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

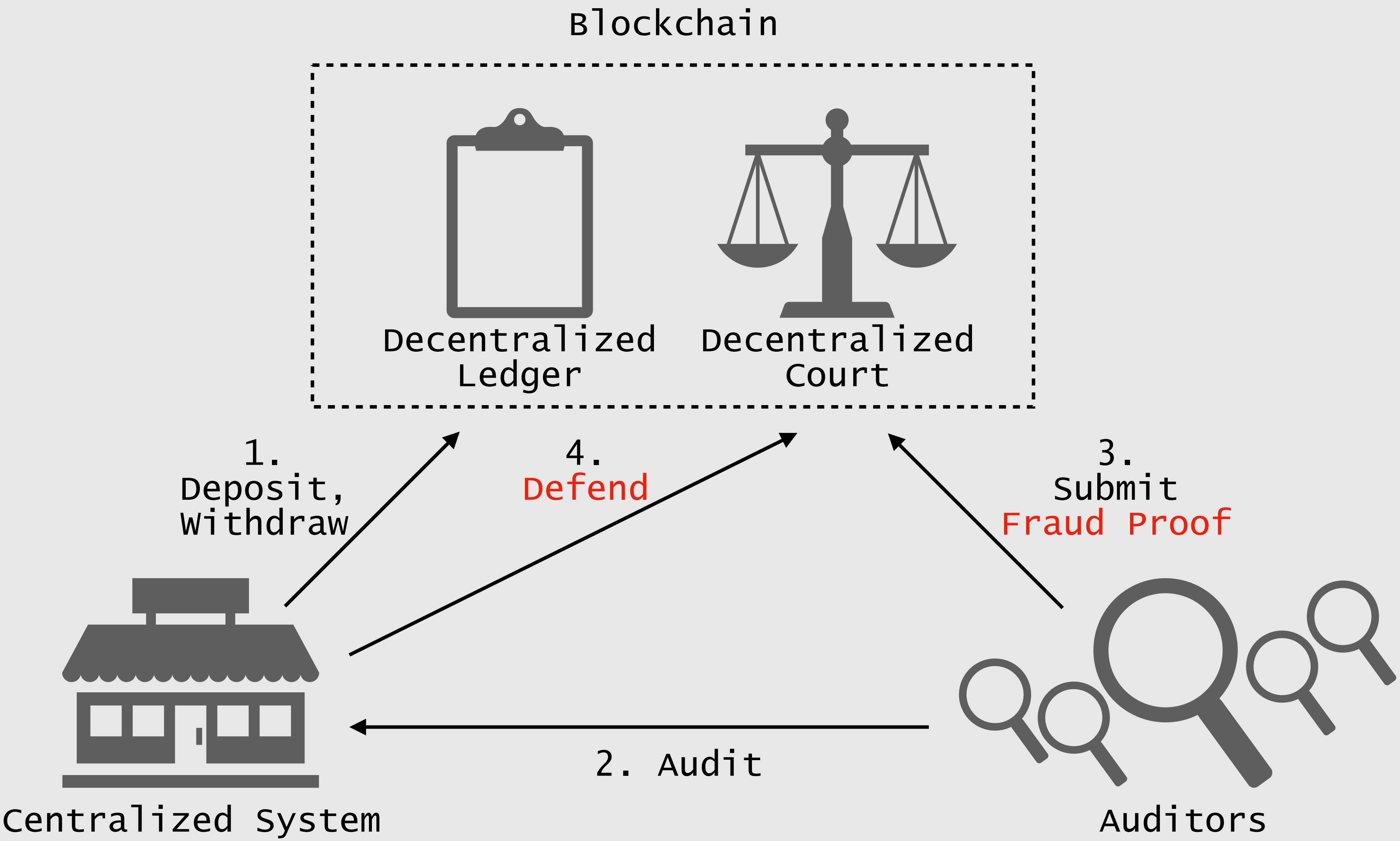
Overview (1)

- BOLT is a layer 2 scalability solution that integrates centralized system
- Borrow ideas from state channel, truebit and plasma
- Use cases include E-commerce, …

