

BOLT: Booster of Ledger Technology

@juinc
@jerry-jheng

davidjuin0519@gmail.com
jerry128371@gmail.com

BOLT.infinitechain.io

Outline

- ▶ Overview
- ▶ Anti-fraud Mechanism
- ▶ Architecture
- ▶ Protocol
- ▶ Demo

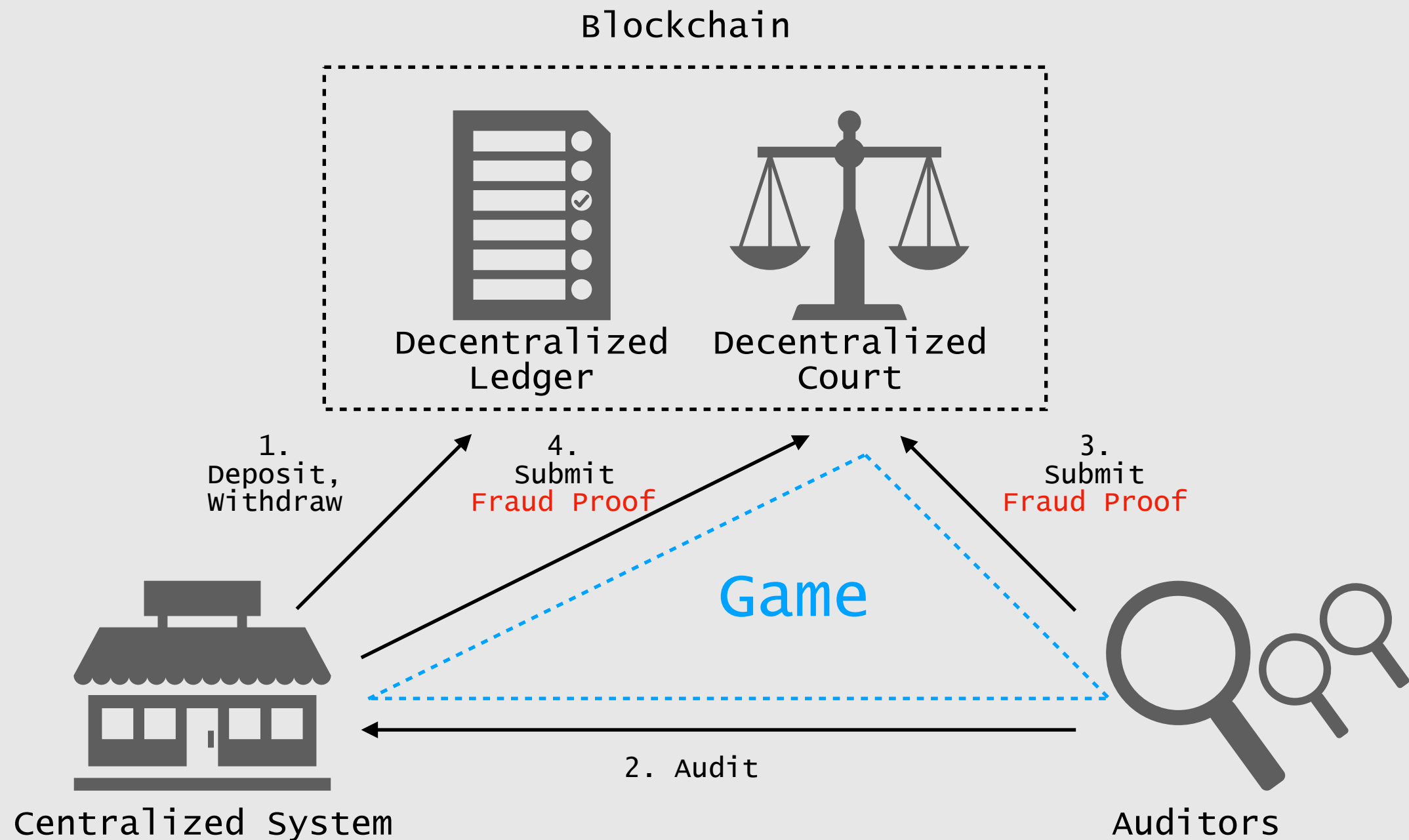
Overview (1)

- ▶ BOLT is a layer 2 scalability solution that integrates centralized system
- ▶ Borrow ideas from Plasma, Truebit and State Channel
- ▶ Use cases include payments, gaming, etc.

Overview (2)

	Plasma MVP	BOLT
Blockchain Trilemma	Decentralized Secure Not Scalable	Scalable Secure Not Decentralized
Fraud Proof	Merkle Proof	Merkle Proof + Receipts
Transactional Model	UTXO	UTXO-like + Account-based
Anti-fraud Mechanism	Mass Exit + Punishment	Mass Exit + Punishment + Auditing

