Replay Attacks and Defenses Against Cross-shard Consensus in Sharded Distributed Ledgers

Alberto Sonnino

Acknowledgments
Authors


Alberto Sonnino


Bano Shehar


Mustafa Al-Bassam

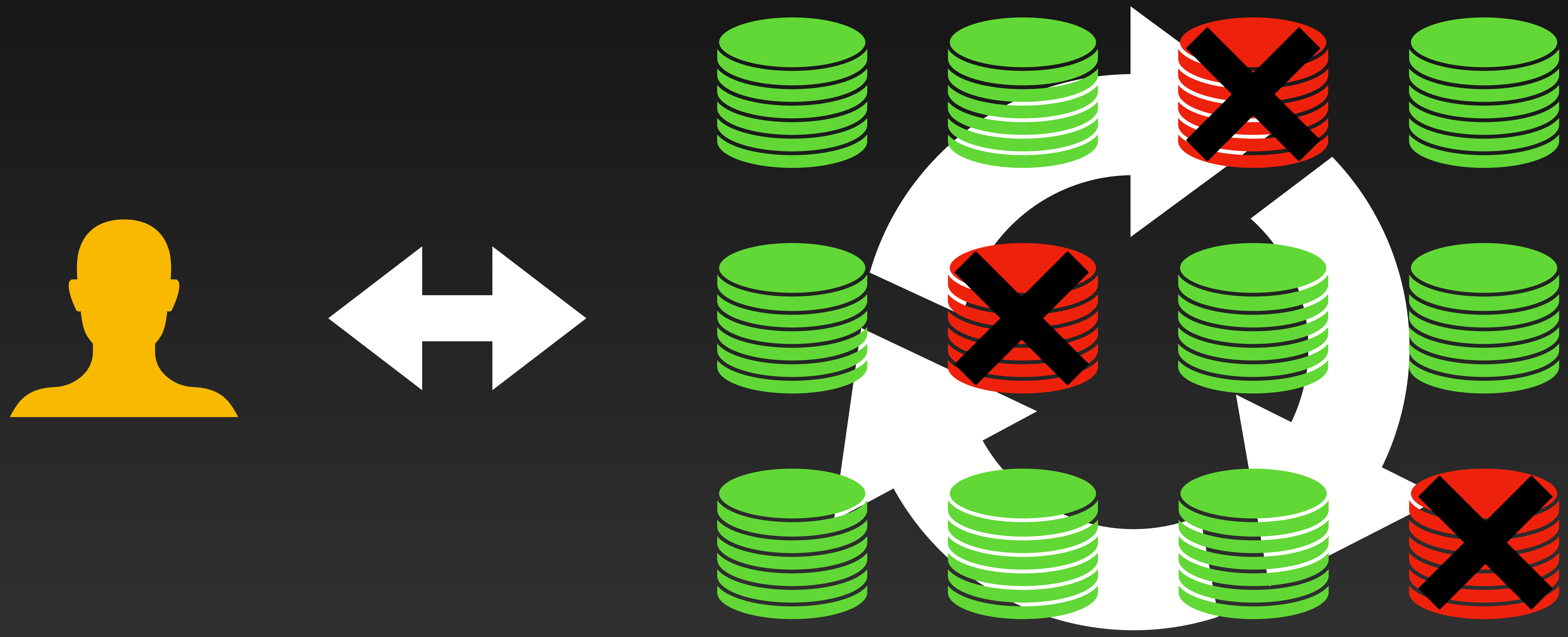

George Danezis

University College London

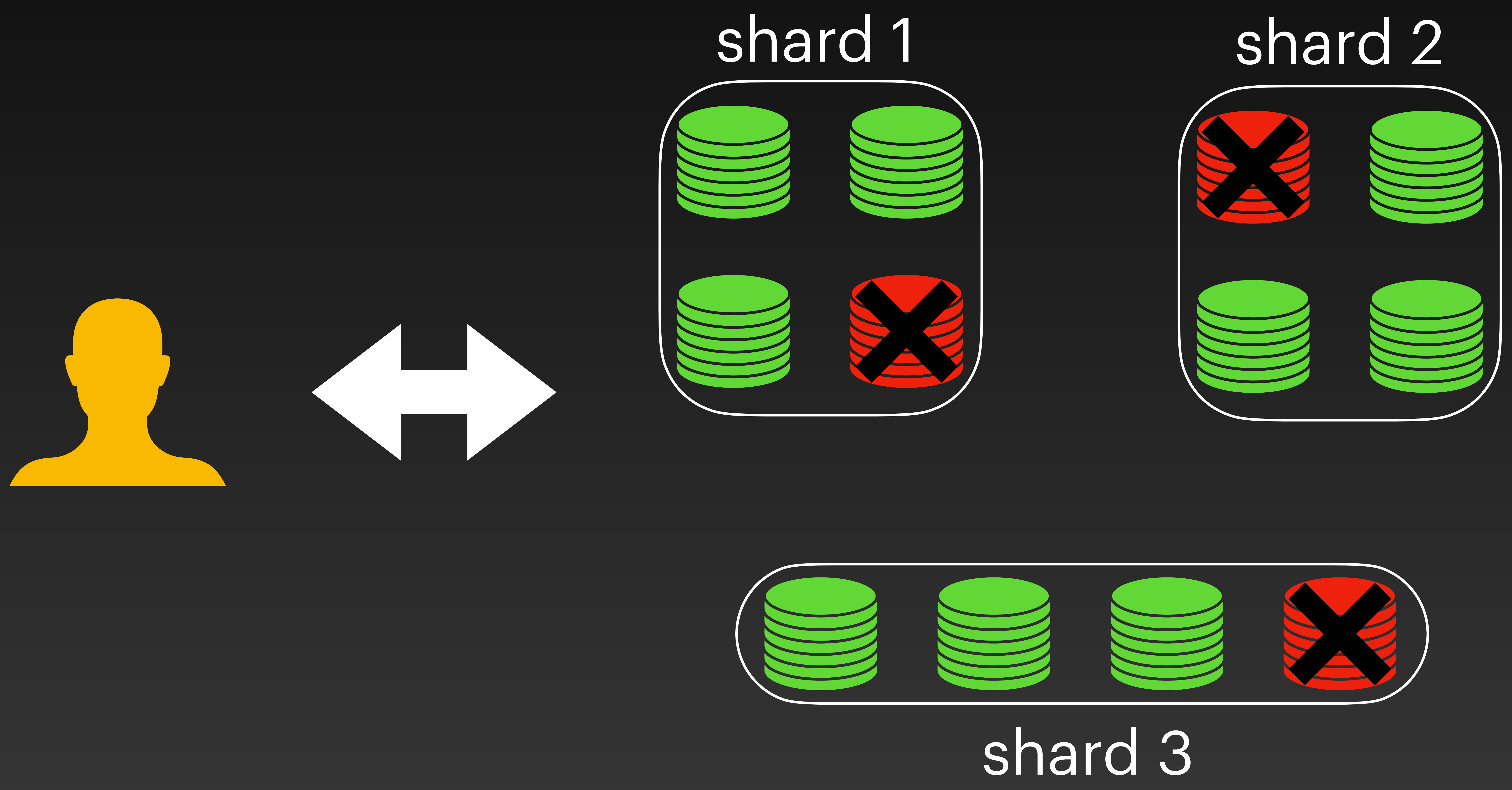
A set of nodes

Byzantine Fault Tolerance

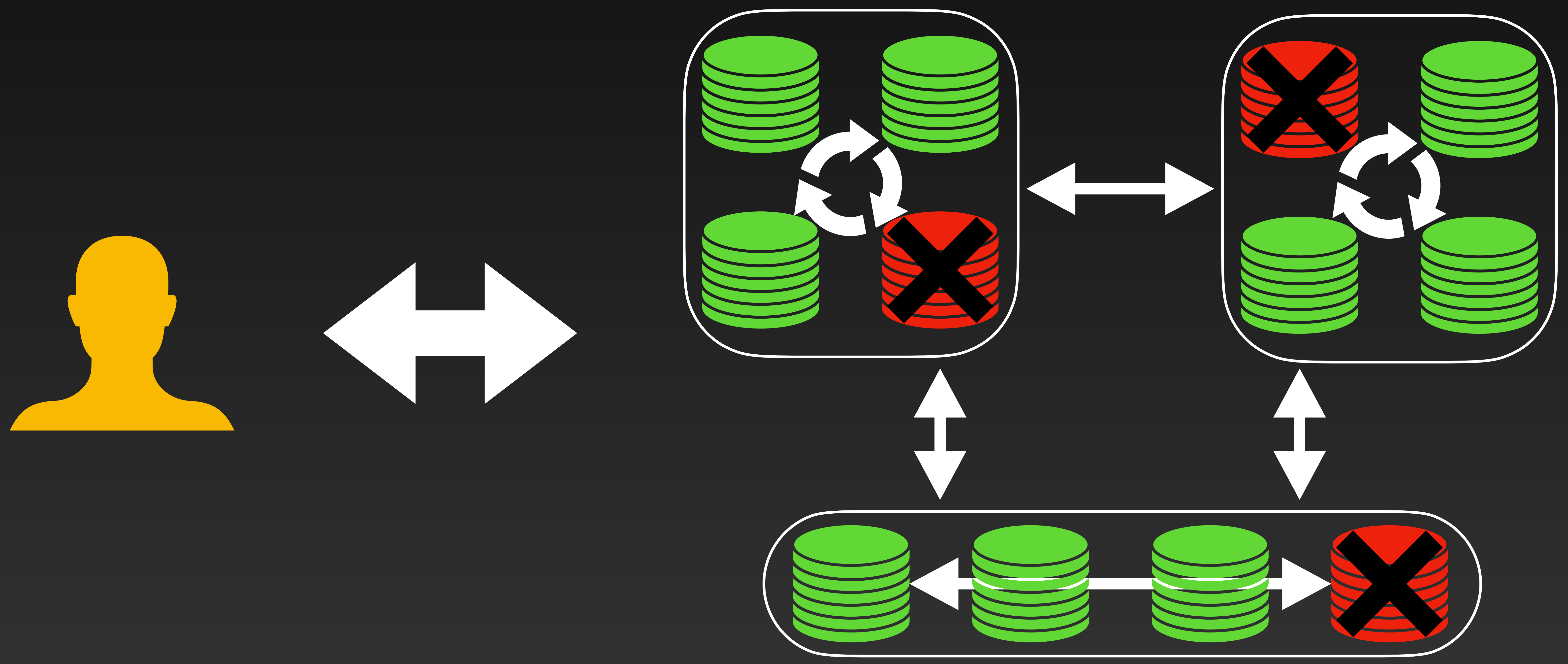
Consensus



State Sharding



