

# BOLT: Booster of Ledger Technology

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

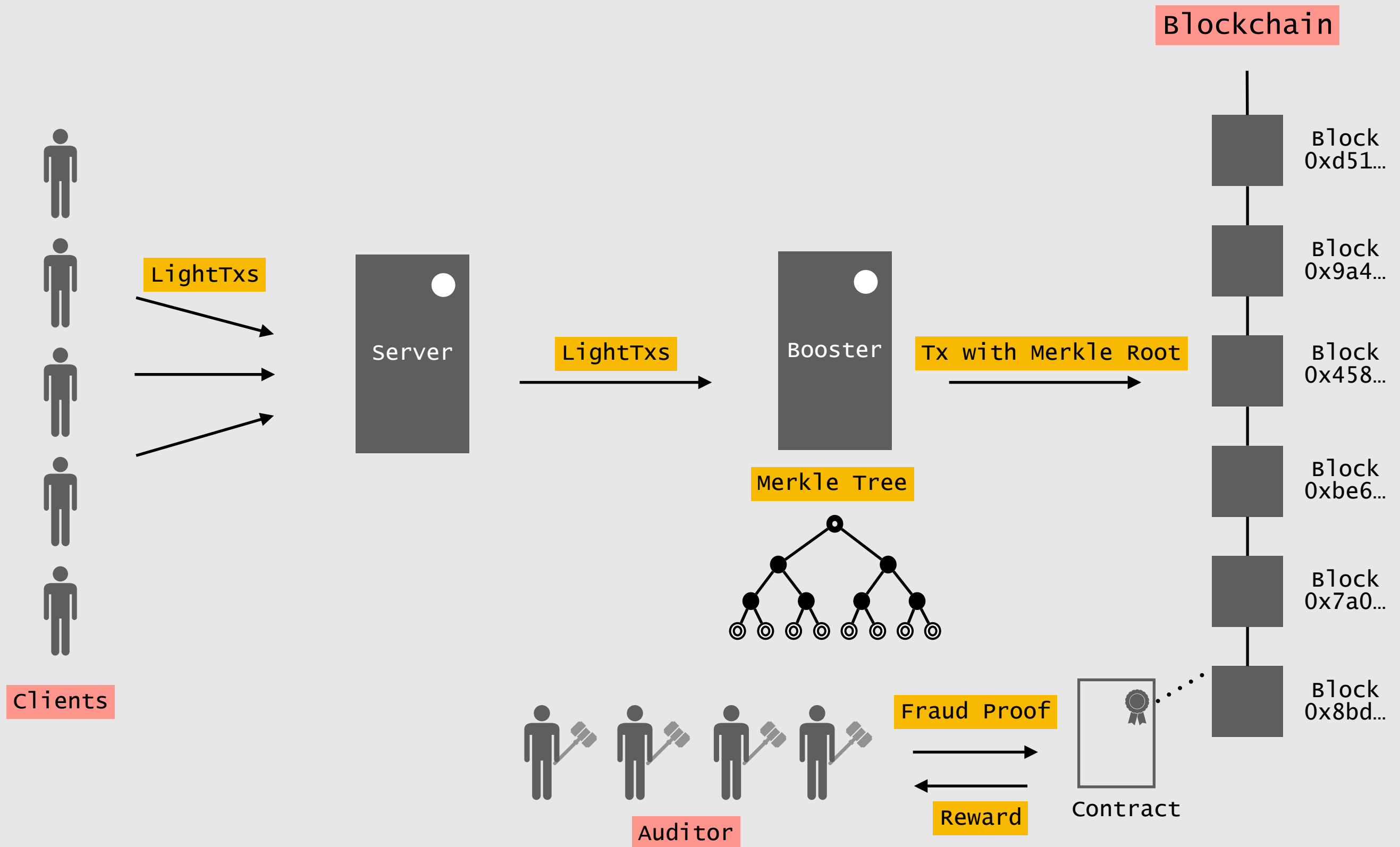


BOLT.infinitechain.io

# Outline

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

