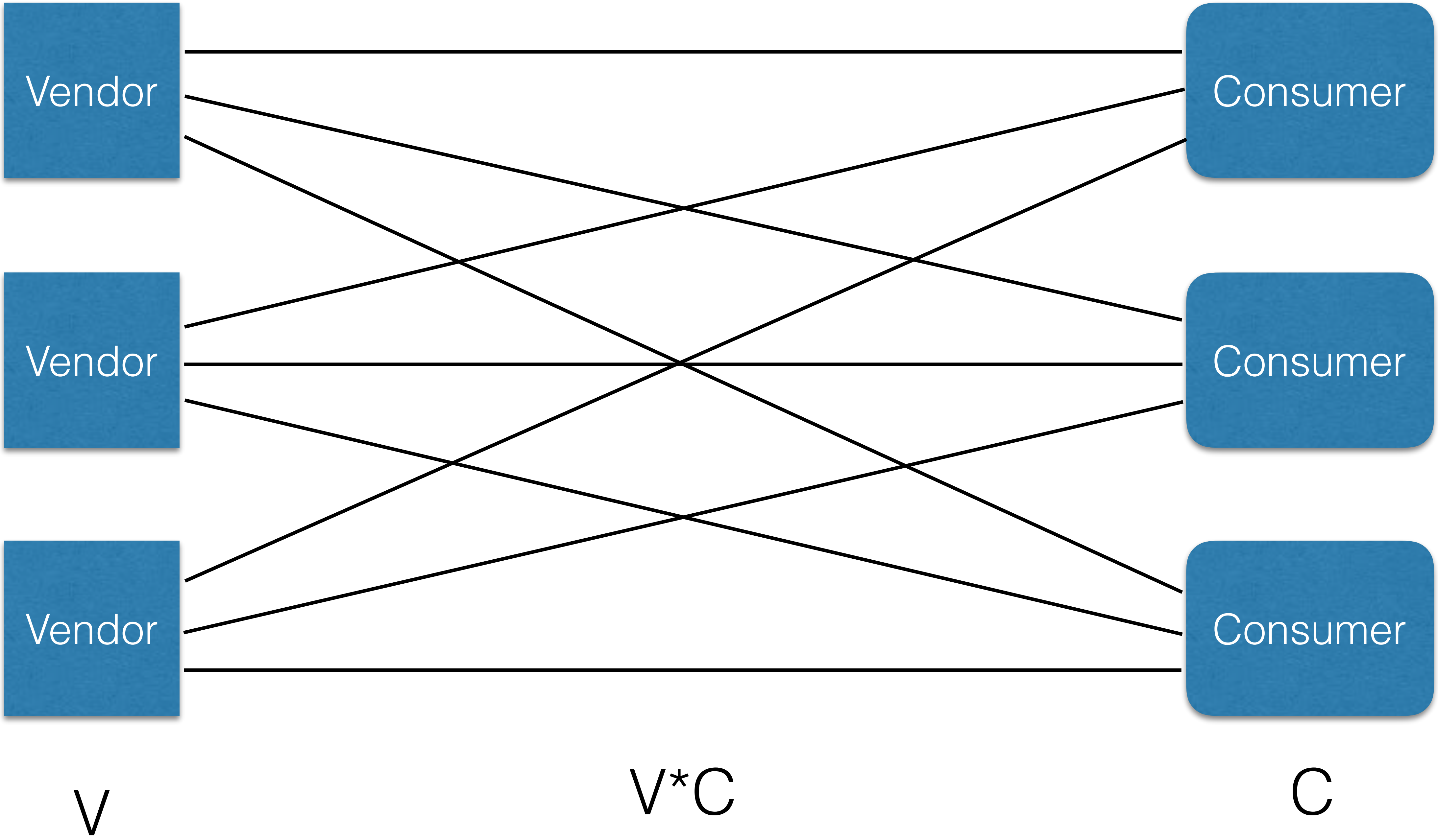
