BOLT: Booster of Ledger Technology

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

BOLT.infinitechain.io

Outline

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

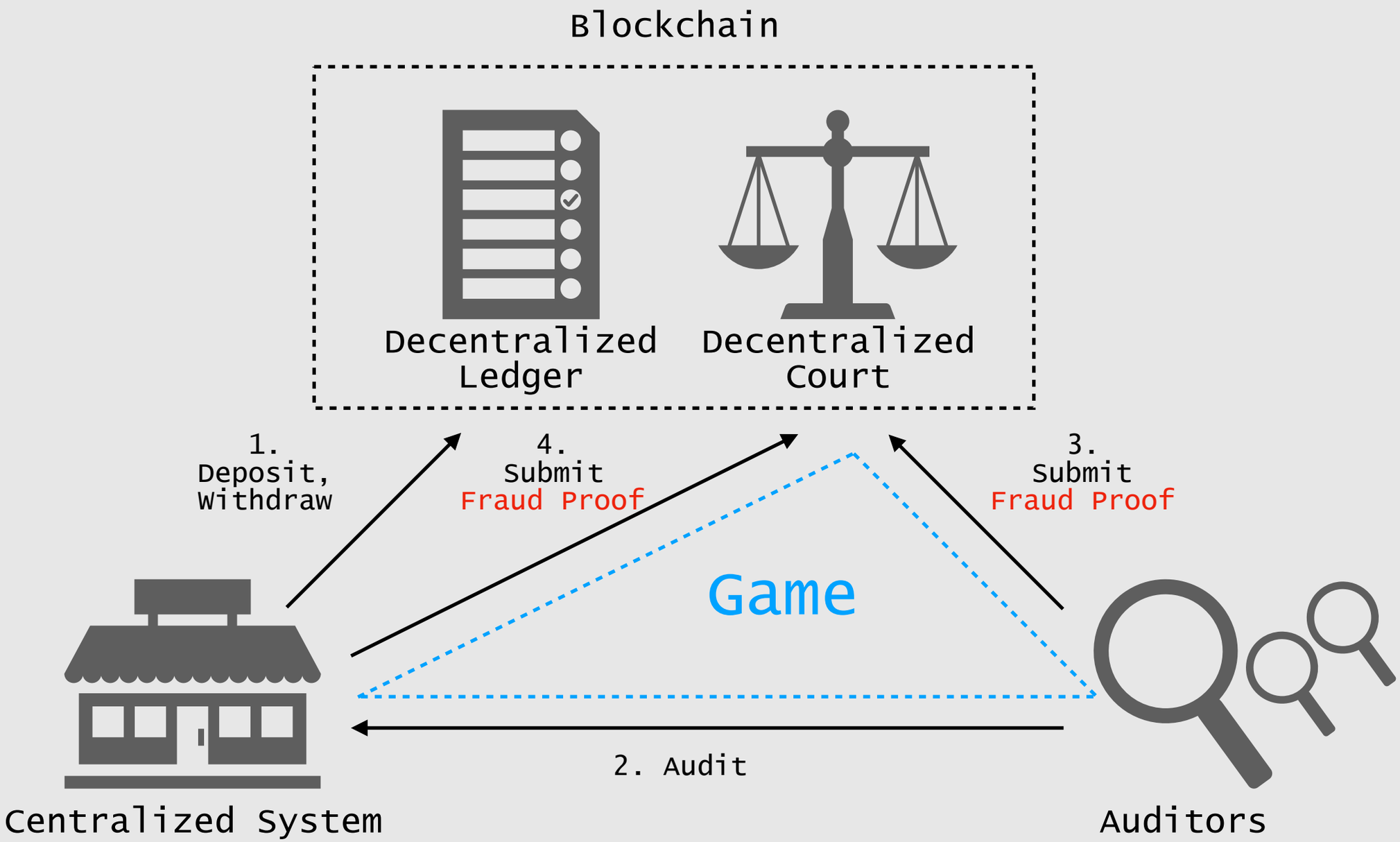
Overview (1)

