

BOLT: Booster of Ledger Technology

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

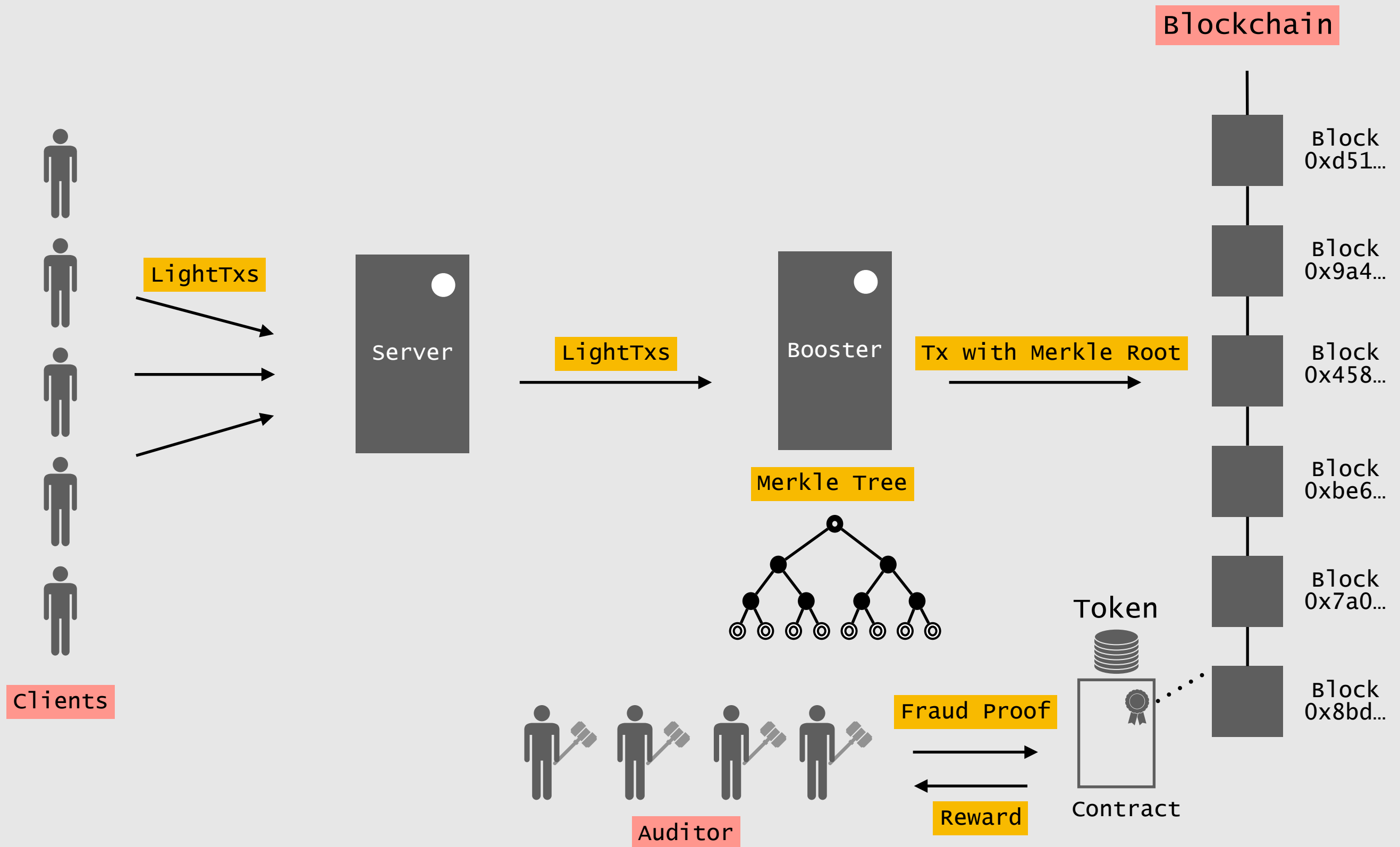


BOLT.infinitechain.io

Outline

