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

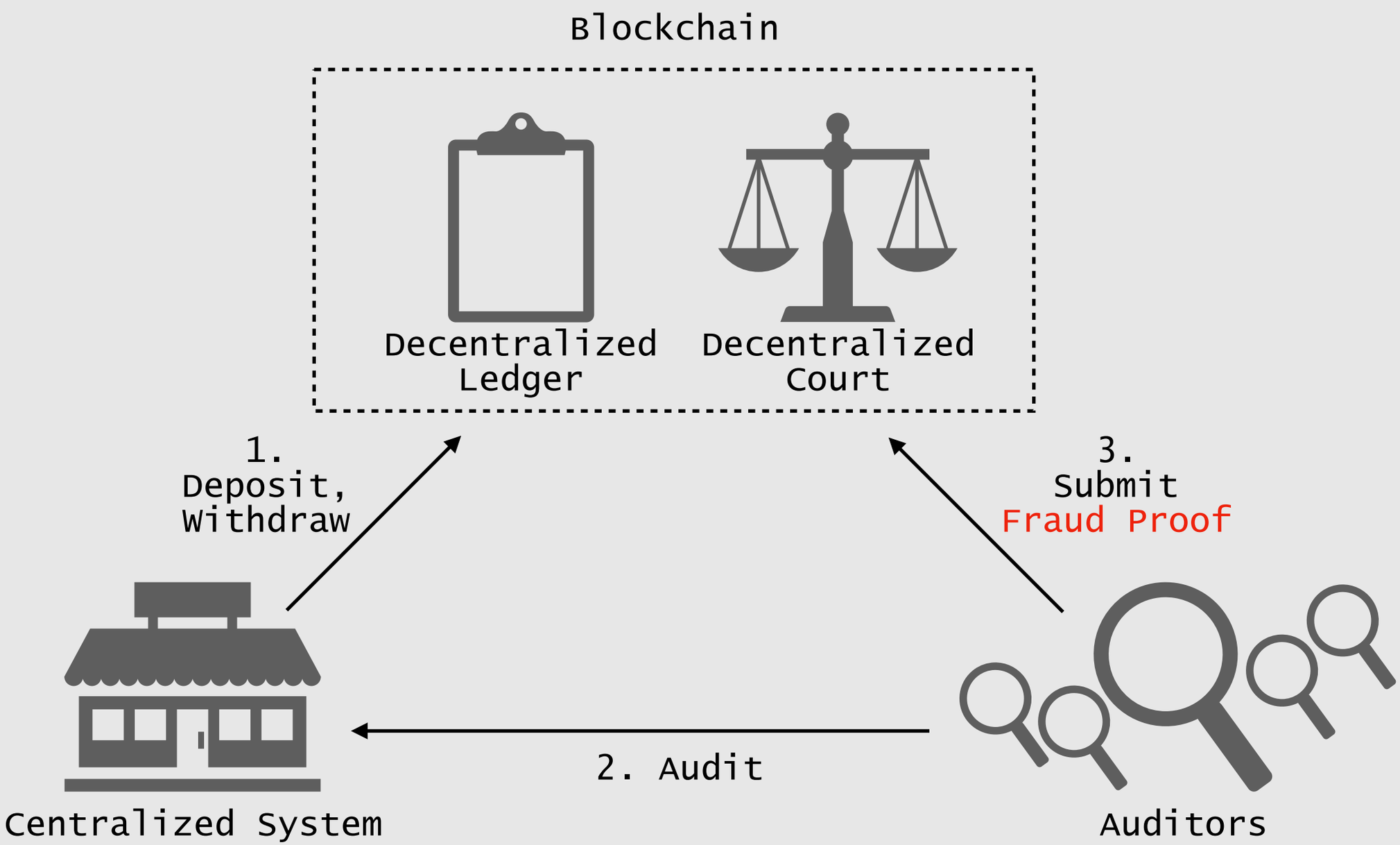
Overview (1)

- 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



Anti-fraud Mechanism

Game

- 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

Anti-fraud Mechanism

Court

- 透過 Fraud Proof 排解紛爭
- Transparent and immutable
- Similar design in Plasma / Truebit