- 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

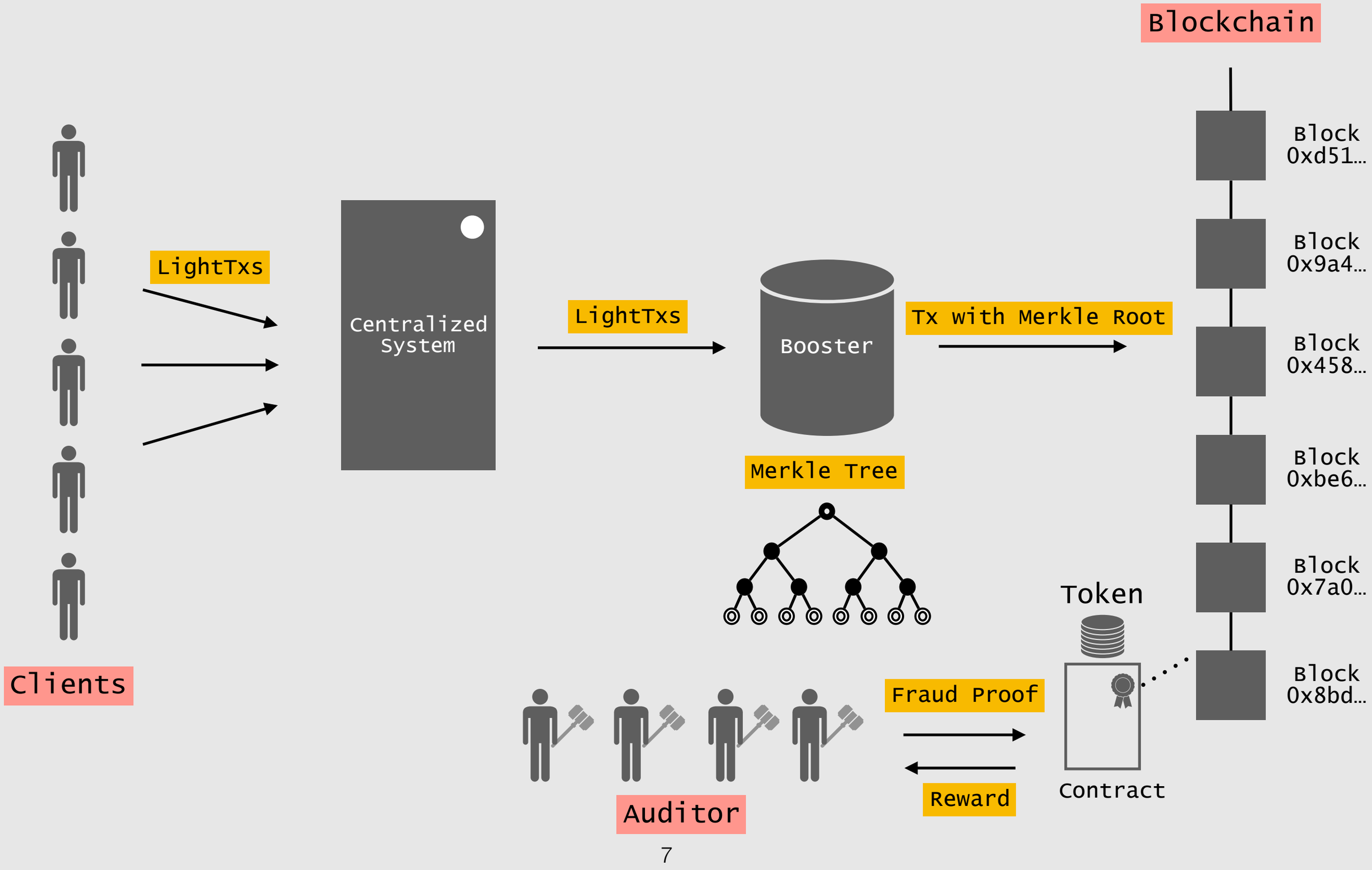
Anti-fraud Mechanism



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

lightTxHash

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

```
metadata = {
  client
}
```

```
sig = {
  clientLightTx,
}
```