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

Architecture: Concept

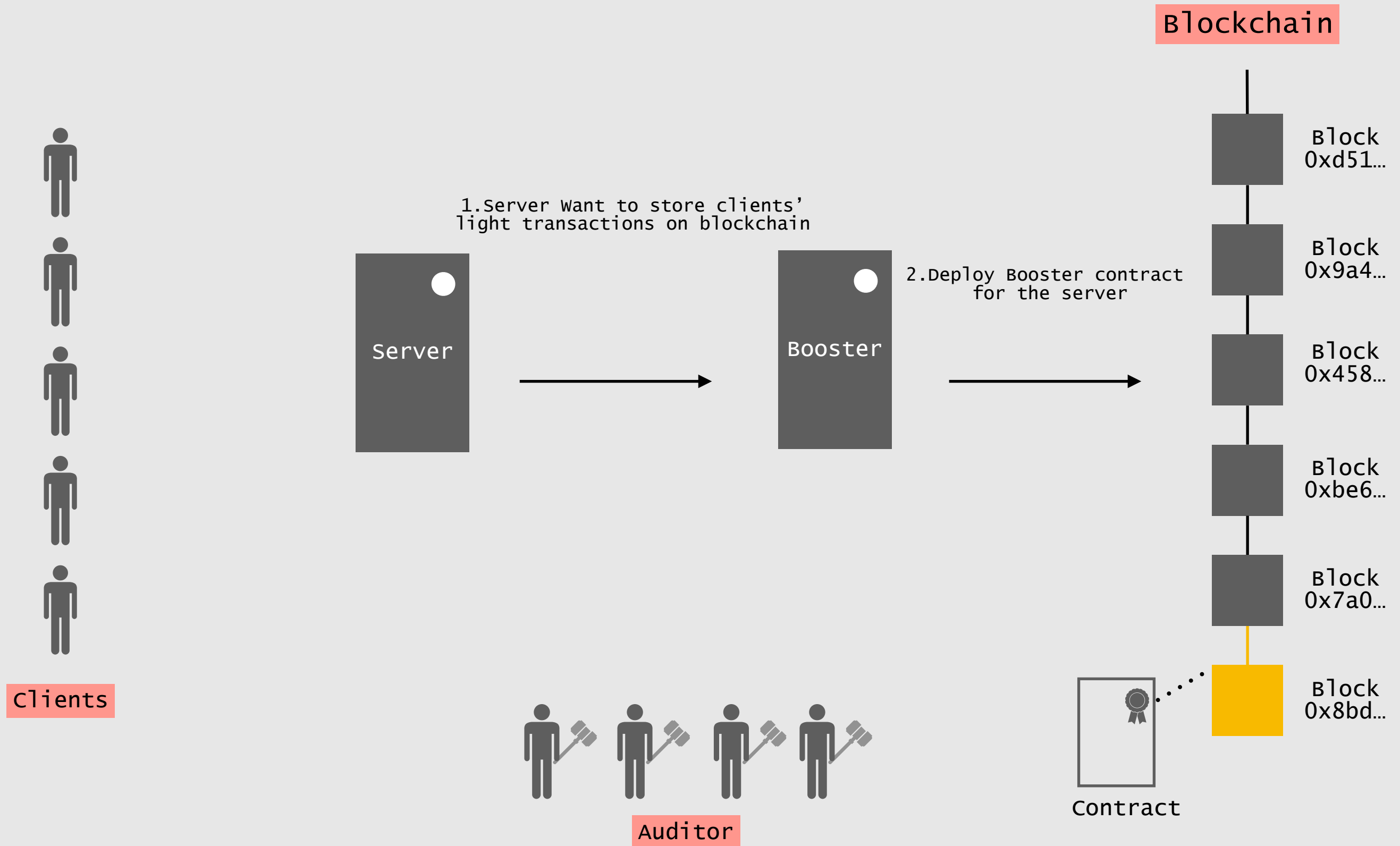


Architecture: Light Transaction

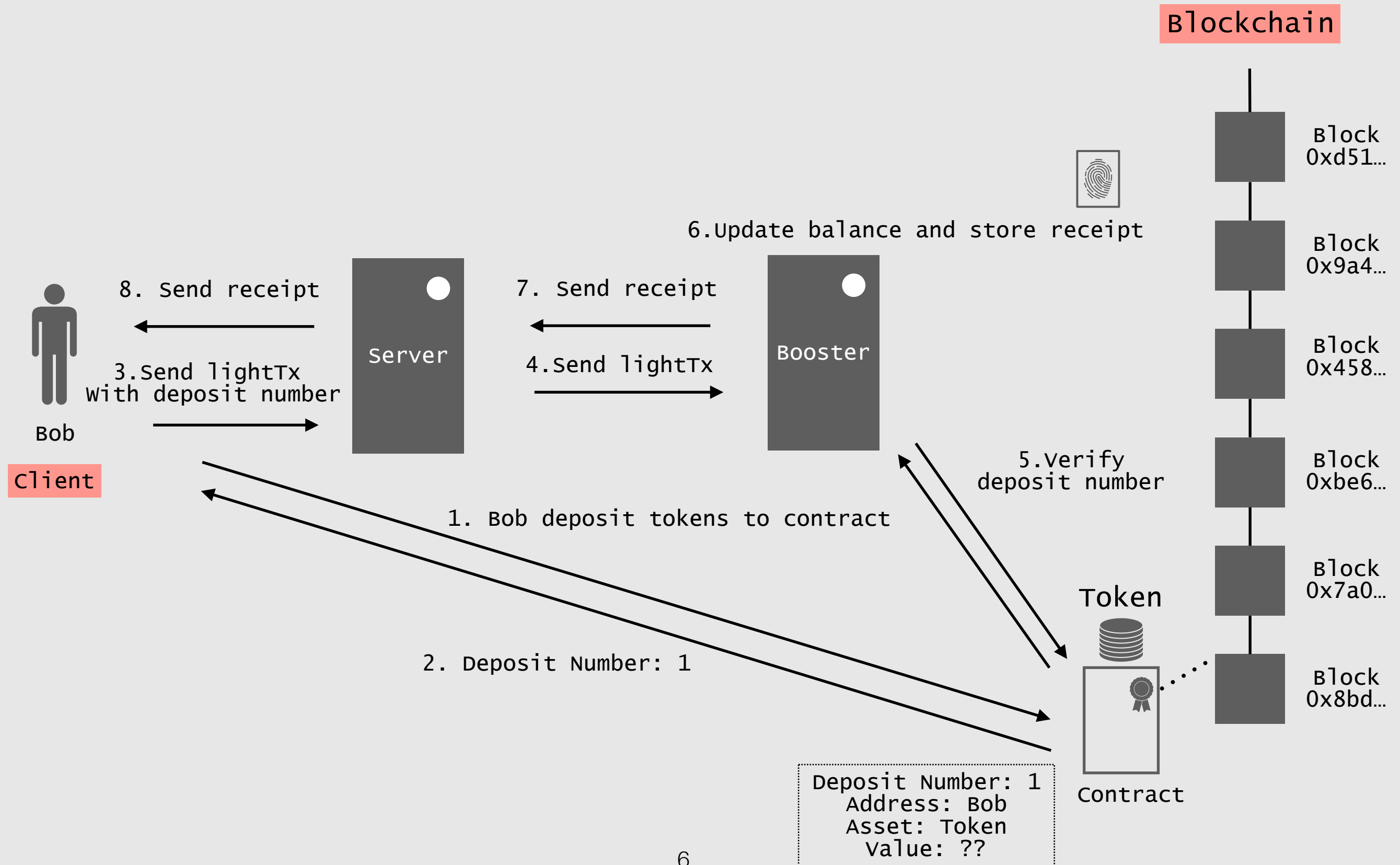
Light Transaction Type:

- ▶ Deposit
- ▶ Remittance
- ▶ withdrawal

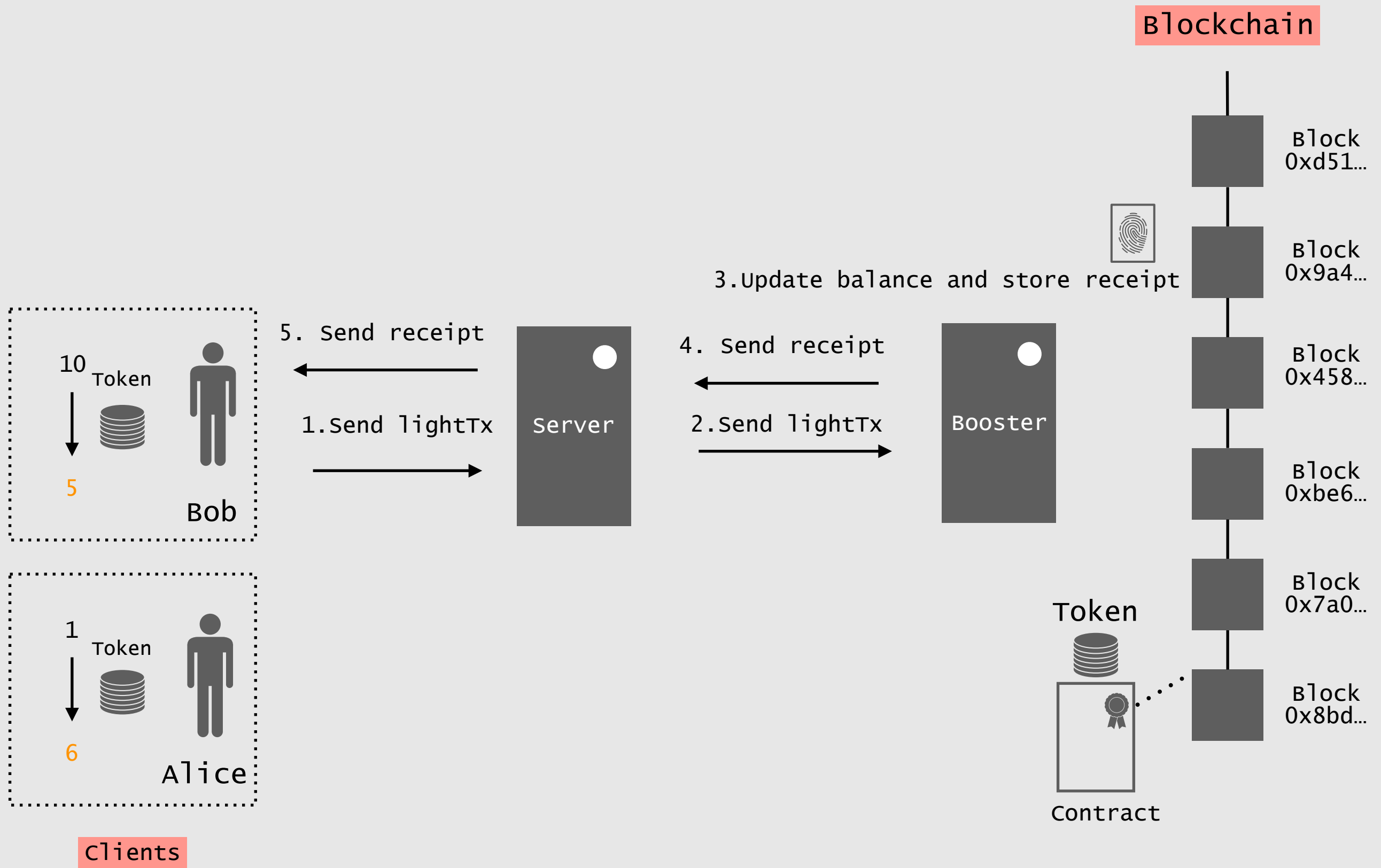
Protocol: 0



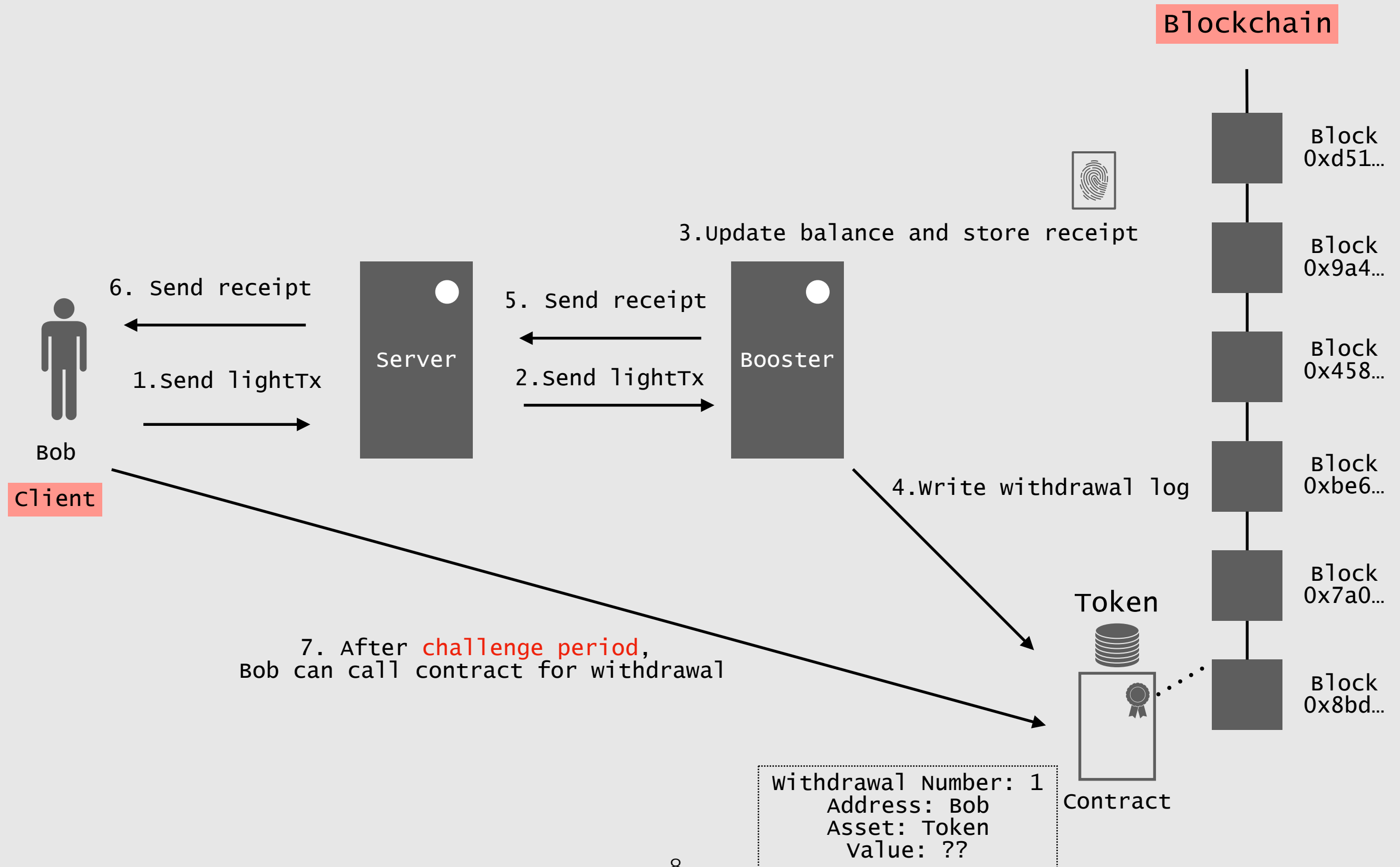
Protocol: Deposit



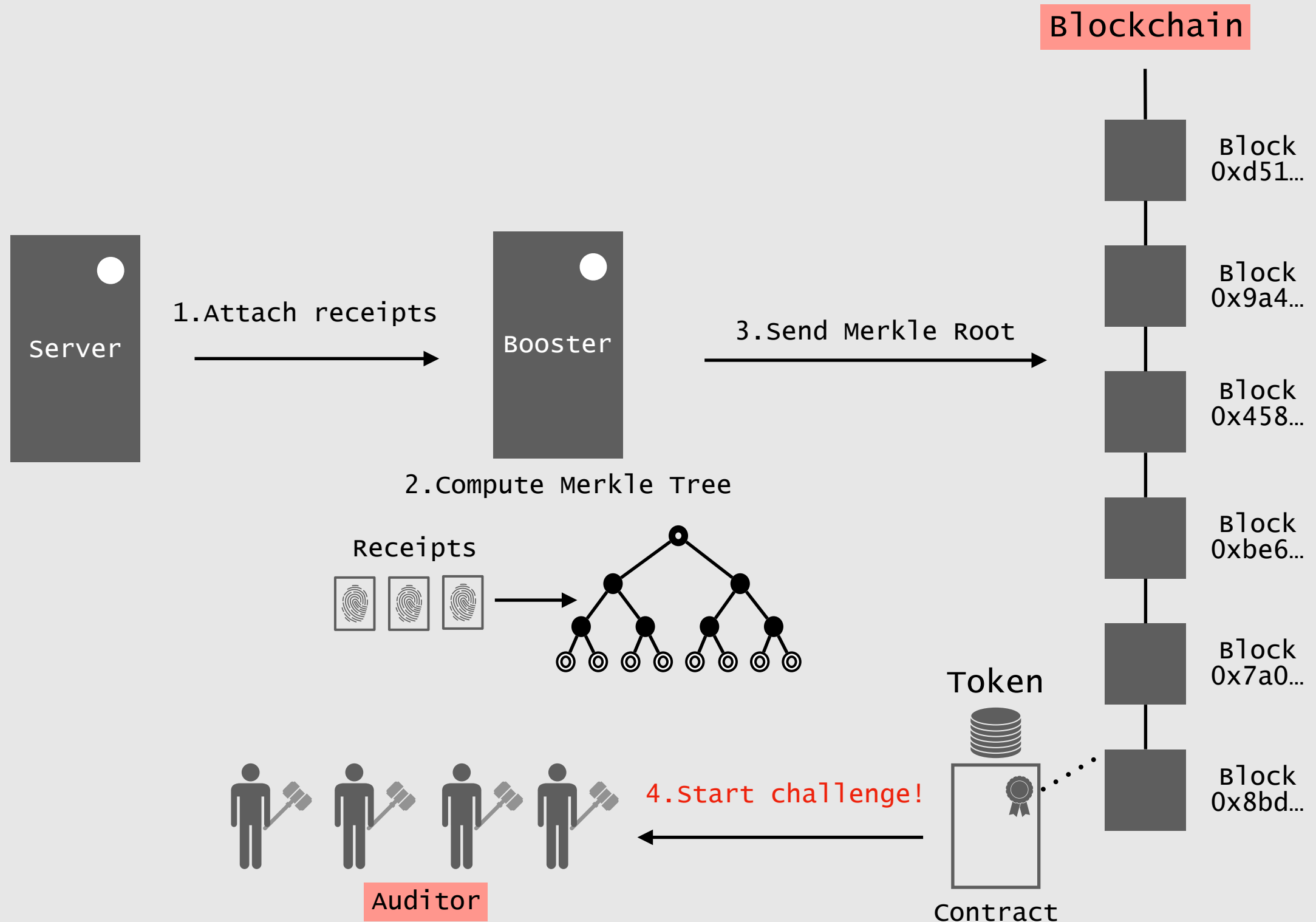
Protocol: Remittance