State Sharding



State Sharding

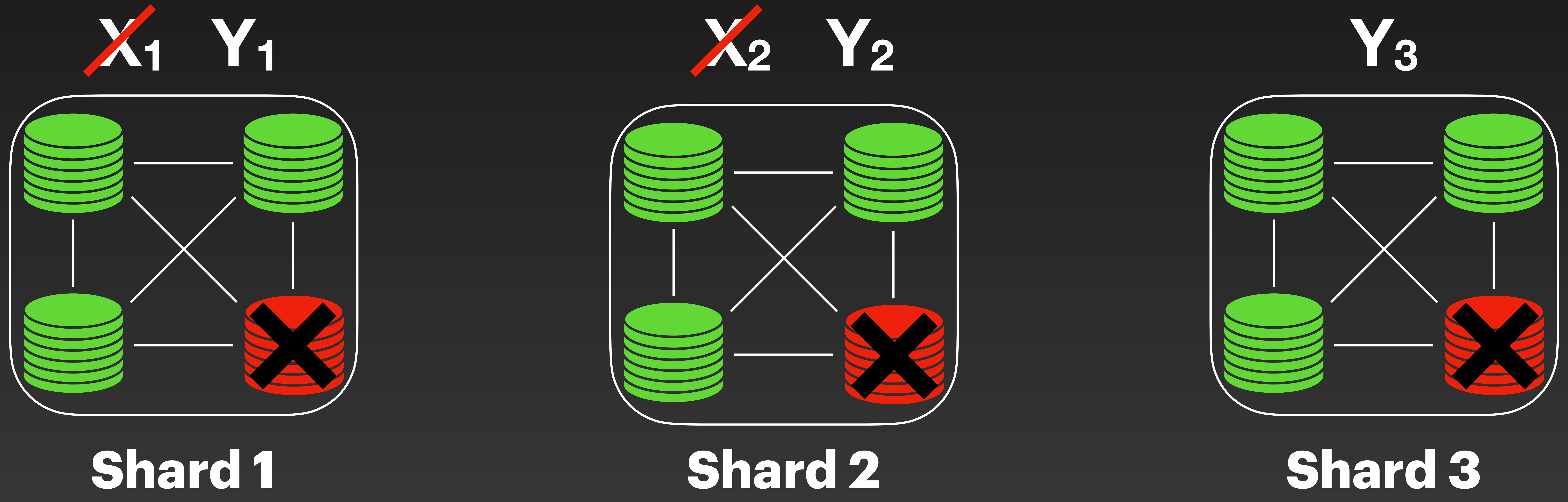
An example transaction

$$T(x_1, x_2) \rightarrow (y_1, y_2, y_3)$$

State Sharding

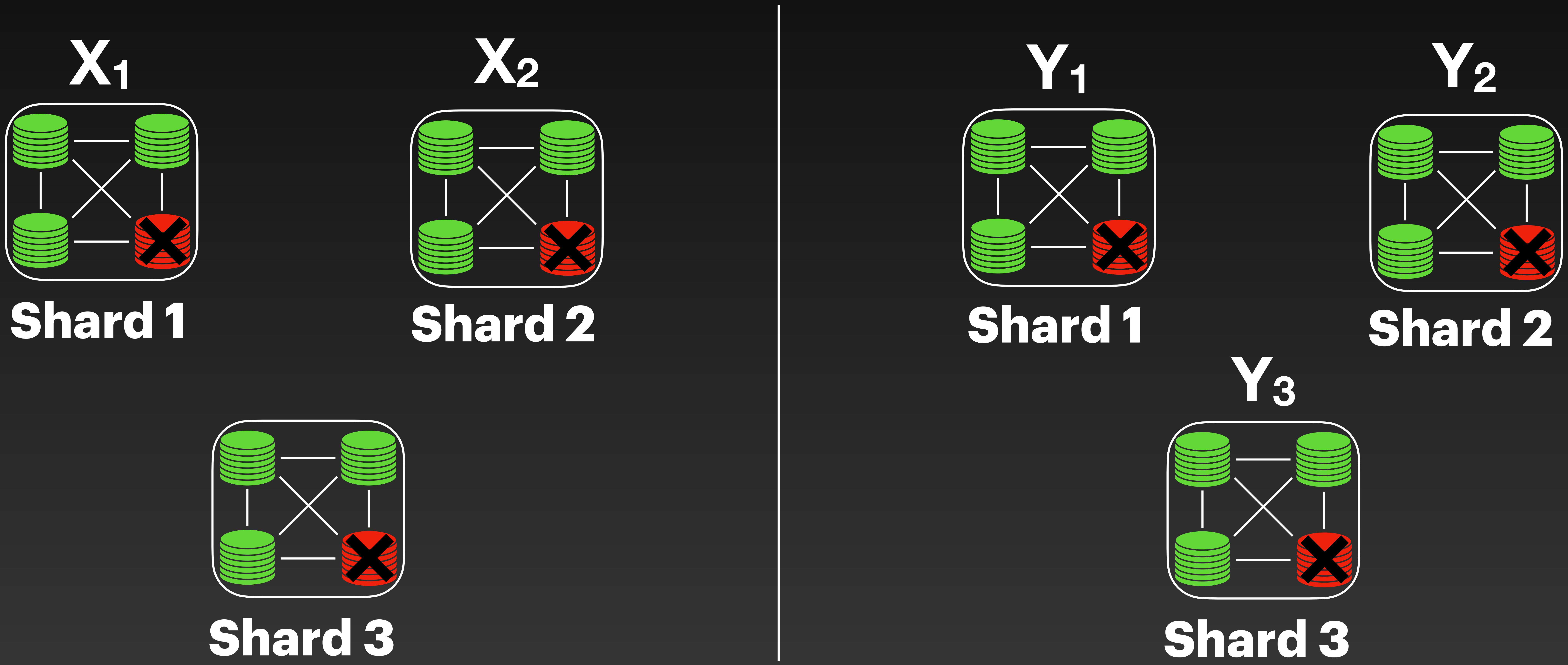
An example transaction

$$T(x_1, x_2) \rightarrow (y_1, y_2, y_3)$$



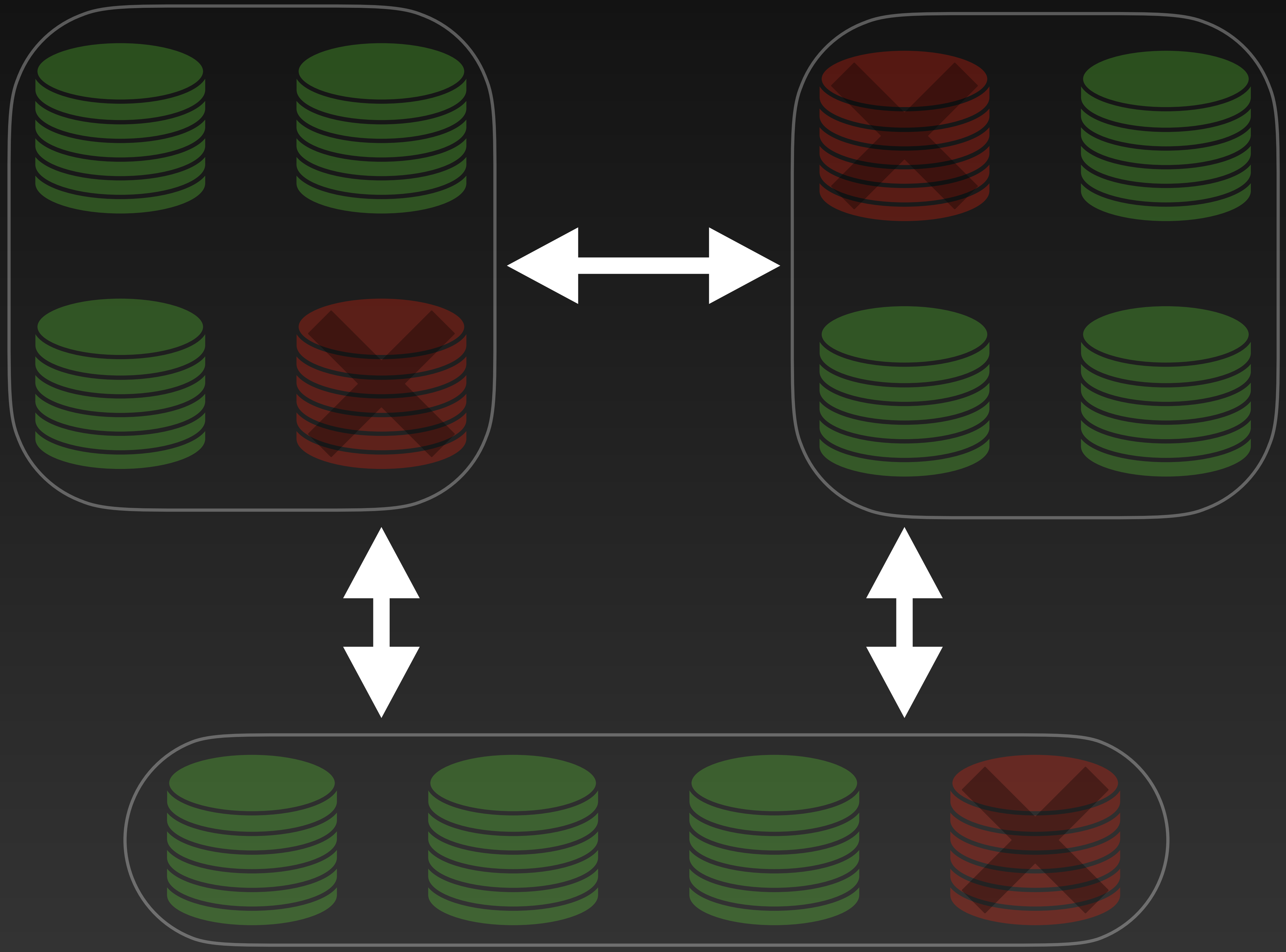
State Sharding

Only two acceptable final states



Cross-Shard Consensus

How do shards communicate with each other?