Protocol

Data Model

Receipt

lightTxHash

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

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

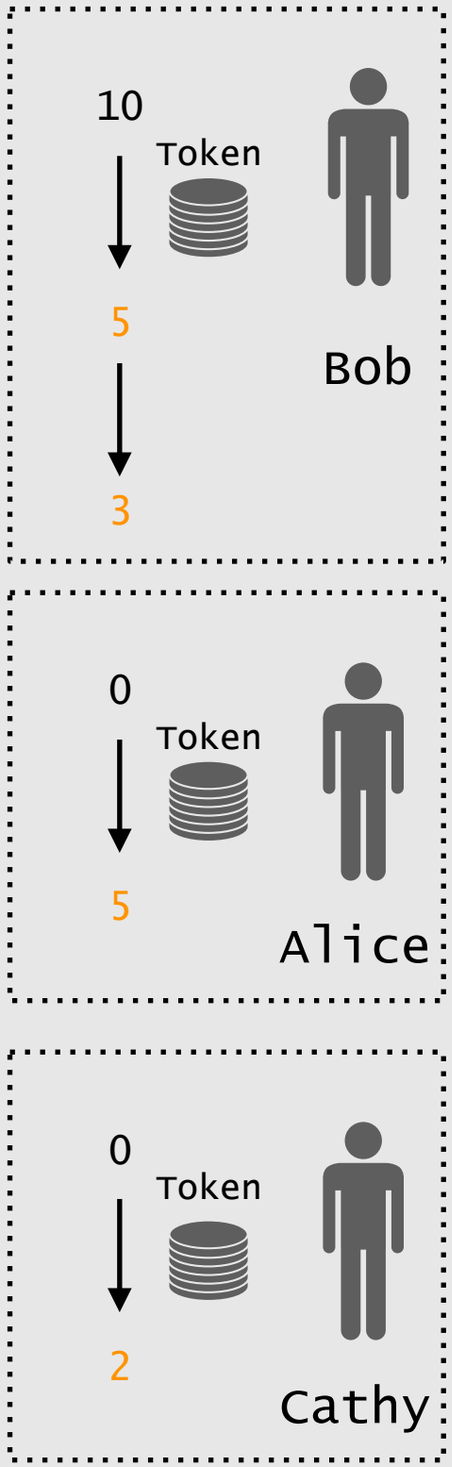
receiptHash

```