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



Blockchain

Decentralized Ledger

Decentralized Court

1. Deposit, Withdraw

2. Audit

3. Submit Fraud Proof

4. Defend

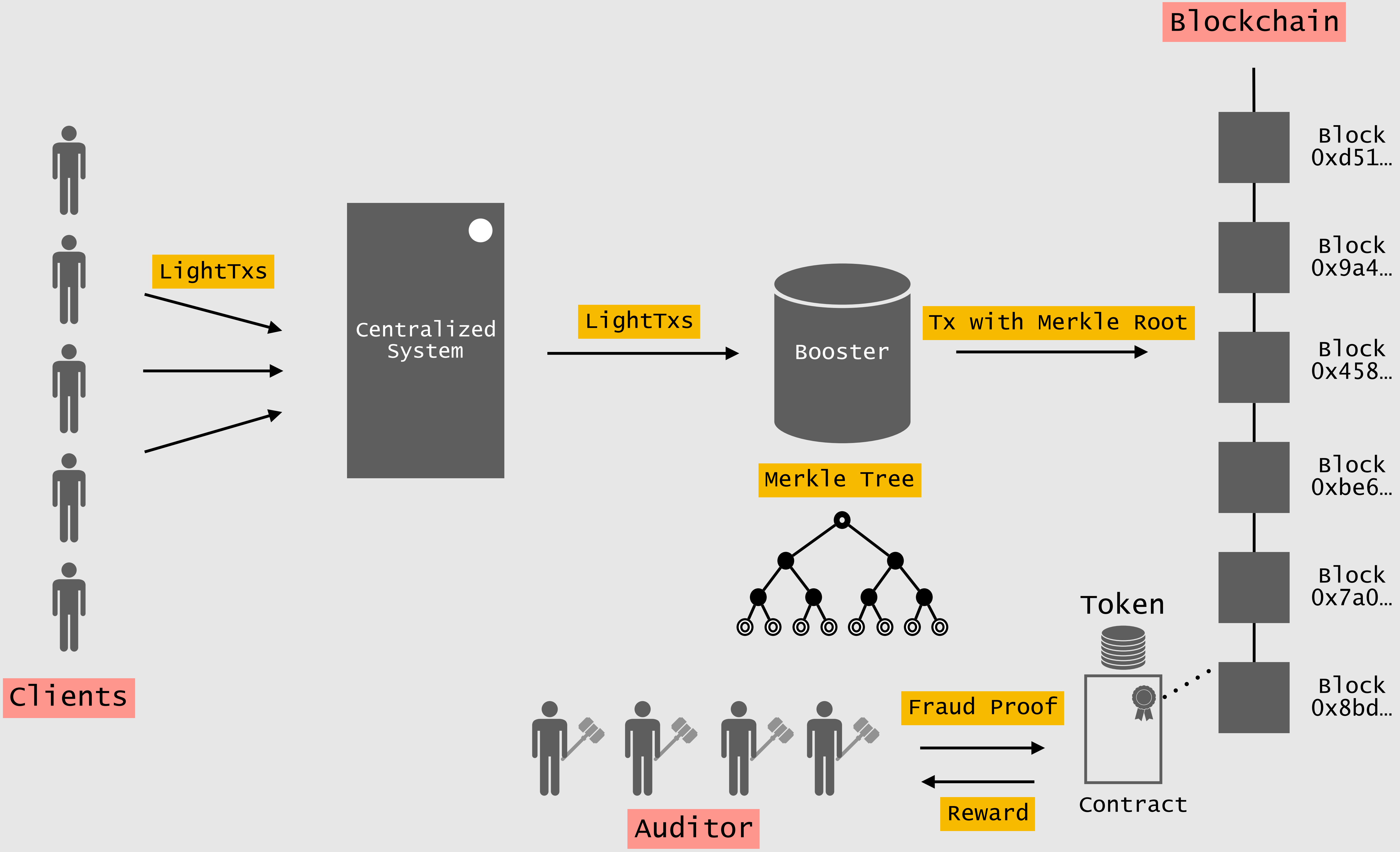
Centralized System

Auditors

Anti-fraud Mechanism

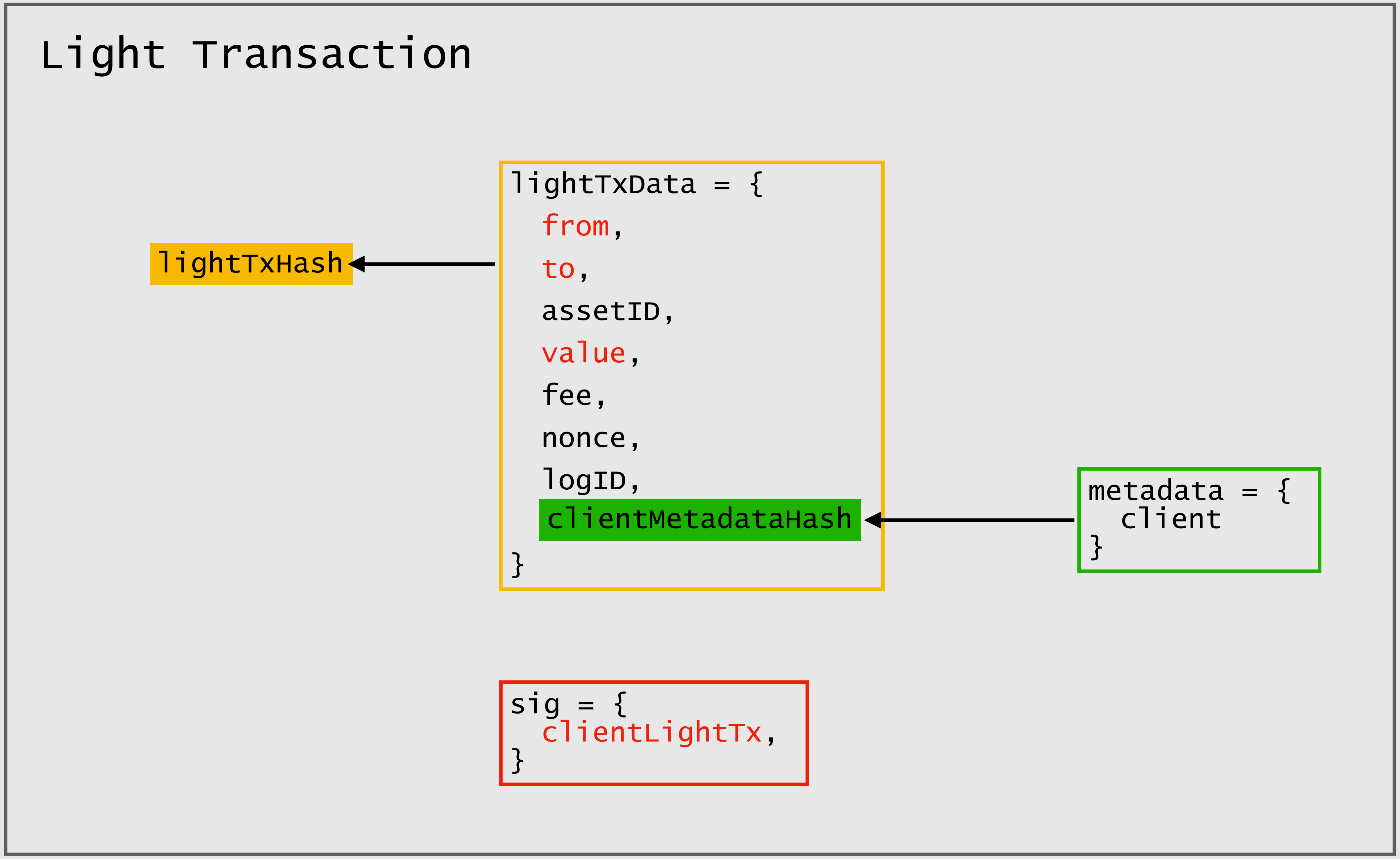
- Centralized System v.s Auditors
- The essential part of decentralization is to design a system that makes participants inspect each other like a game and incentivize participants to do the right thing
- Similar design in Truebit

Architecture



Protocol

Data Model



Light Transaction

lightTxHash

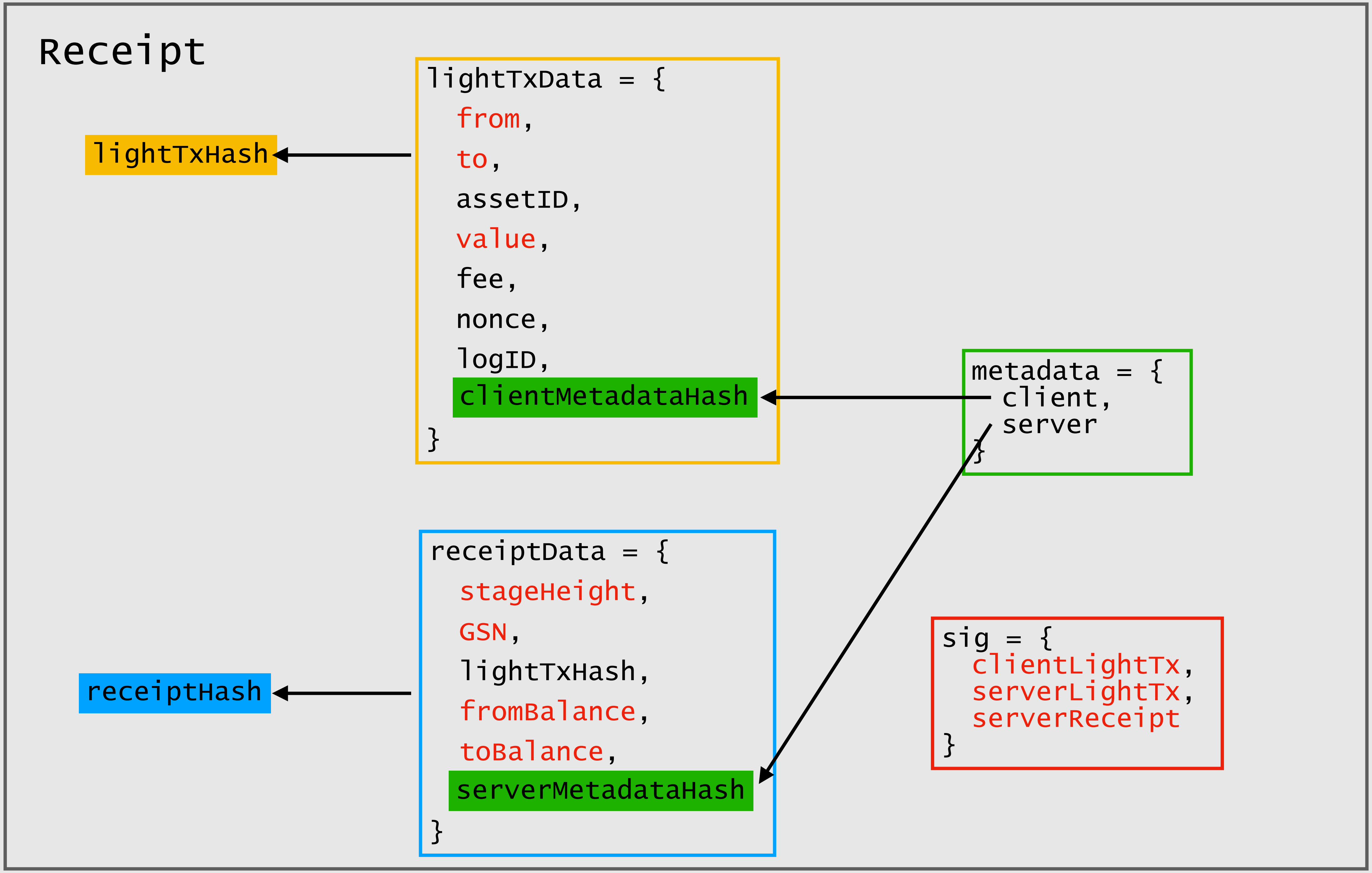
```
lightTxData = {
  from,
  to,
  assetID,
  value,
  fee,
  nonce,
  logID,
  clientMetadataHash
}
```

```
metadata = {
  client
}
```