S-BAC

Chainspace: A Sharded Smart Contracts Platform

Mustafa Al-Bassam*, Alberto Sonnino*, Shehar Bano*, Dave Hrycyszyn† and George Danezis*

NDSS’18

Atomix

OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding

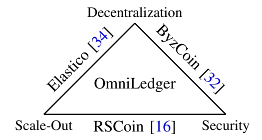
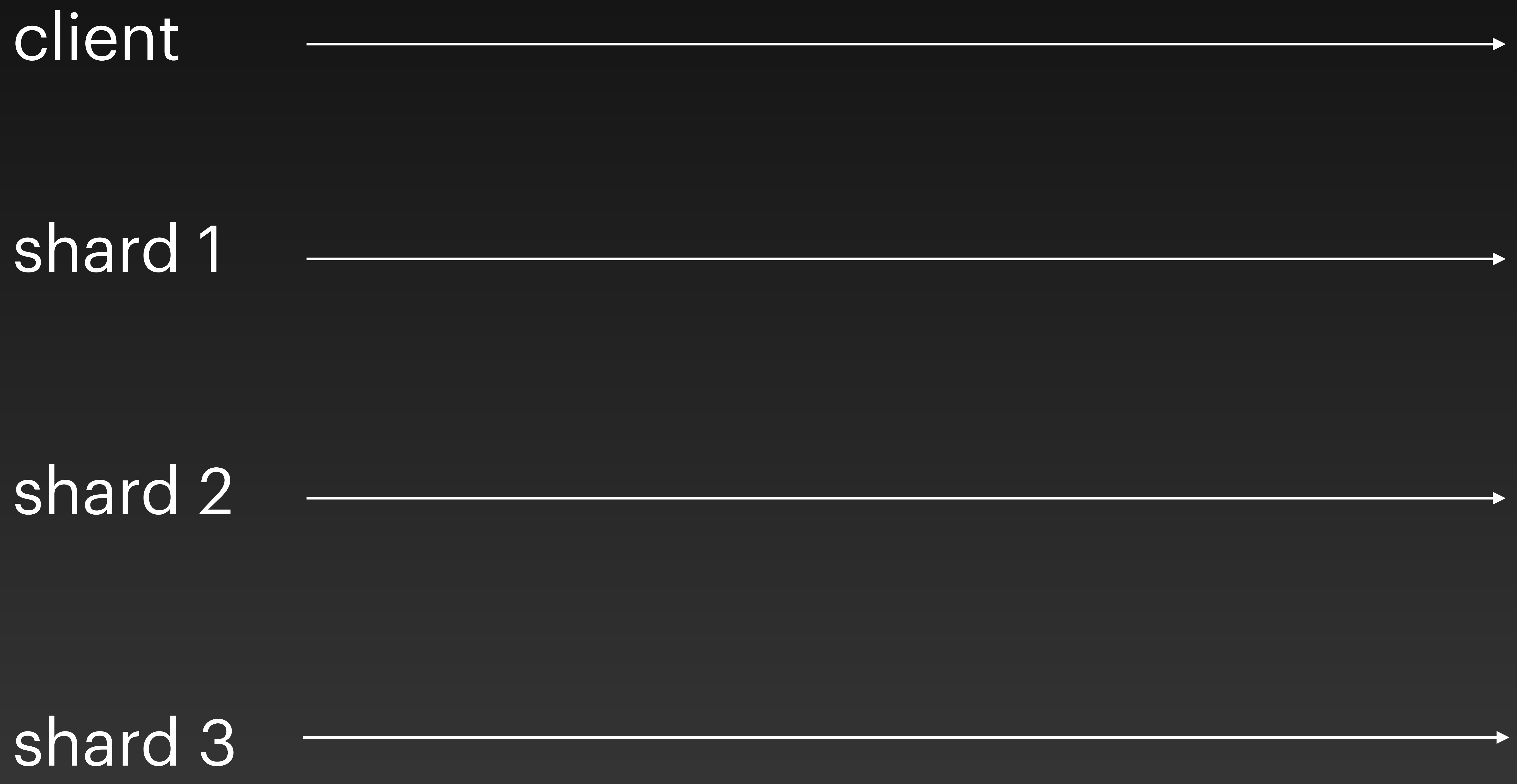


Fig. 1: Trade-offs in current DL systems.