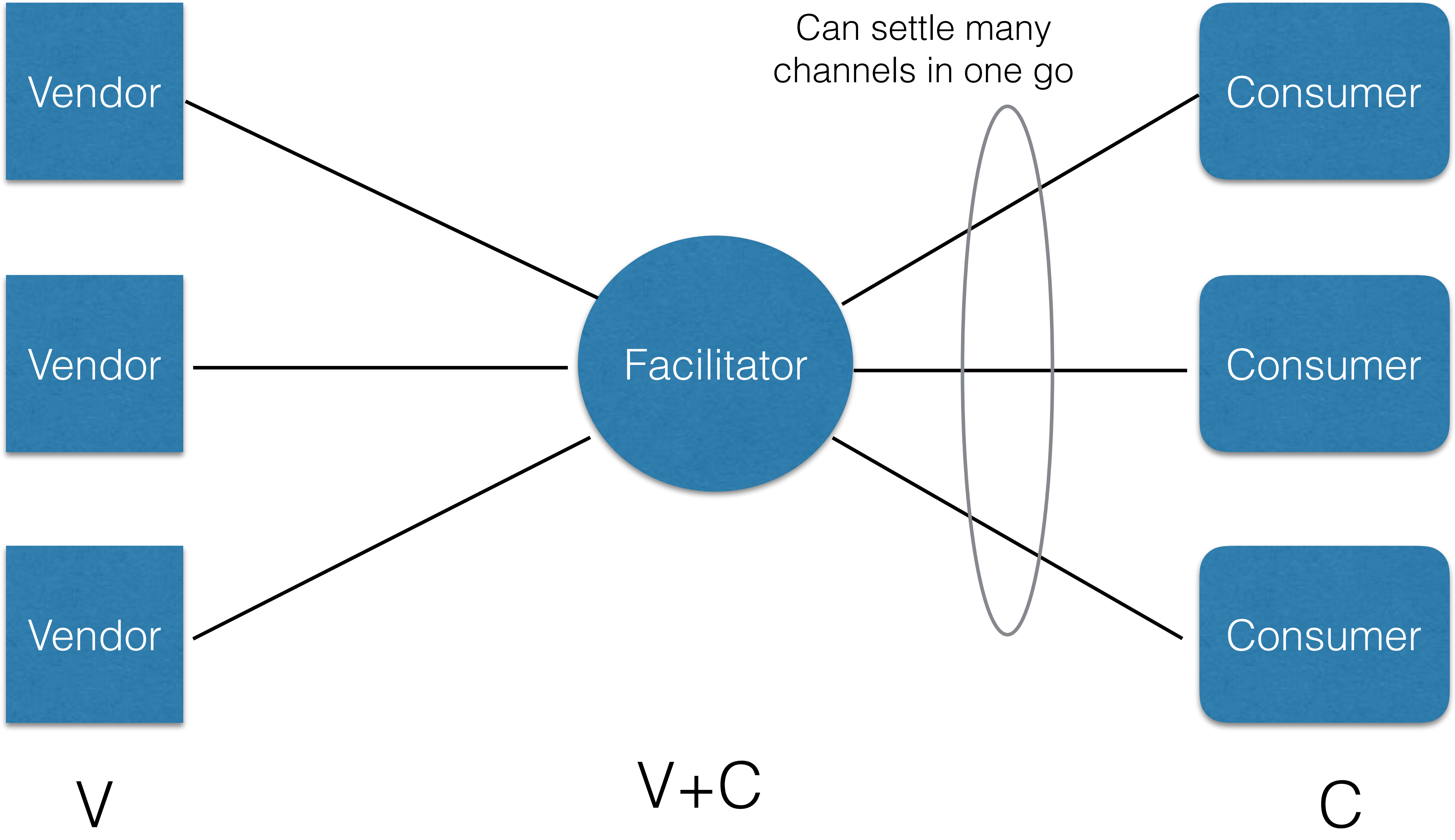