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

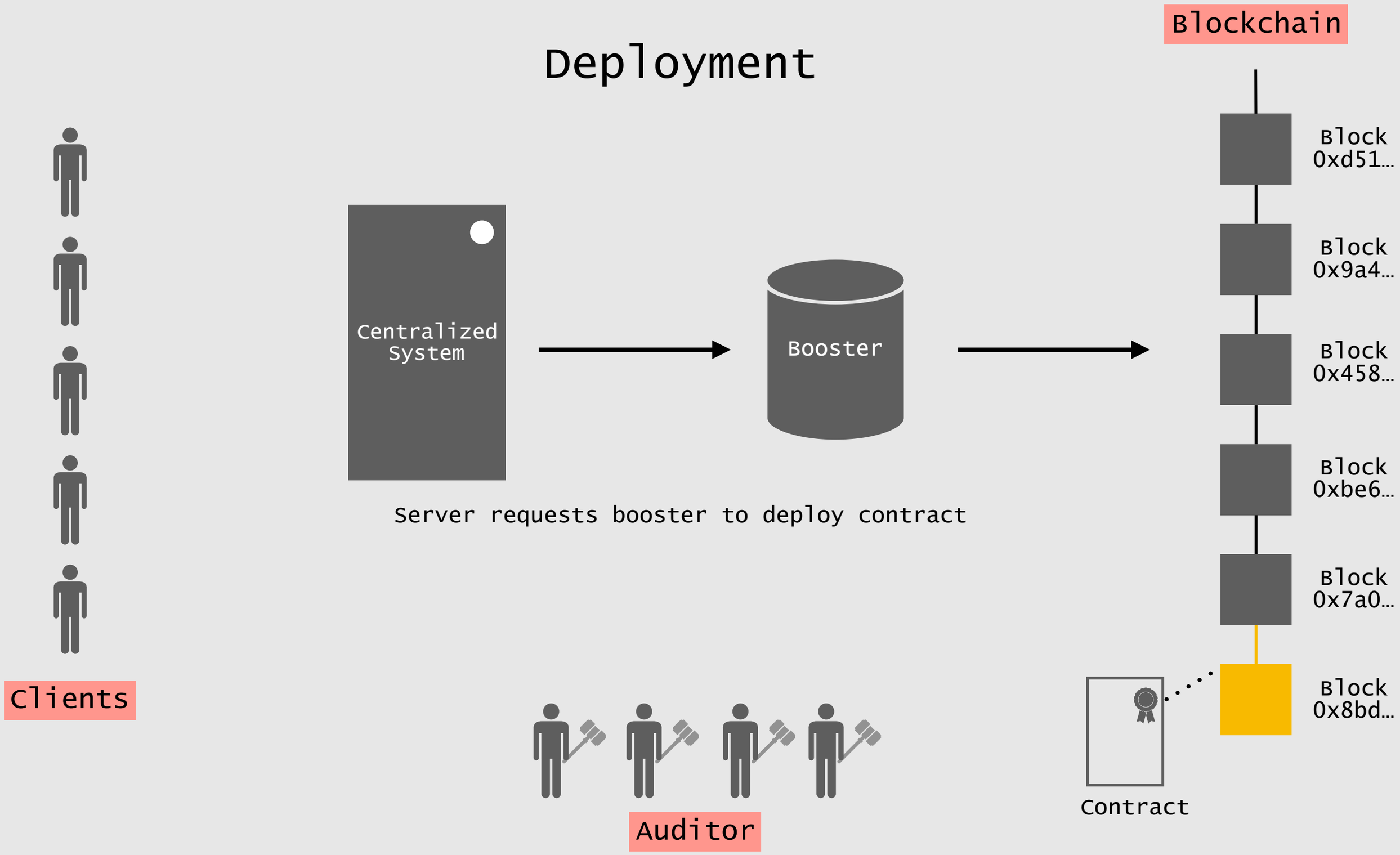
Receipt 1

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

Receipt 2

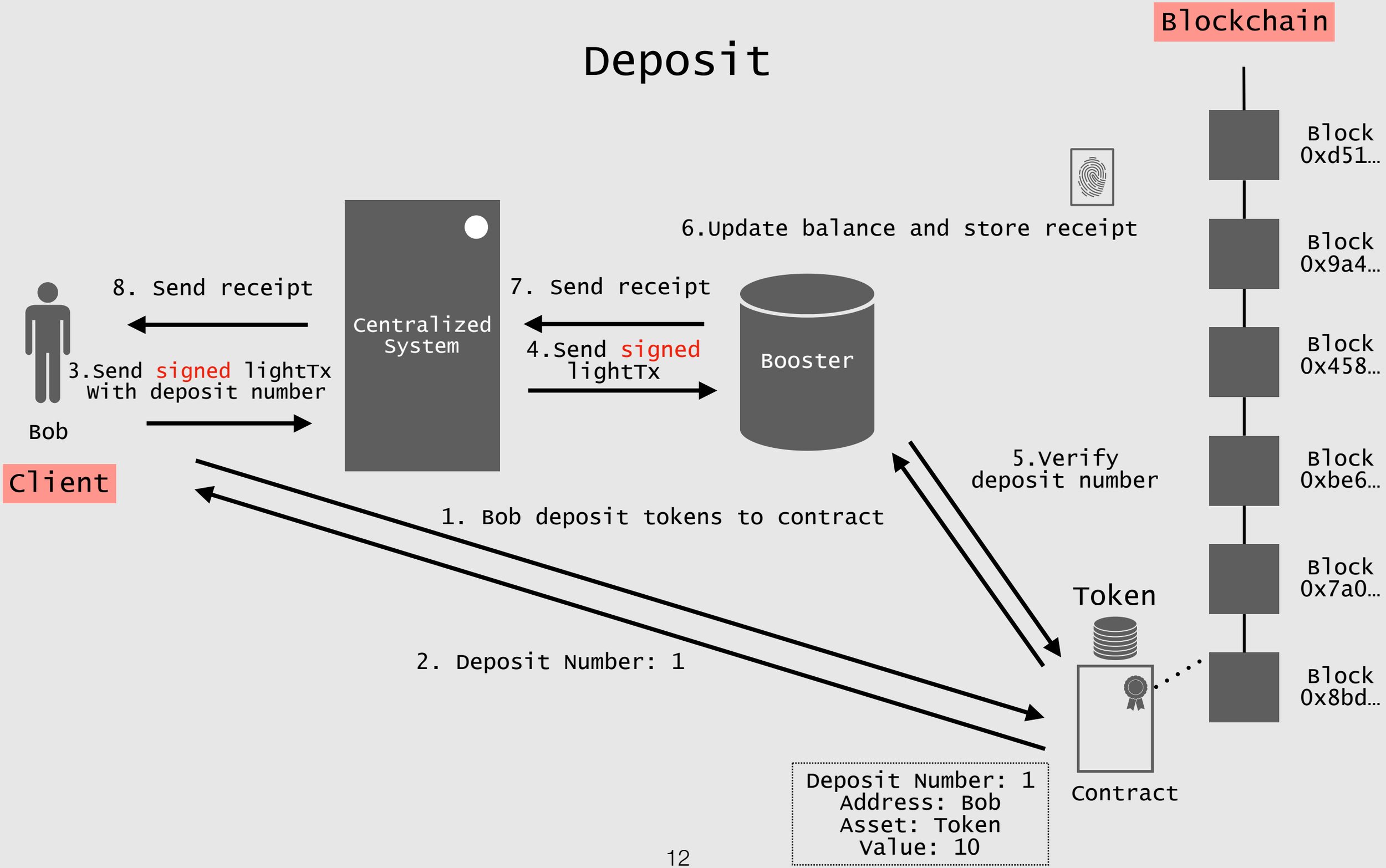
Protocol

