BOLT: Booster of Ledger Technology

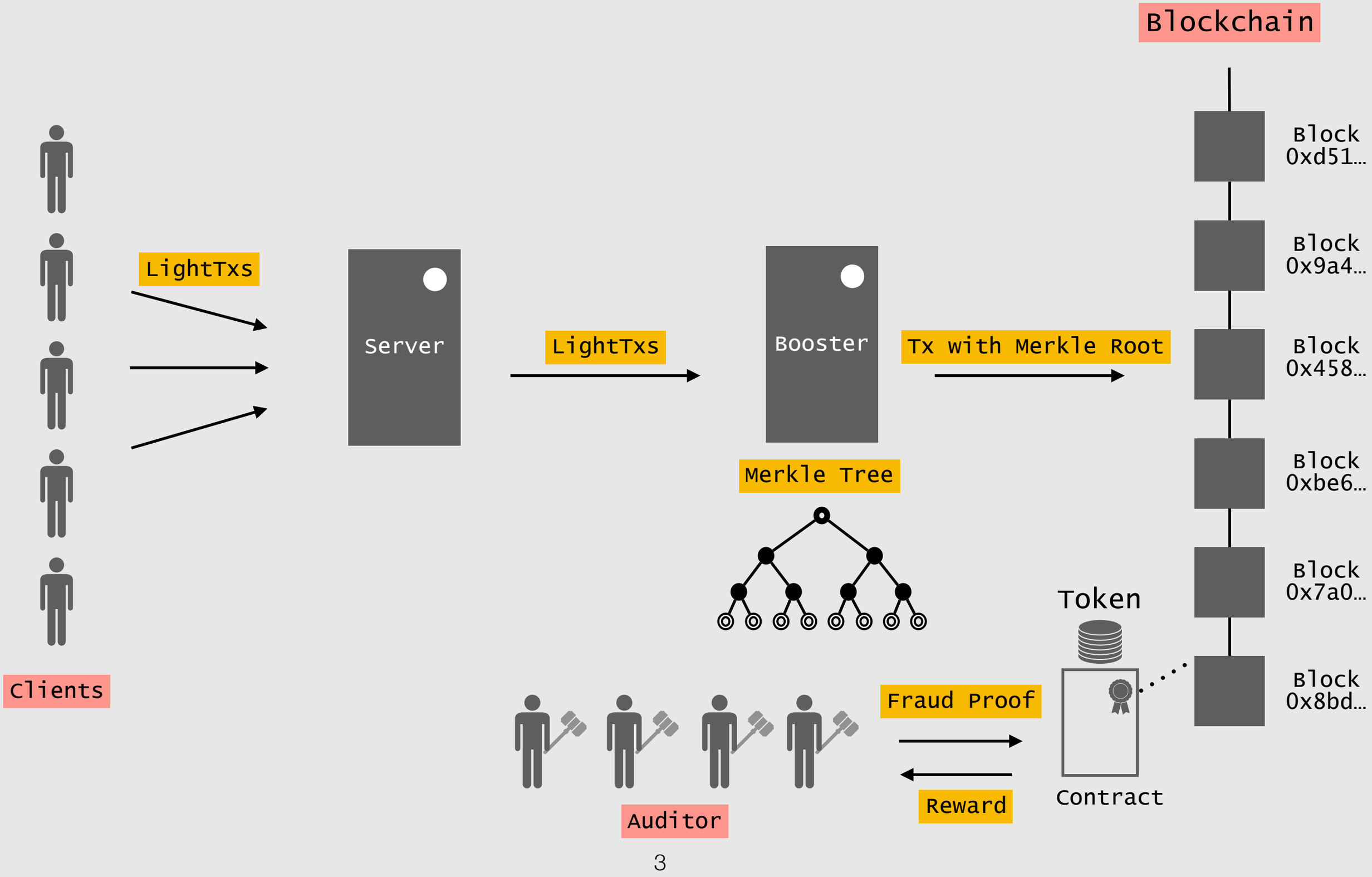
@juinc davidjuin0519@gmail.com
@jerry-jheng jerry128371@gmail.com

BOLT.infinitechain.io

Outline

- Overview
- Is BOLT Secure?
- Game, Court and Fraud Proof
- Architecture
- Protocol
- Demo