Figure 1: Construction of a Merkle tree chequebook

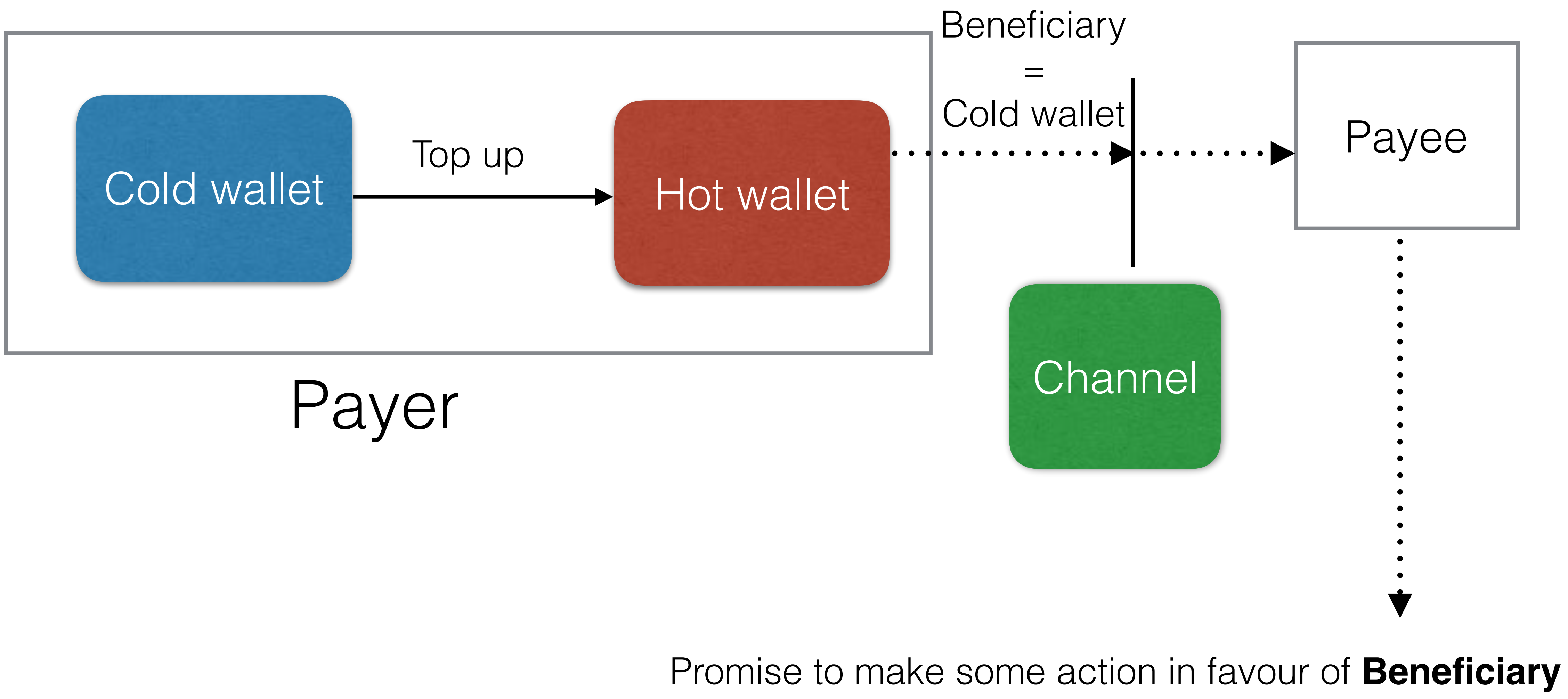
“Too many channels” problem