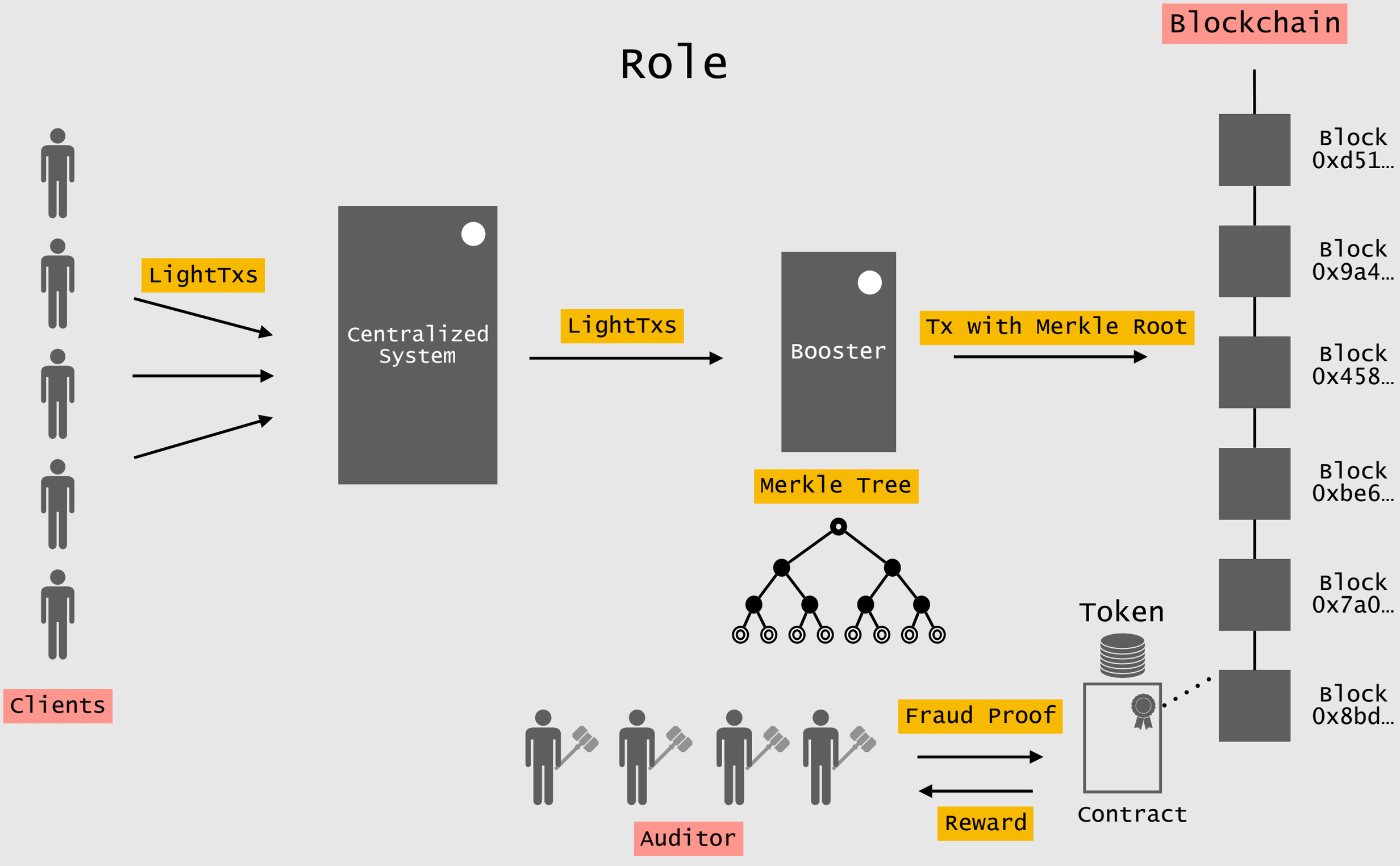
Anti-fraud Mechanism

Fraud Proof

- Merle proof

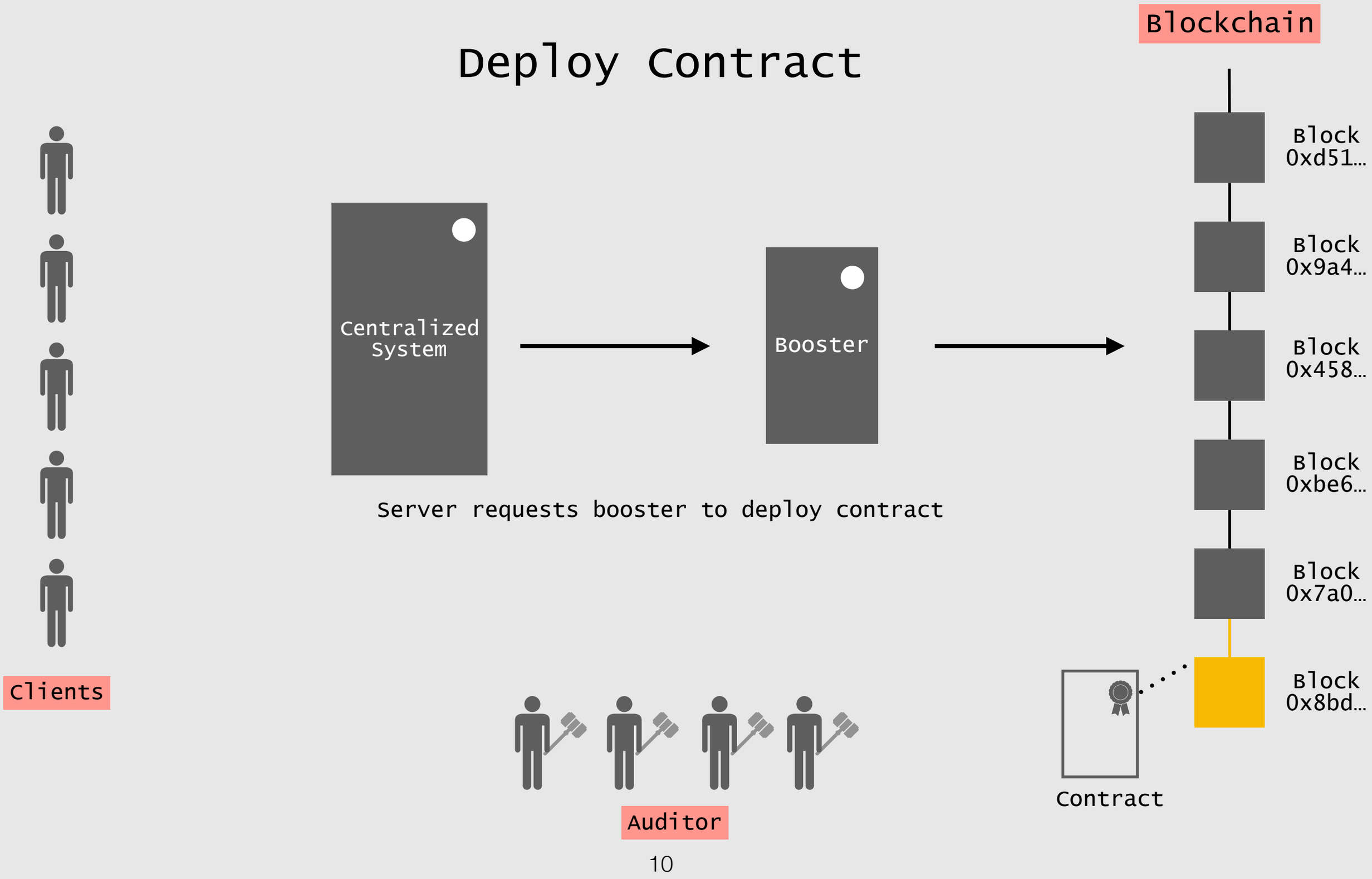
Architecture

Role



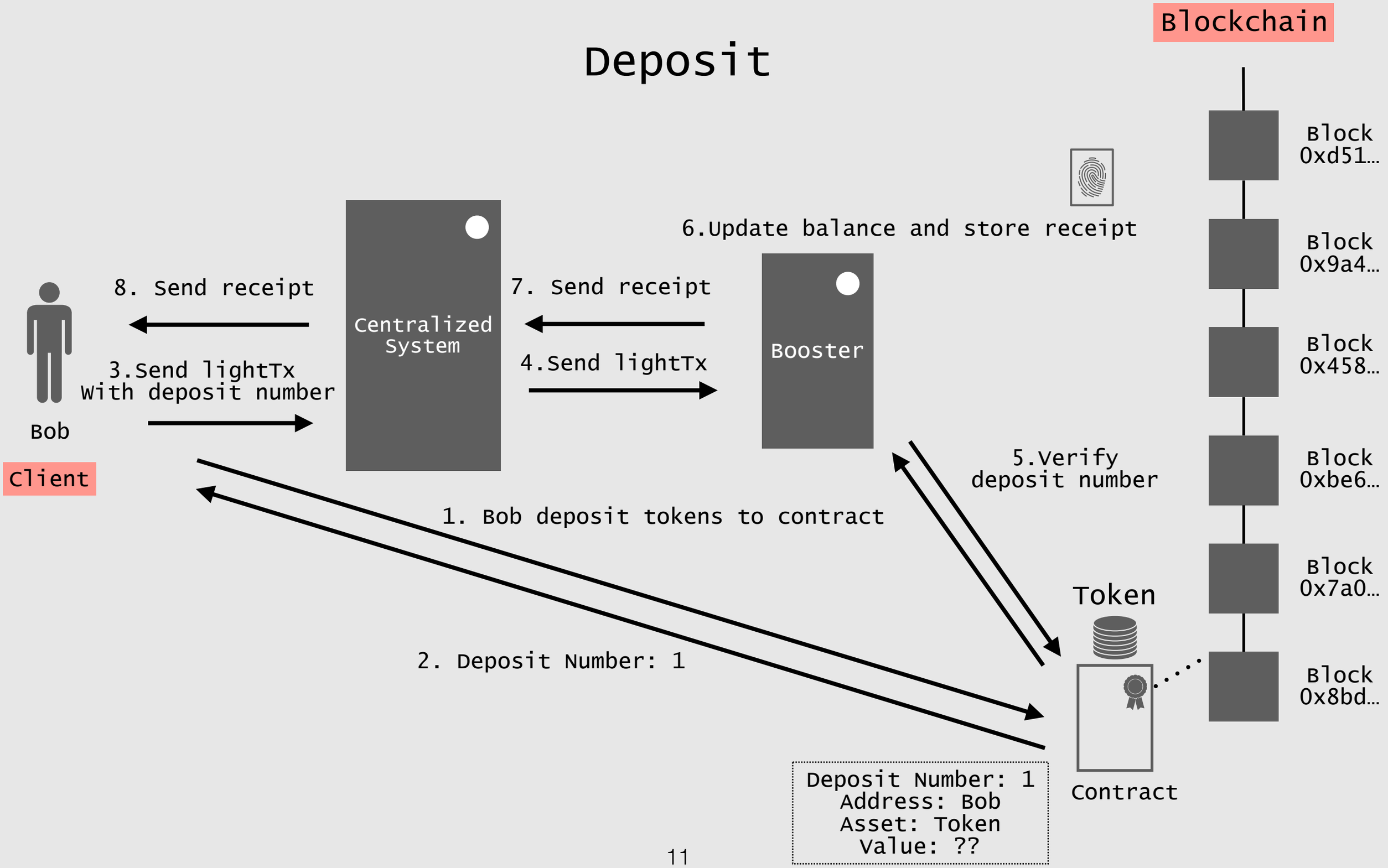
Protocol (1)