# Architecture: Concept

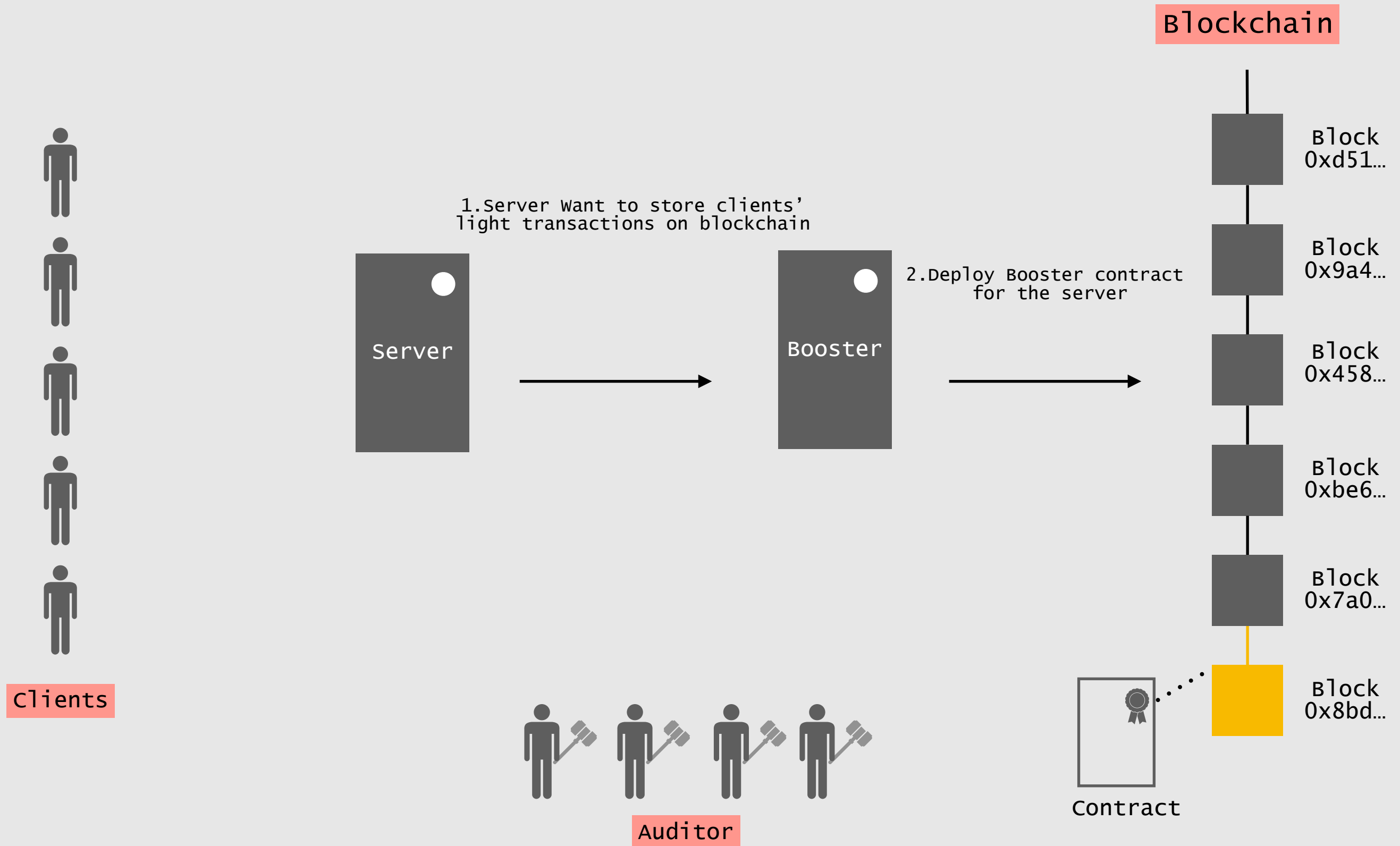


# Architecture: Light Transaction

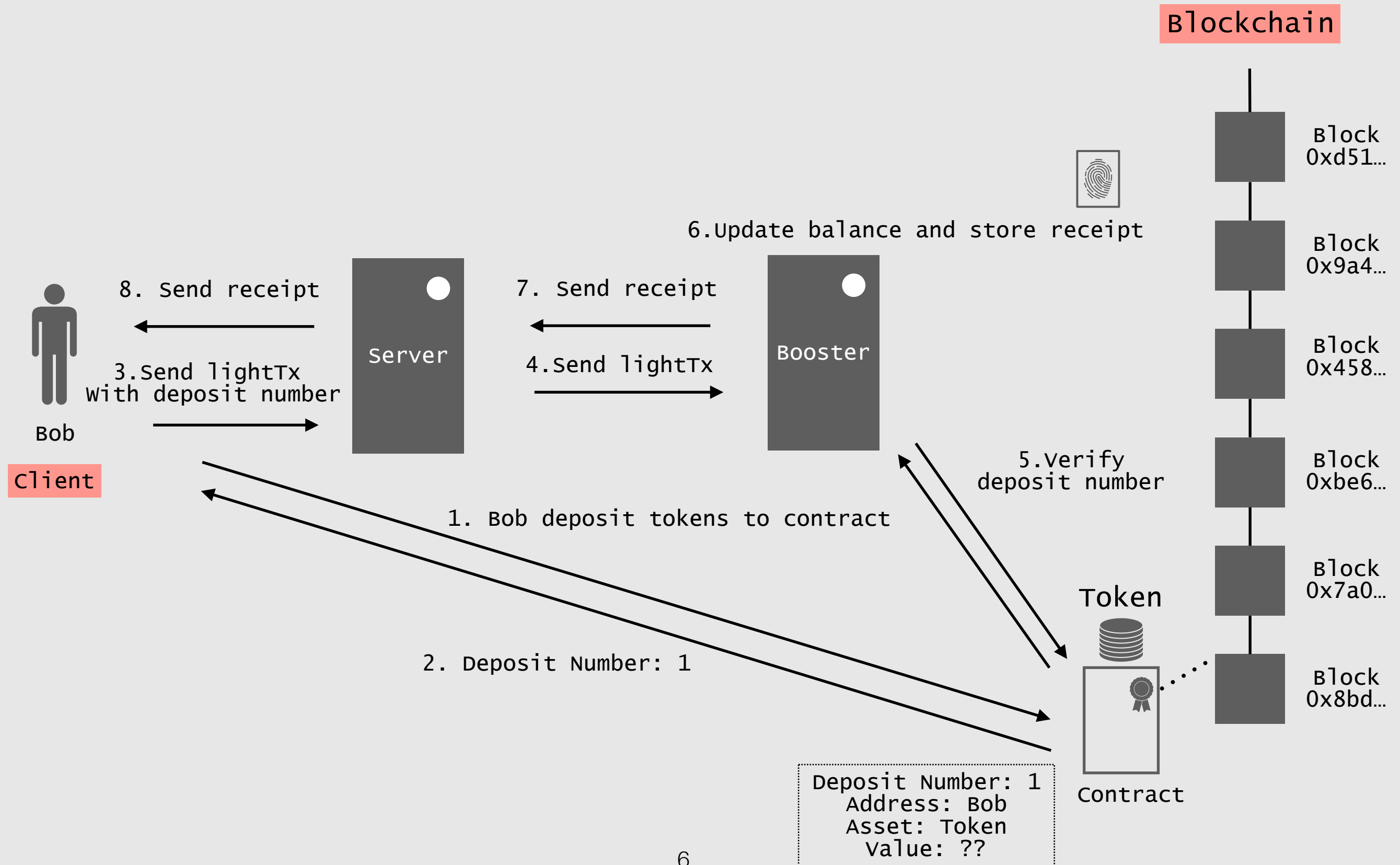
Light Transaction Type:

- ▶ Deposit
- ▶ Remittance
- ▶ withdraw

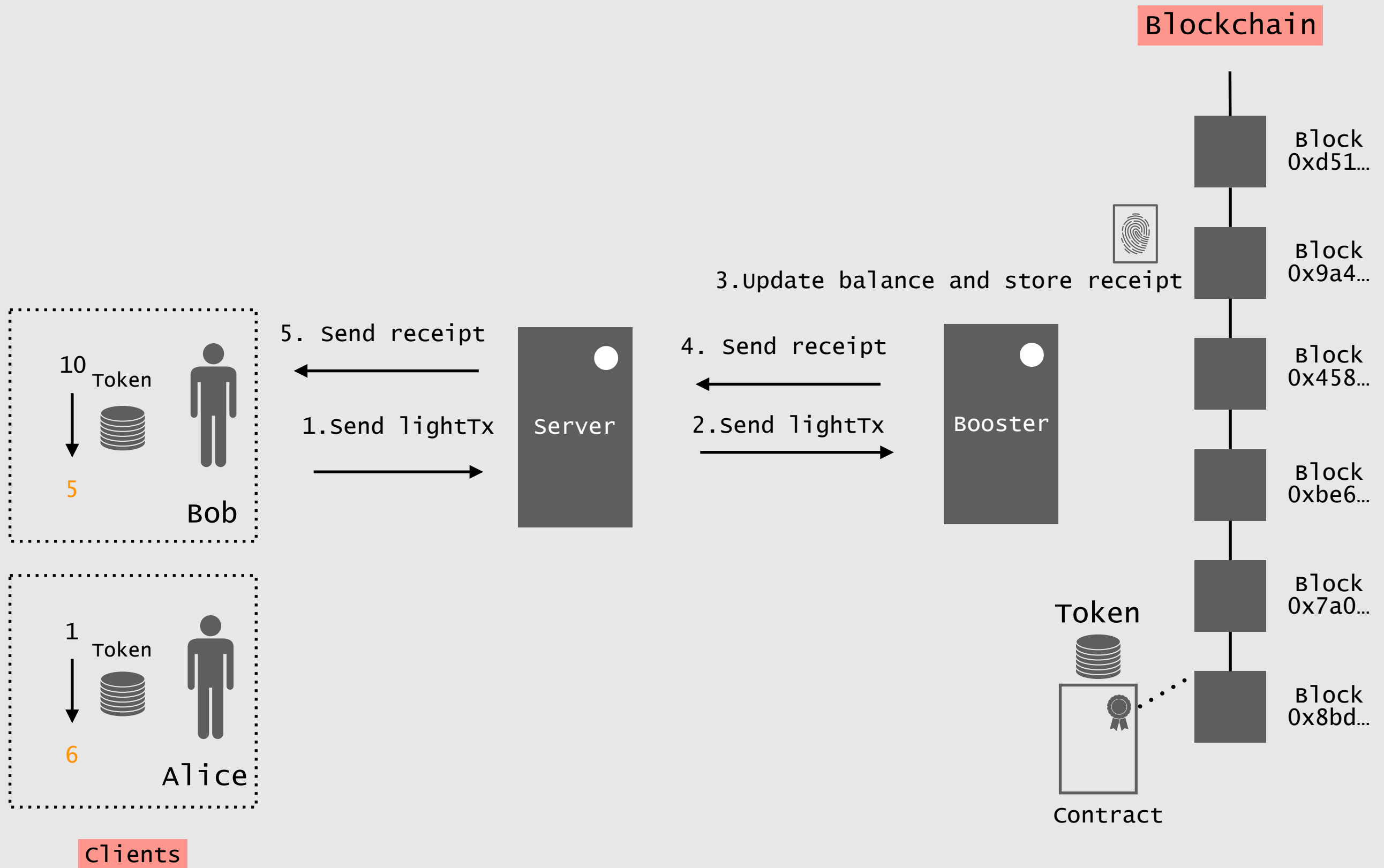
# Protocol: 0



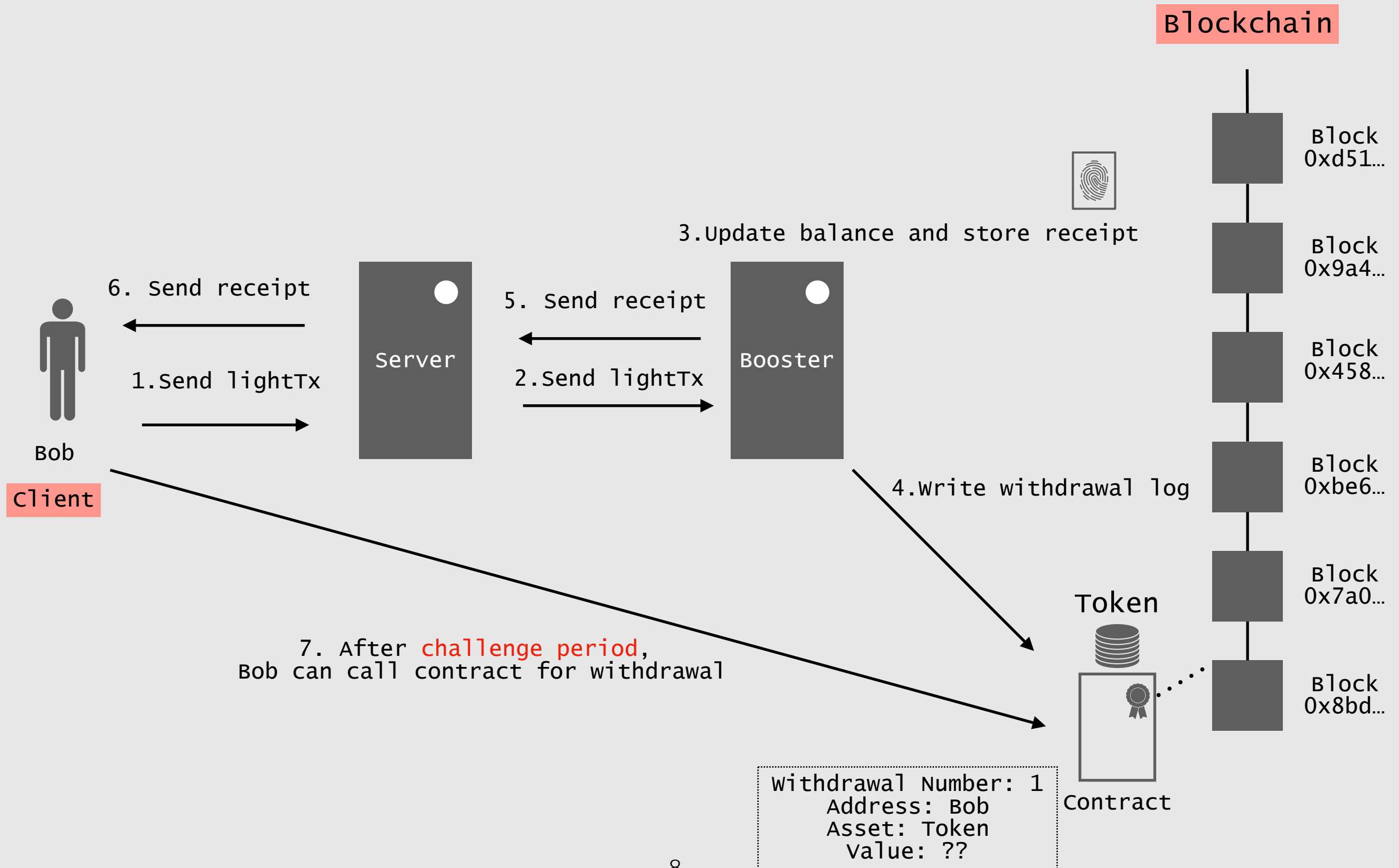