S&P'18

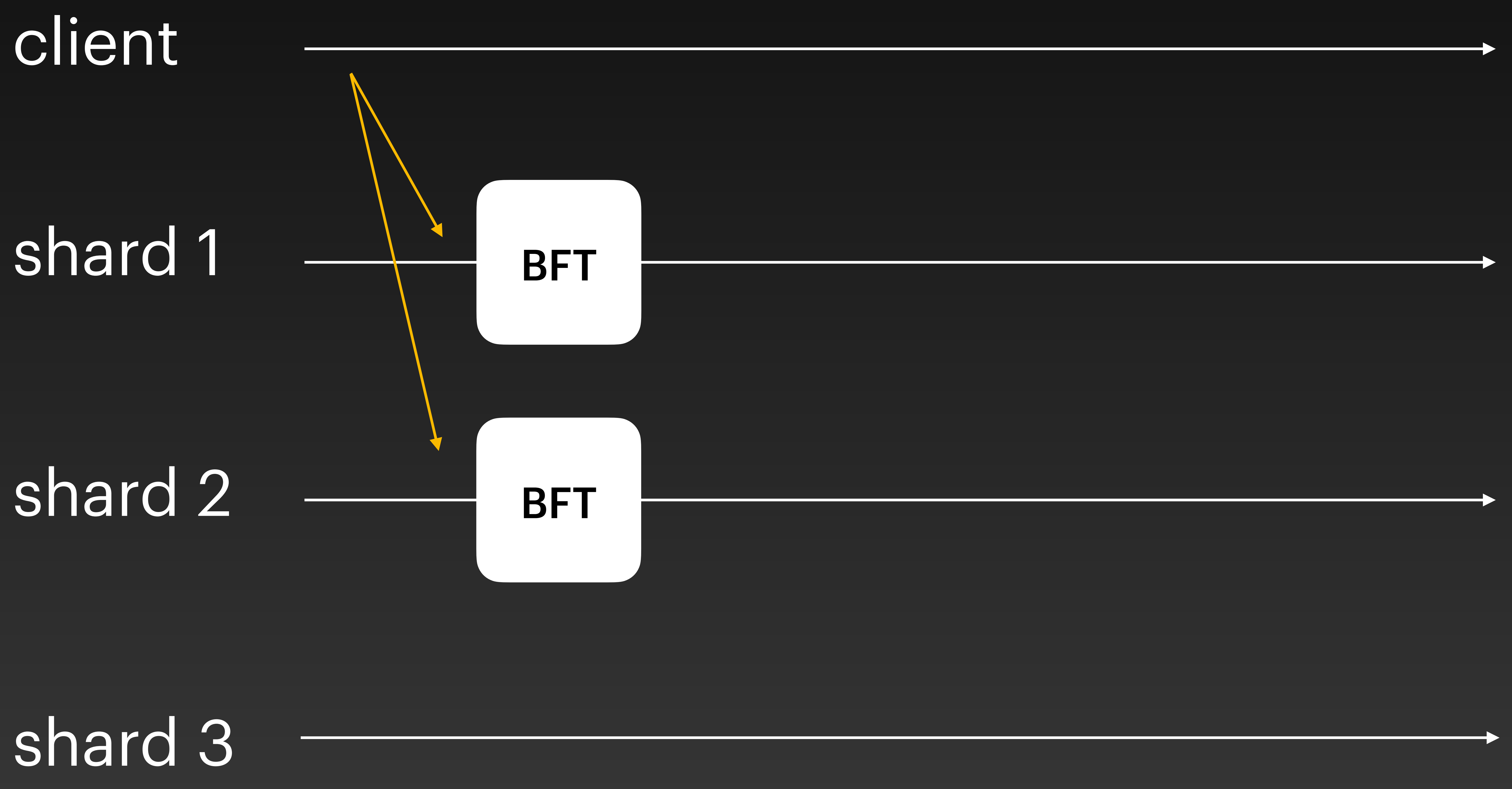
S-BAC

$$T(x_1, x_2) \rightarrow (y_1, y_2, y_3)$$



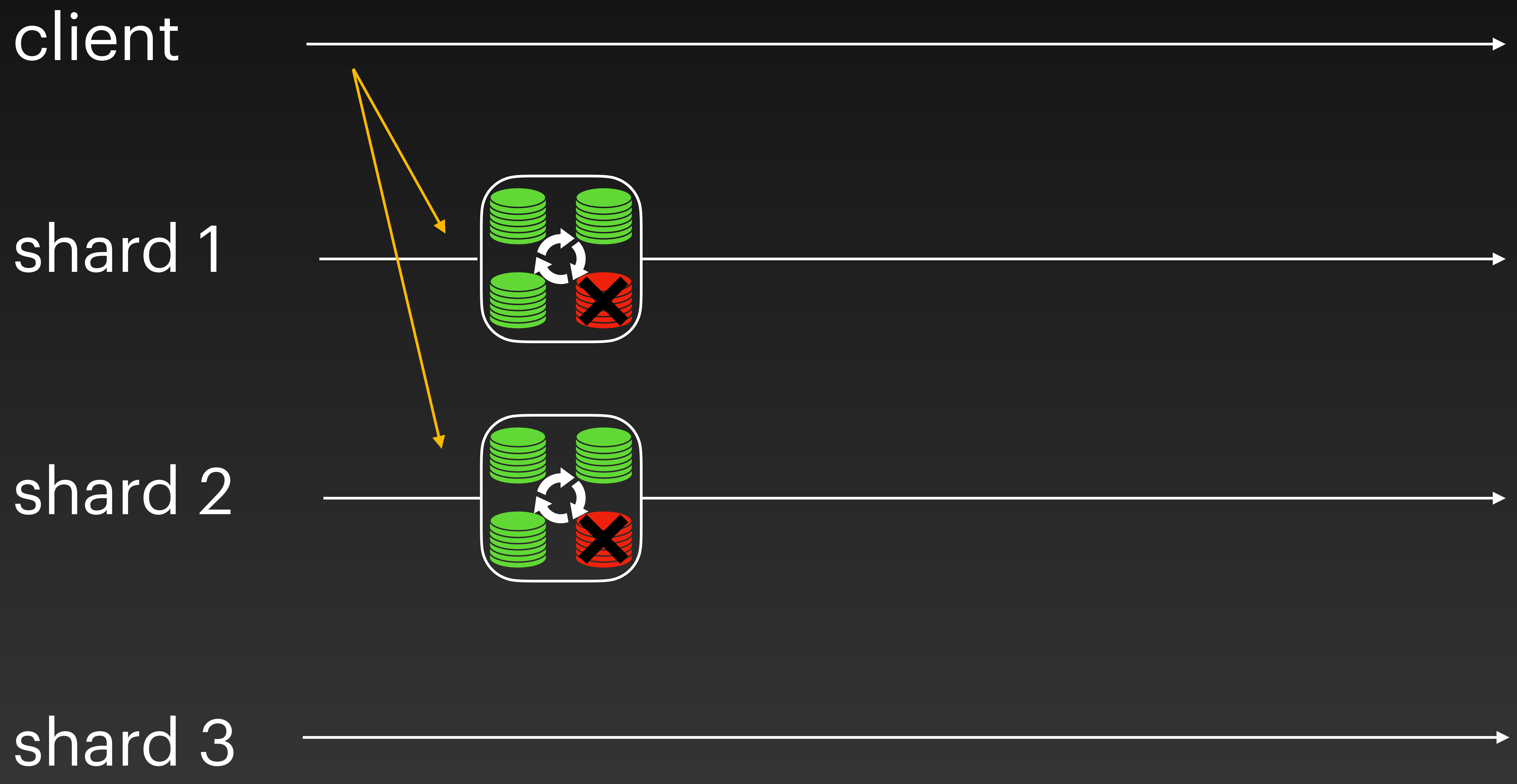
S-BAC

$$T(x_1, x_2) \rightarrow (y_1, y_2, y_3)$$



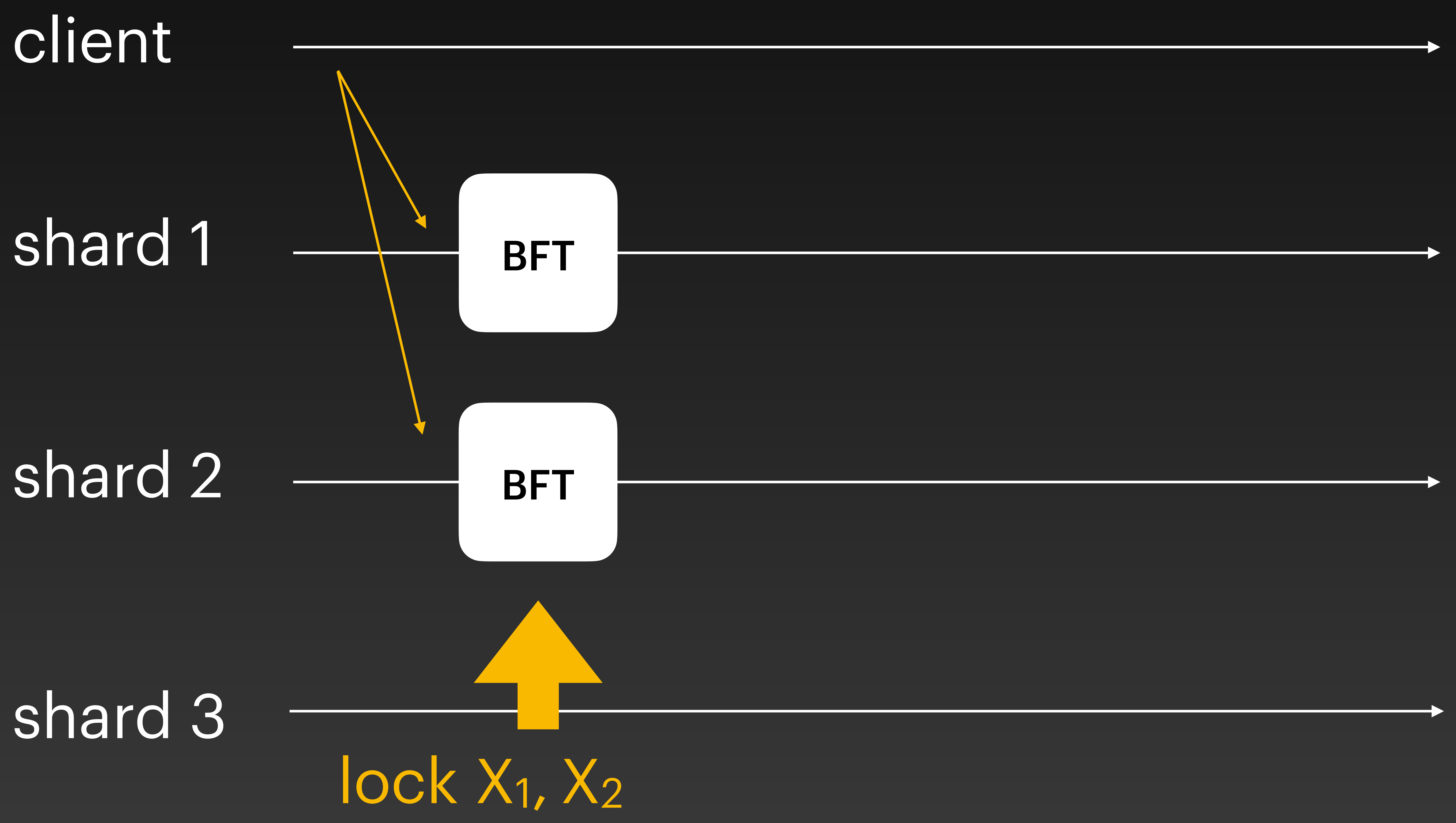
S-BAC

$$T(x_1, x_2) \rightarrow (y_1, y_2, y_3)$$



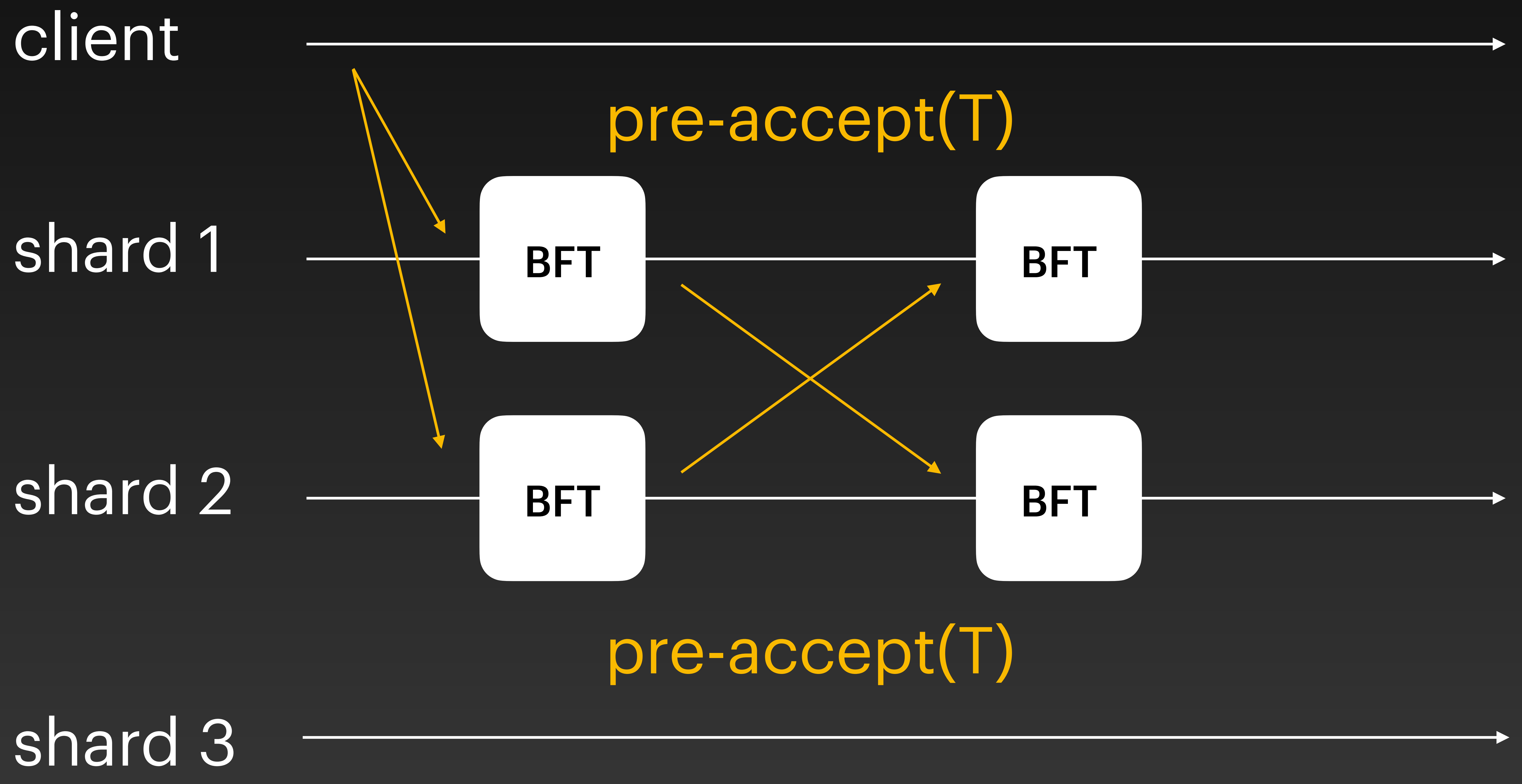
S-BAC

$$T(x_1, x_2) \rightarrow (y_1, y_2, y_3)$$