Architecture: Concept

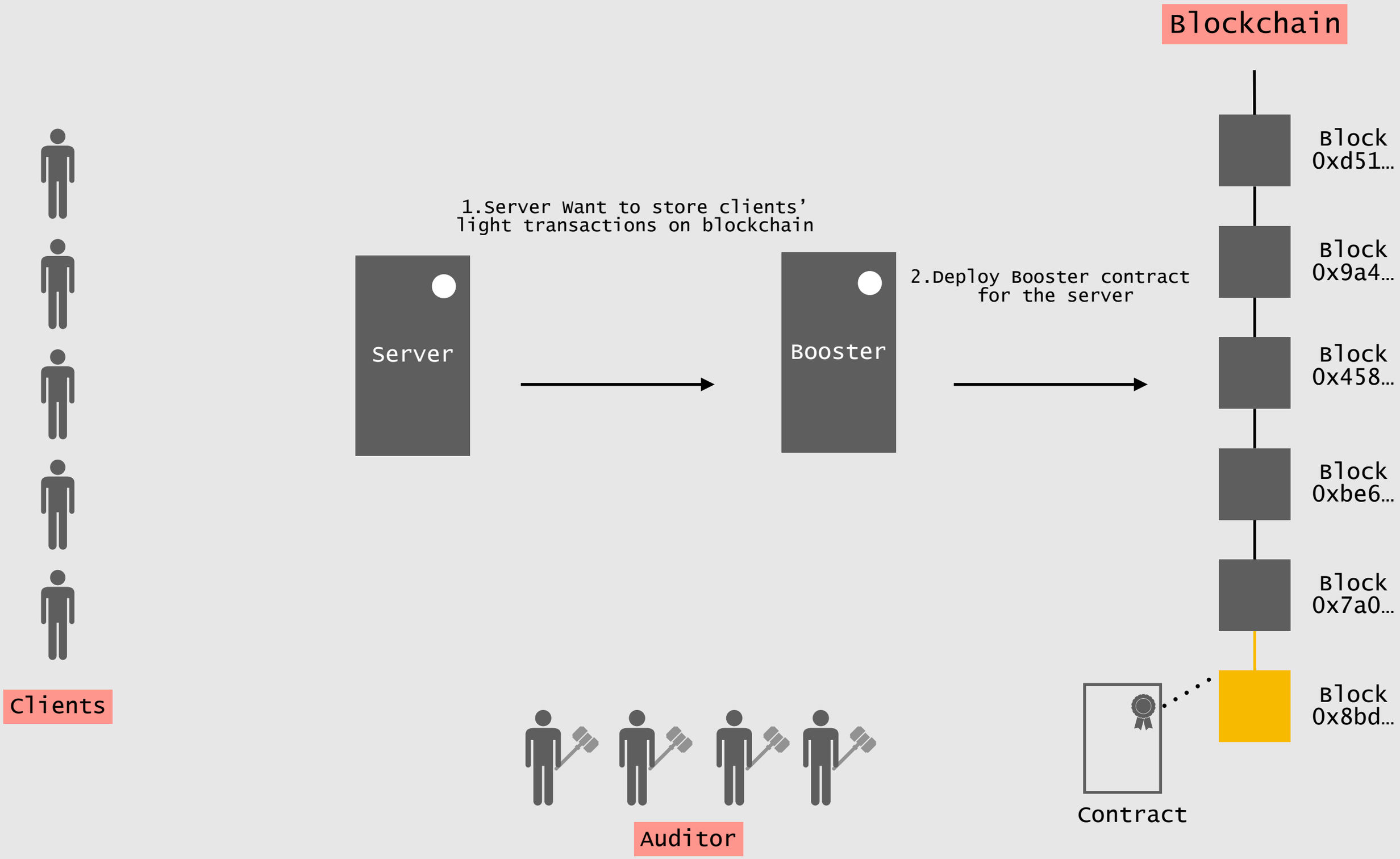


Architecture: Light Transaction

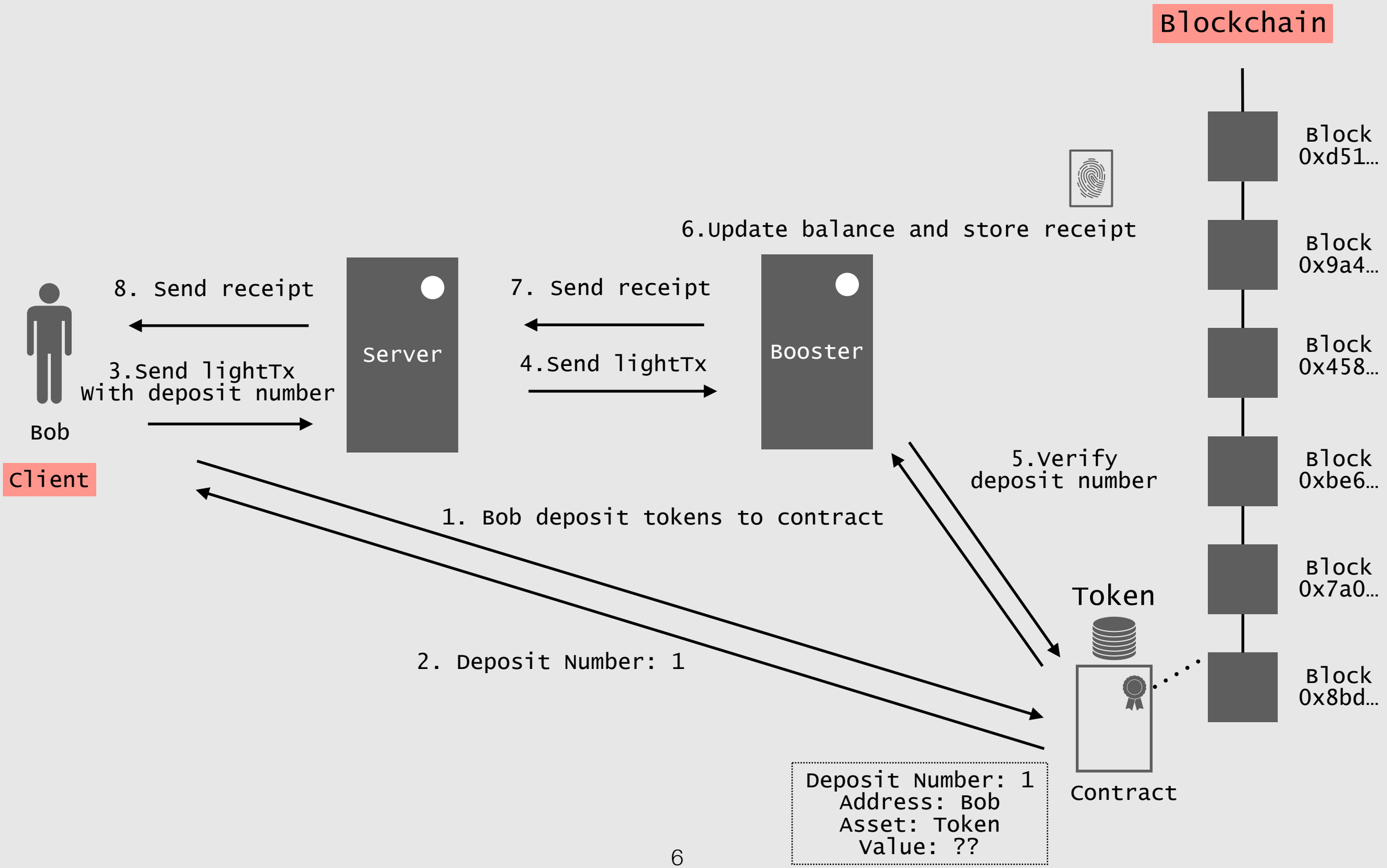
Light Transaction Type:

- Deposit
- Remittance
- Withdrawal

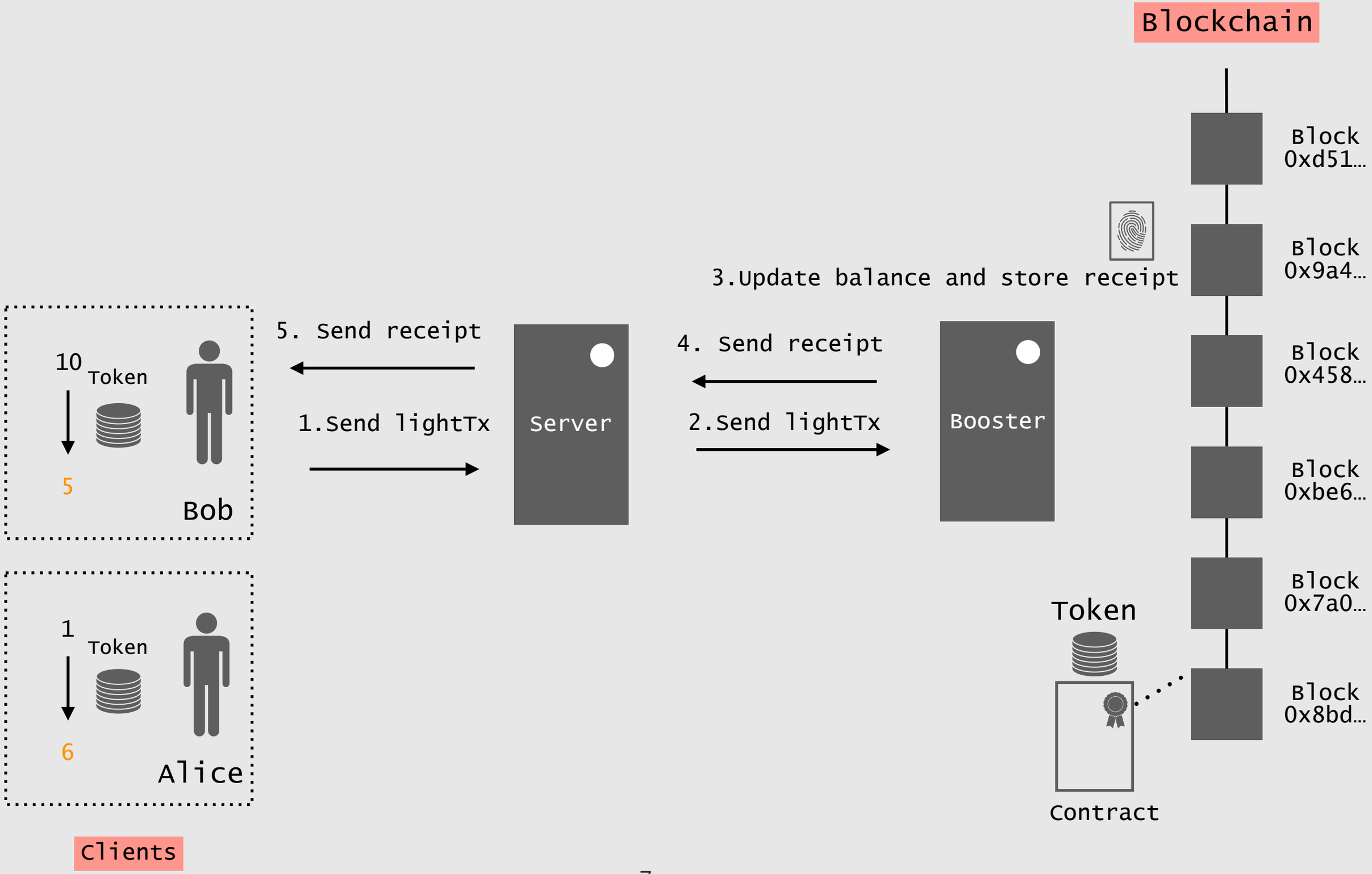
Protocol: 0


Blockchain
1.Server Want to store clients'
light transactions on blockchain
Server
Booster
2.Deploy Booster contract
for the server
Block
0xd51…
Block
0x9a4…
Block
0x458…
Block
0xbe6…
Block
0x7a0…
Block
0x8bd…
Clients
Auditor
Contract