Deployment



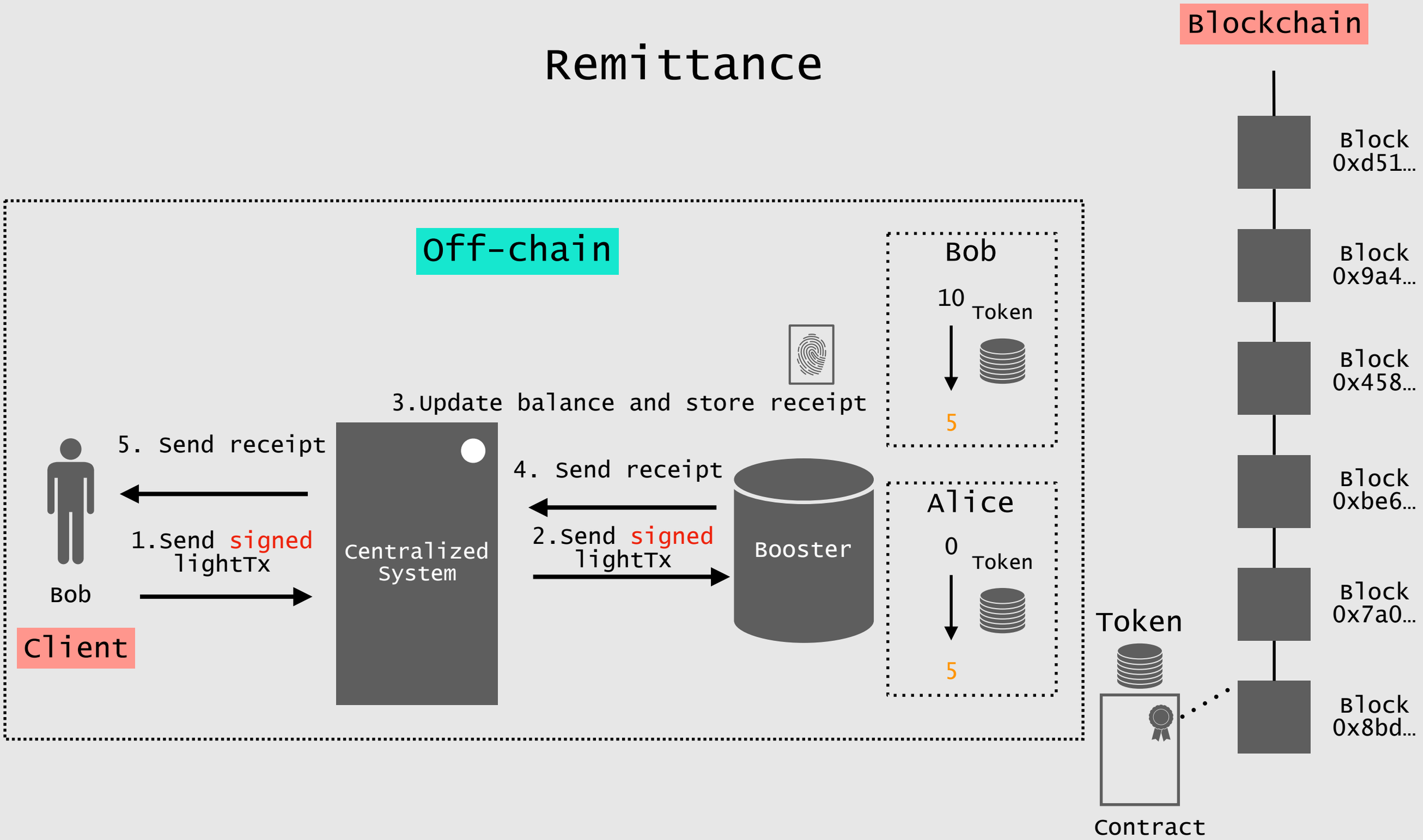
Protocol

Deposit



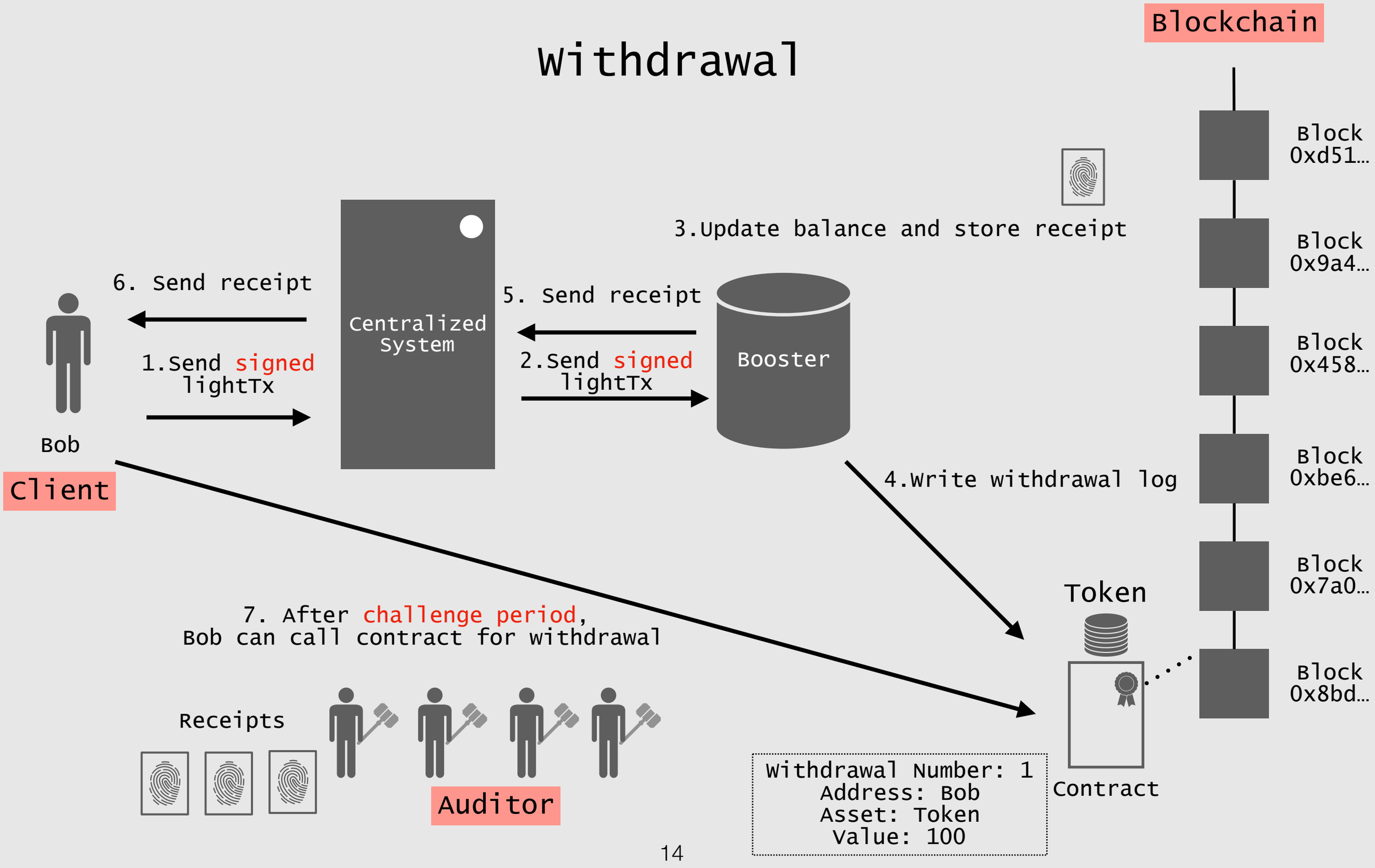
Protocol

Remittance



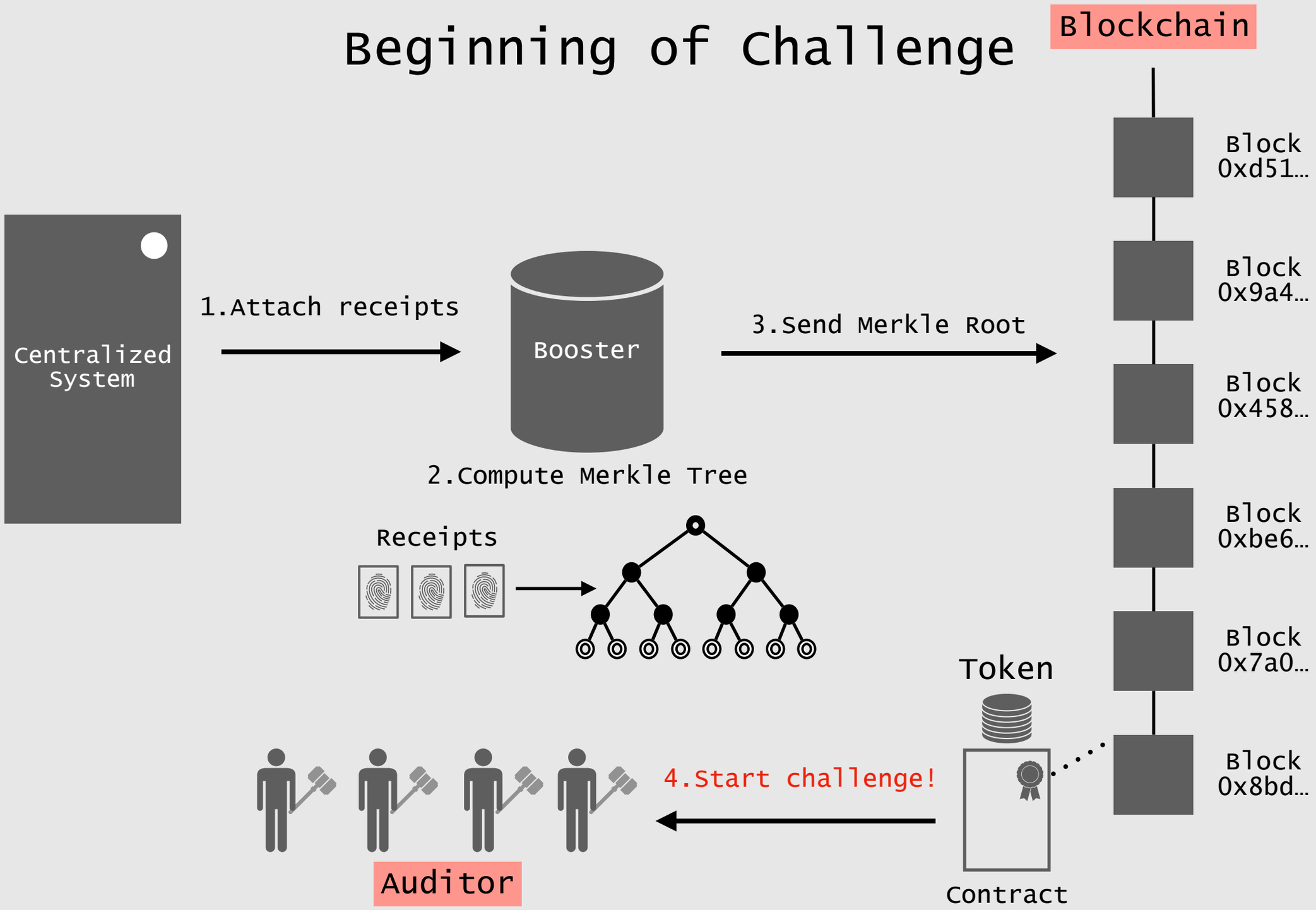
Protocol

Withdrawal