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

Protocol

Data Model



Receipt

lightTxHash

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

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

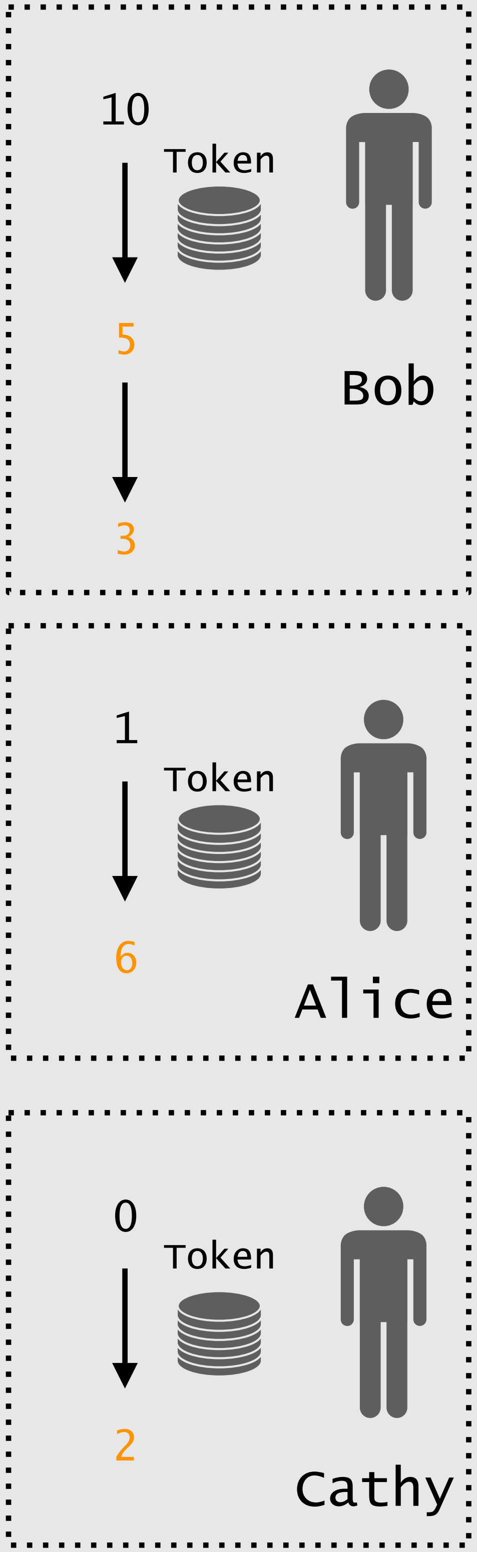
receiptHash

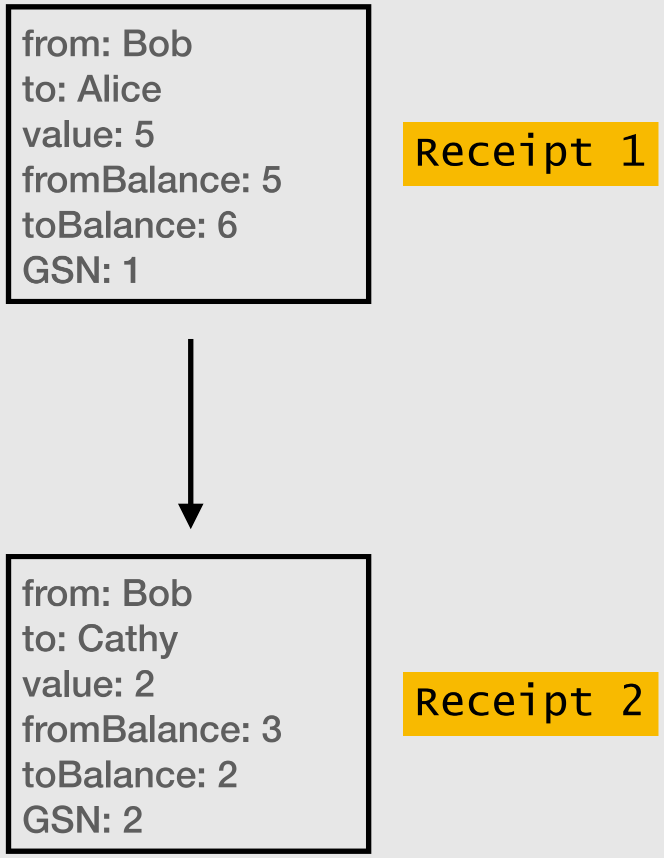
```
receiptData = {
  stageHeight,
  GSN,
  lightTxHash,
  fromBalance,
  toBalance,
  serverMetadataHash
}
```