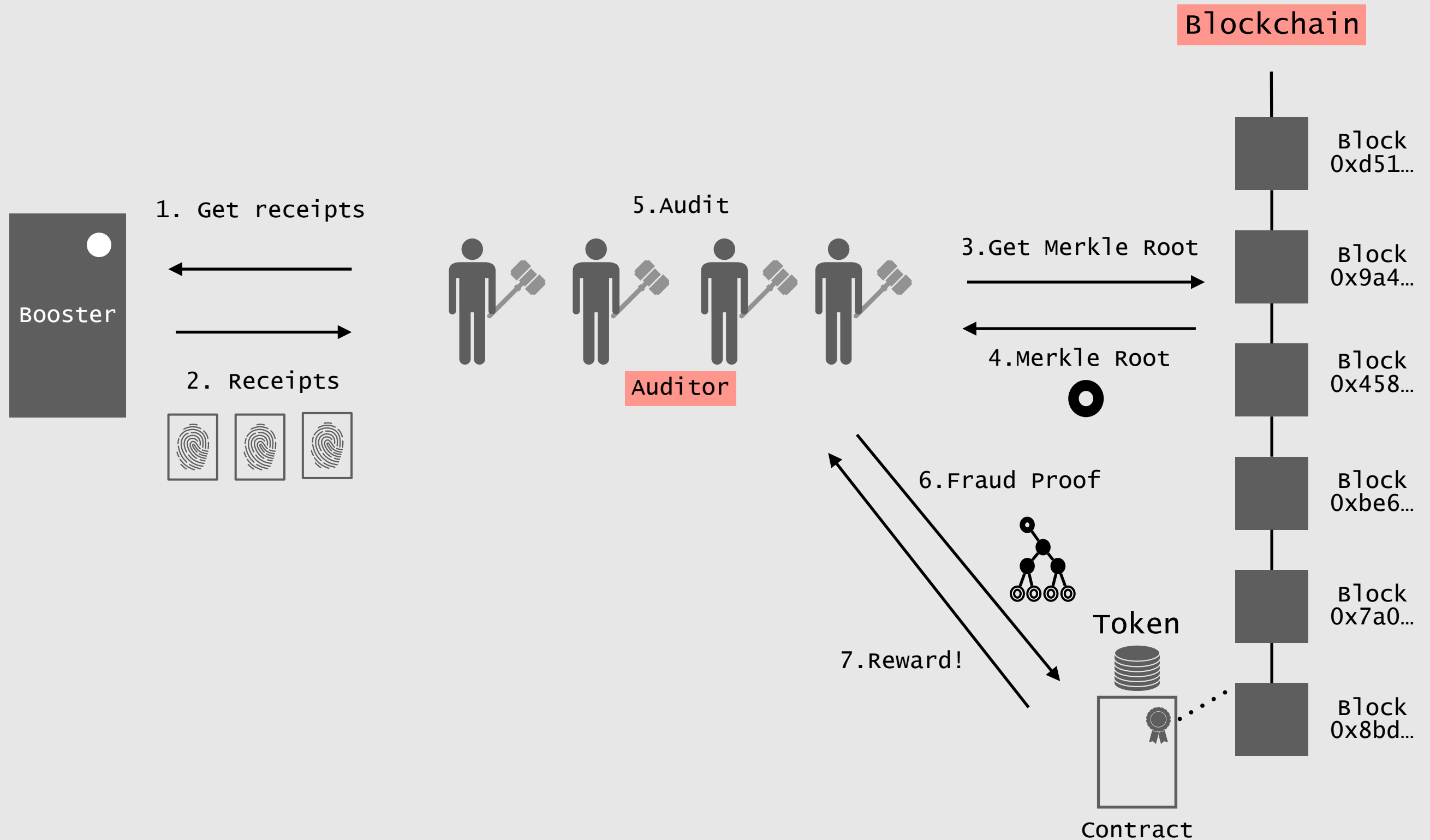
Protocol: withdrawal



Protocol: Challenge Start



Protocol: Challenge Period

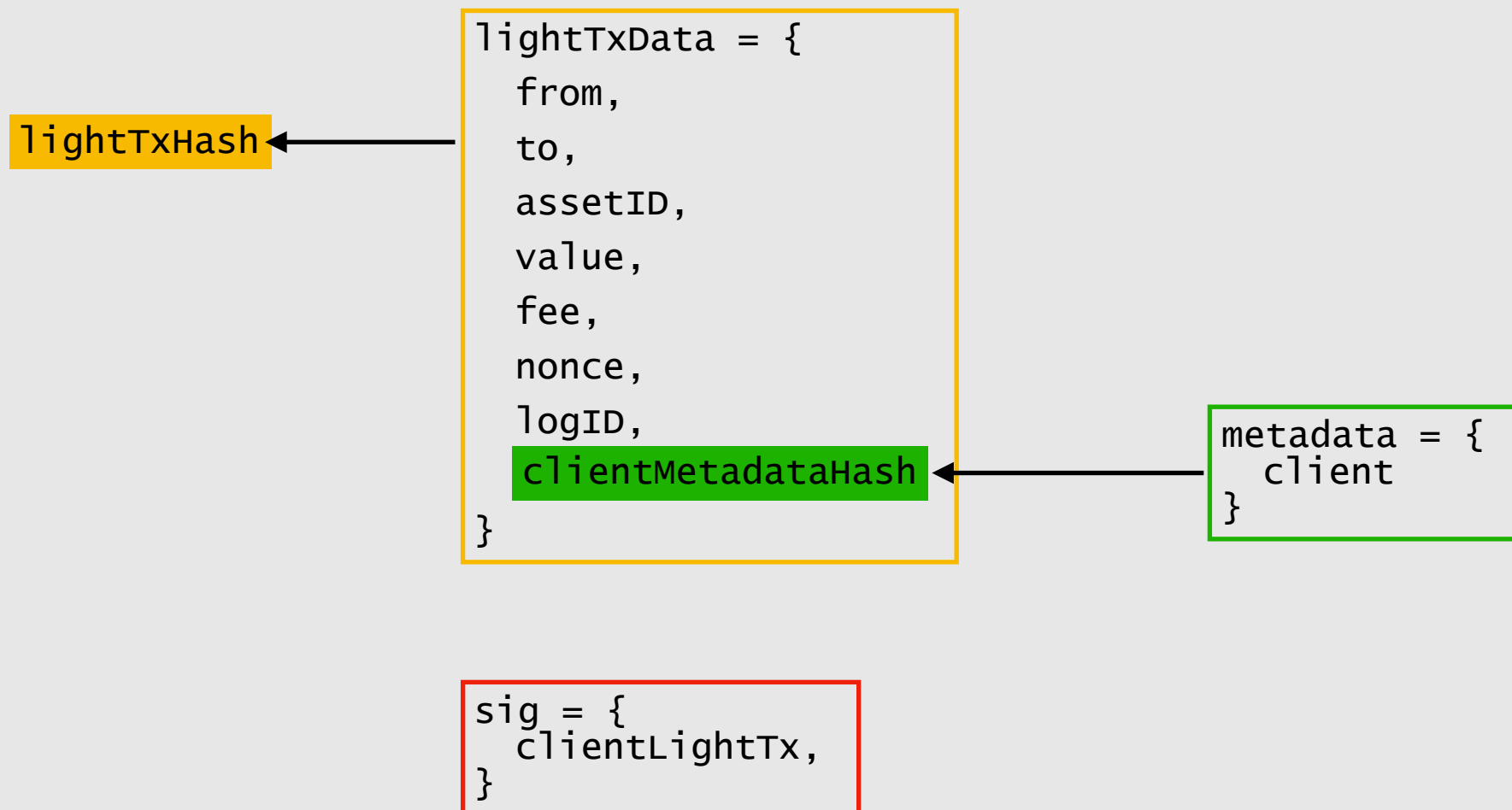


Protocol: Fraud Type

1. Proof of existence
2. Repeated GSN
3. Skipped GSN