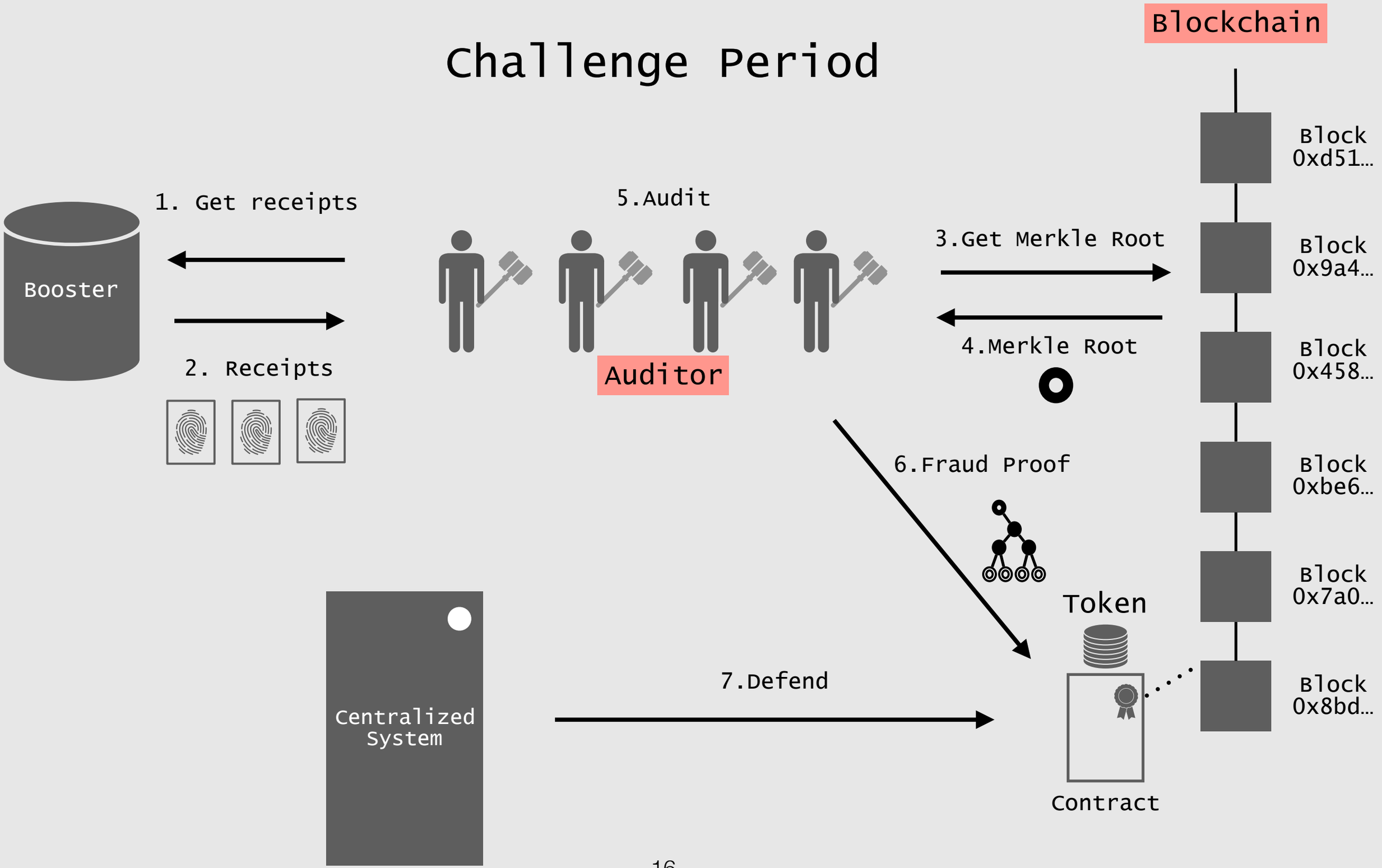
Protocol

Beginning of Challenge



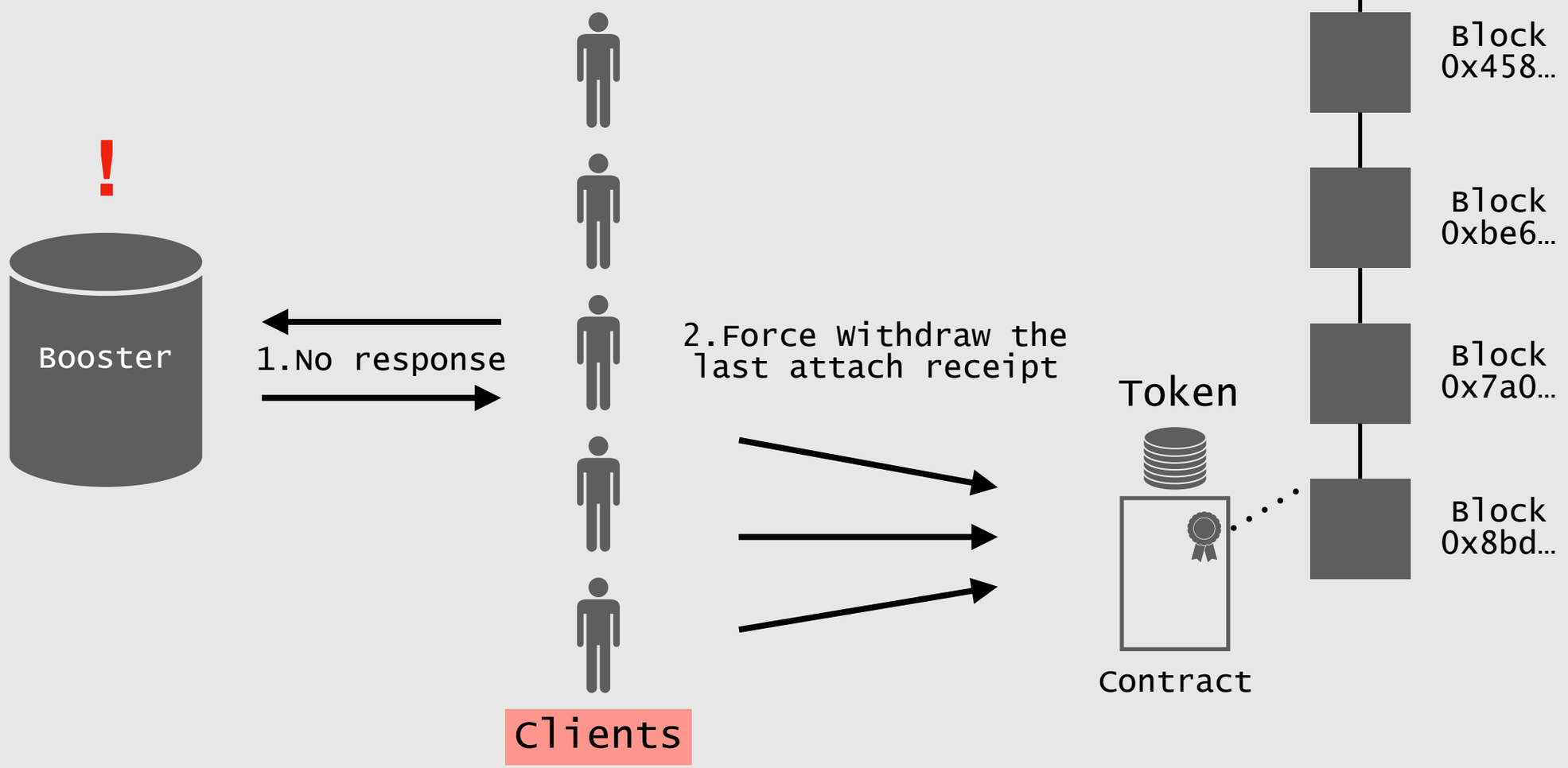
Protocol

Challenge Period



Protocol

Forced Withdrawal



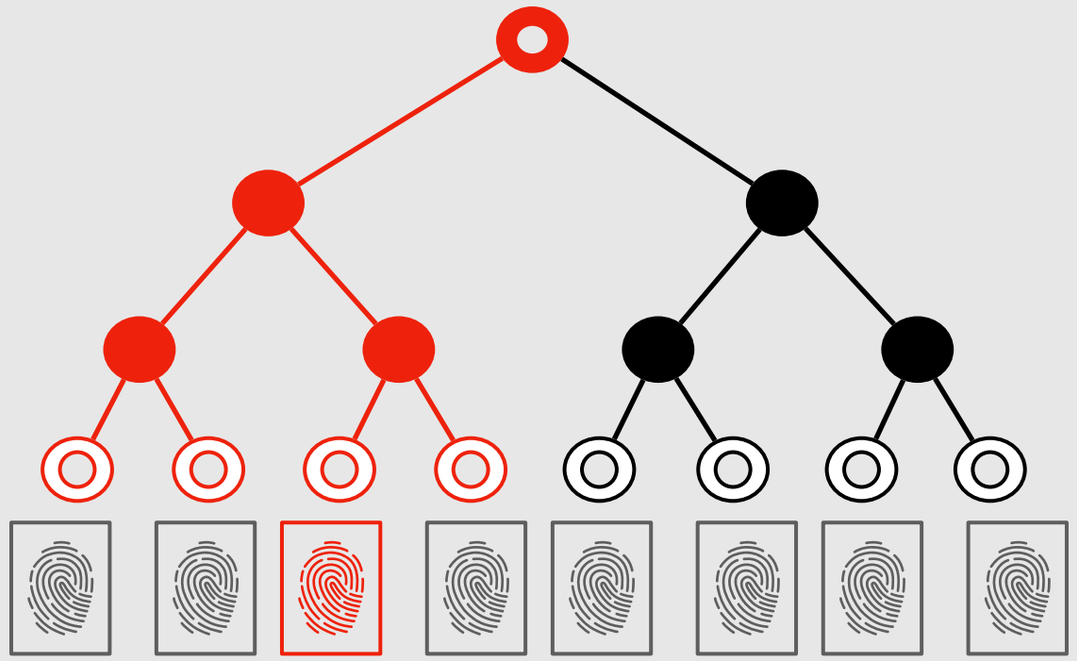
Protocol