Deploy Contract



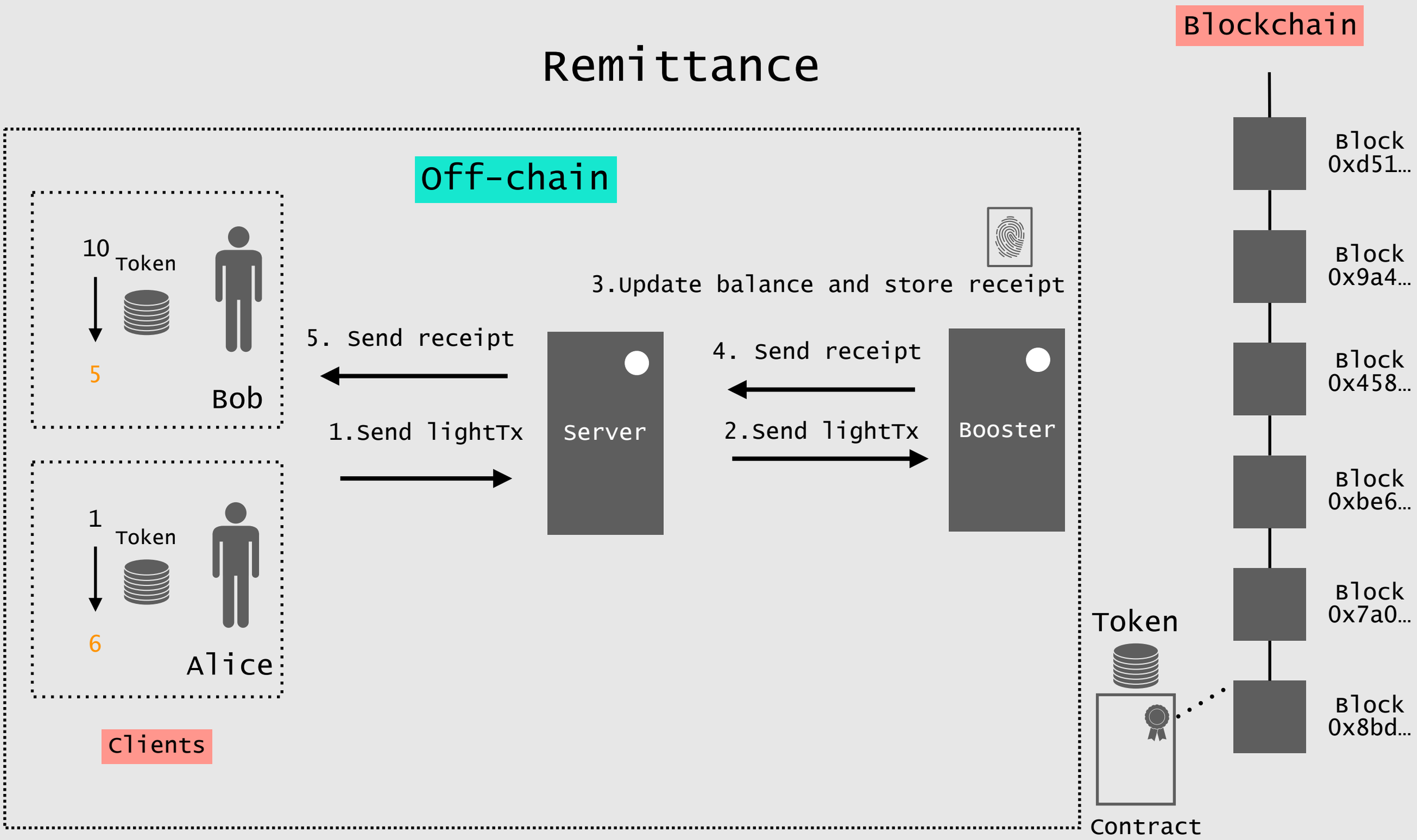
Protocol (2)

Deposit



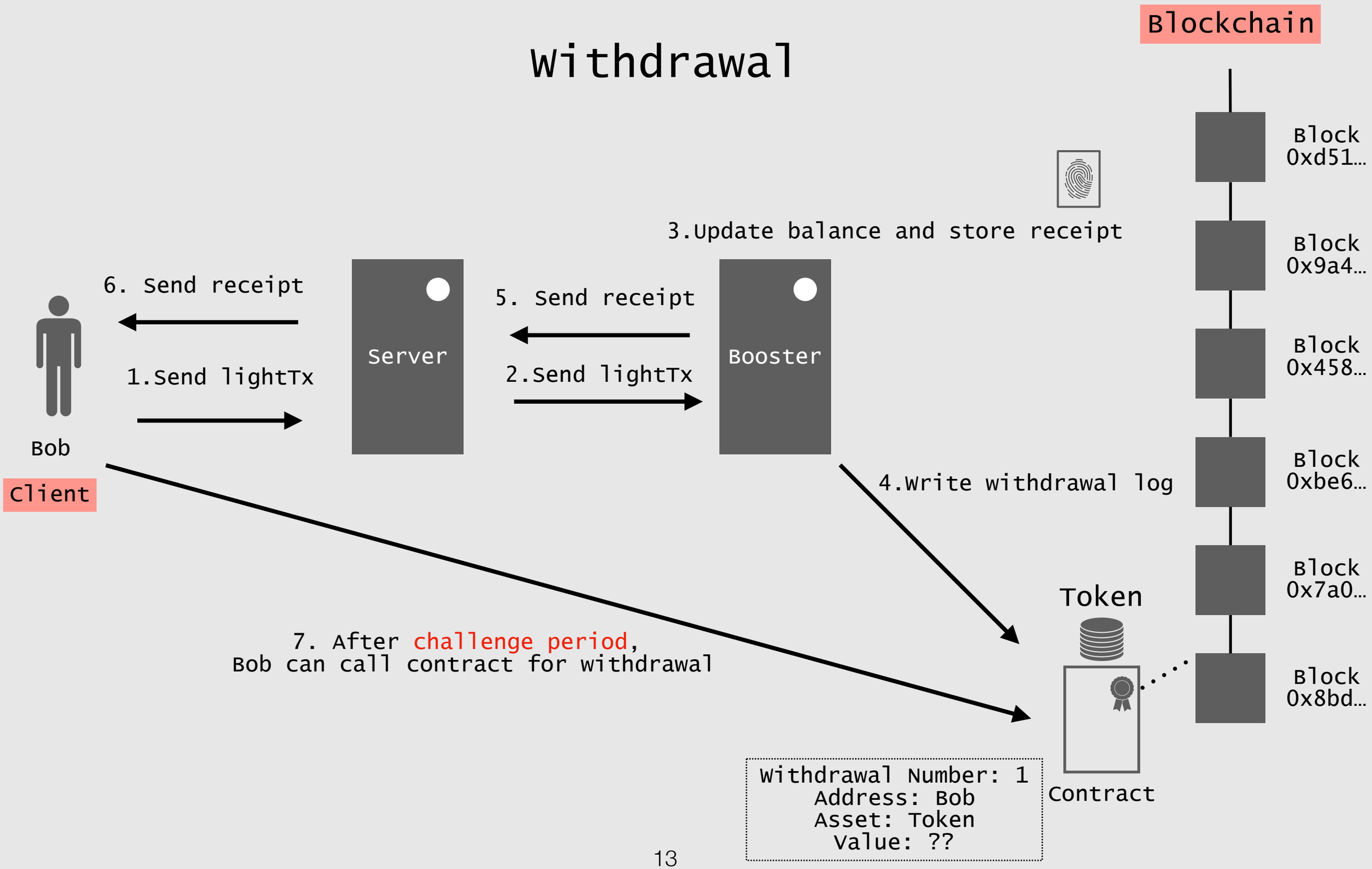
Protocol (3)