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

Protocol

Example





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

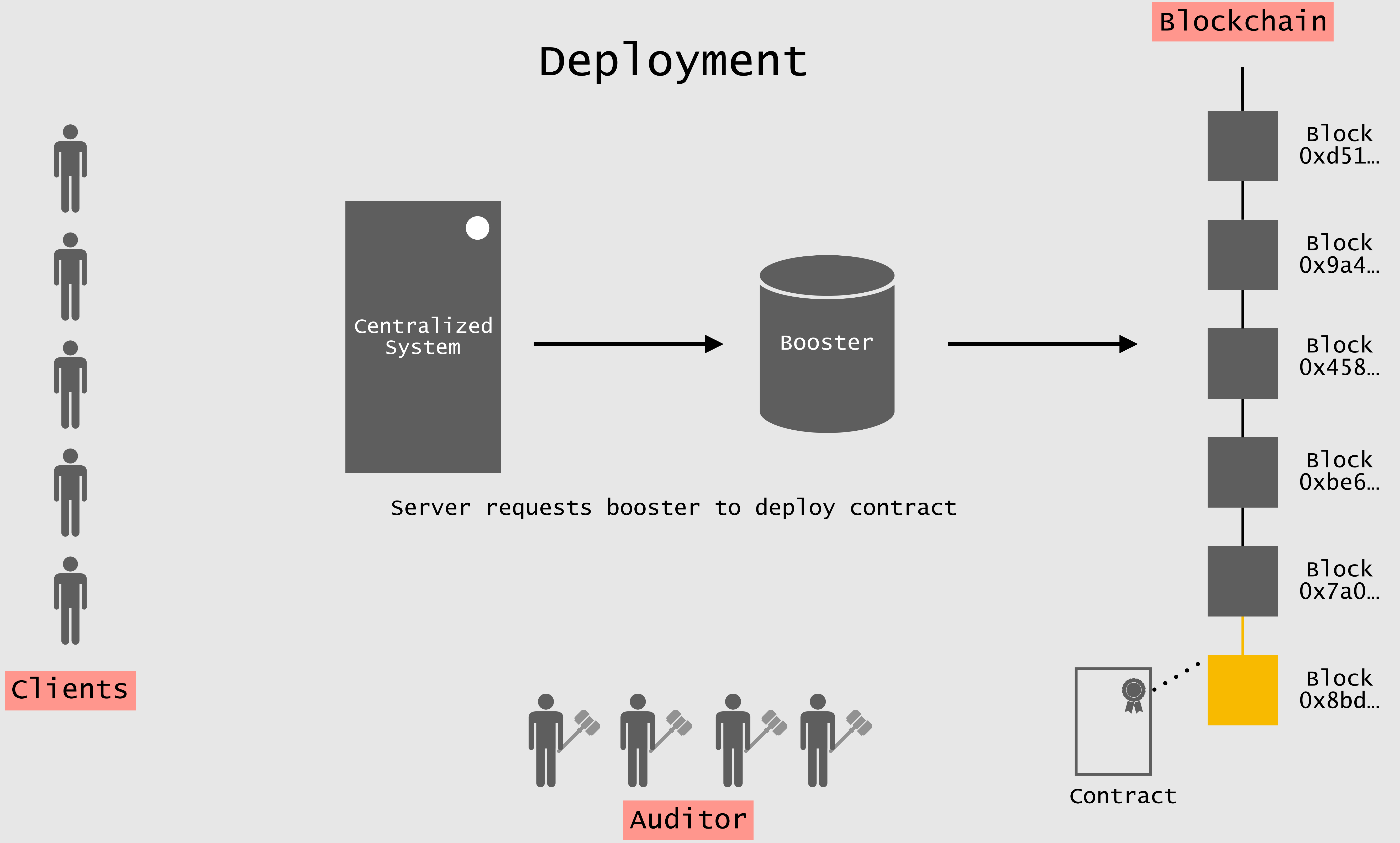
Receipt 1

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

Receipt 2

Protocol

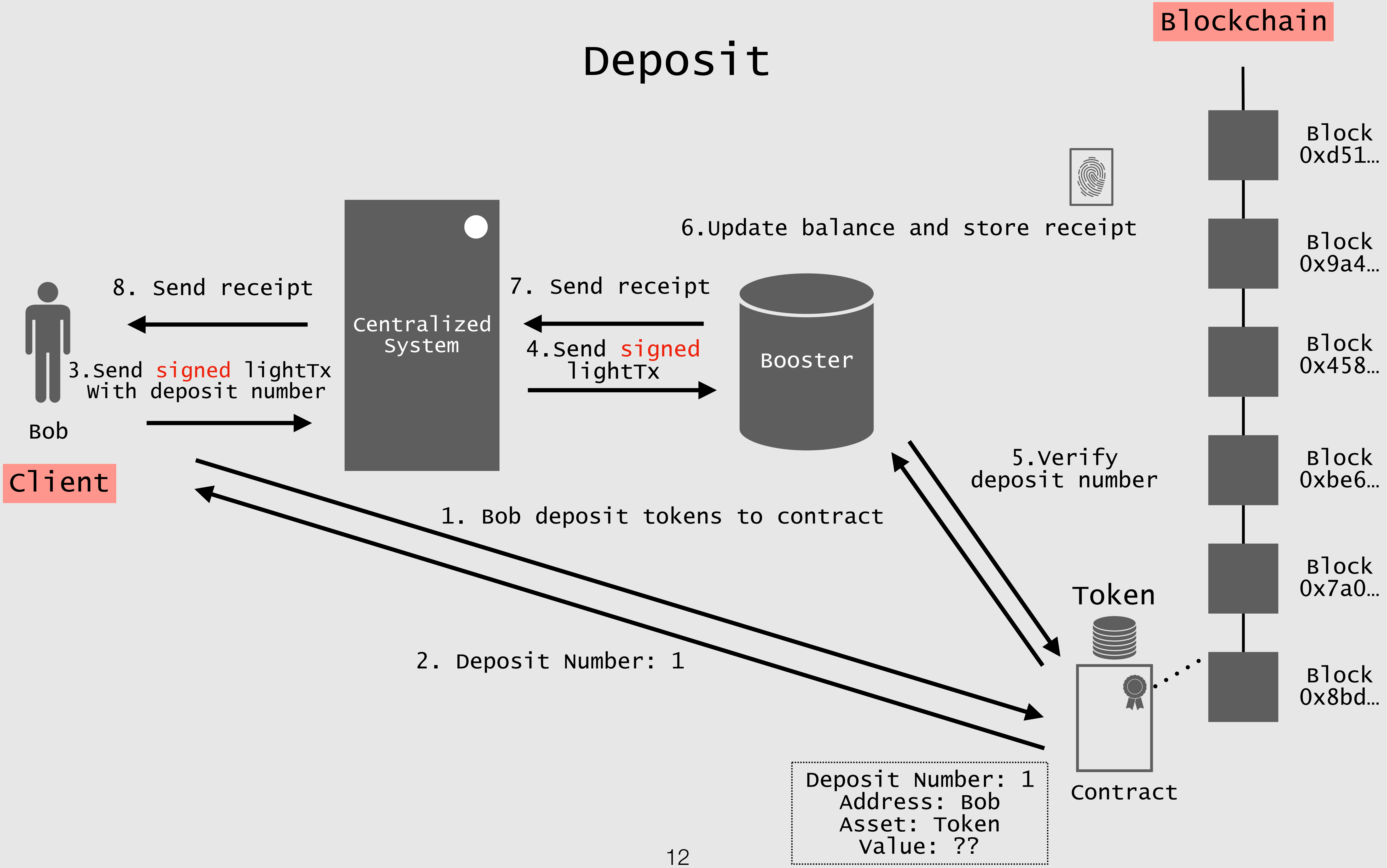
Deployment