Fraud Proof

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

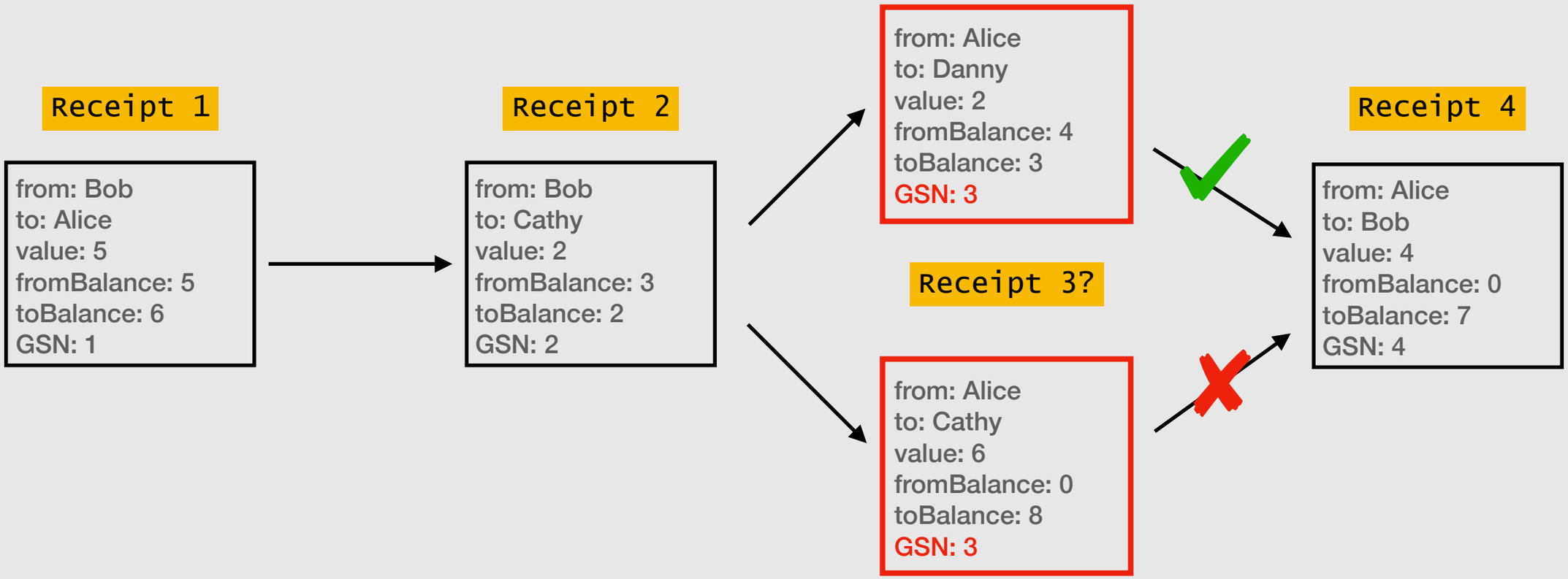
Fraud Proof (1)

Non-existed Receipt



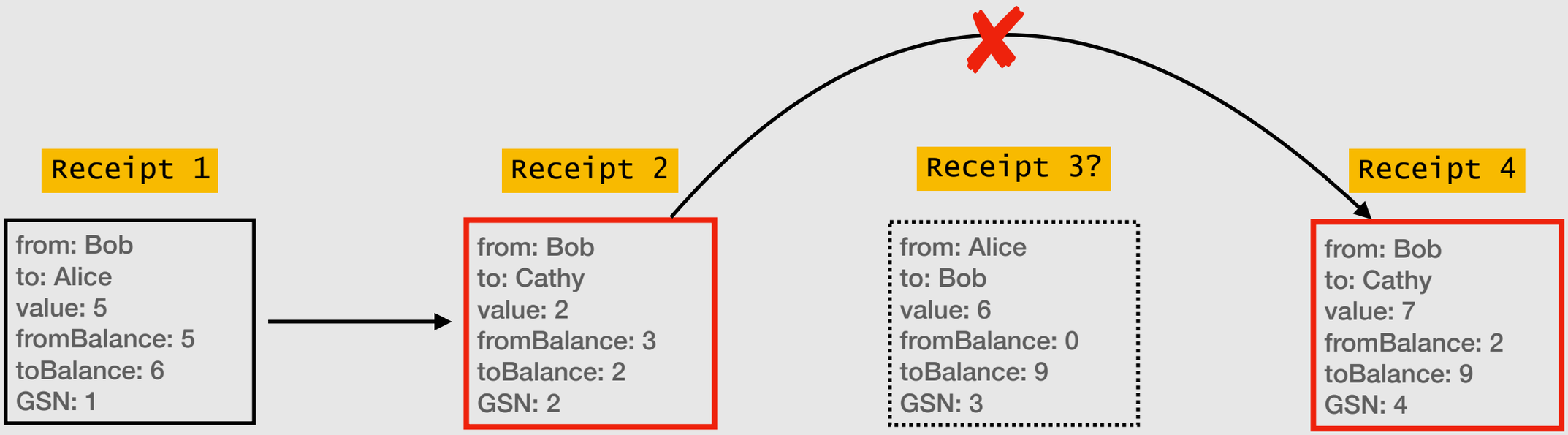
Fraud Proof (2)