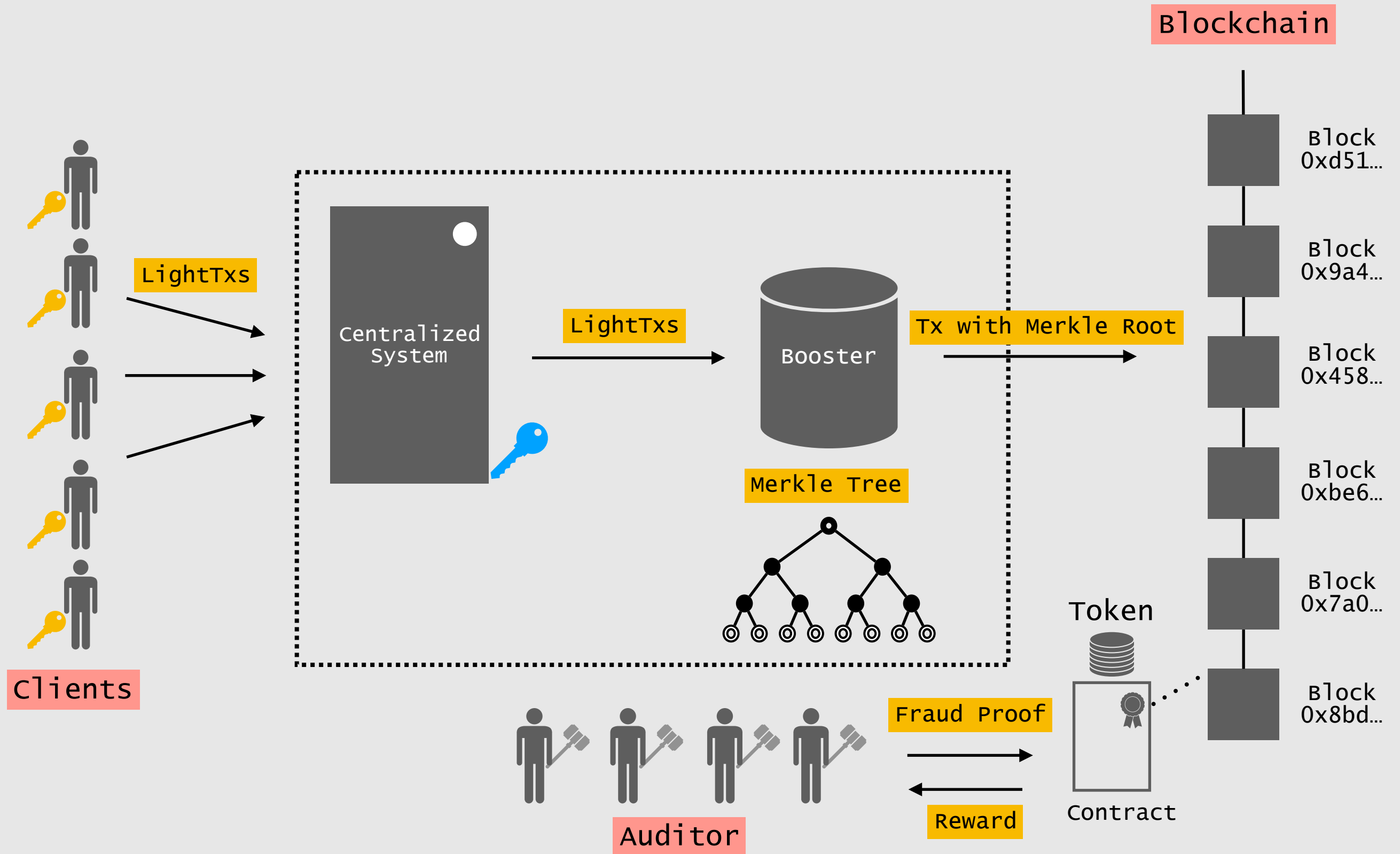
Anti-fraud Mechanism



Anti-fraud Mechanism

- ▶ Centralized System v.s Auditors
- ▶ Participants are incentivized to inspect each other
- ▶ Similar design in Plasma and Truebit

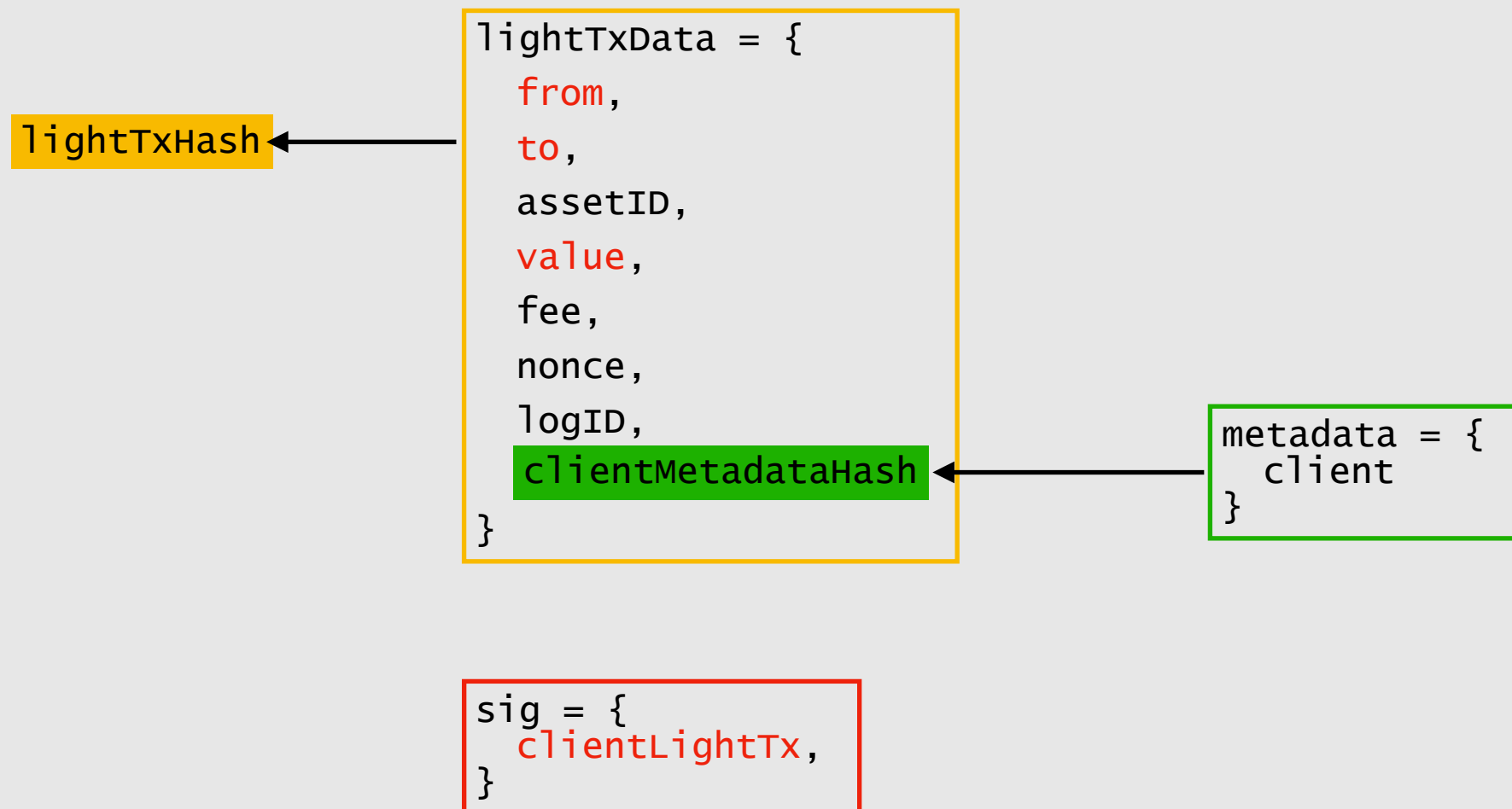
Architecture



Protocol

Data Model

Light Transaction



Protocol

Data Model

Receipt

lightTxHash

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

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

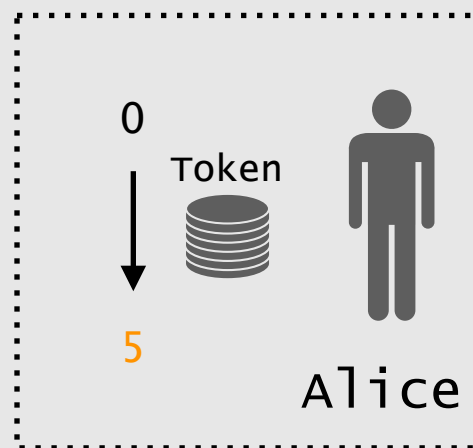
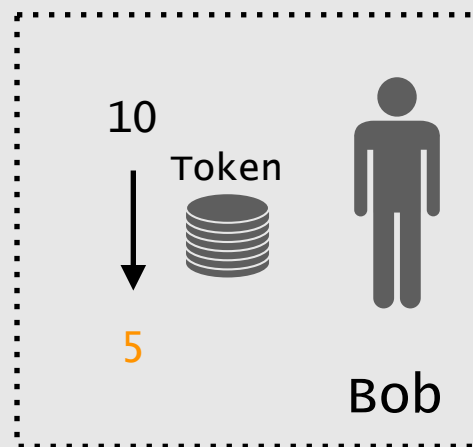
receiptHash