Server requests booster to deploy contract

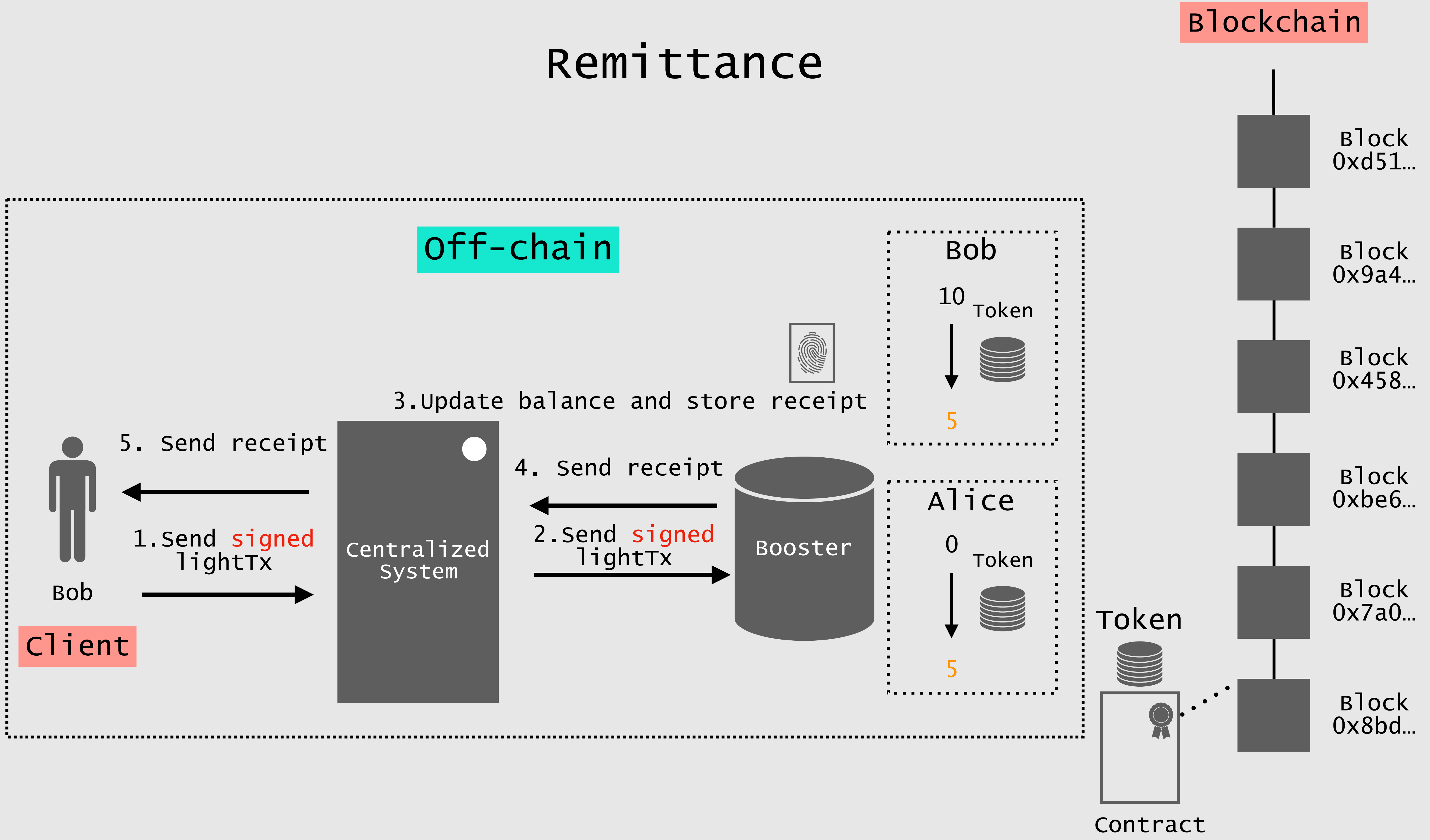
Protocol

Deposit



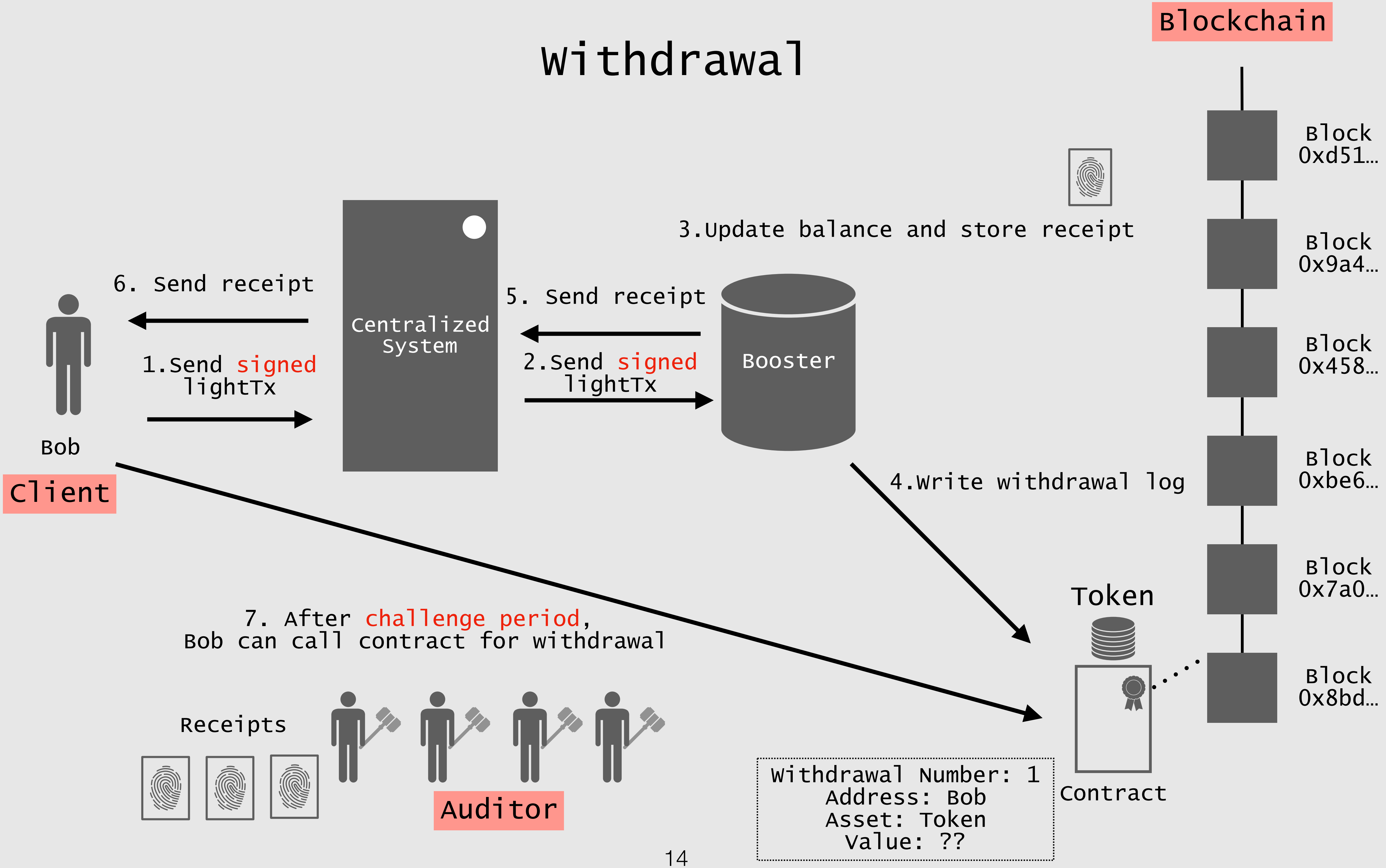
Protocol

Remittance



Protocol

Withdrawal



Blockchain

Block
0xd51…

Block
0x9a4…

Block
0x458…

Block
0xbe6…

Block
0x7a0…

Block
0x8bd…

3.Update balance and store receipt

6. Send receipt