4. Wrong balance status

Data Model: Light Transaction

Light Transaction



Data Model: Receipt

Receipt

lightTxHash

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

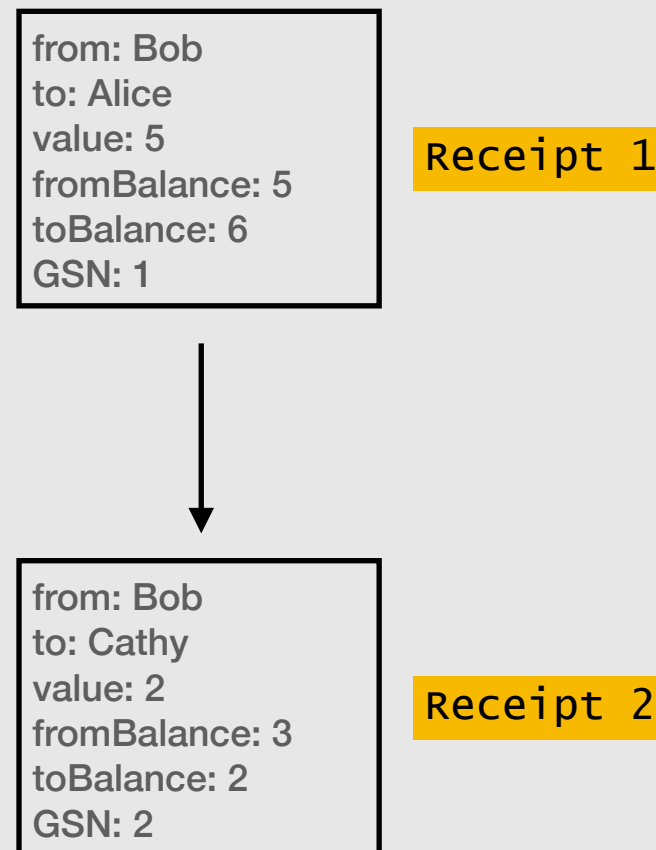
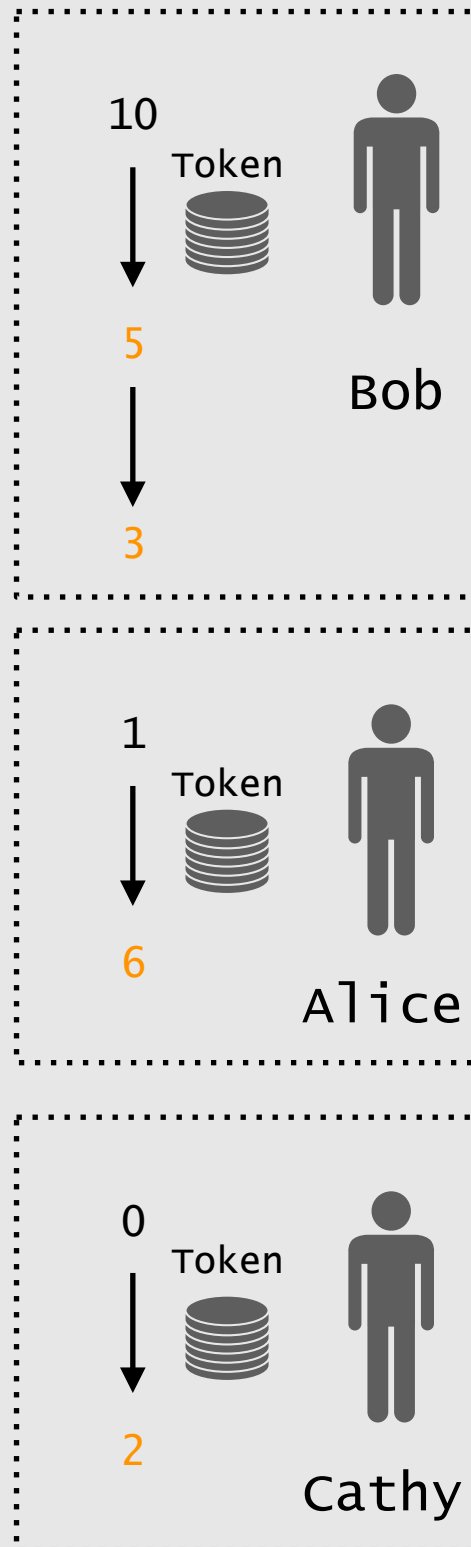