# Protocol: Deposit



# Protocol: Remittance

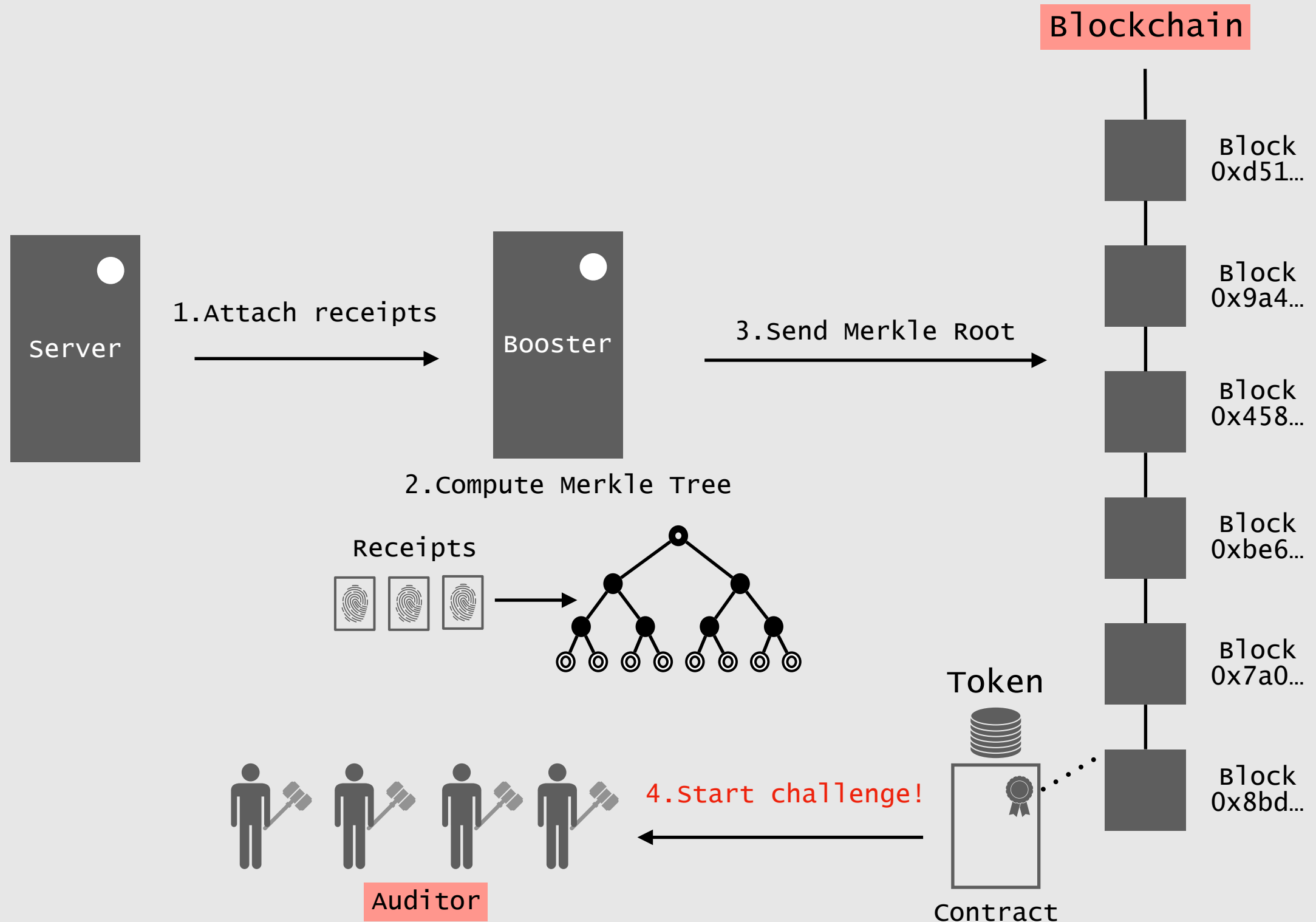


# Protocol: withdrawal

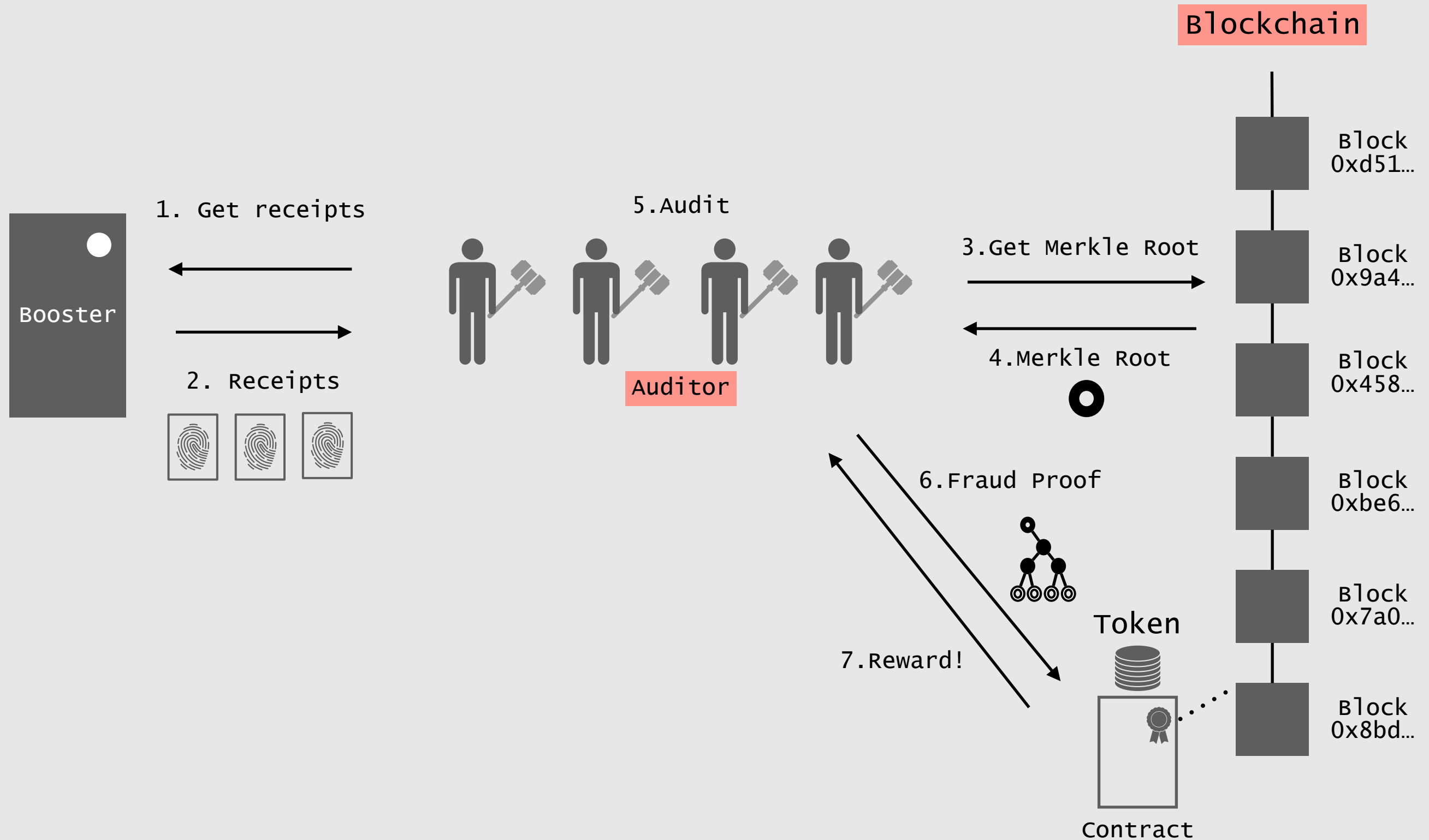




# Protocol: Challenge Start