5. Send receipt

Centralized System

Booster

1.Send signed lightTx

2.Send signed lightTx

Bob

Client

4.Write withdrawal log

Token

7. After challenge period, Bob can call contract for withdrawal

Receipts

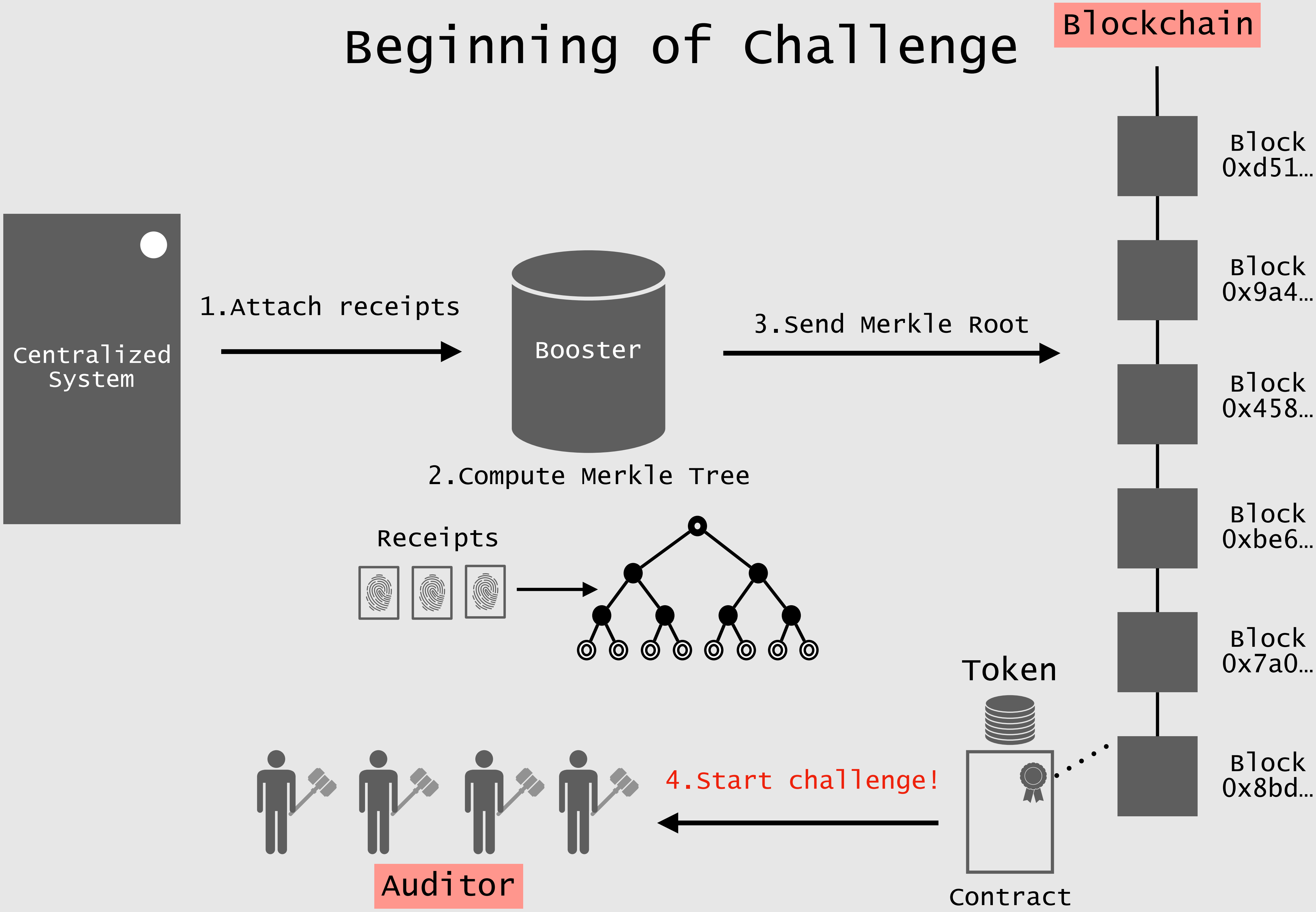
Auditor

Withdrawal Number: 1
Address: Bob
Asset: Token
Value: ??