```
metadata = {  
  client,  
  server  
}
```

receiptHash

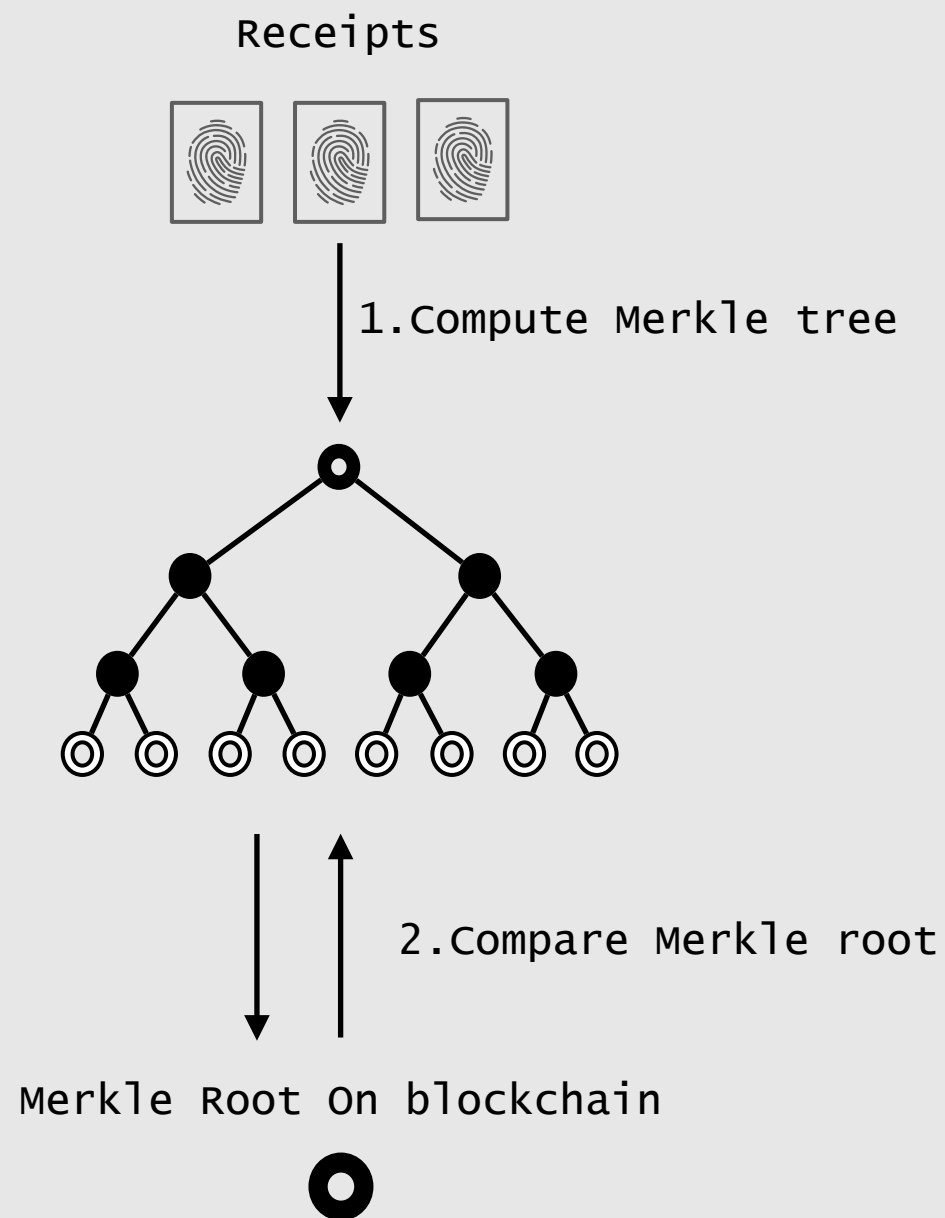
```
receiptData = {  
  stageHeight,  
  GSN,  
  lightTxHash,  
  fromBalance,  
  toBalance,  
  serverMetadataHash  
}
```