Remittance



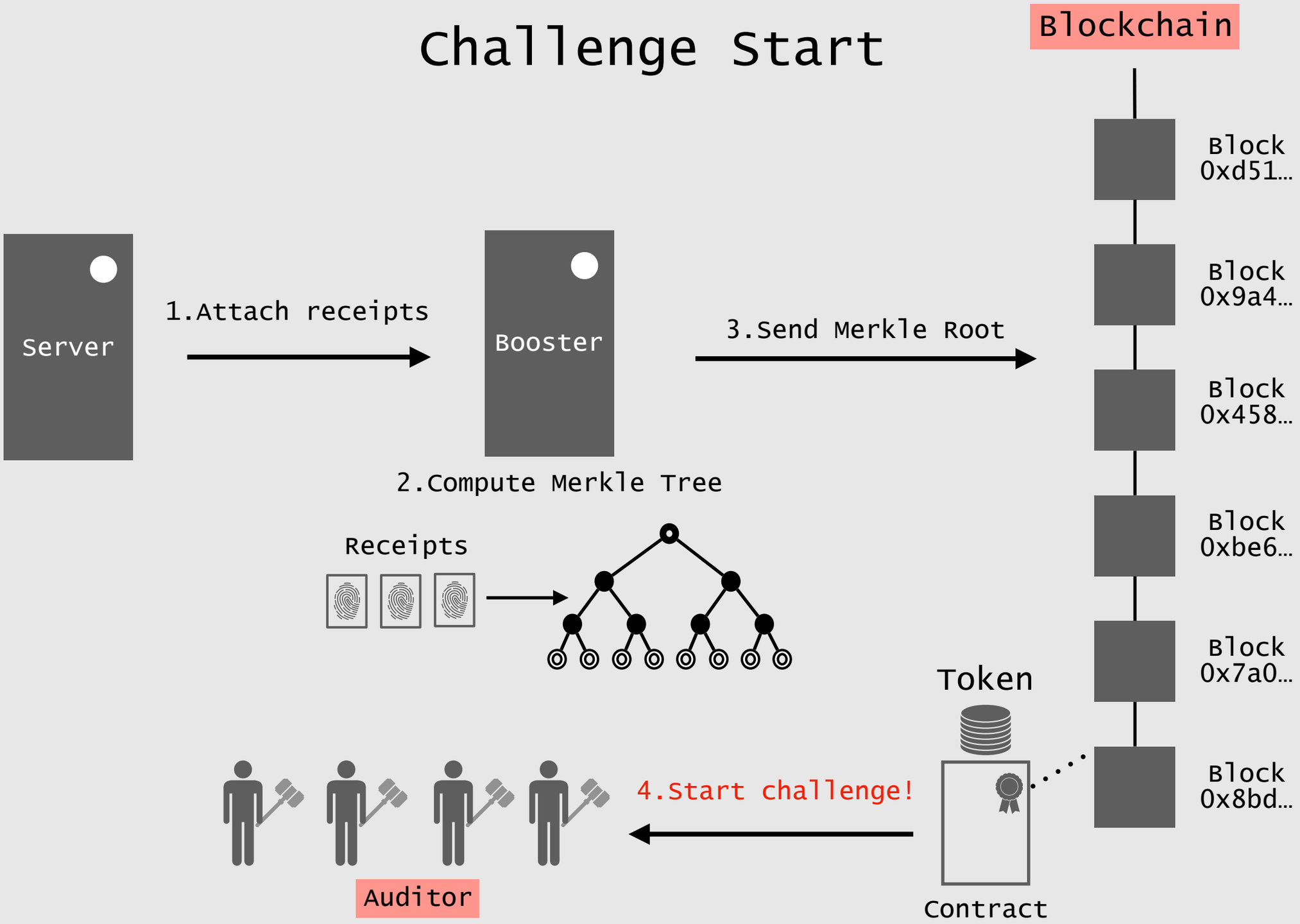
Protocol (4)