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

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

Protocol

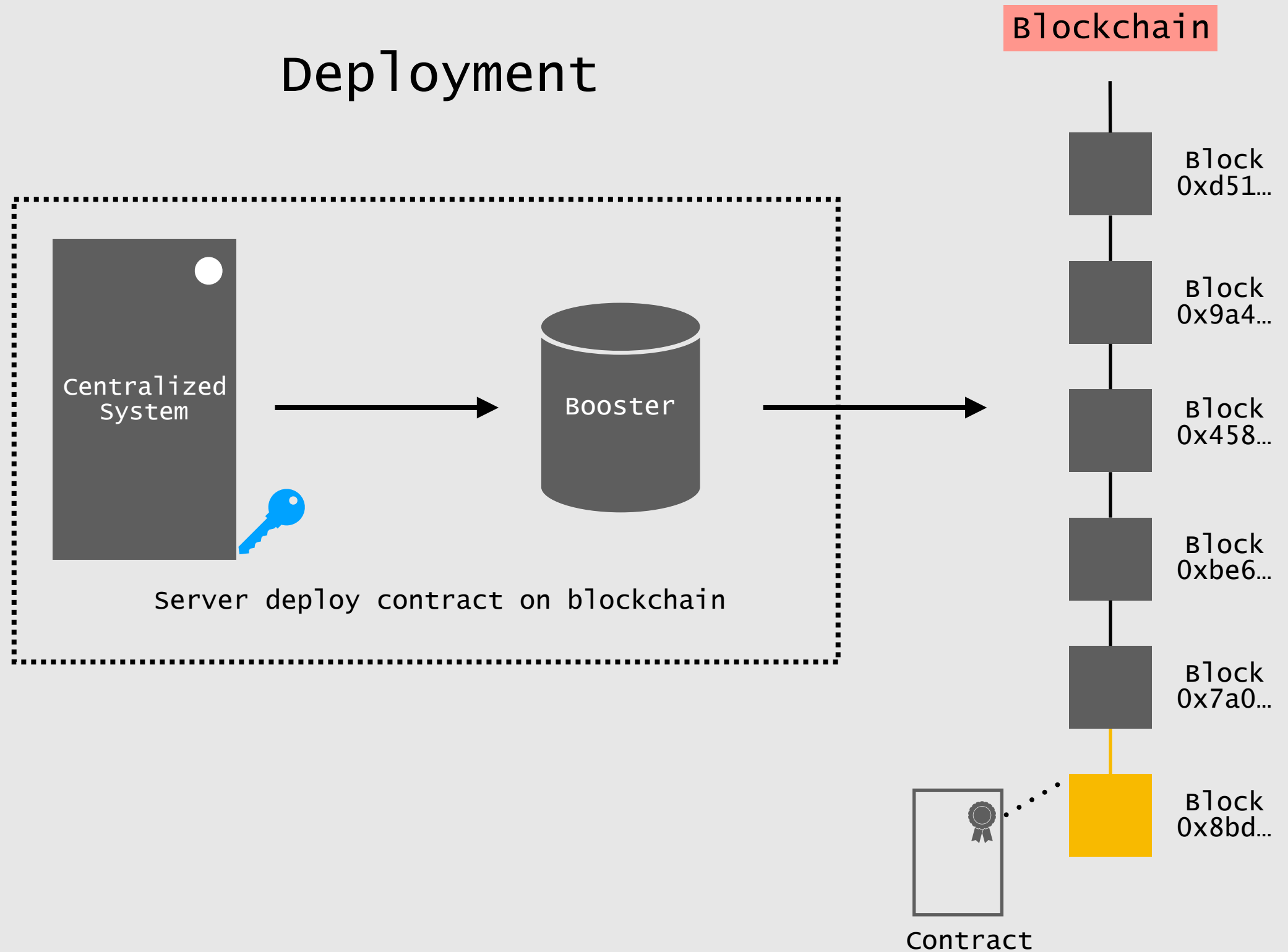
Example



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

Receipt 1

Protocol Deployment