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

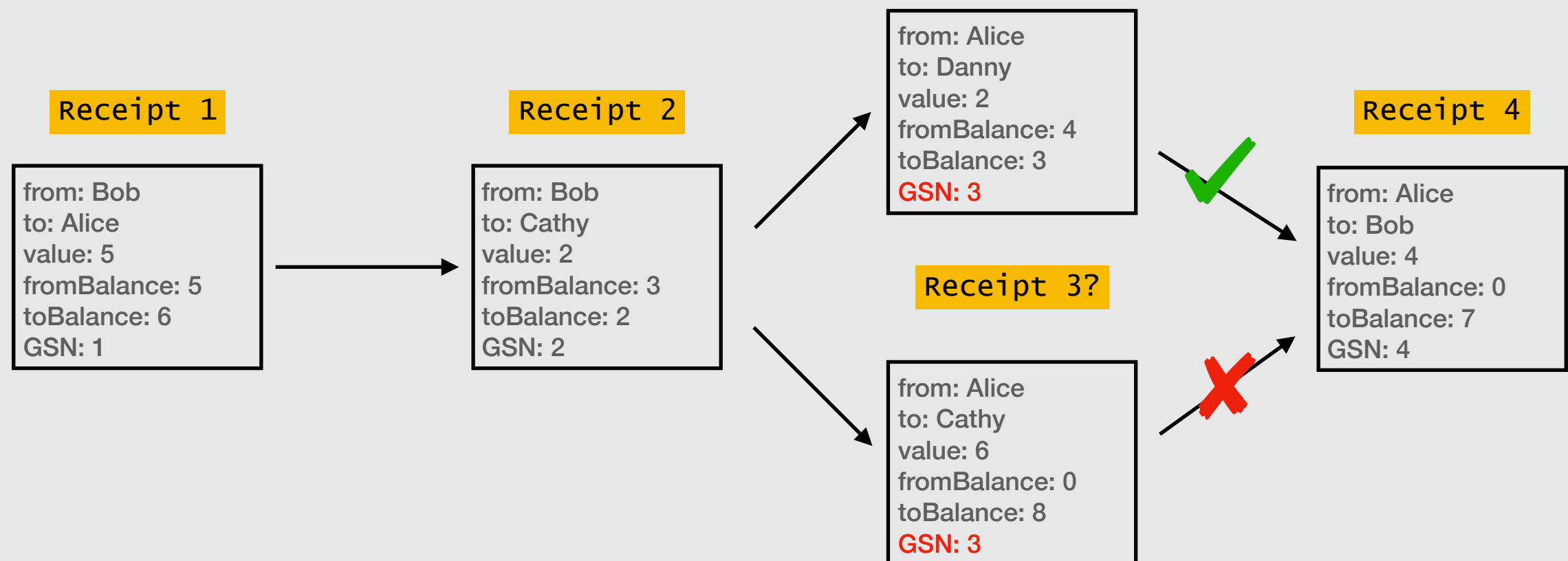
Protocol: Receipt State Change



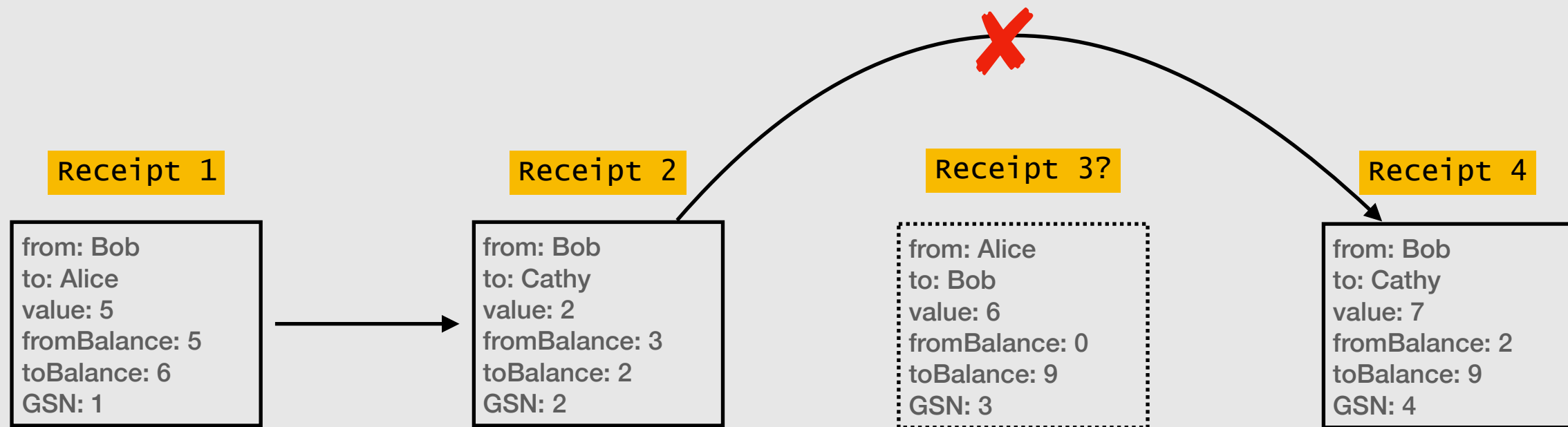
Fraud Proof: Proof of existence