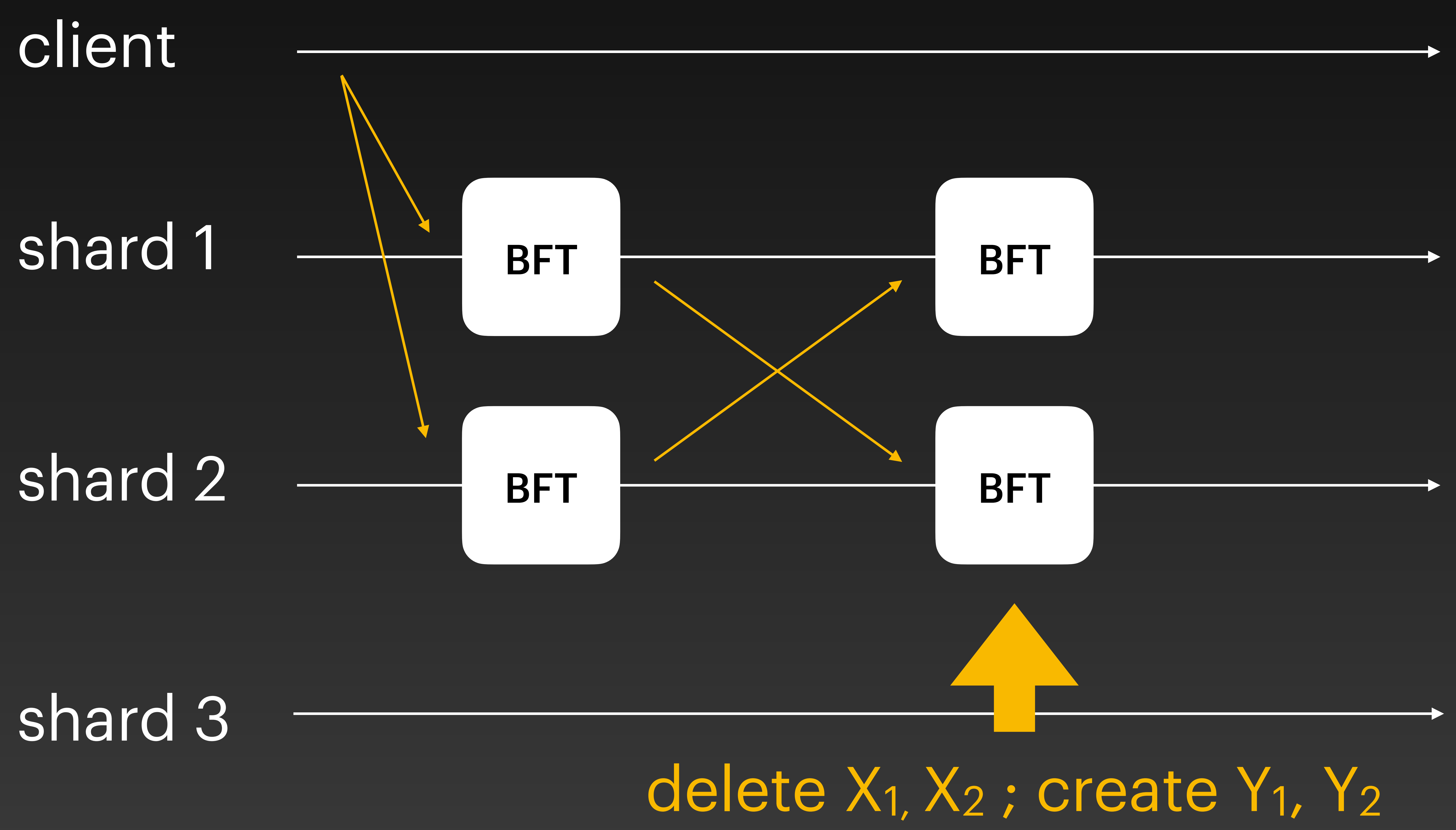
S-BAC

$$T(x_1, x_2) \rightarrow (y_1, y_2, y_3)$$



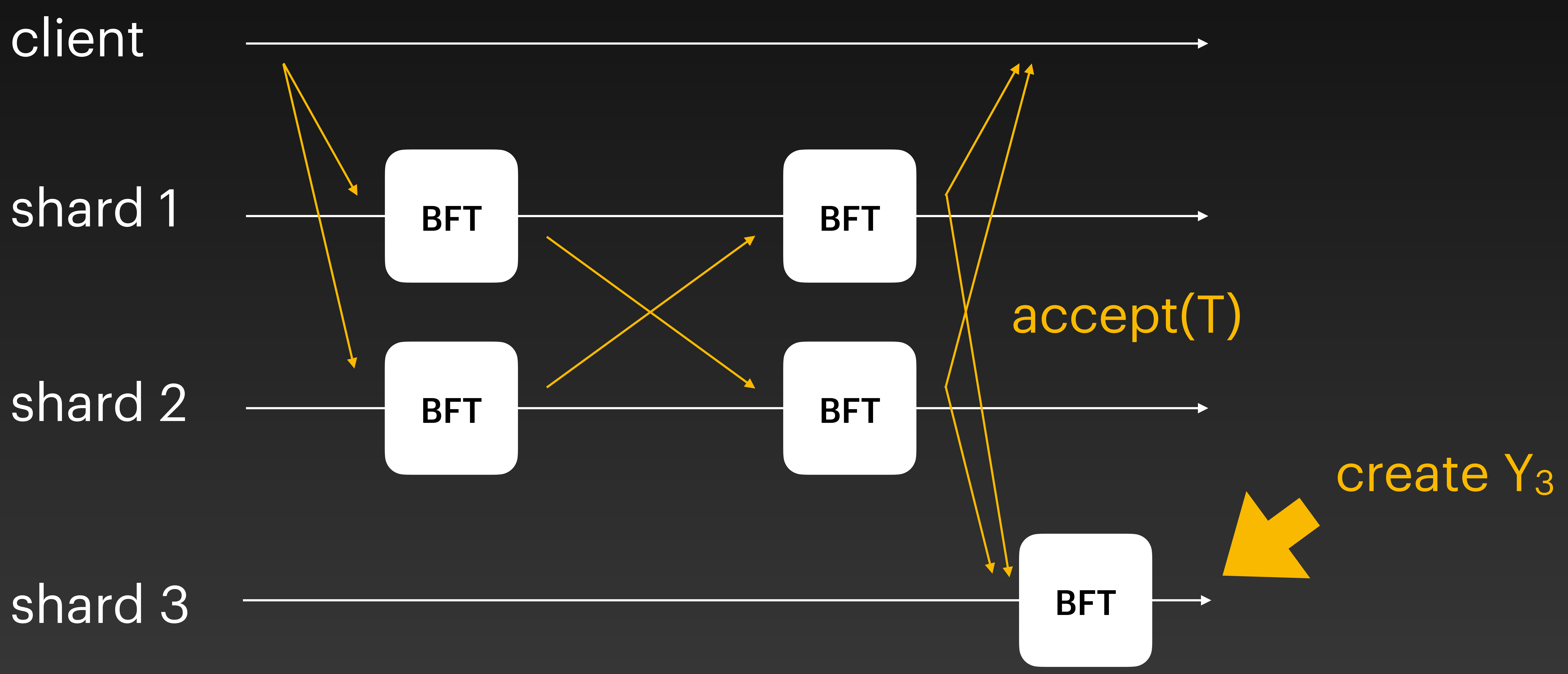
S-BAC

$$T(x_1, x_2) \rightarrow (y_1, y_2, y_3)$$



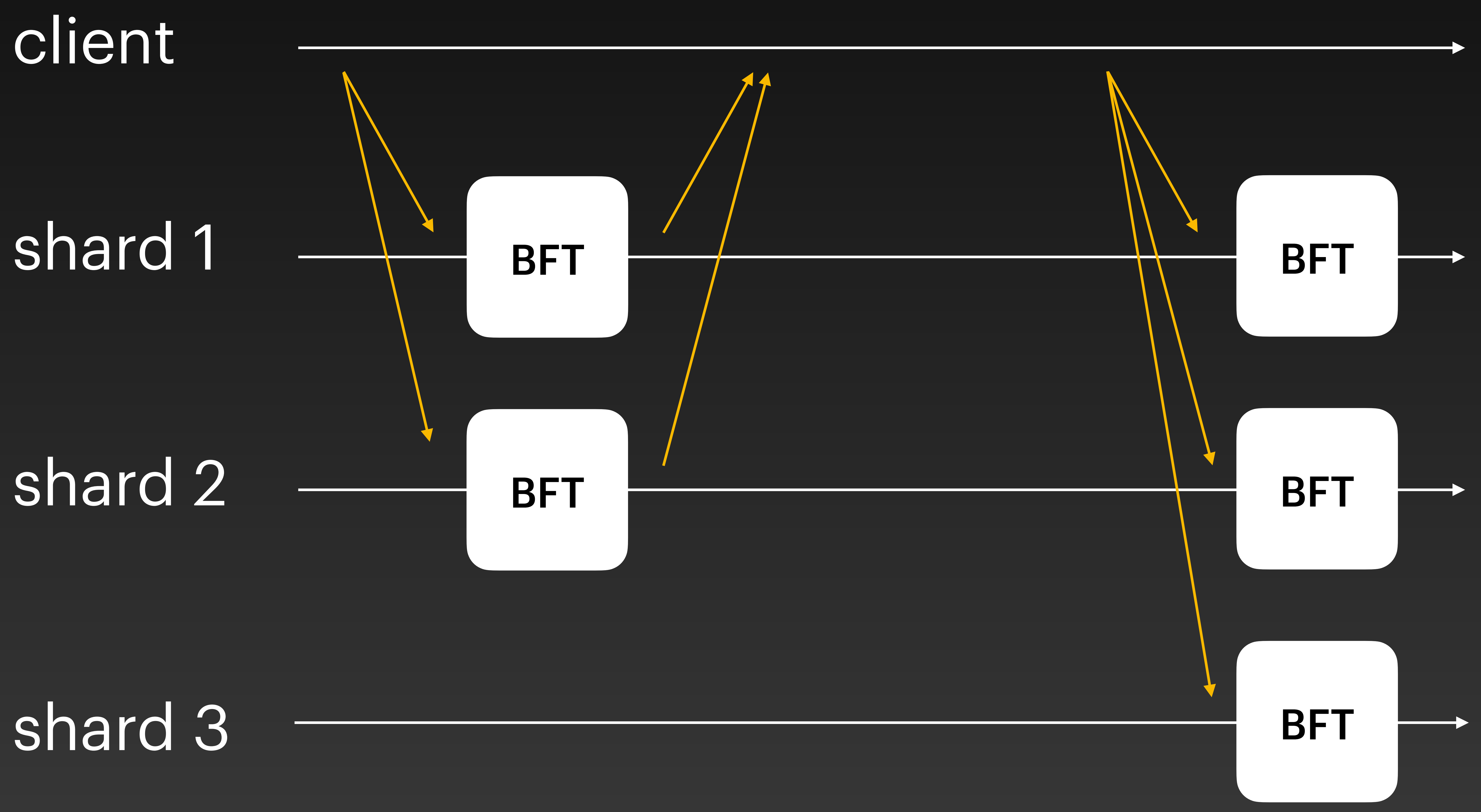
S-BAC

$$T(x_1, x_2) \rightarrow (y_1, y_2, y_3)$$



Atomix

$$T(x_1, x_2) \rightarrow (y_1, y_2, y_3)$$