Withdrawal



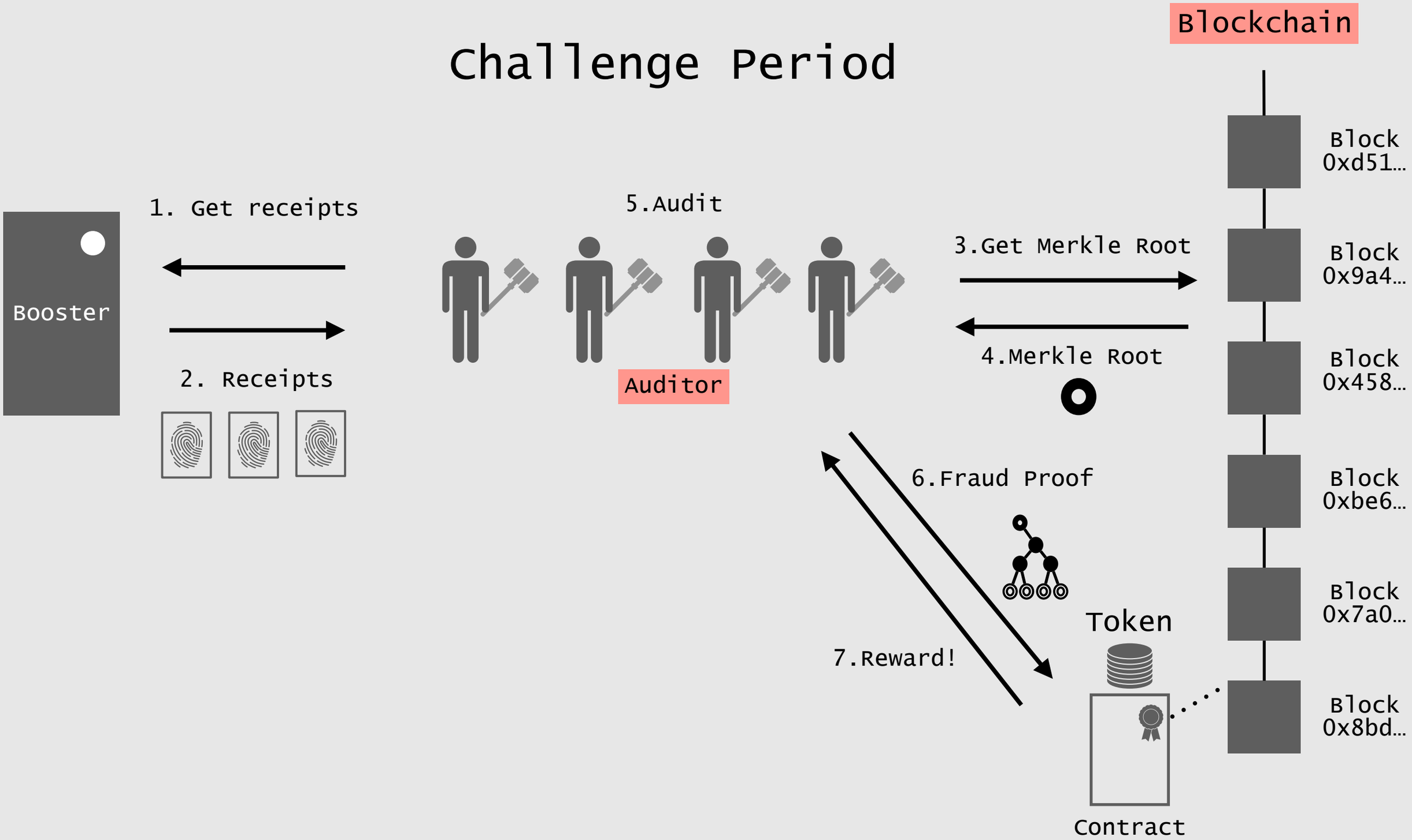
Protocol (5)

Challenge Start



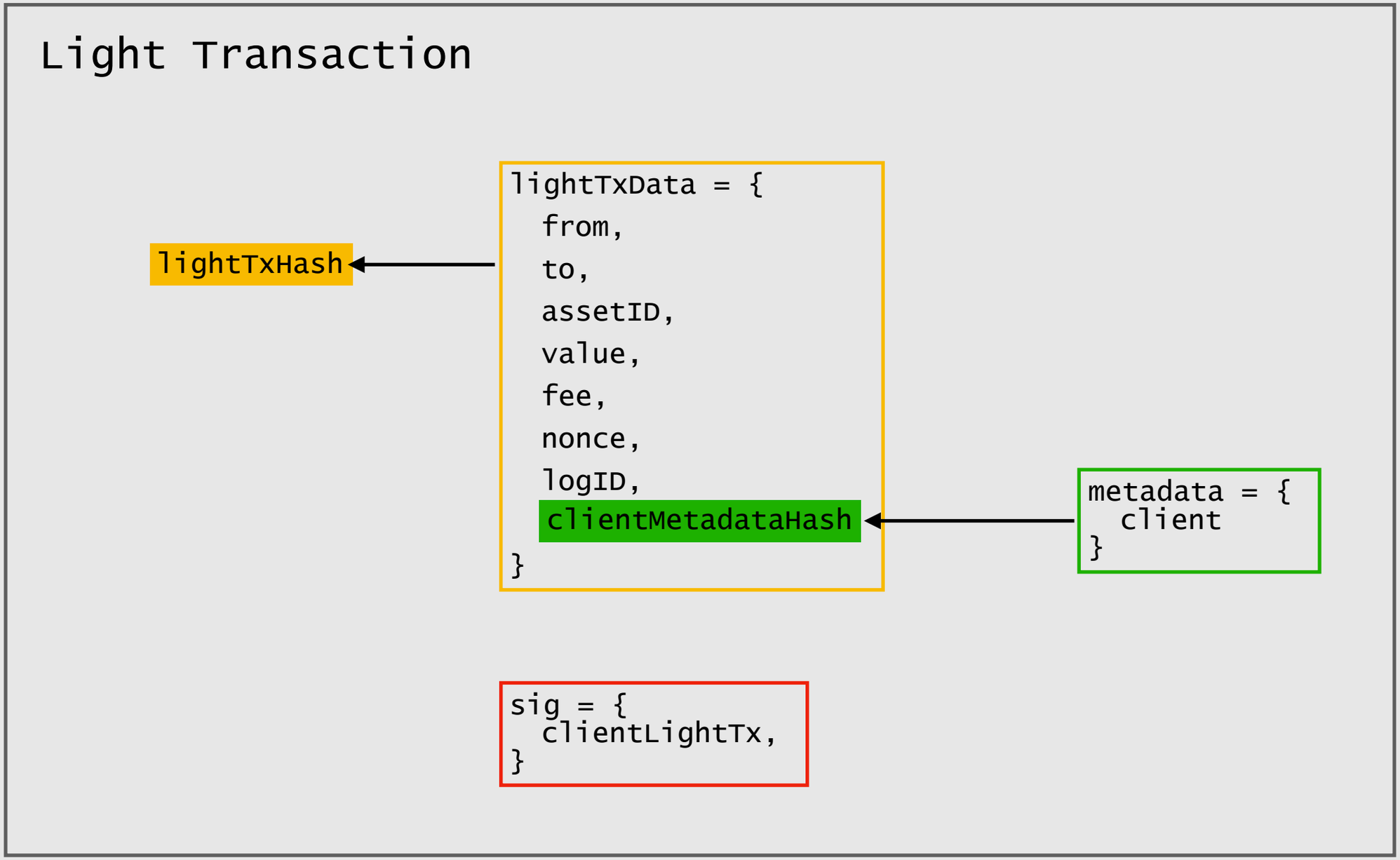
Protocol (6)