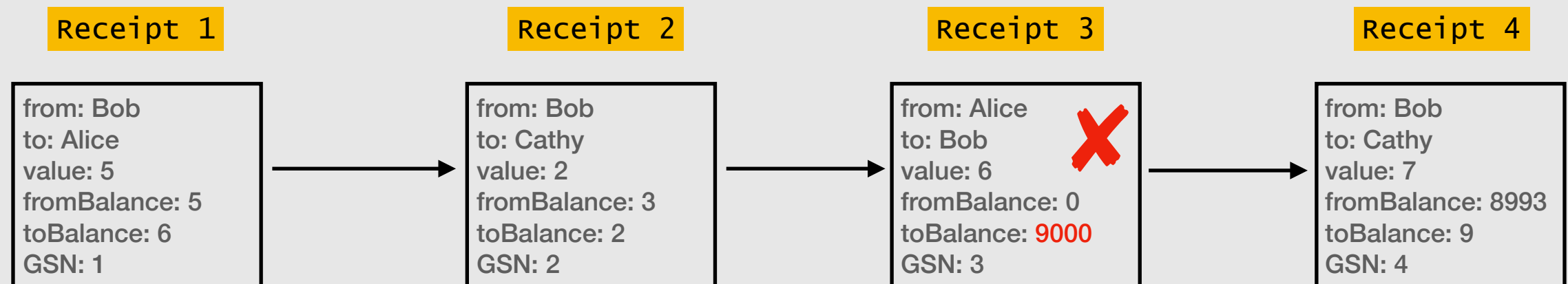
Fraud Proof: Repeated GSN



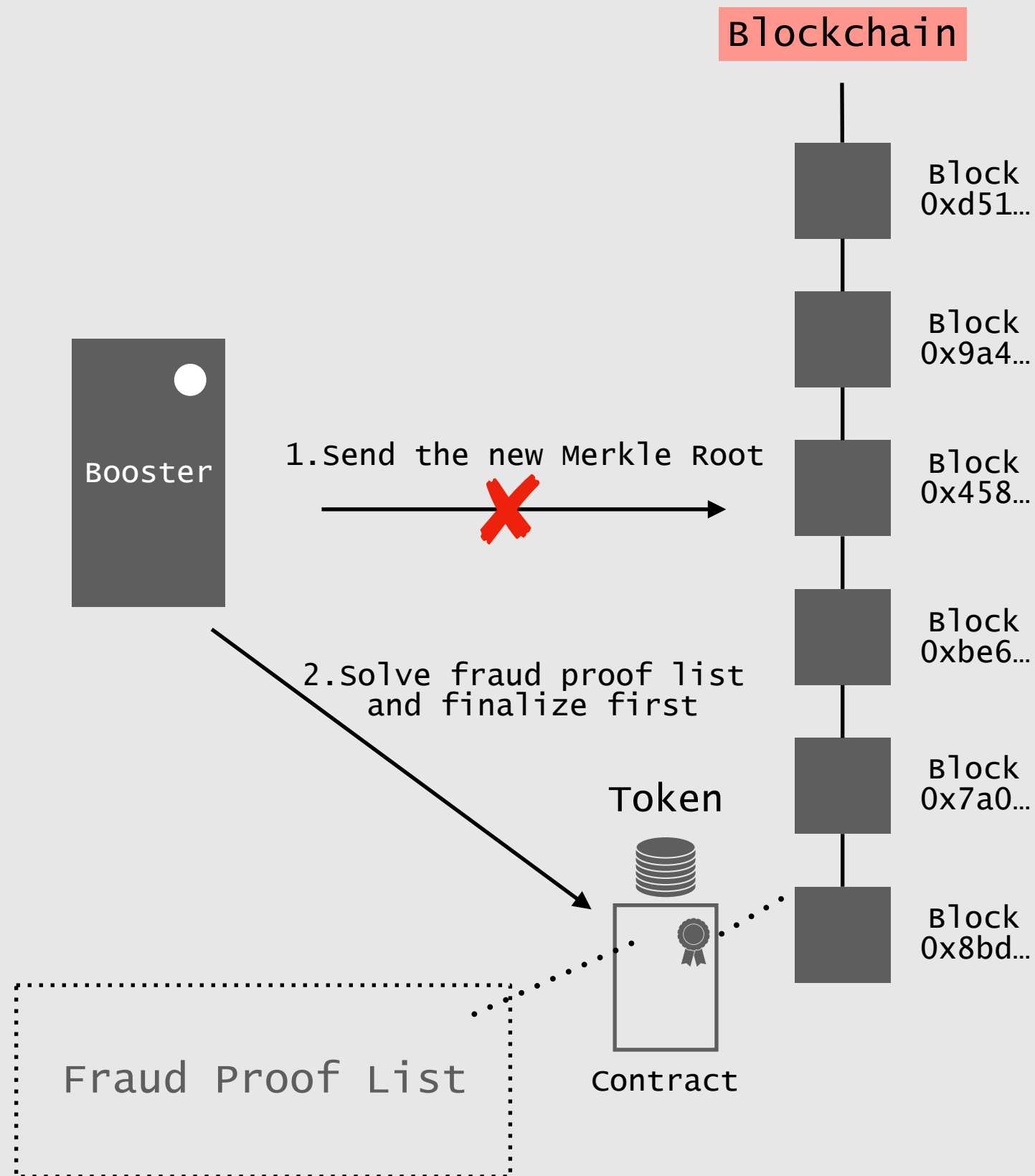
Fraud Proof: Skipped GSN



Fraud Proof: Wrong Balance Status



Protocol: Finalize



Protocol: Force withdraw