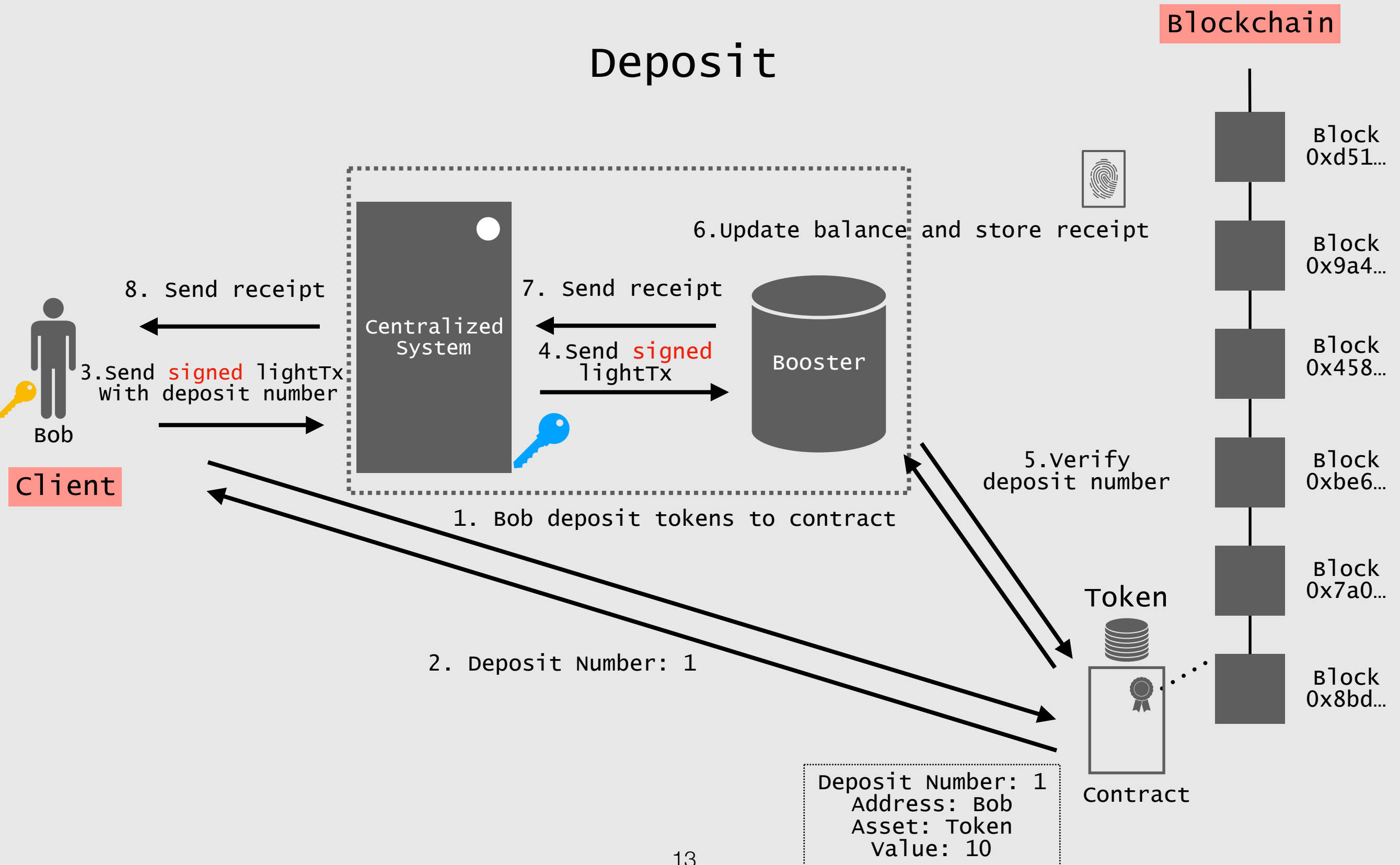
Protocol

Light Transaction Type

1. Deposit
2. Remittance
3. withdrawal

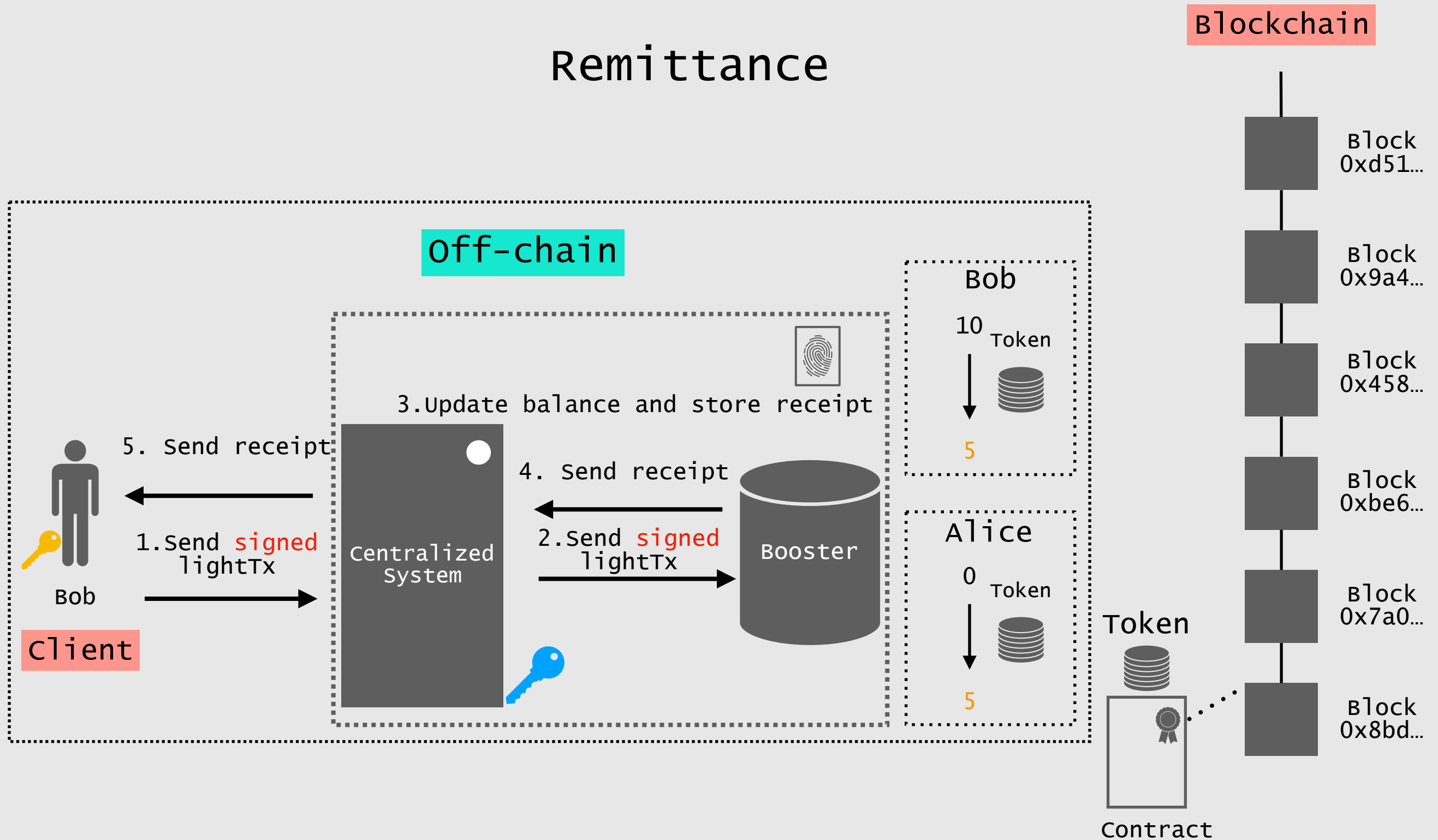
Protocol

Deposit



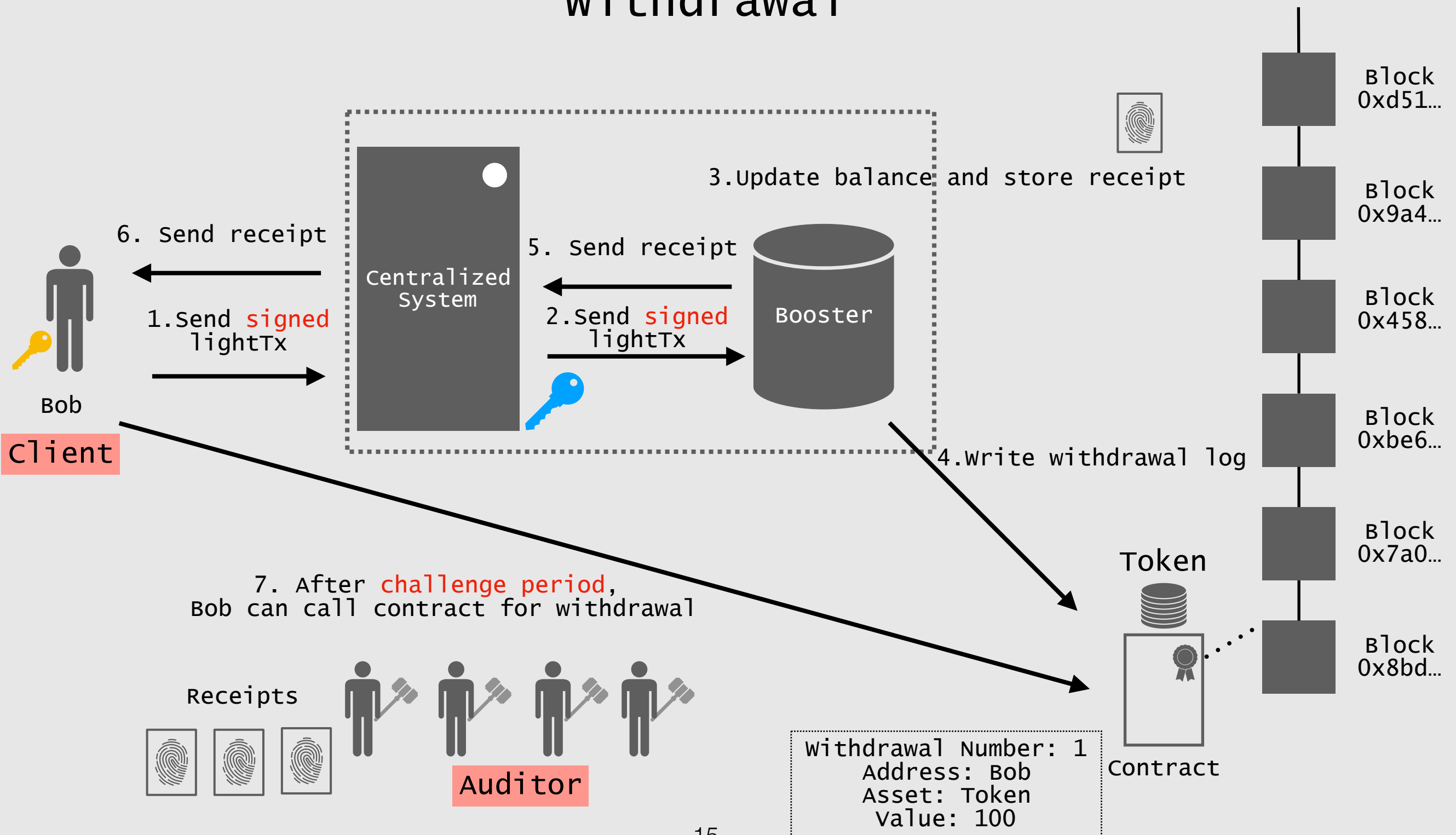
Protocol

Remittance



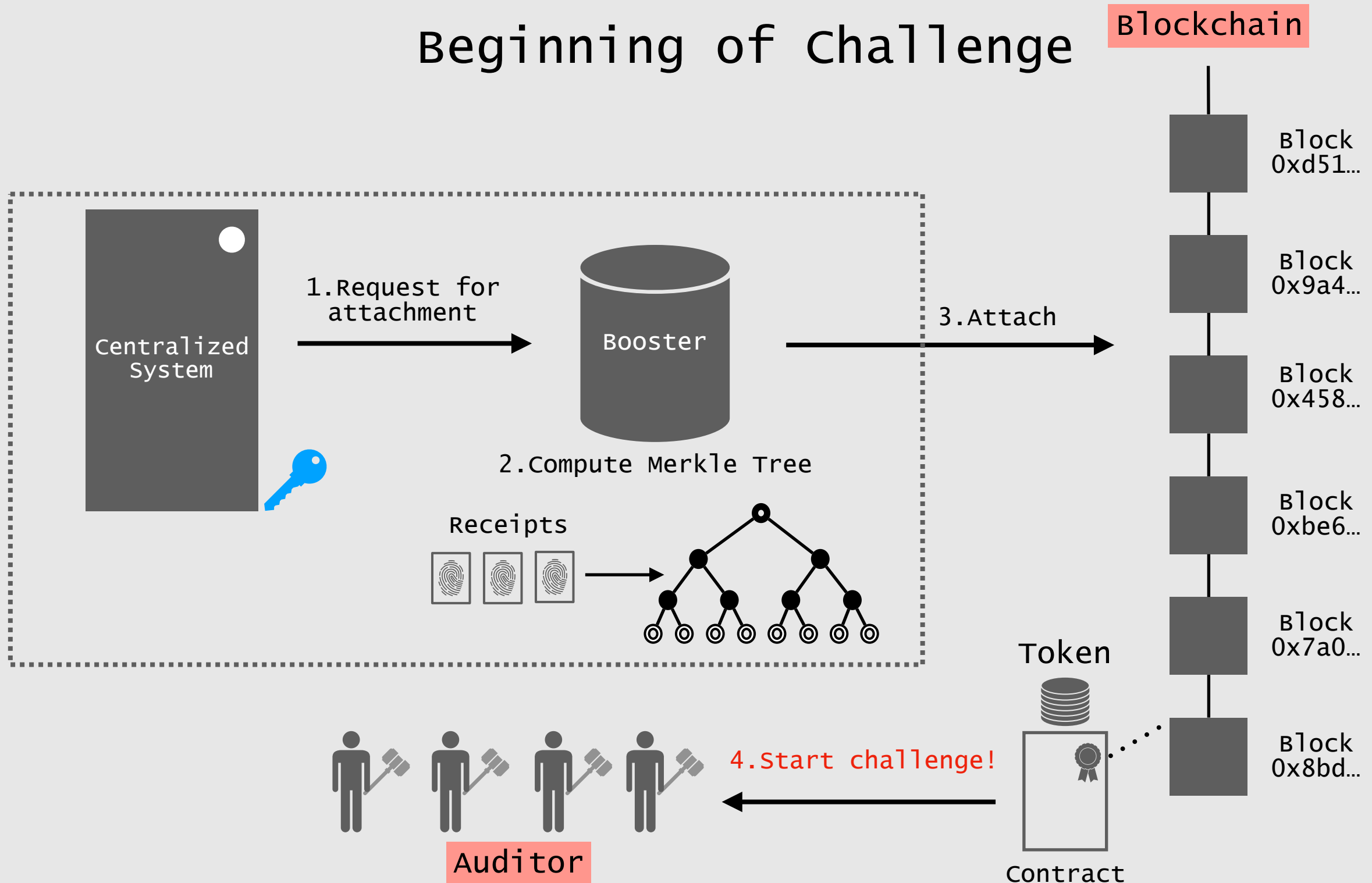