Optimisation - intermediary

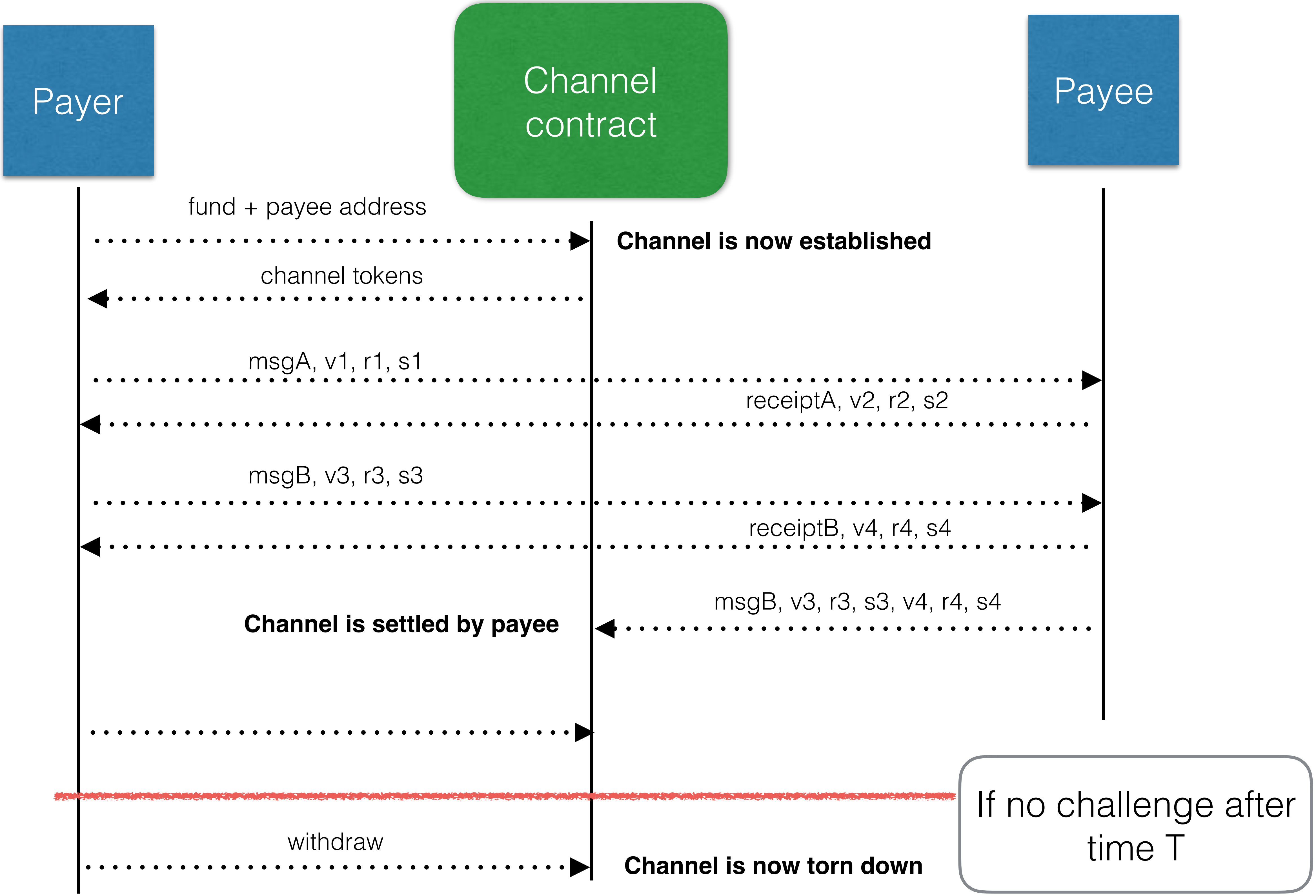


What does payee do in return for payment?