# 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  
}
```

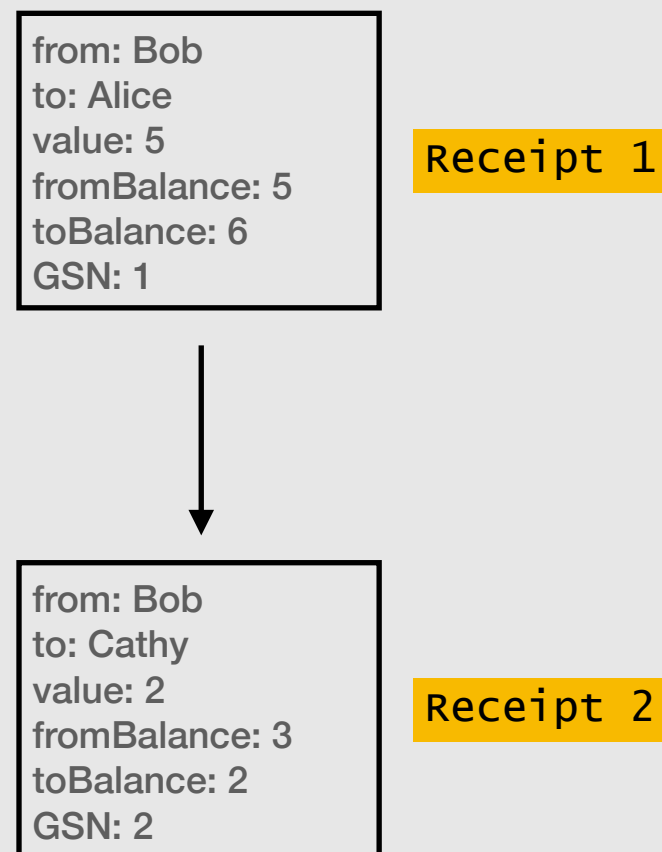
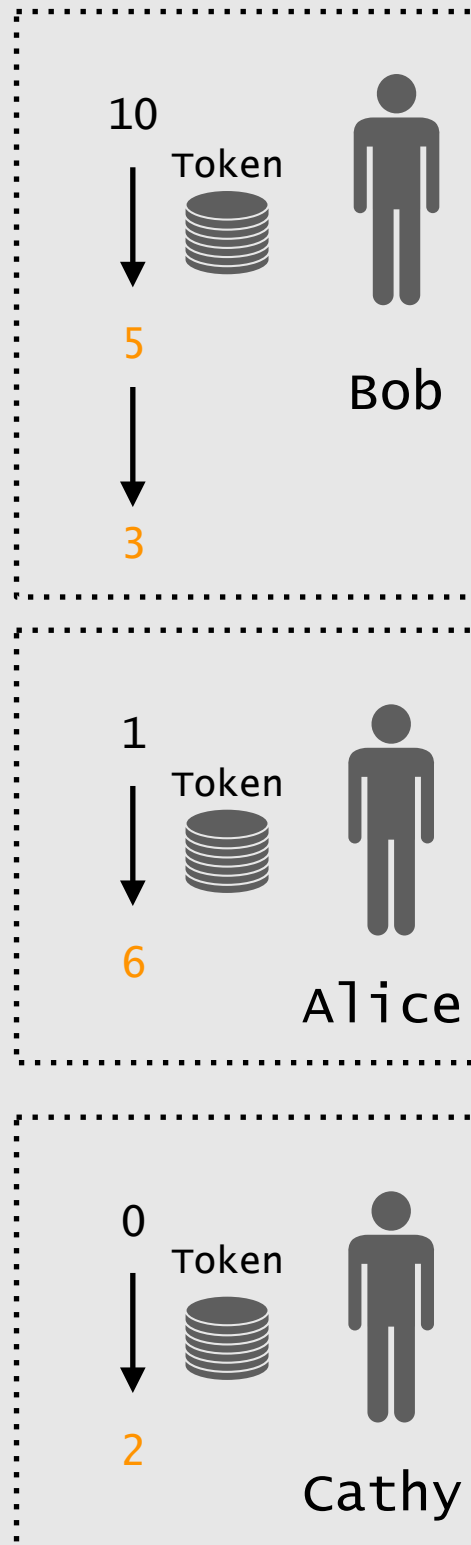
Receipt