Contract

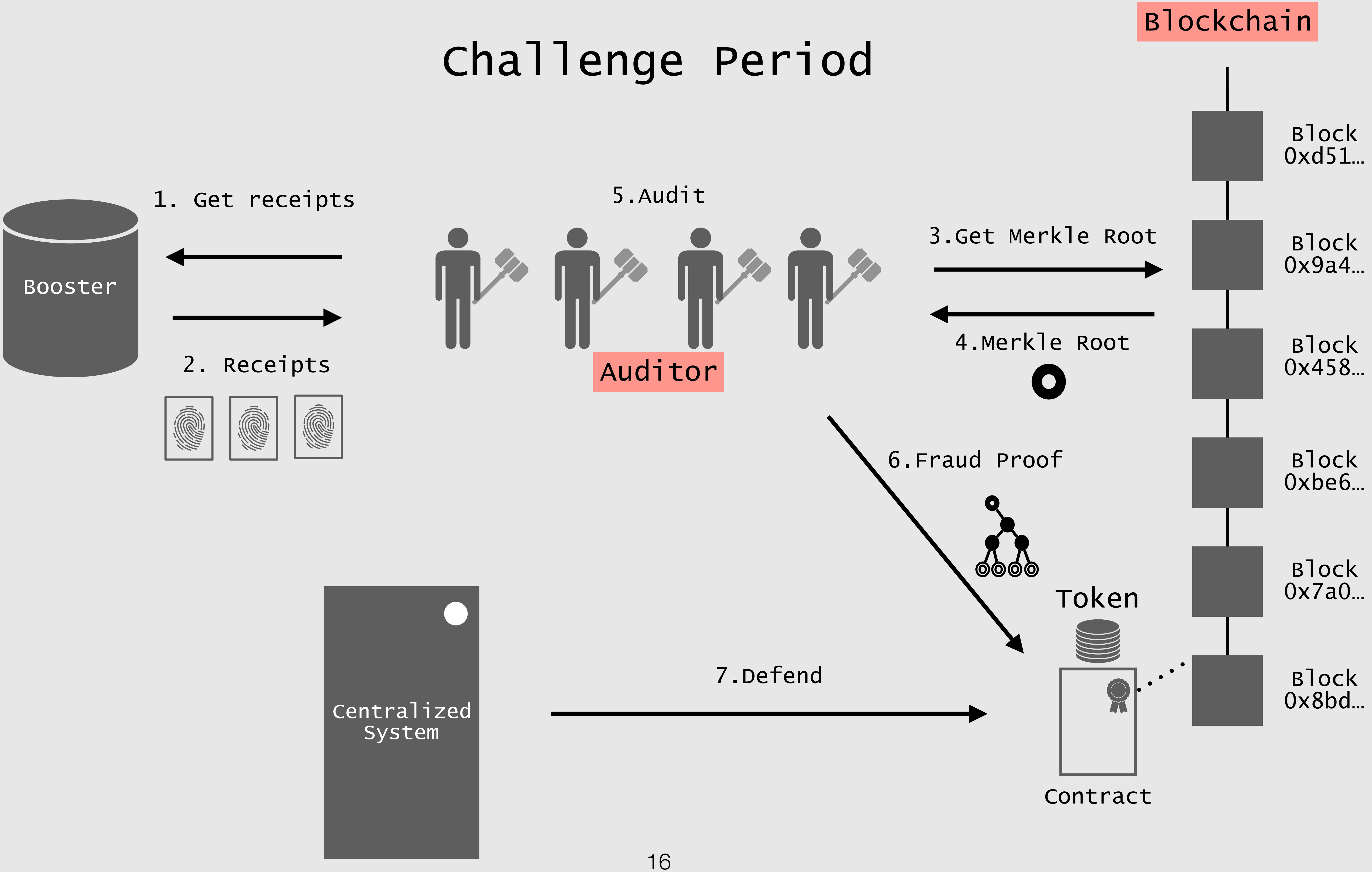
Protocol

Beginning of Challenge



Protocol

Challenge Period



Blockchain

Block 0xd51…

Block 0x9a4…

Block 0x458…

Block 0xbe6…

Block 0x7a0…

Block 0x8bd…

Booster

1. Get receipts

2. Receipts

5.Audit

Auditor

3.Get Merkle Root

4.Merkle Root

6.Fraud Proof

Token

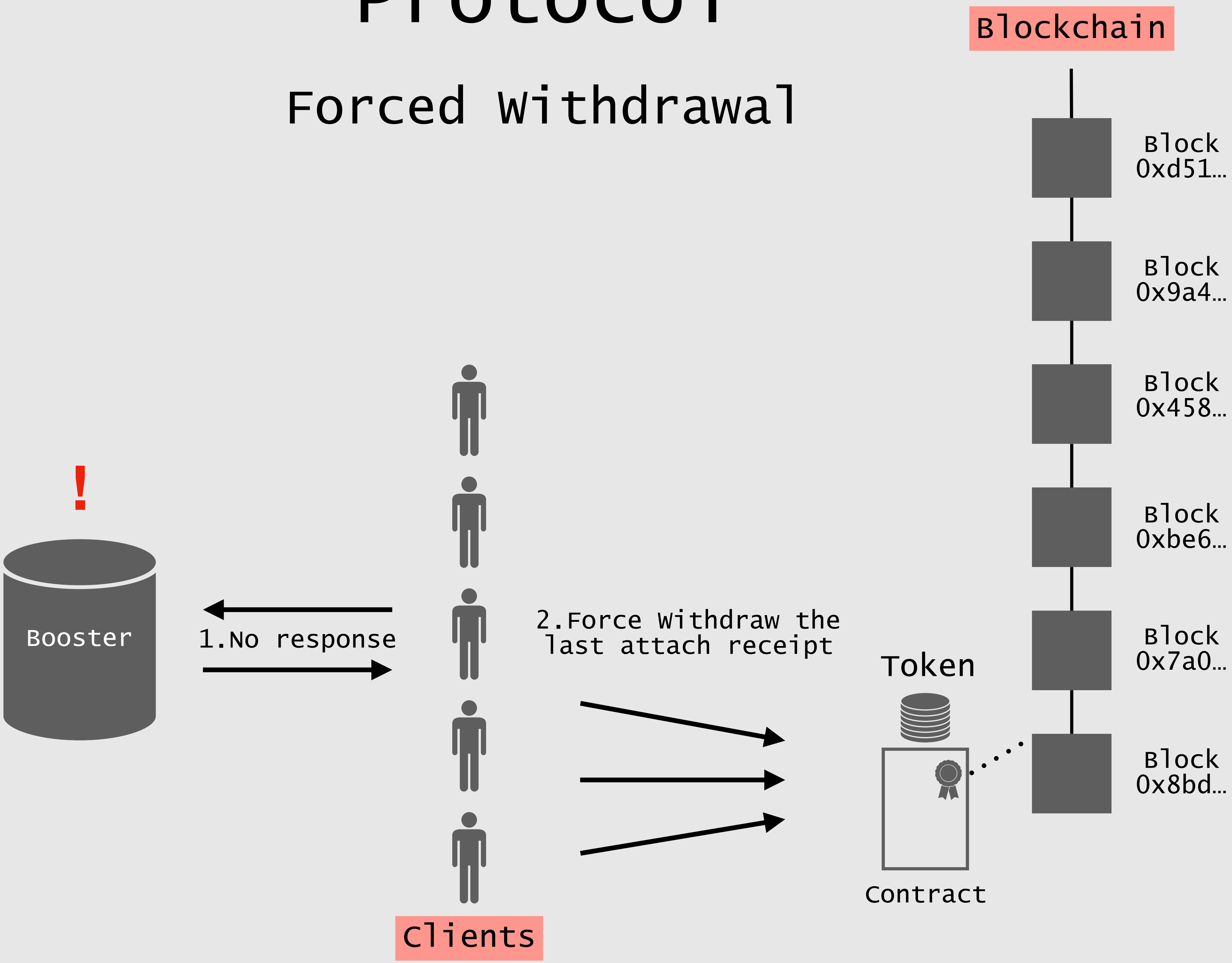
Contract

Centralized System

7.Defend

Protocol

Forced Withdrawal



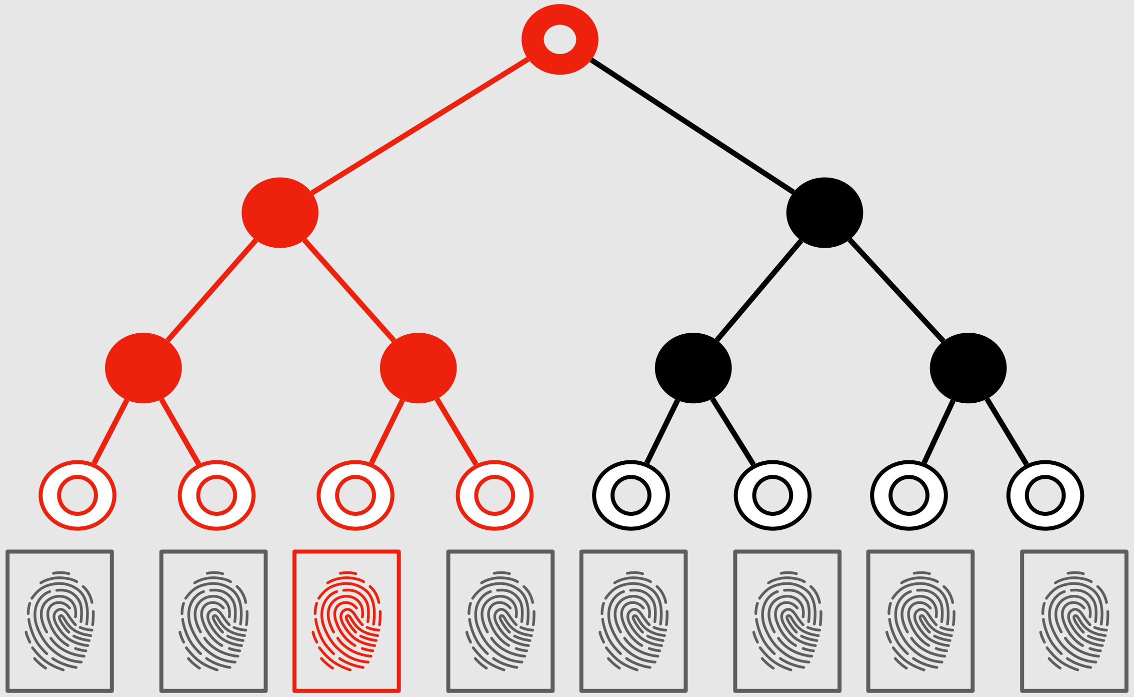
Protocol

Fraud Proof

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

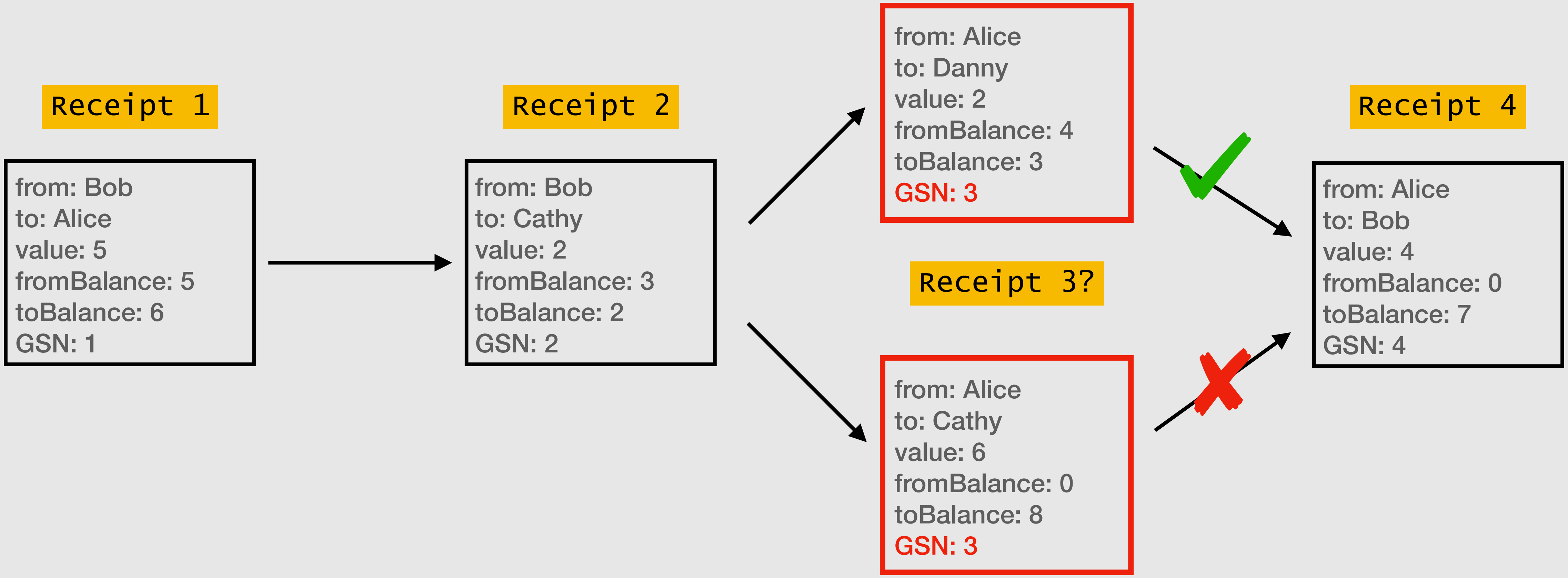
Fraud Proof (1)

Non-existed Receipt



Fraud Proof (2)

Receipt with Repeated GSN



Receipt 1

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

Receipt 2

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

Receipt 3?

from: Alice
to: Danny
value: 2
fromBalance: 4
toBalance: 3
GSN: 3

✓