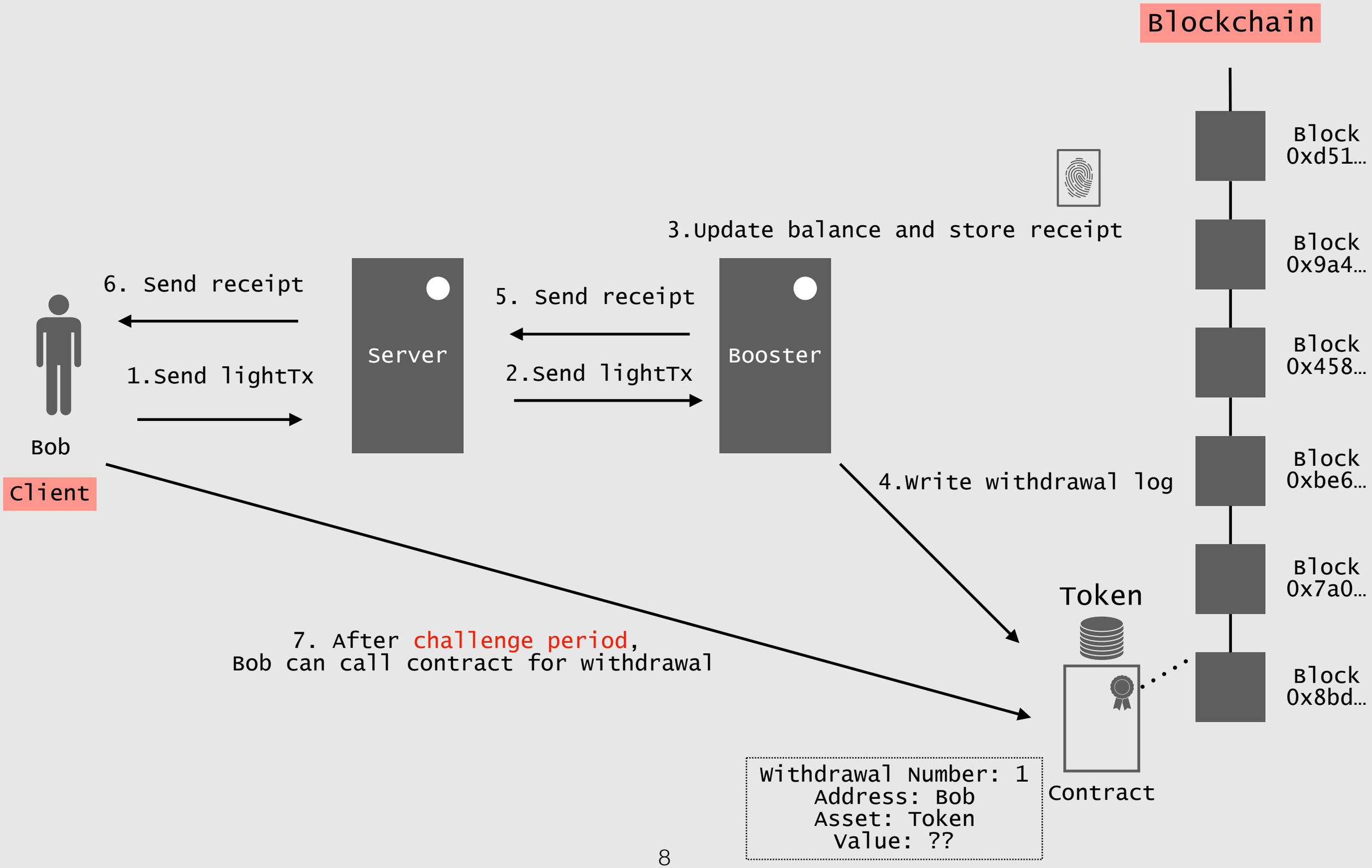
Protocol: Deposit



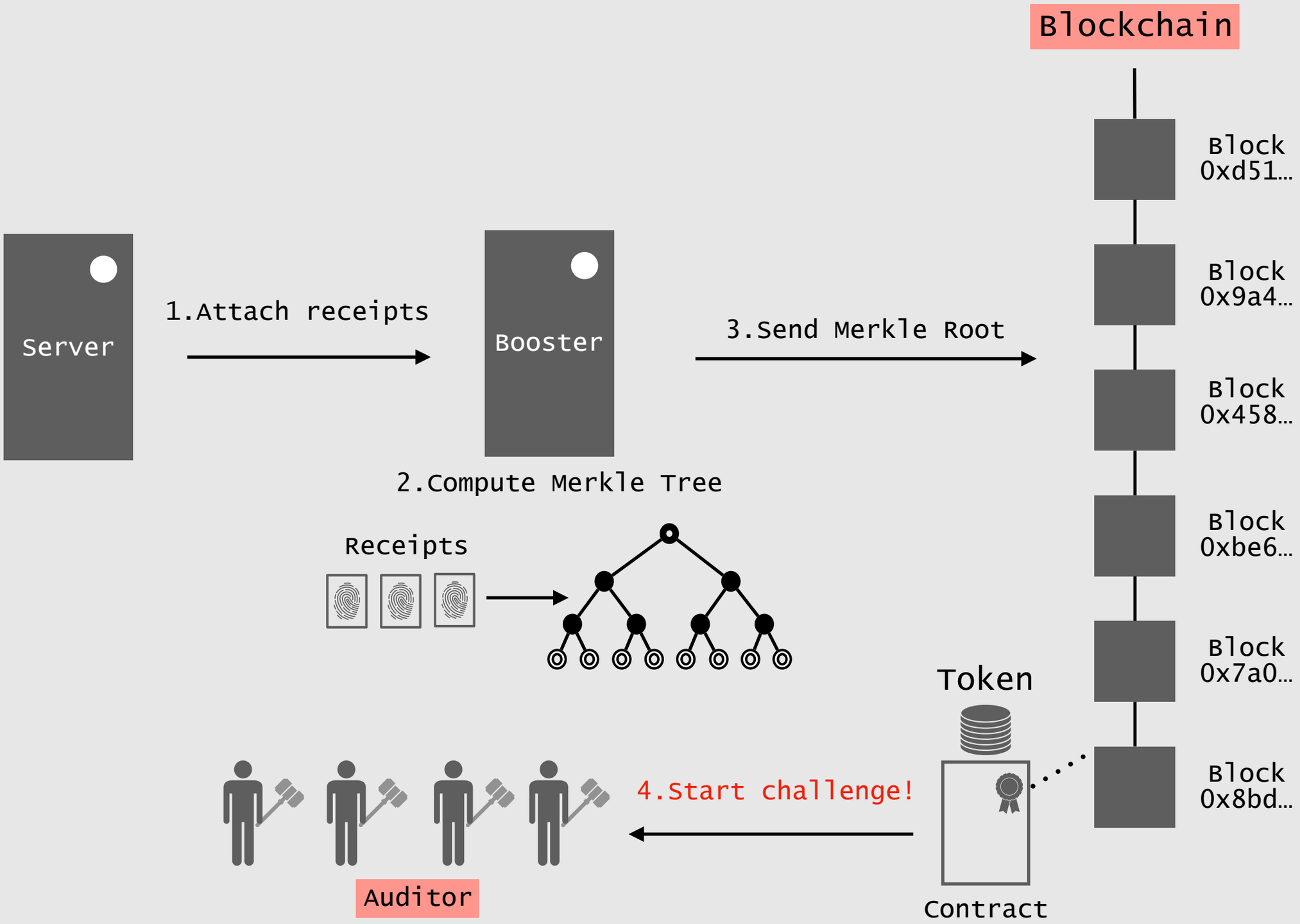
Protocol: Remittance



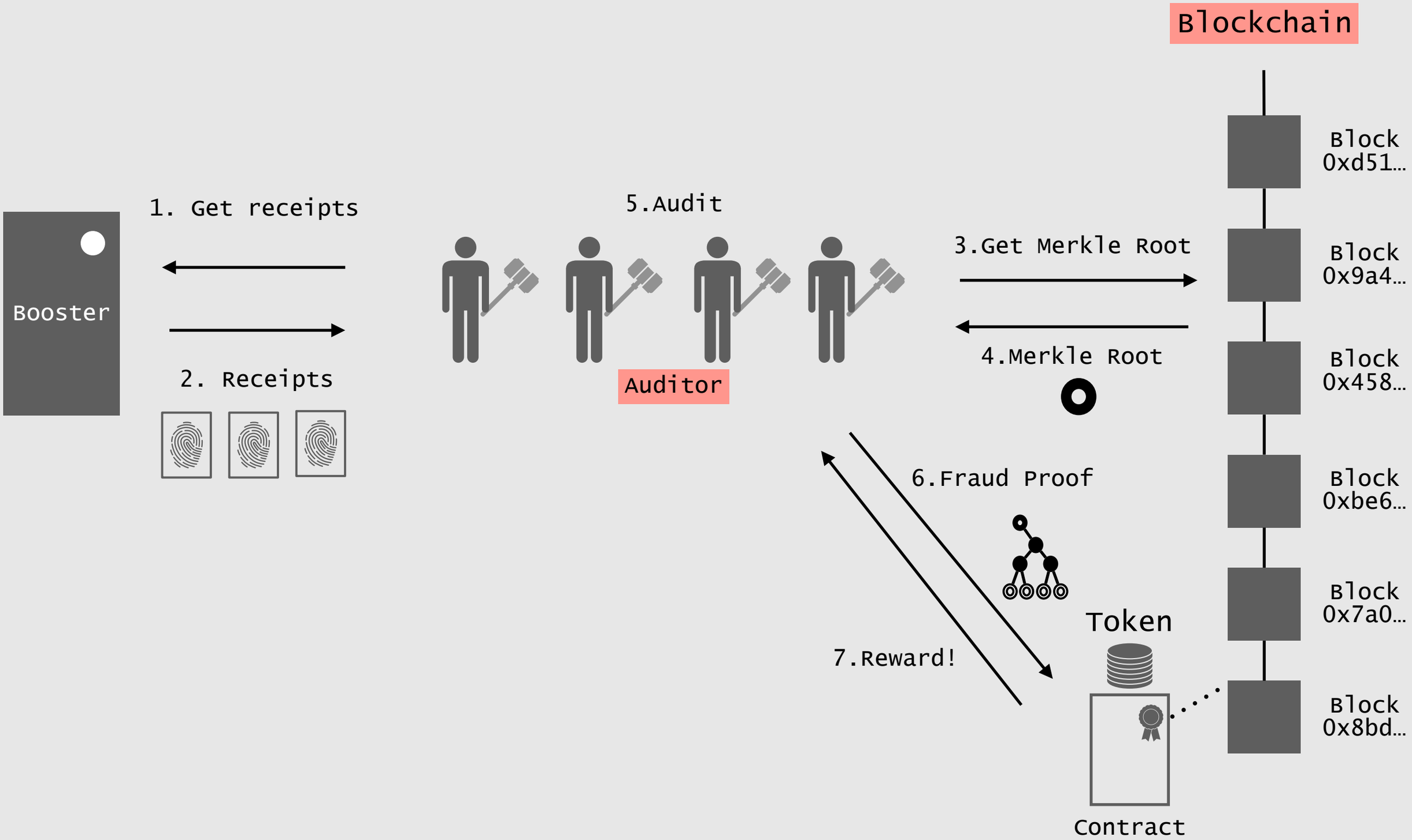
Protocol: Withdrawal



Protocol: Challenge Start



Protocol: Challenge Period



Protocol: Fraud Type

- Proof of existence
- Repeated GSN
- Skipped GSN
- Wrong balance status

Protocol: Light Transaction and Receipt

Client

```
lightTxData = {
   from,
   to,
   assetID,
   value,
   fee,
   nonce,
   logID,
   clientMetadataHash
}


sig = {
   clientLightTx
}

metadata = {
   client
}
```

Light transaction

Booster

```
lightTxData = {
   from,
   to,
   assetID,
   value,
   fee,
   nonce,
   logID,
   clientMetadataHash
}
```

```
receiptData = {
   stageHeight,
   GSN,
   lightTxHash,
   fromBalance,
   toBalance,
   serverMetadataHash
}
```