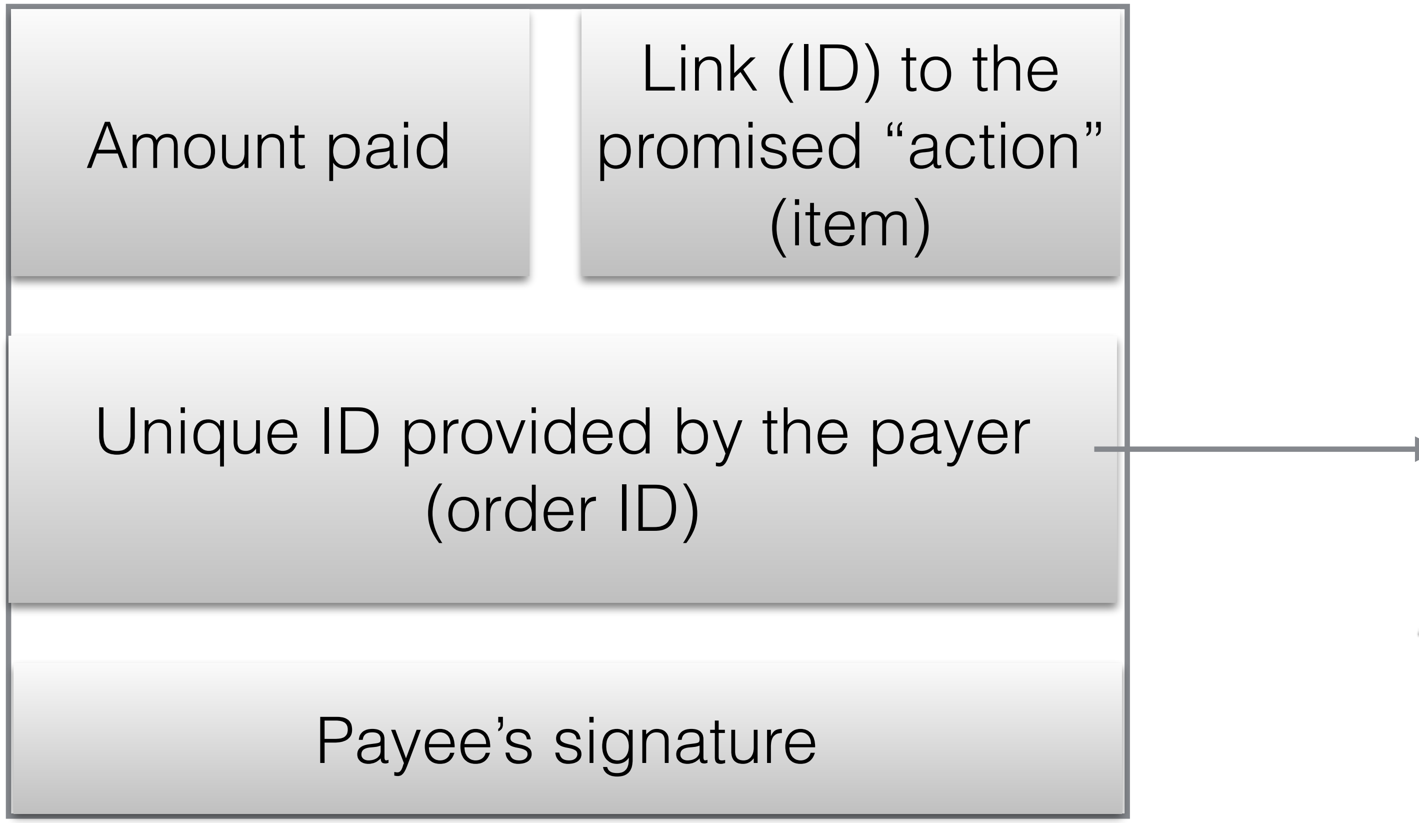
Promise to make some action in favour of **Beneficiary**