Insecure under parallel composition

Attacks

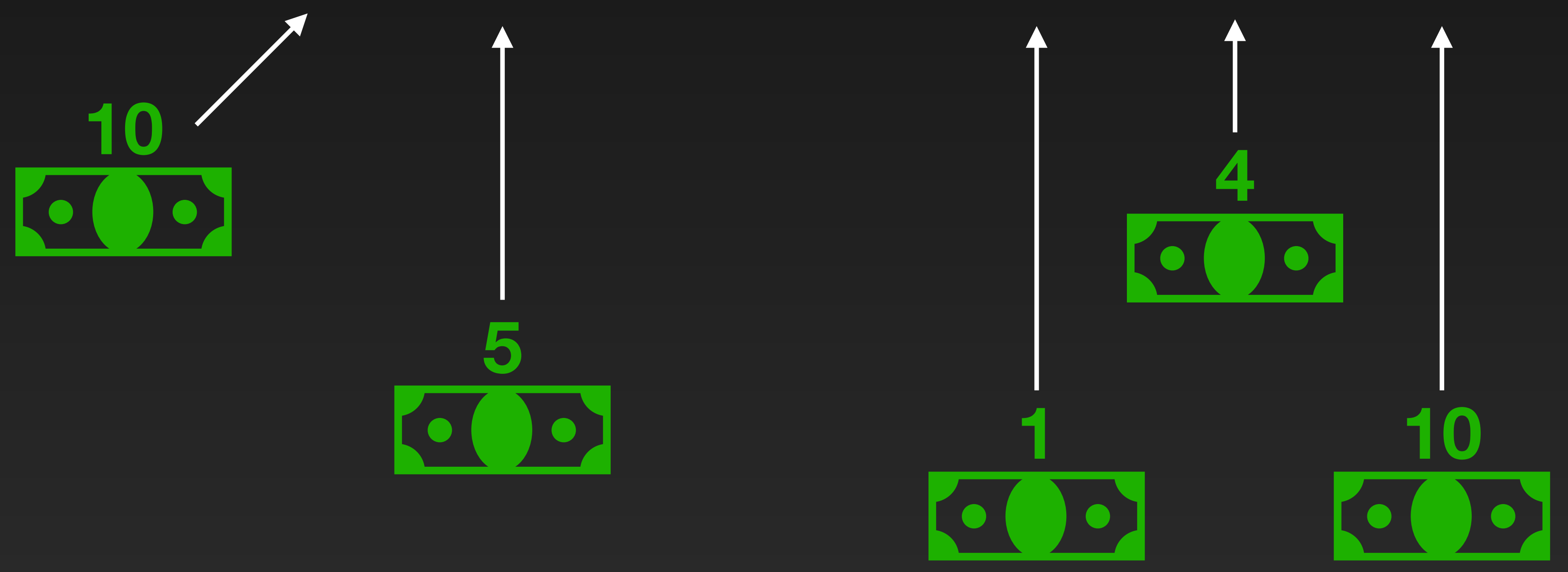
Double spend any object

- Does not need to collude with any node
- Acts as client or passive observer
- Re-orders network messages (not always needed)

Attack against S-BAC

Double-spend X_1

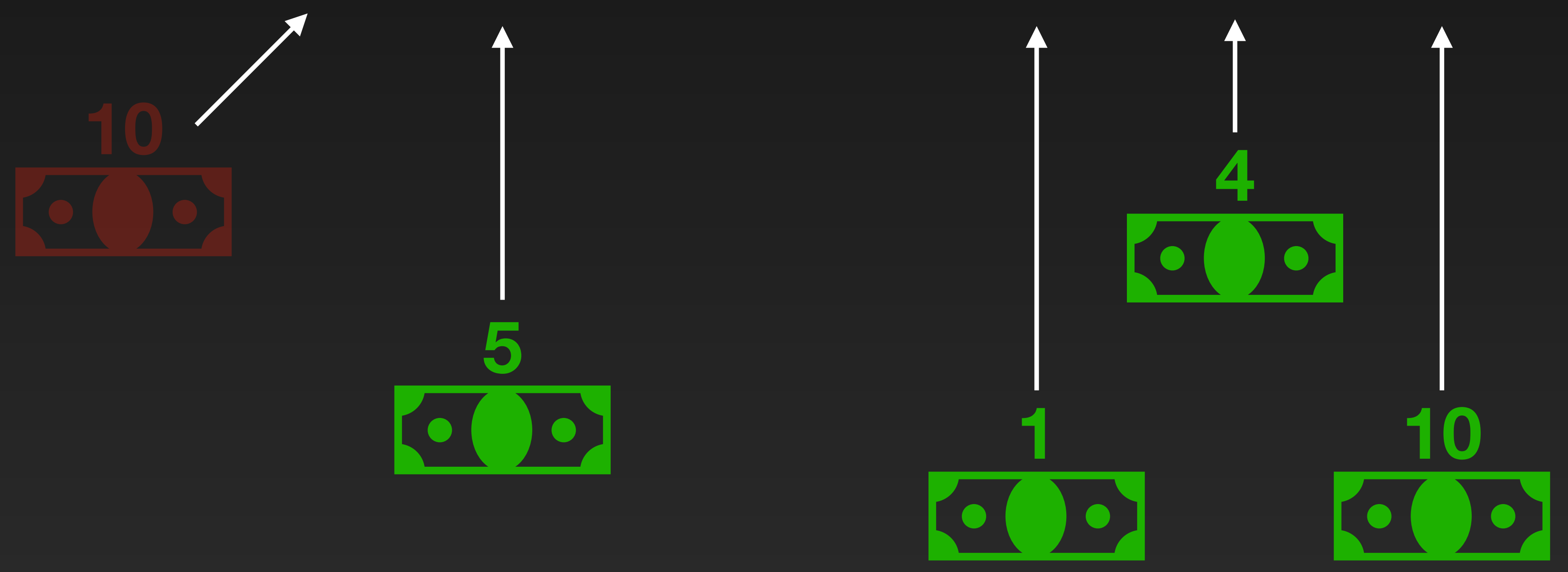
$$T(x_1, x_2) \rightarrow (y_1, y_2, y_3)$$