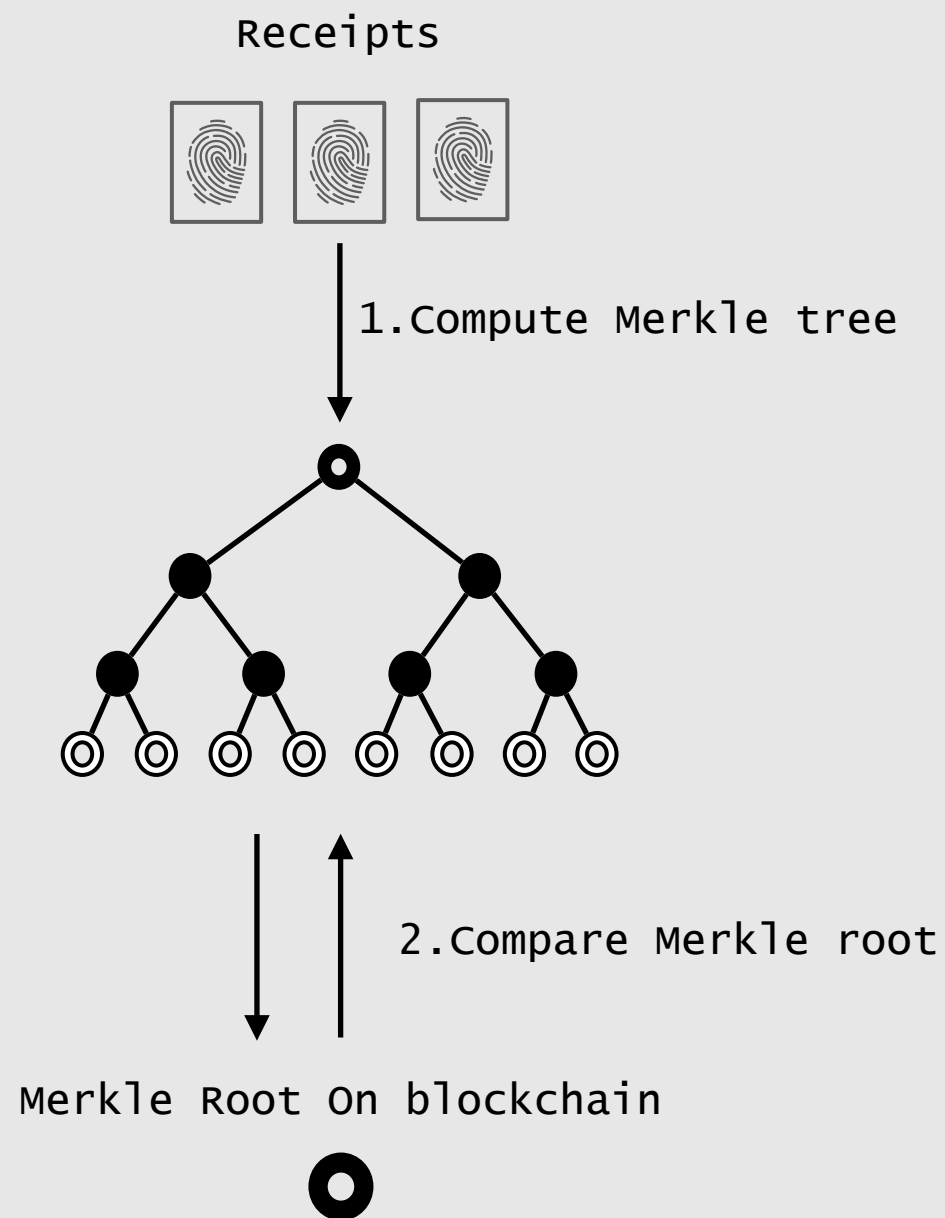
↓

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

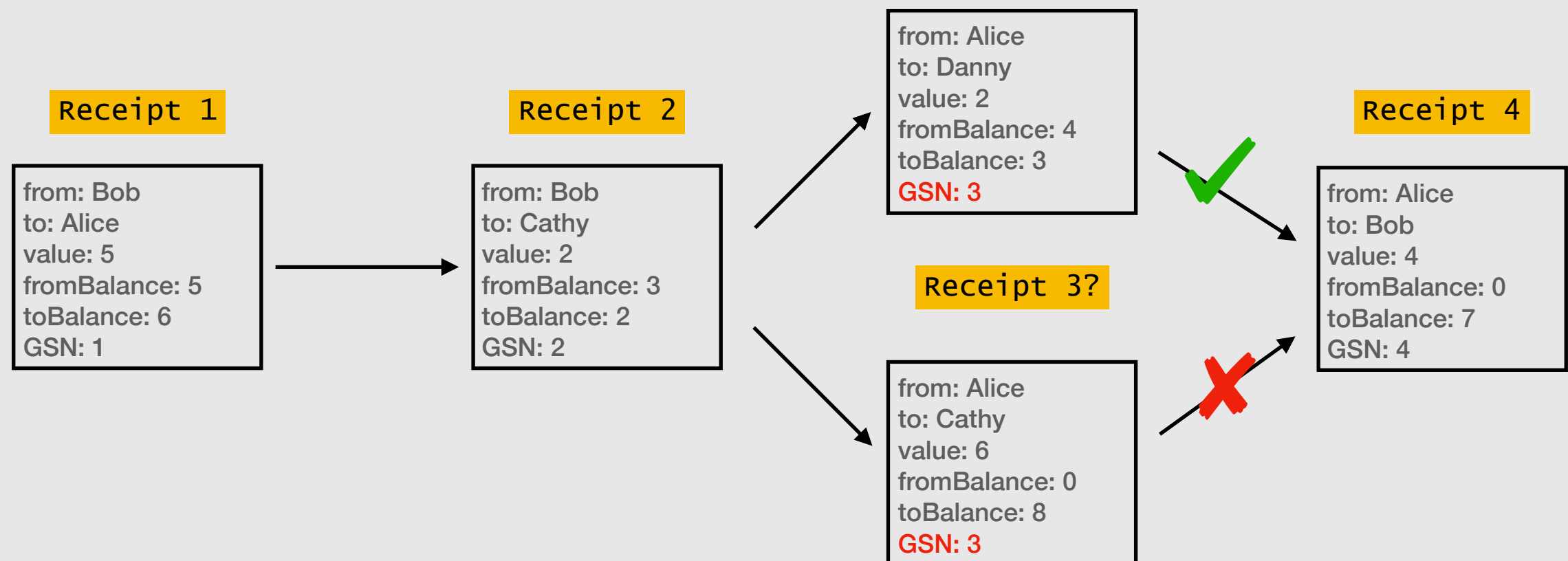