Protocol withdrawal

Blockchain



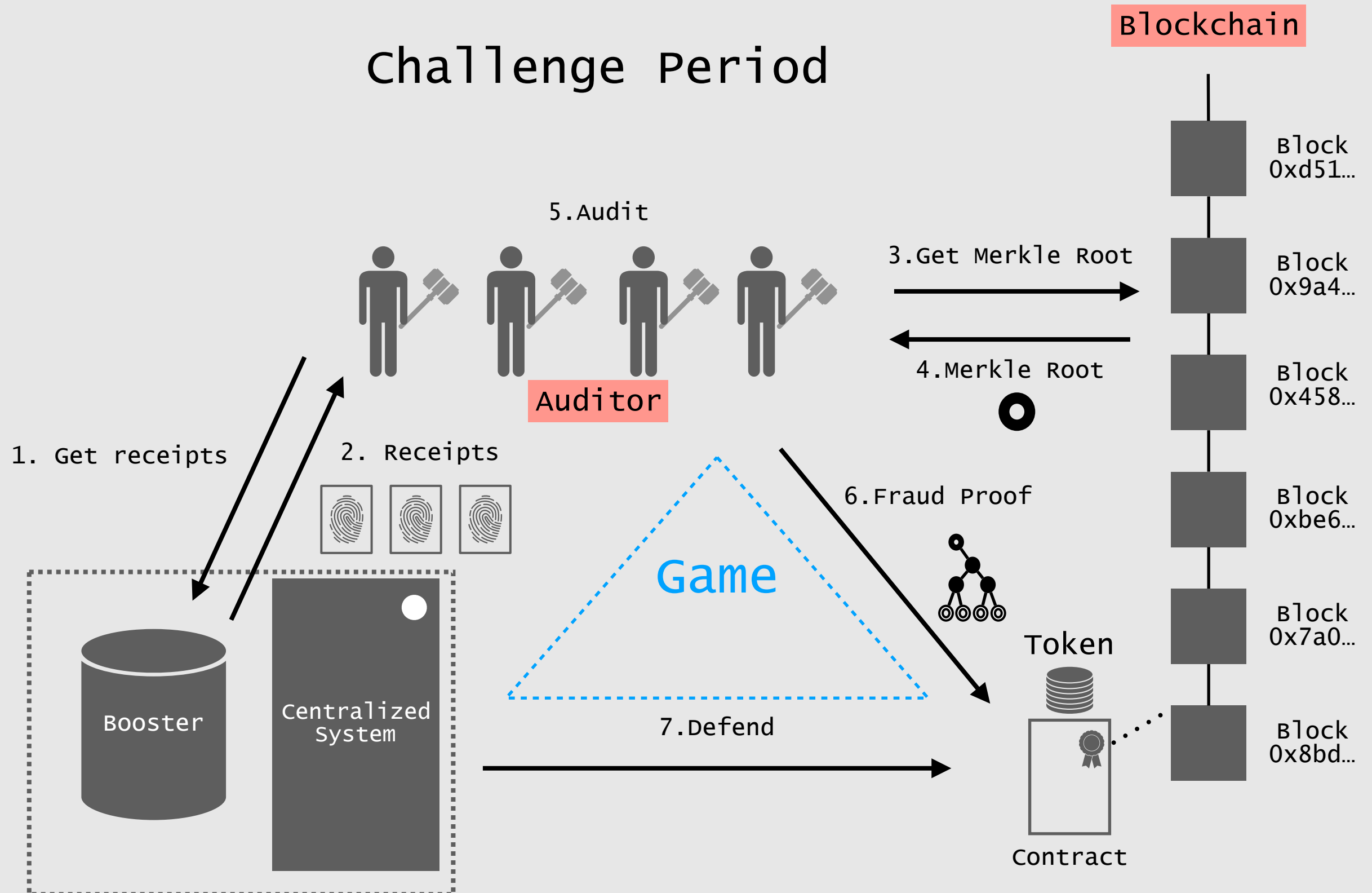
Protocol

Beginning of Challenge



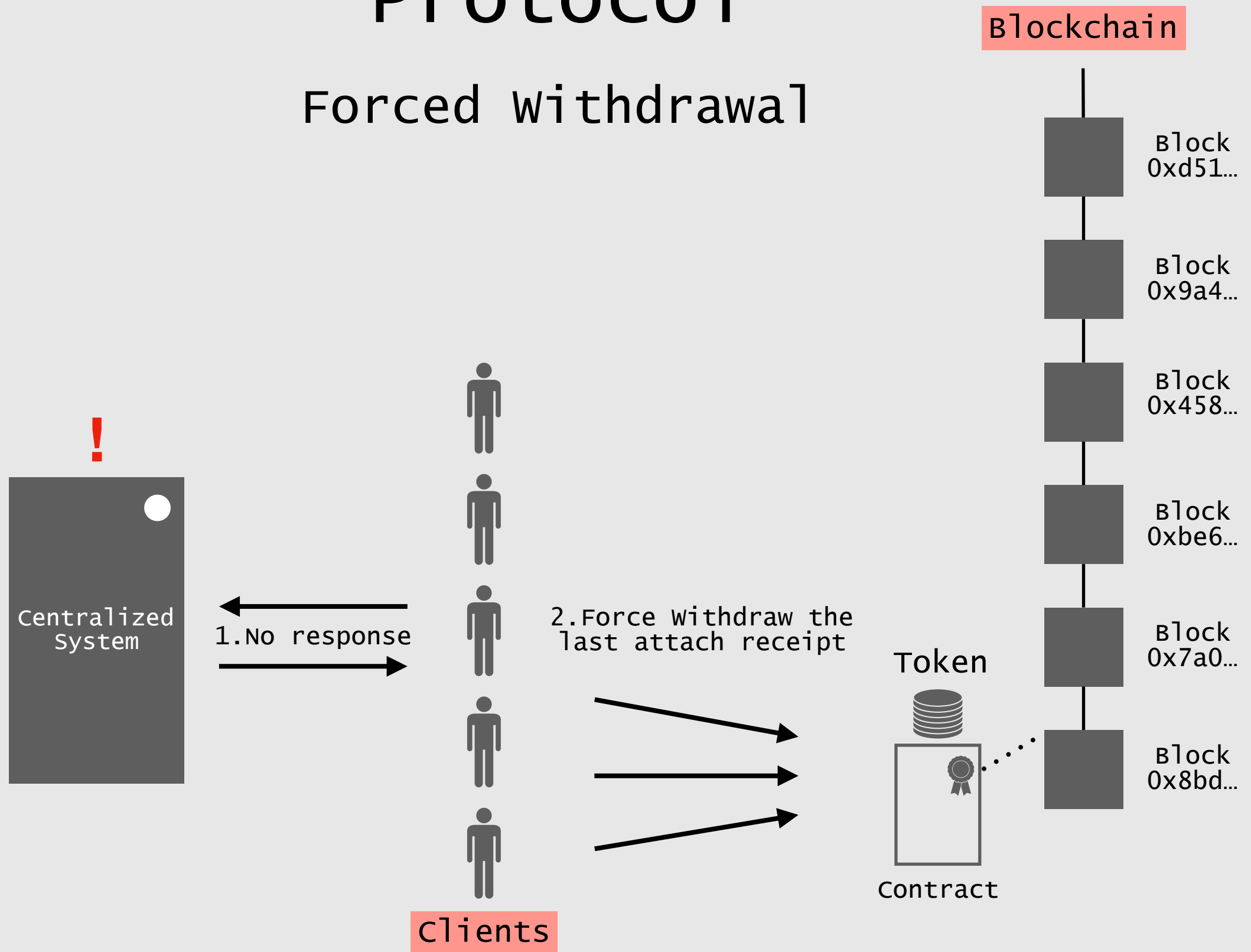
Protocol

Challenge Period

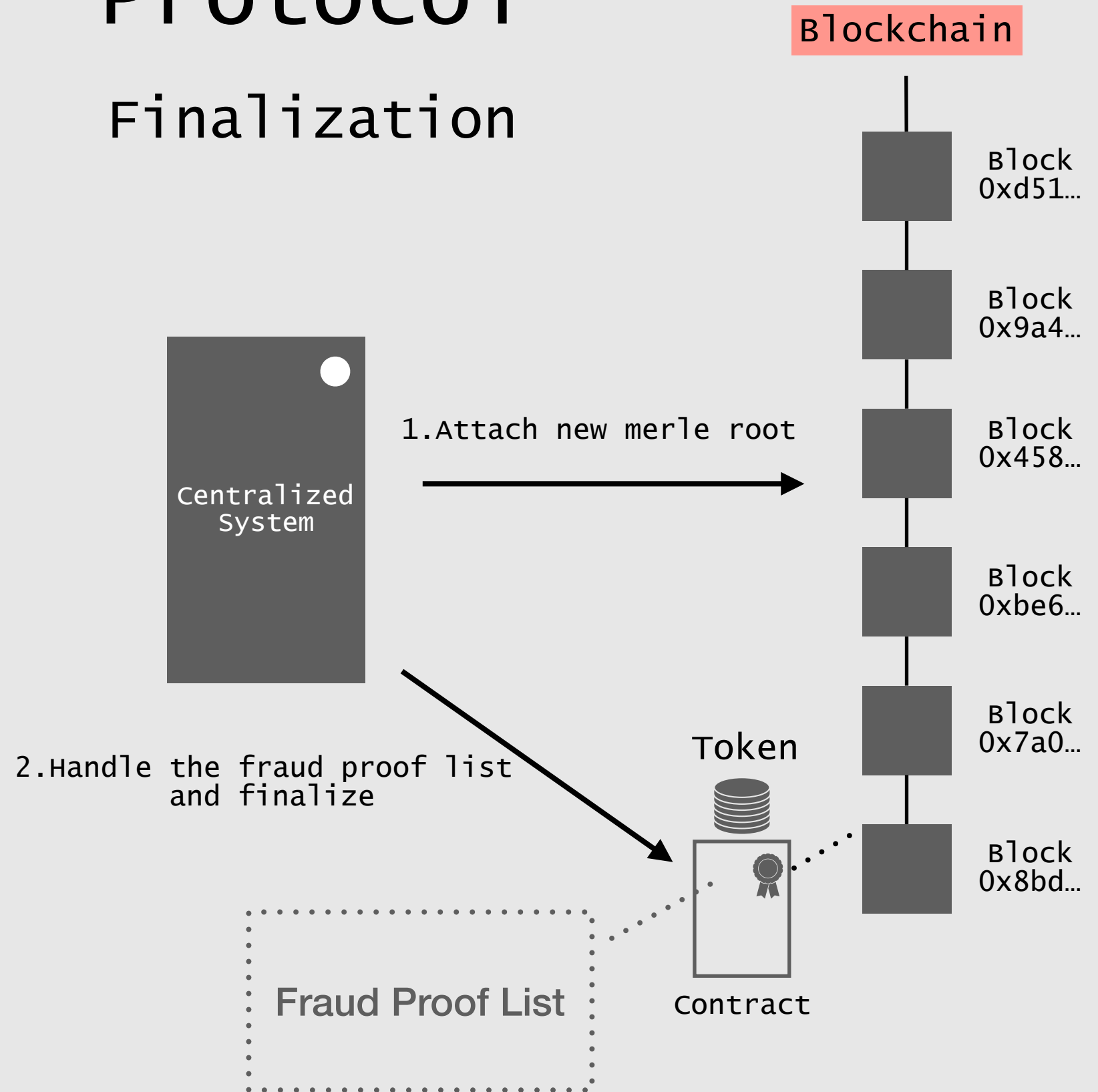


Protocol

Forced withdrawal