Attack against S-BAC

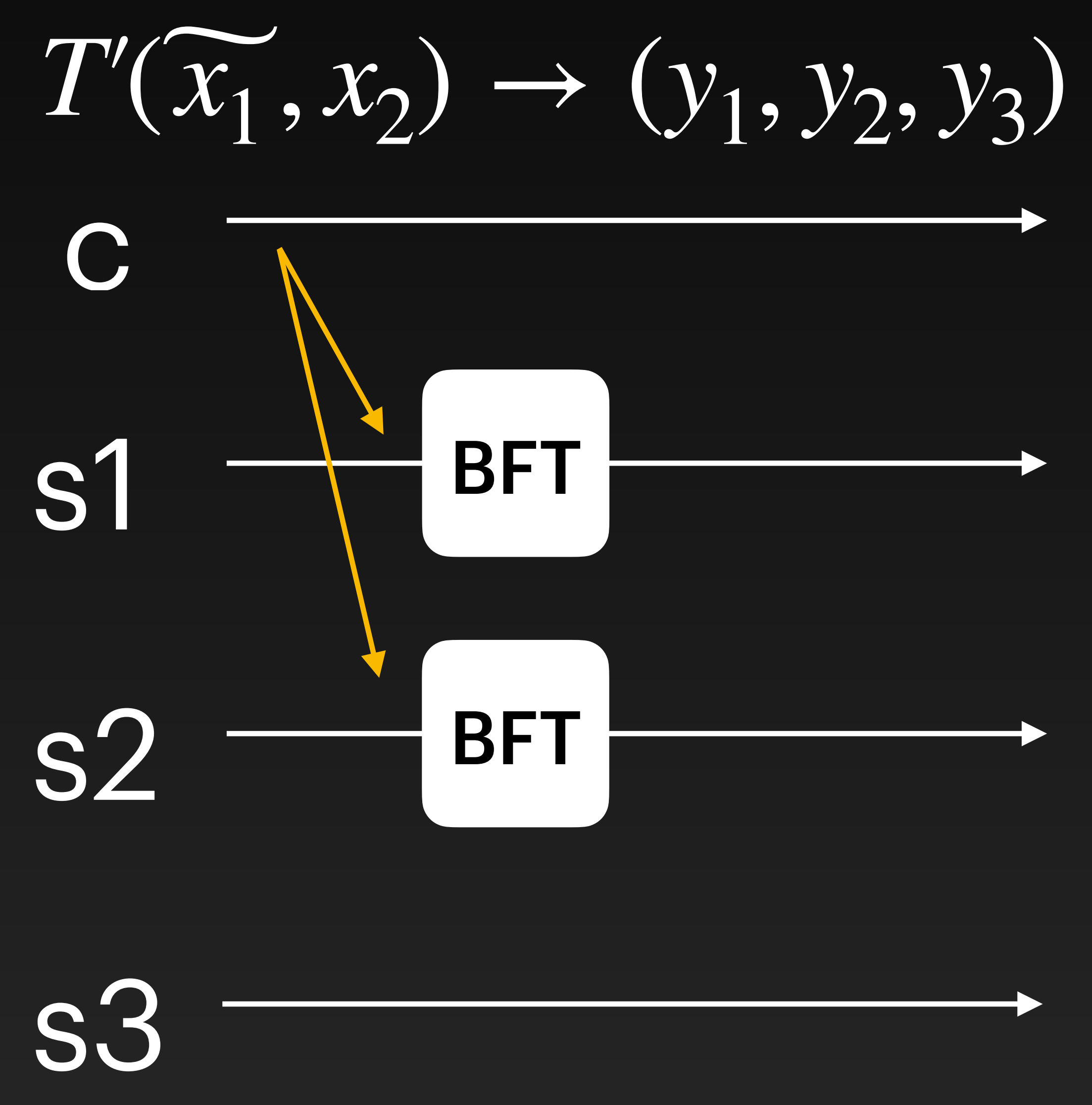
Double-spend X_1

$$T'(\widetilde{x_1}, x_2) \rightarrow (y_1, y_2, y_3)$$



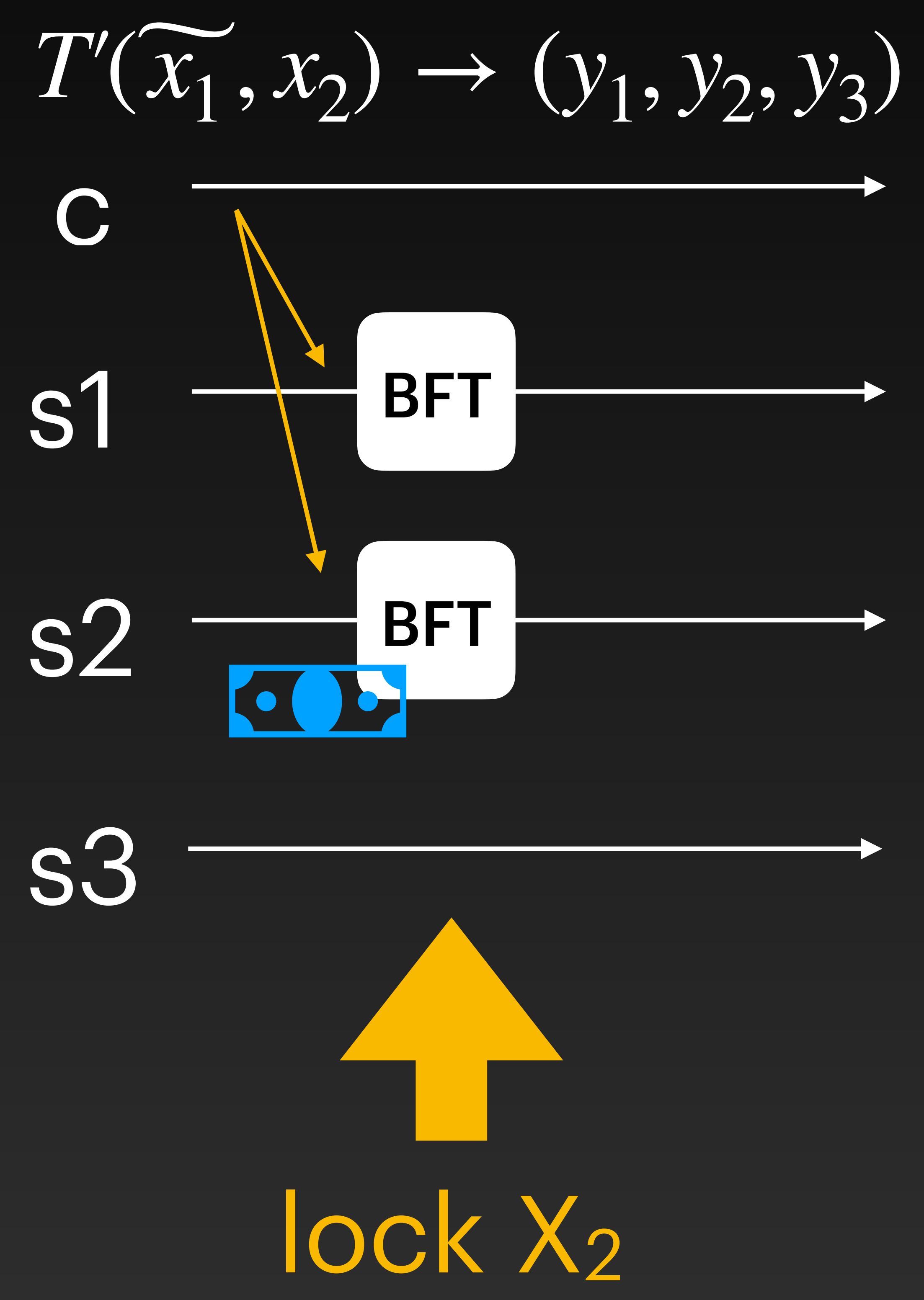
Attack against S-BAC

Double-spend X_1