from: Alice
to: Cathy
value: 6
fromBalance: 0
toBalance: 8
GSN: 3

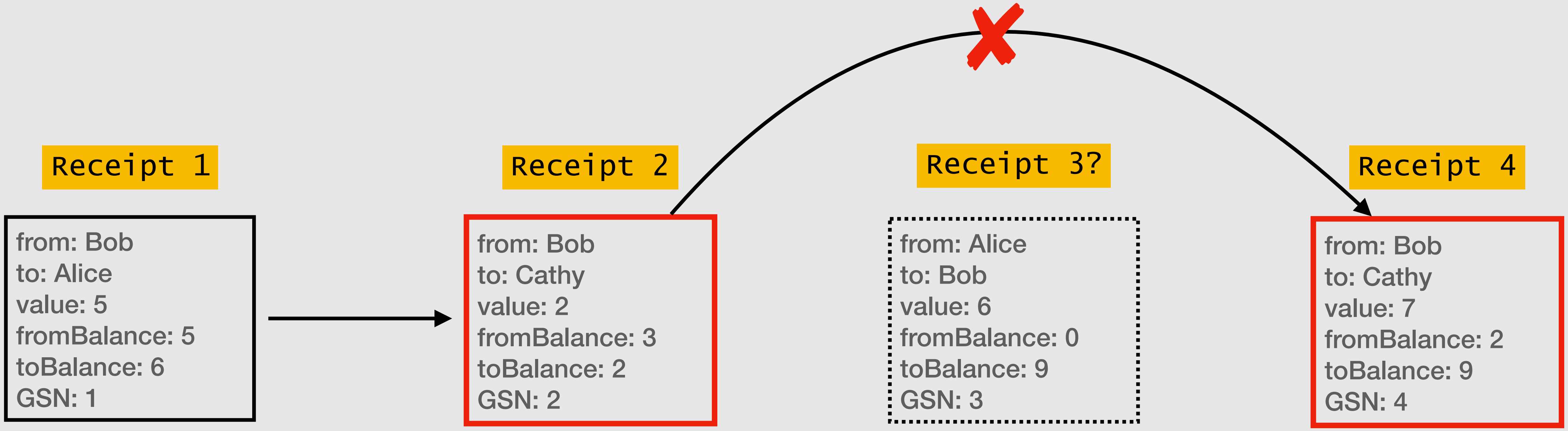
✗

Receipt 4

from: Alice
to: Bob
value: 4
fromBalance: 0
toBalance: 7
GSN: 4

Fraud Proof (3)

Receipt with Skipped GSN



Receipt 1

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

Receipt 2

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

Receipt 3?

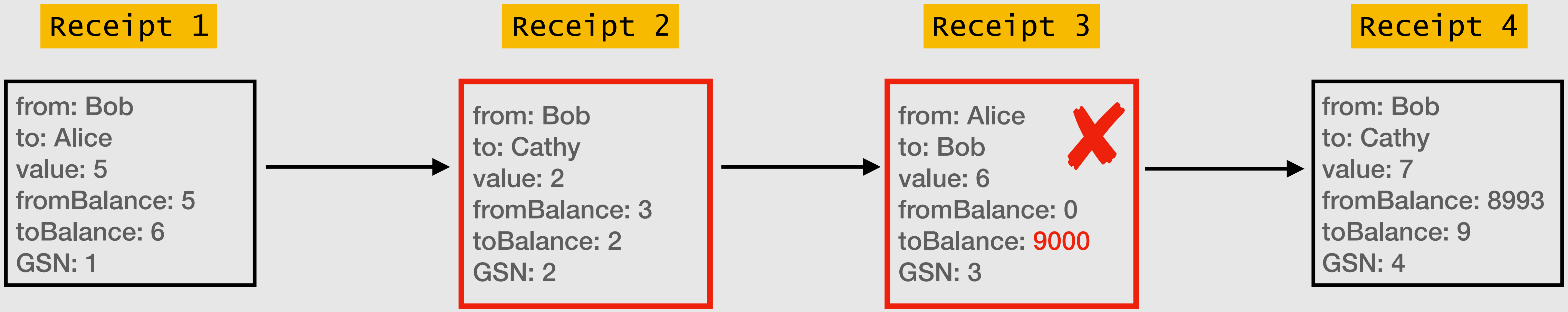
from: Alice
to: Bob
value: 6
fromBalance: 0
toBalance: 9
GSN: 3

Receipt 4

from: Bob
to: Cathy
value: 7
fromBalance: 2
toBalance: 9
GSN: 4

Fraud Proof (4)

Receipt with Wrong Balance



Receipt 1

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

Receipt 2

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

Receipt 3

from: Alice ✗
to: Bob
value: 6
fromBalance: 0
toBalance: 9000
GSN: 3

Receipt 4

from: Bob
to: Cathy
value: 7
fromBalance: 8993
toBalance: 9
GSN: 4

Demo