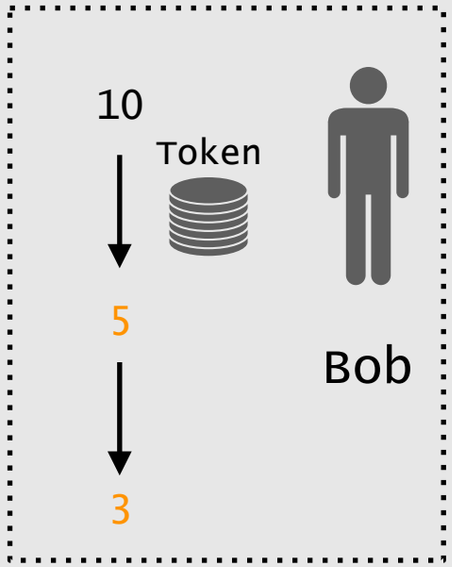
```
sig = {
   clientLightTx,
   serverLightTx,
   serverReceipt
}
```

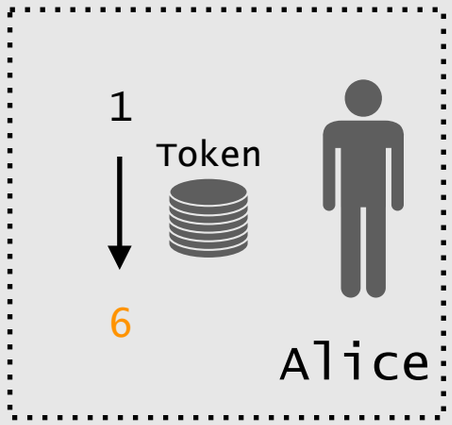
```
metadata = {
   client,
   server
}
```

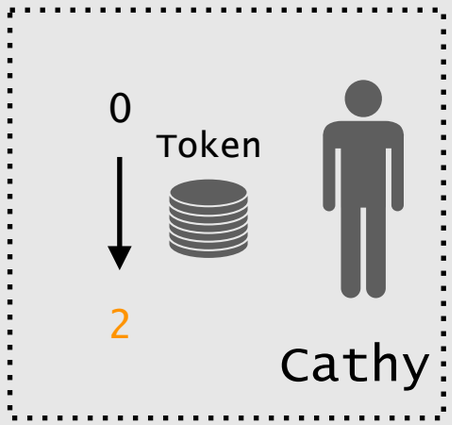
Receipt

```
receipt = {
   lightTxHash,
   lightTxData,
   receiptHash,
   receiptData,
   sig,
   metadata
}
```

Protocol: Receipt State Change







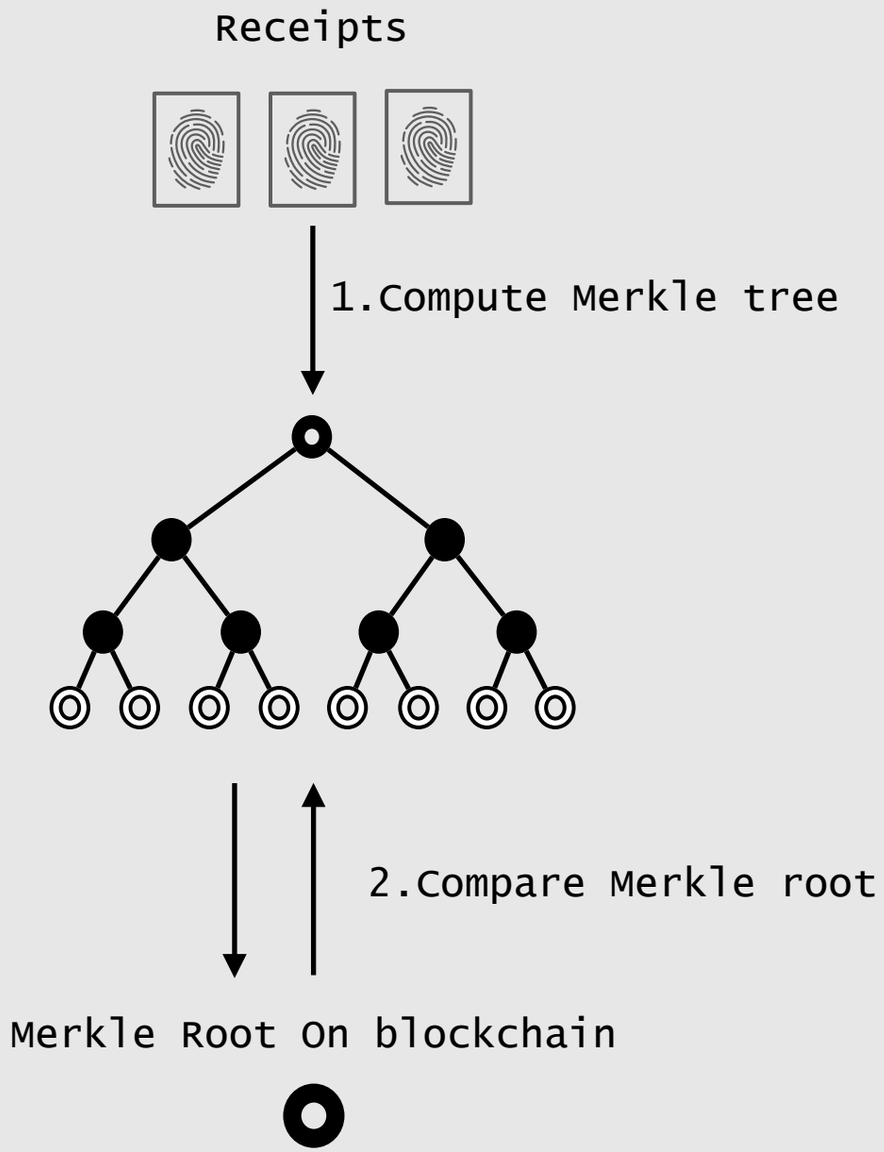
from: Bob
to: Alice
value: 5
fromBalance: 5
toBalance: 6
GSN: 1