# Protocol: Receipt State Change



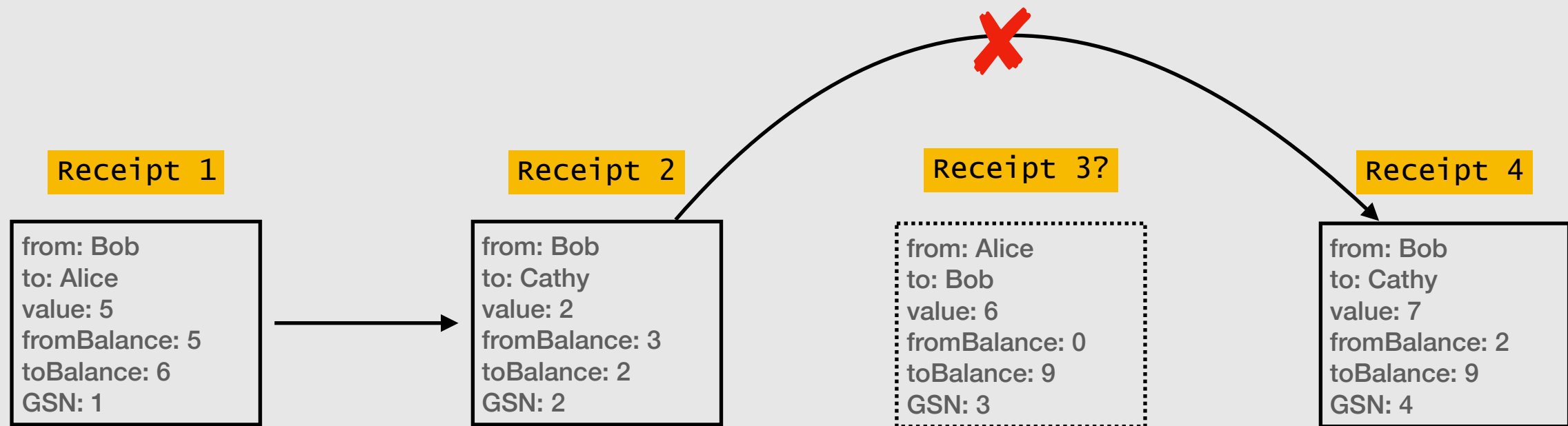
# Fraud Proof: Proof of existence



# Fraud Proof: Repeated GSN

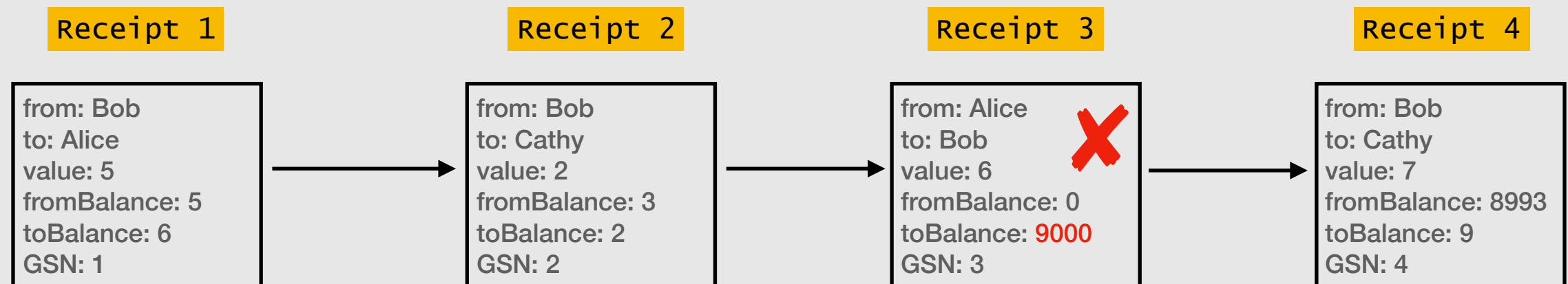