Challenge Period



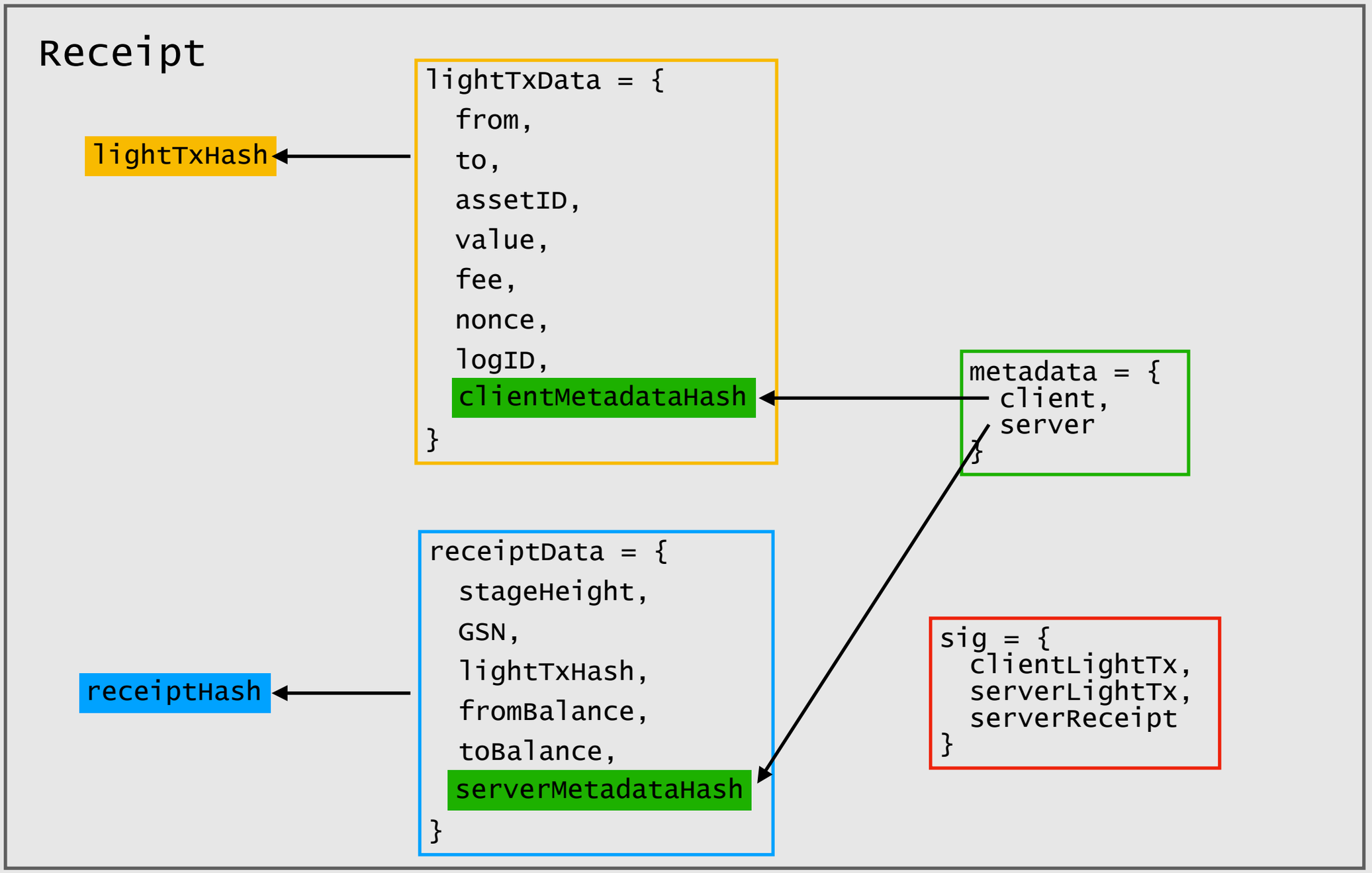
Protocol (7)

Data Model



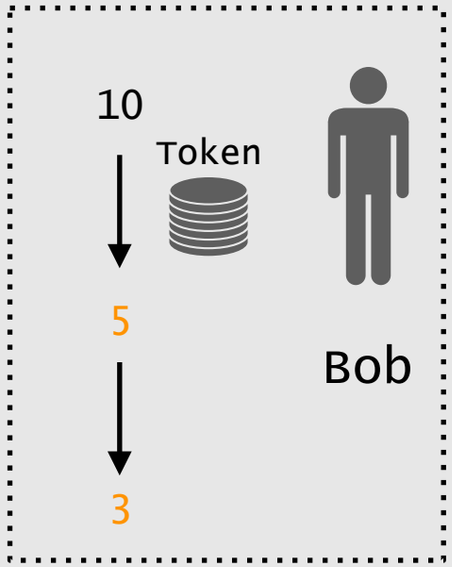
Protocol (8)

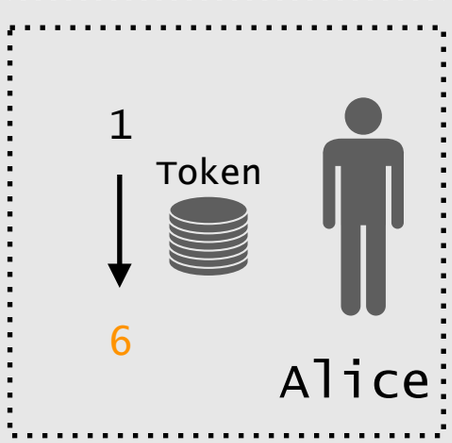
Data Model

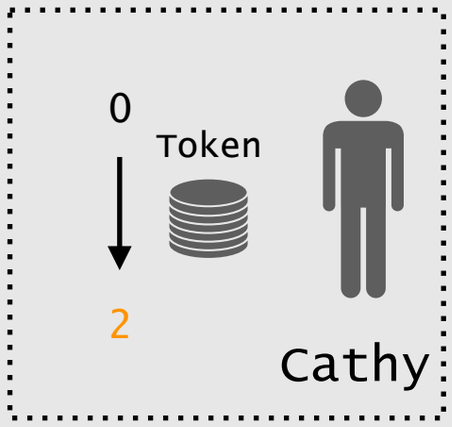


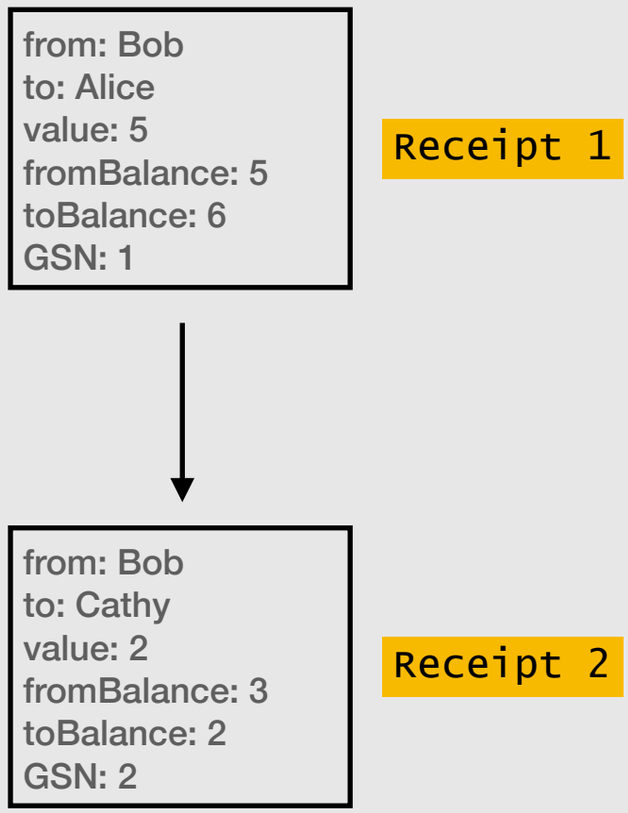
Protocol (9)