Receipt 1

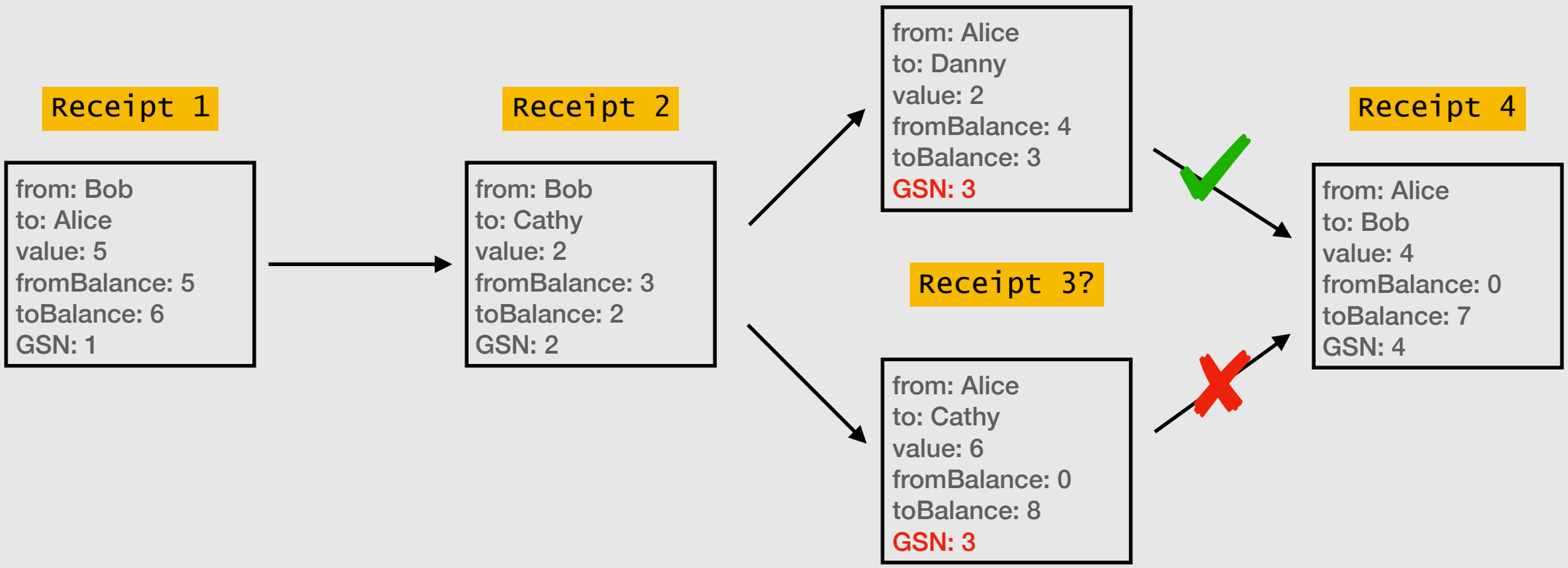
from: Bob
to: Cathy
value: 2
fromBalance: 3
toBalance: 2
GSN: 2