Receipts



Payer
Channel contract
Payee
fund + payee address
Channel is now established
channel tokens
msgA, v1, r1, s1
receiptA, v2, r2, s2
msgB, v3, r3, s3
receiptB, v4, r4, s4
msgB, v3, r3, s3, v4, r4, s4
Channel is settled by payee
If no challenge after time T
withdraw
Channel is now torn down

Properties of a receipts



Amount paid

Link (ID) to the promised “action” (item)

Unique ID provided by the payer (order ID)

Payee’s signature

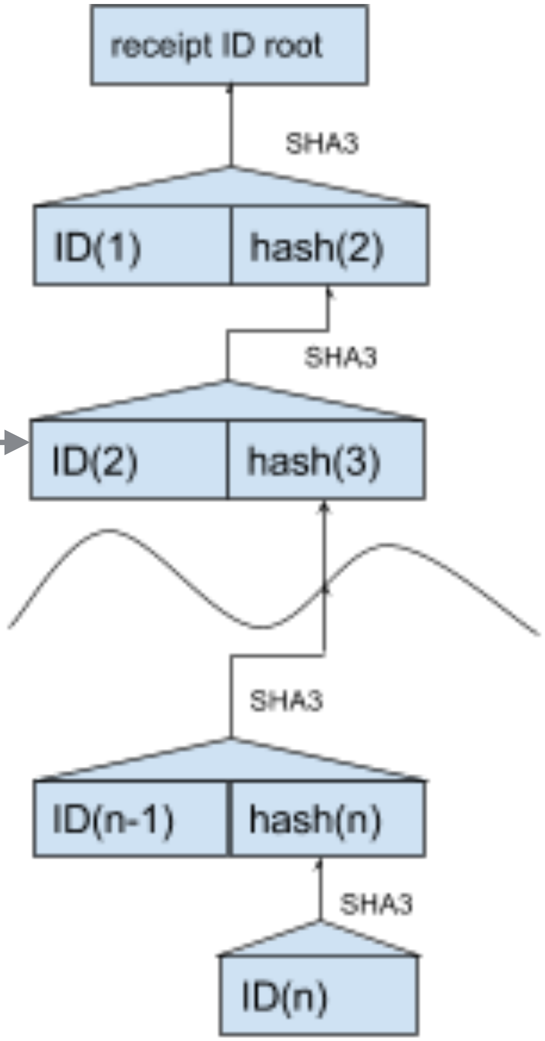


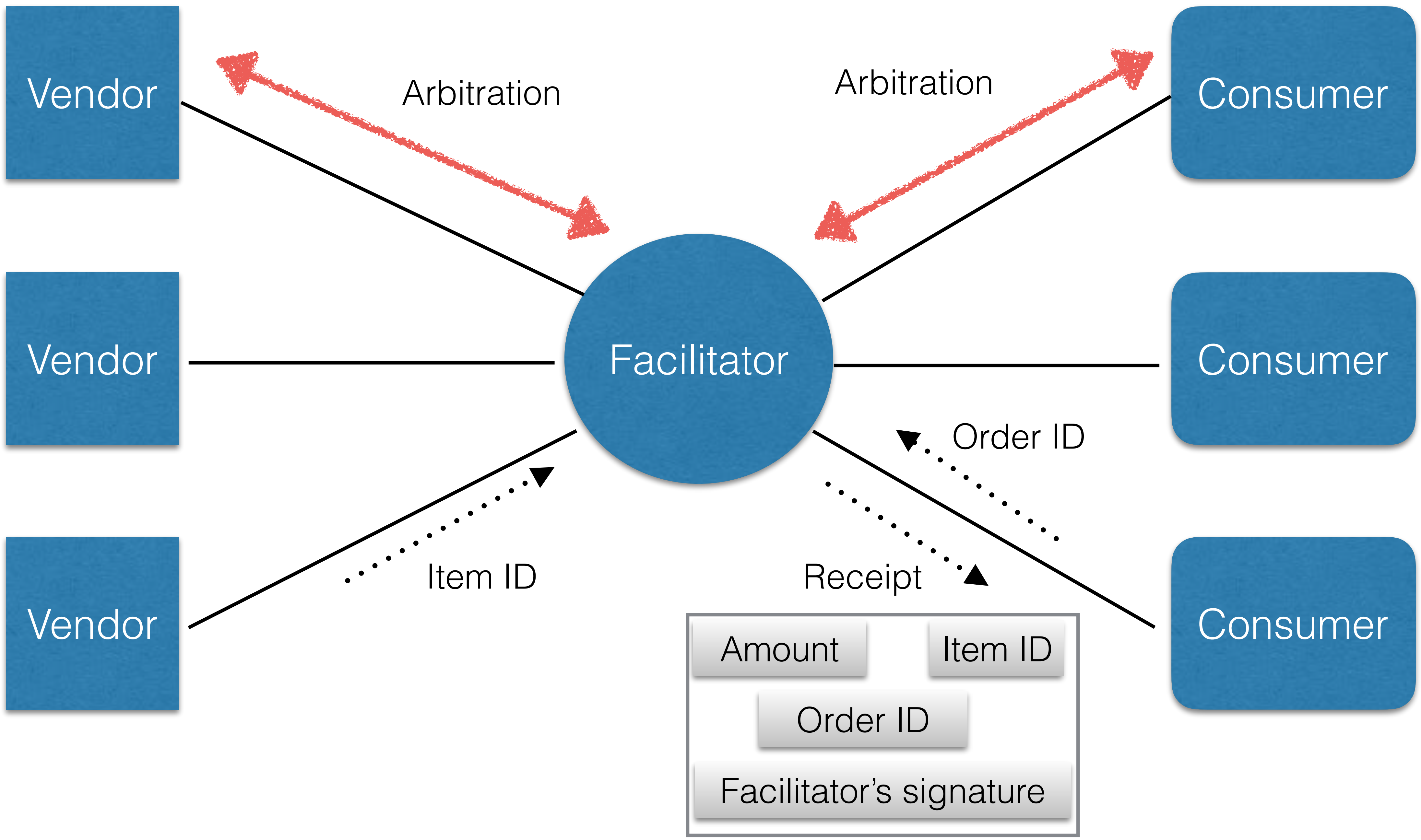
Figure 2: Construction of a receipt ID hash chain

Two possible flows

- Receipt given after payment. Payer never reveals the next order ID without getting receipt for a previous item.

- Payment given after receipt. Payee never gives the next receipt without payment for the previous item. Payer can refuse to pay if the receipt is for an item she did not want

Facilitator's roles


Vendor
Vendor
Vendor
Arbitration
Arbitration
Consumer
Consumer
Consumer
Facilitator
Order ID
Item ID
Receipt
Amount
Item ID
Order ID
Facilitator's signature