Example









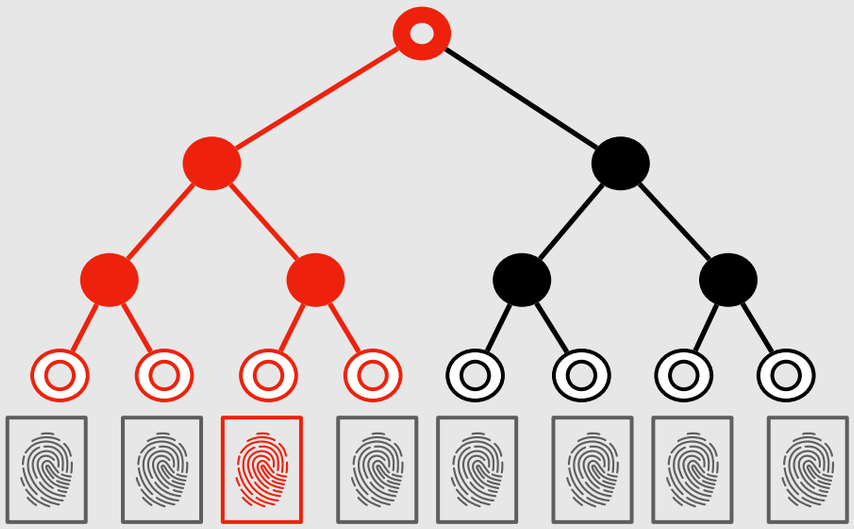
Protocol (10)

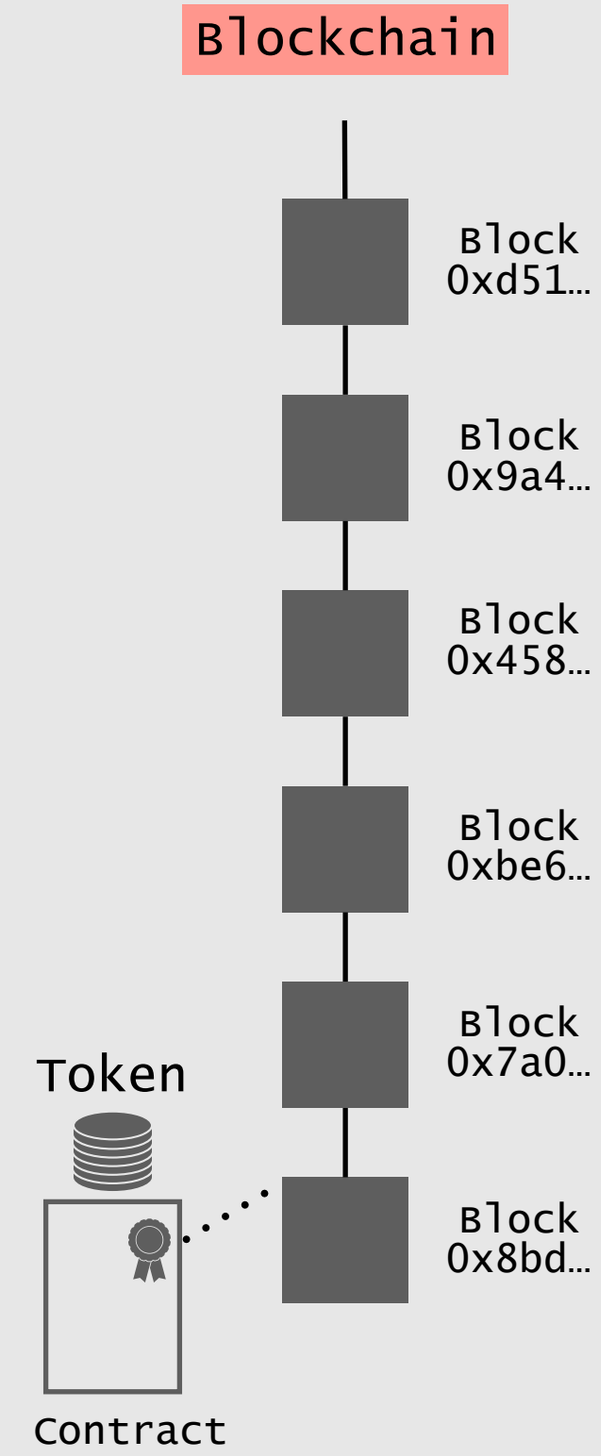
Fraud Proof

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

Fraud Proof (1)