Receipt 2

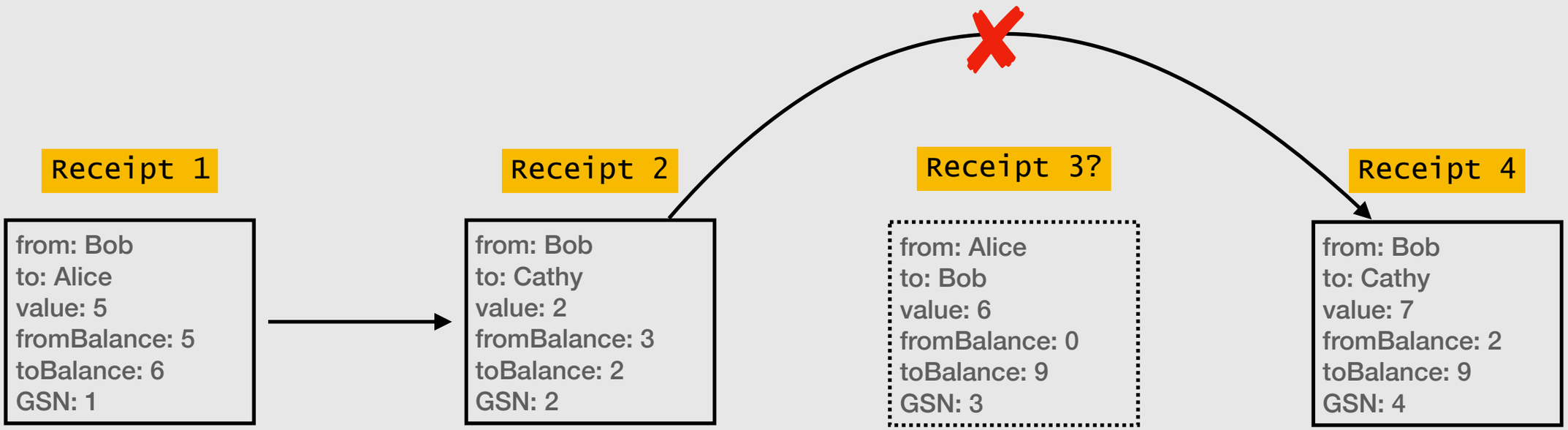
Fraud Proof: Proof of existence



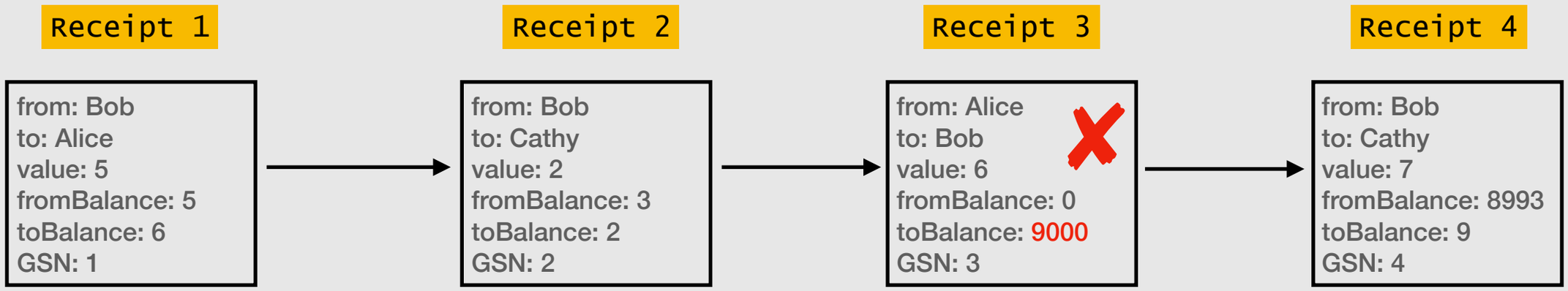
Fraud Proof: Repeated GSN



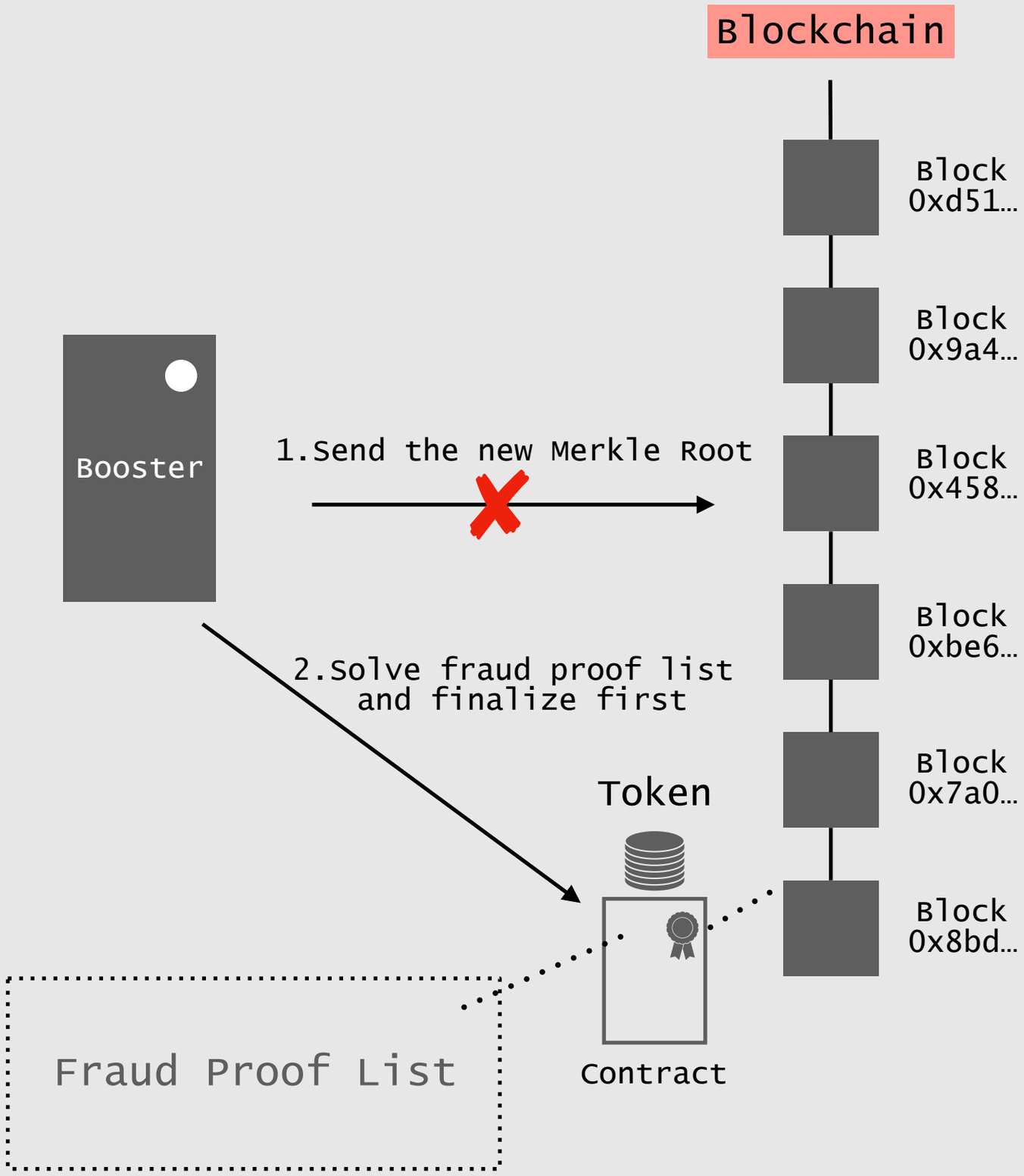
Fraud Proof: Skipped GSN



Fraud Proof: Wrong Balance Status



Protocol: Finalize



Protocol: Force Withdraw