# Fraud Proof: Skipped GSN

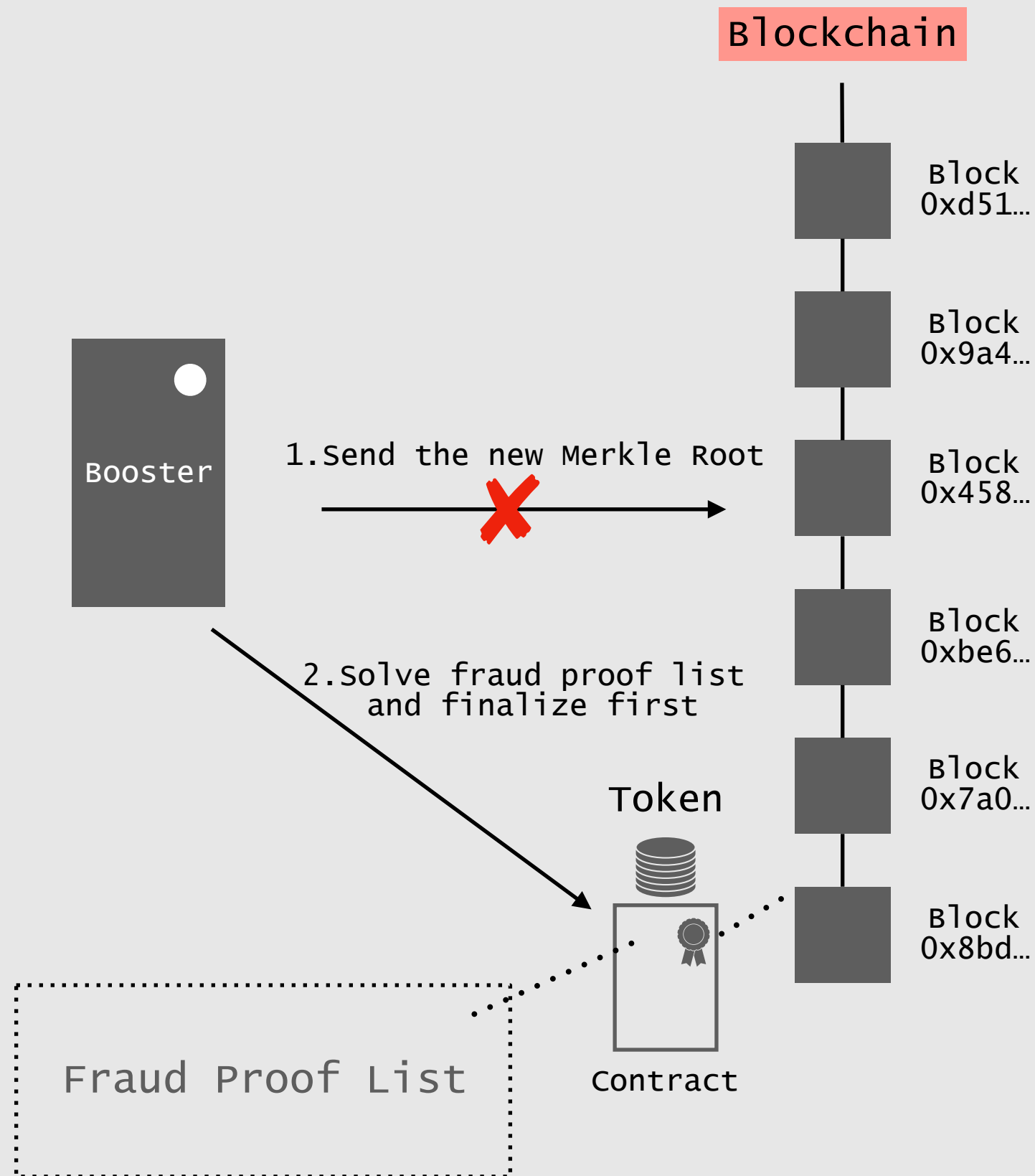




# Fraud Proof: Wrong Balance Status



# Protocol: Finalize



# Protocol: Force withdraw