Receipt with Repeated GSN



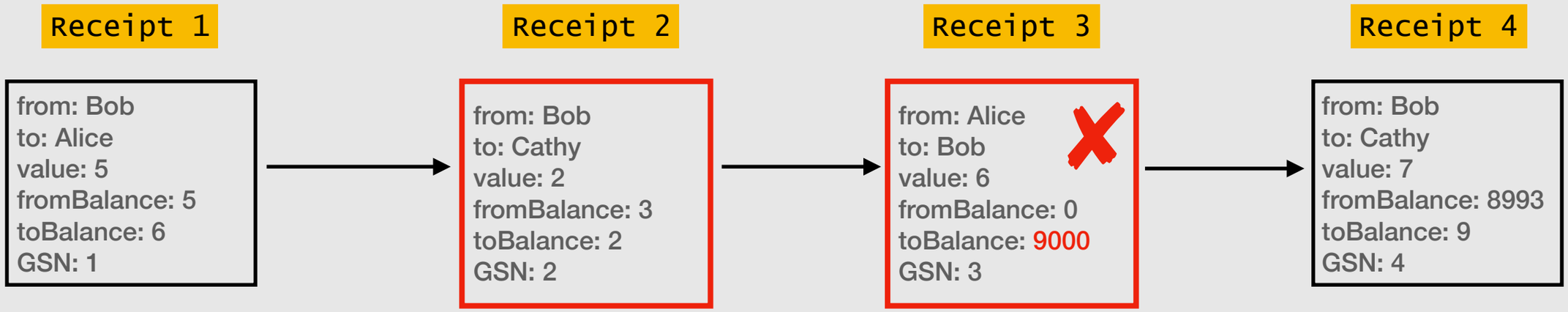
Fraud Proof (3)

Receipt with Skipped GSN



Fraud Proof (4)

Receipt with Wrong Balance



Demo

PingPay is a blockchain wallet that also connects to BOLT booster