Protocol Finalization



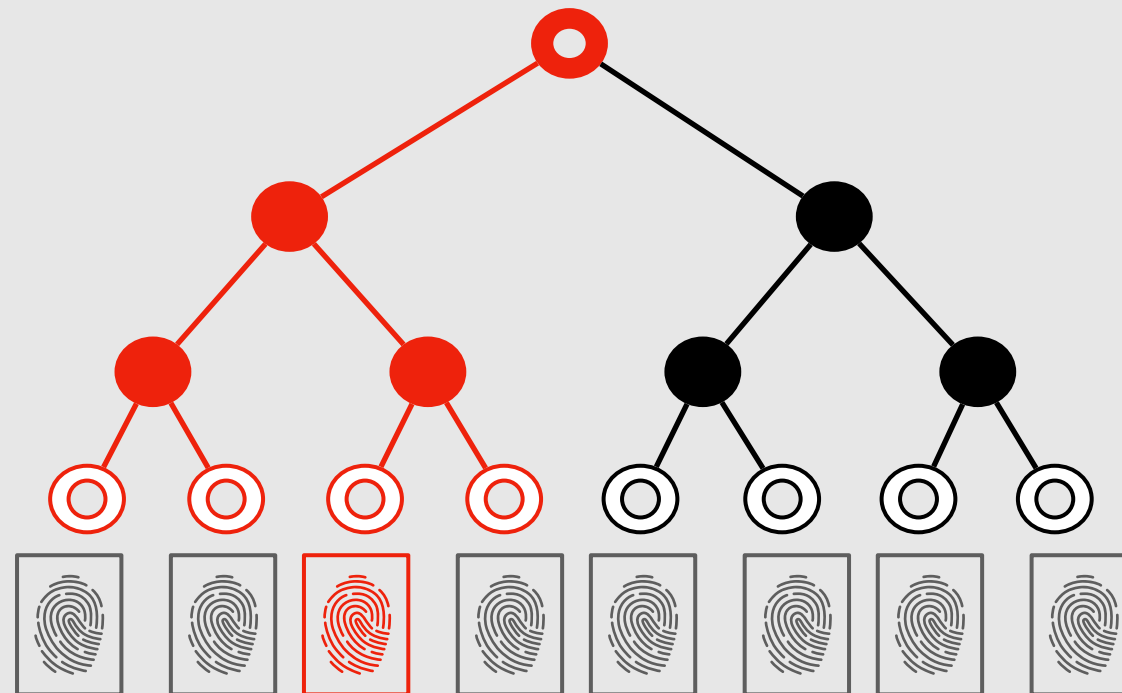
Protocol

Fraud Proof

1. Non-existed receipt
2. Receipt with Repeated GSN
3. Receipt with Skipped GSN
4. Receipt with wrong balance

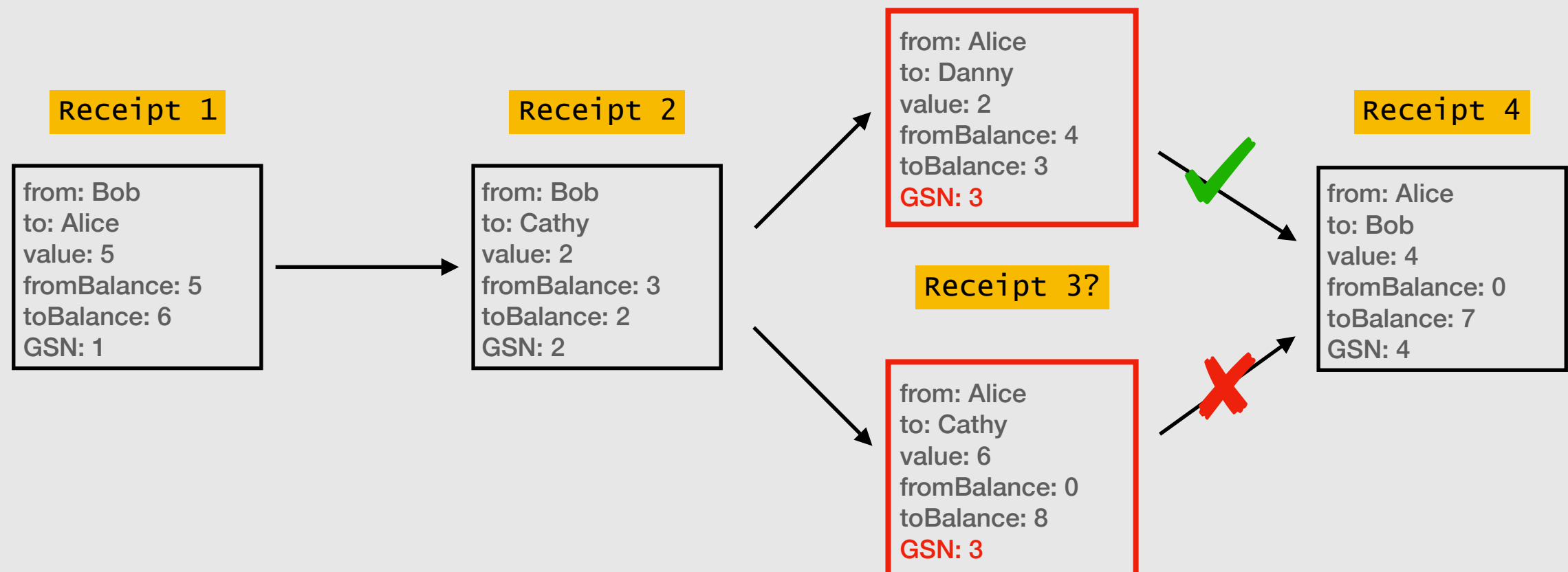
Fraud Proof (1)