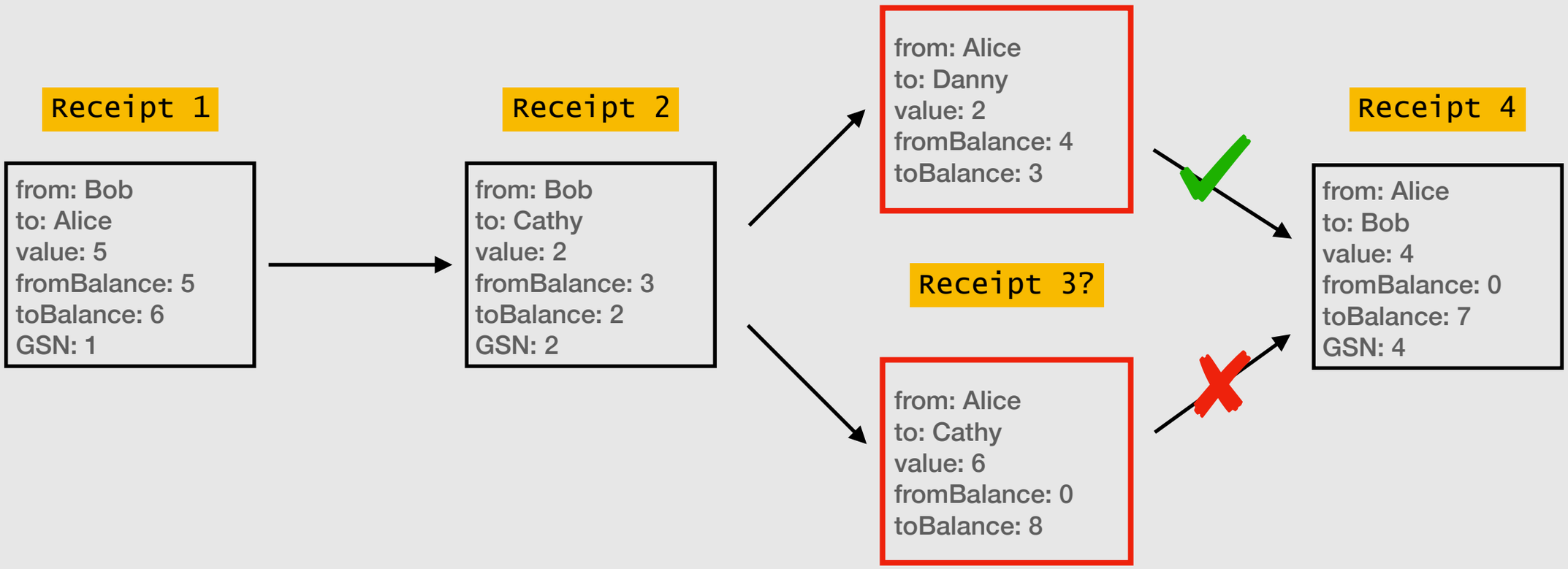
Non-existed Receipt





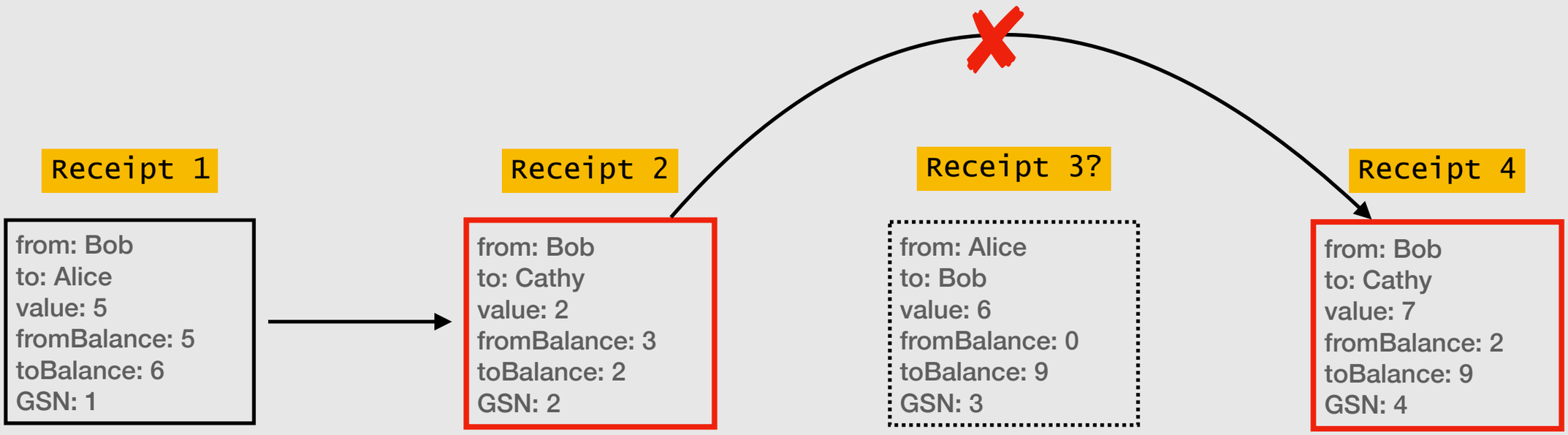
Fraud Proof (2)

Repeated GSN



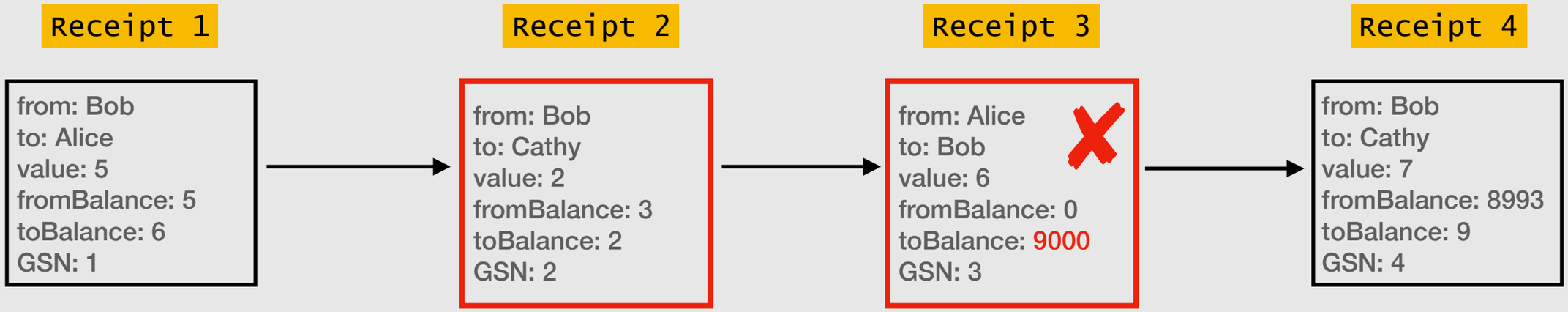
Fraud Proof (3)

Skipped GSN



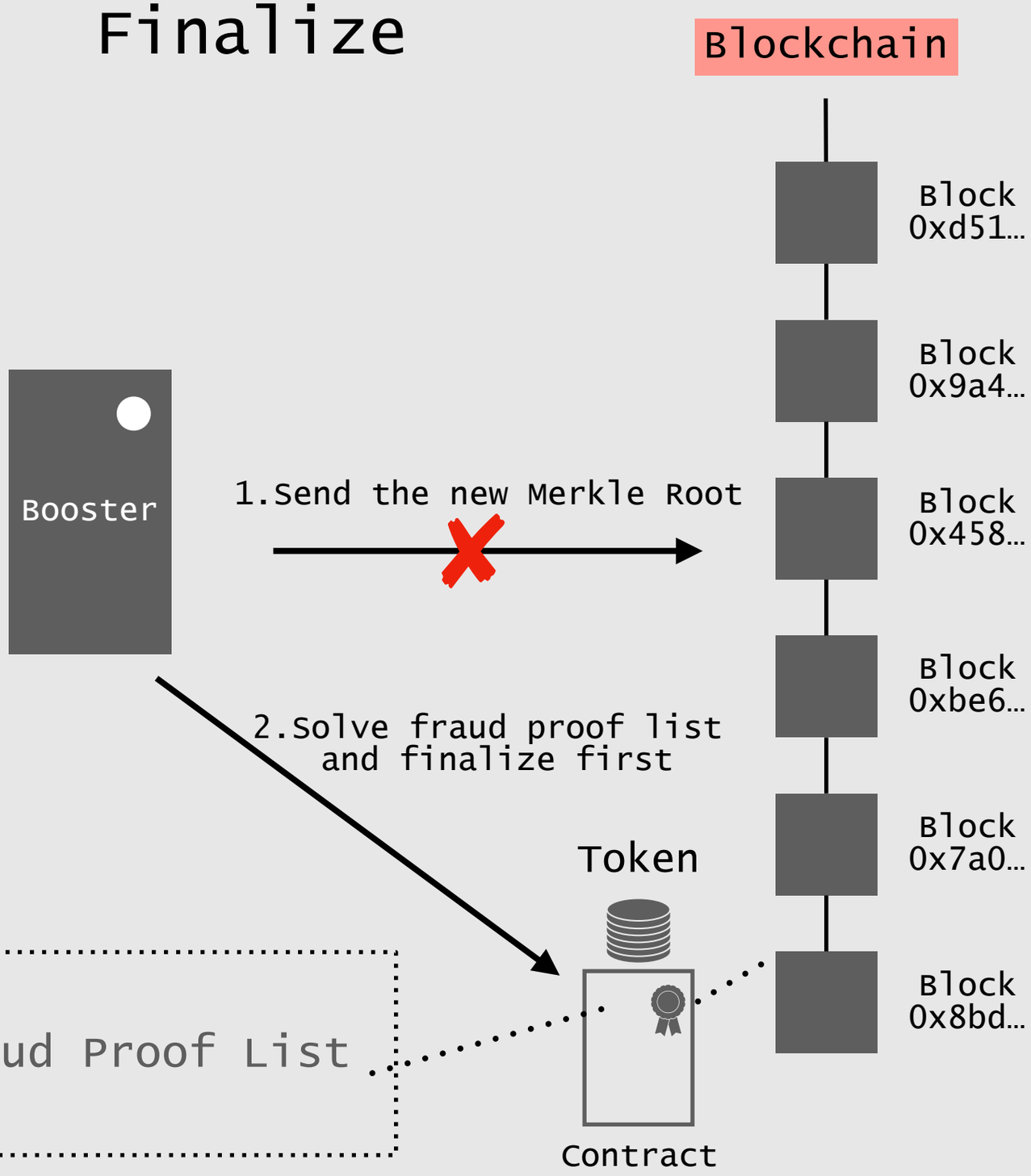
Fraud Proof (4)

Wrong Balance Status



Protocol (11)

Finalize



Protocol (12)

Force Withdraw