Non-existed Receipt



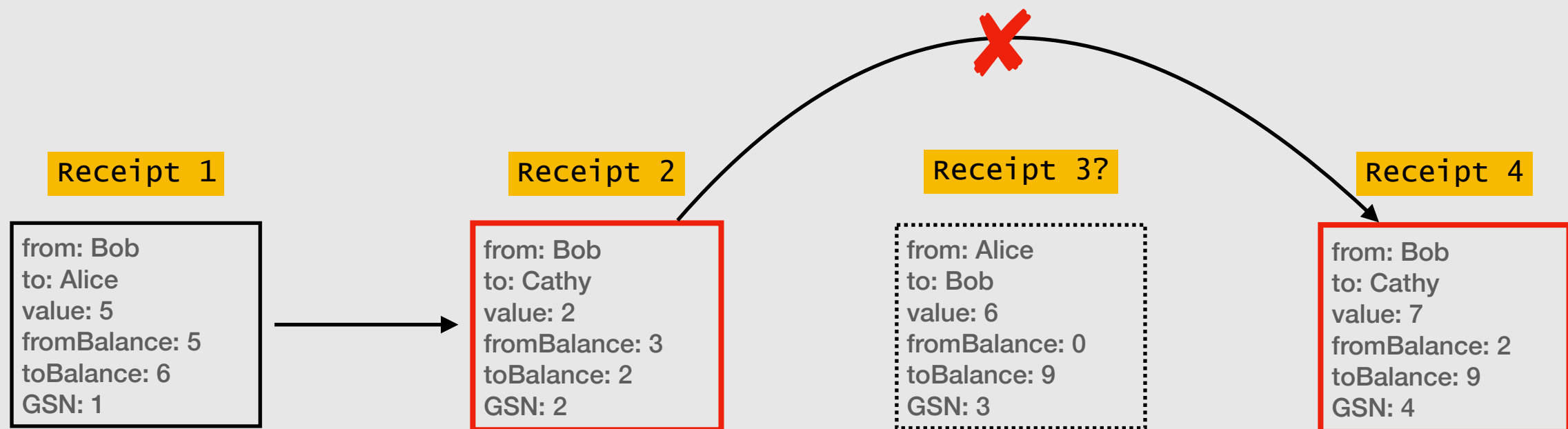
Fraud Proof (2)

Receipt with Repeated GSN



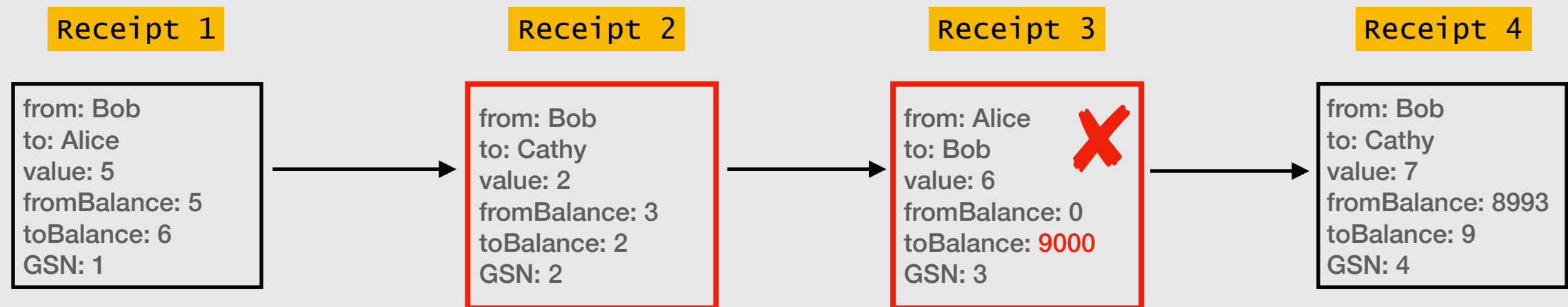
Fraud Proof (3)

Receipt with Skipped GSN



Fraud Proof (4)

Receipt with Wrong Balance



Conclusion

- ▶ The essential part of layer 2 solution is to design a system that incentivizes participants to do the right thing
- ▶ Website: <https://bolt.infinitechain.io/en/>
- ▶ Github: <https://github.com/BOLT-Protocol>

Demo



PingPay is a blockchain wallet that
also connects to BOLT booster