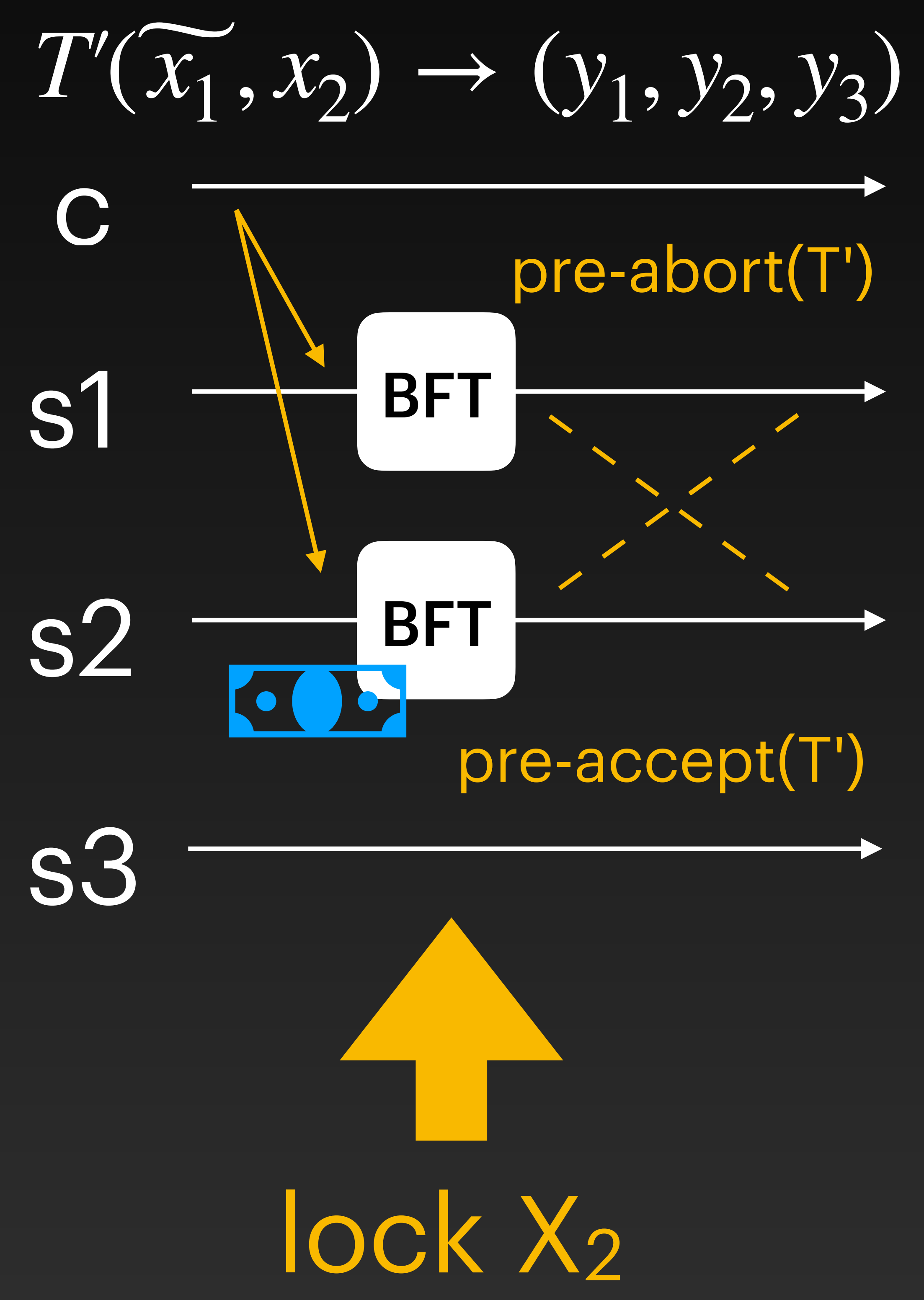
Attack against S-BAC

Double-spend X_1



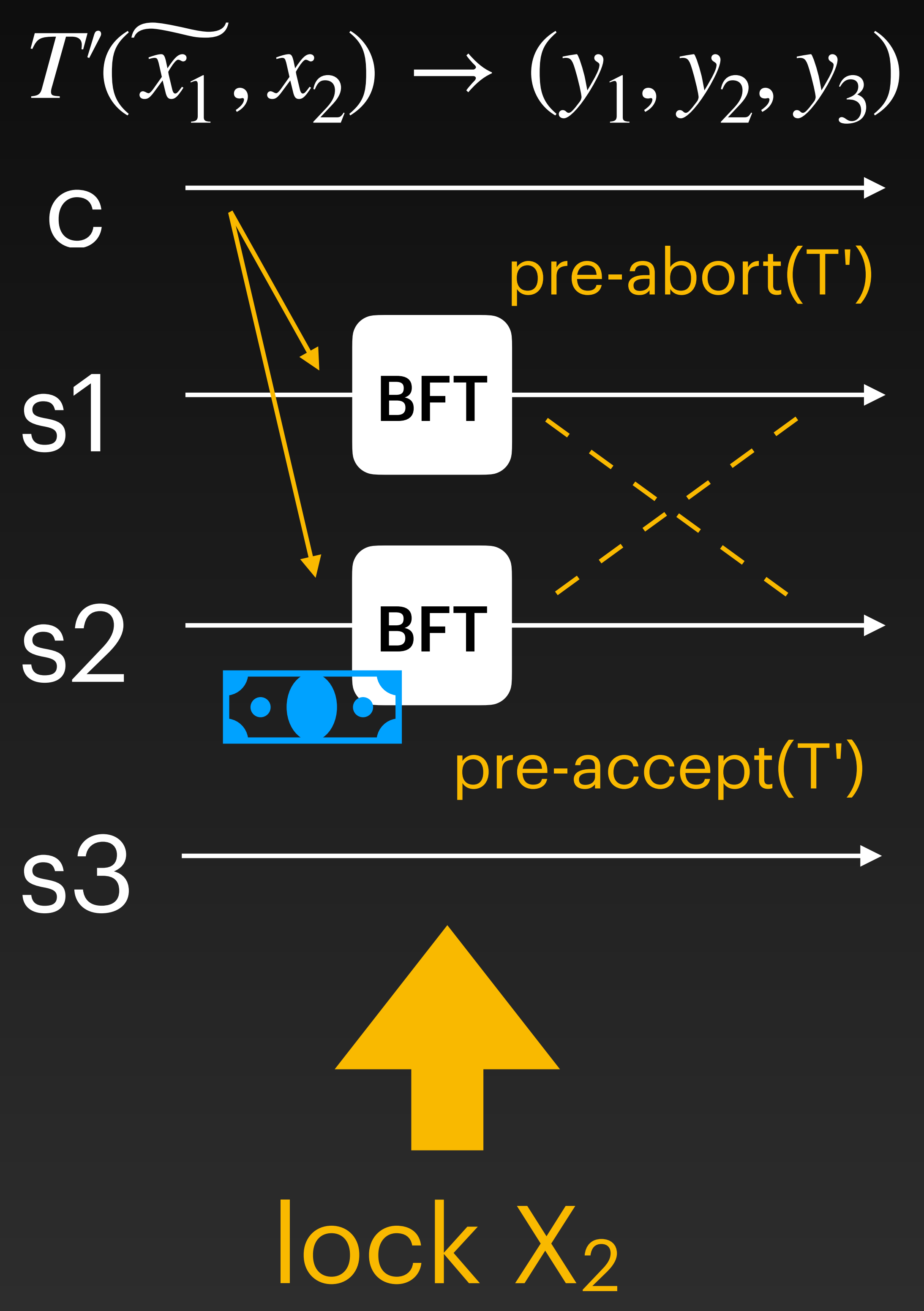
Attack against S-BAC

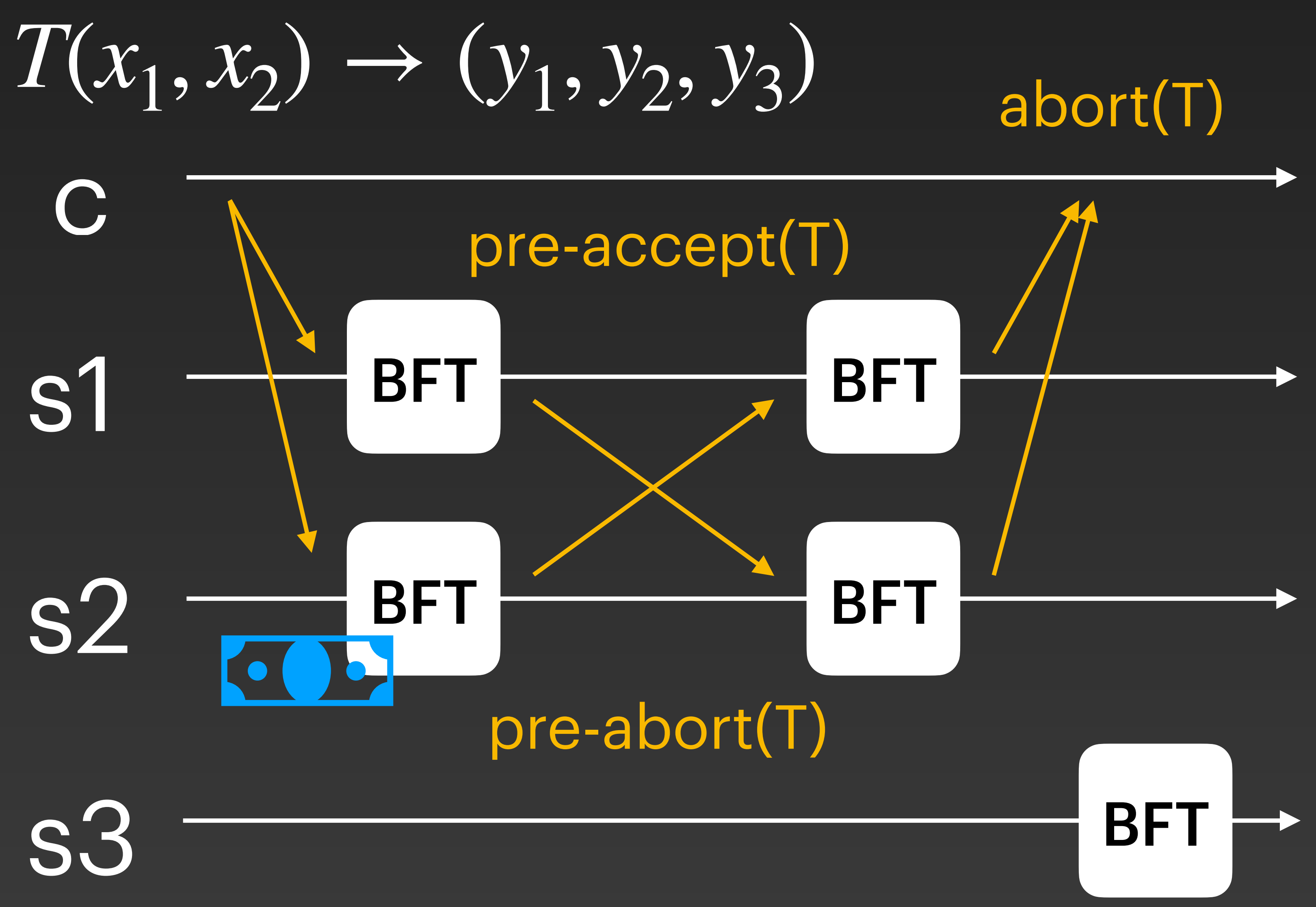
Double-spend X_1



Attack against S-BAC

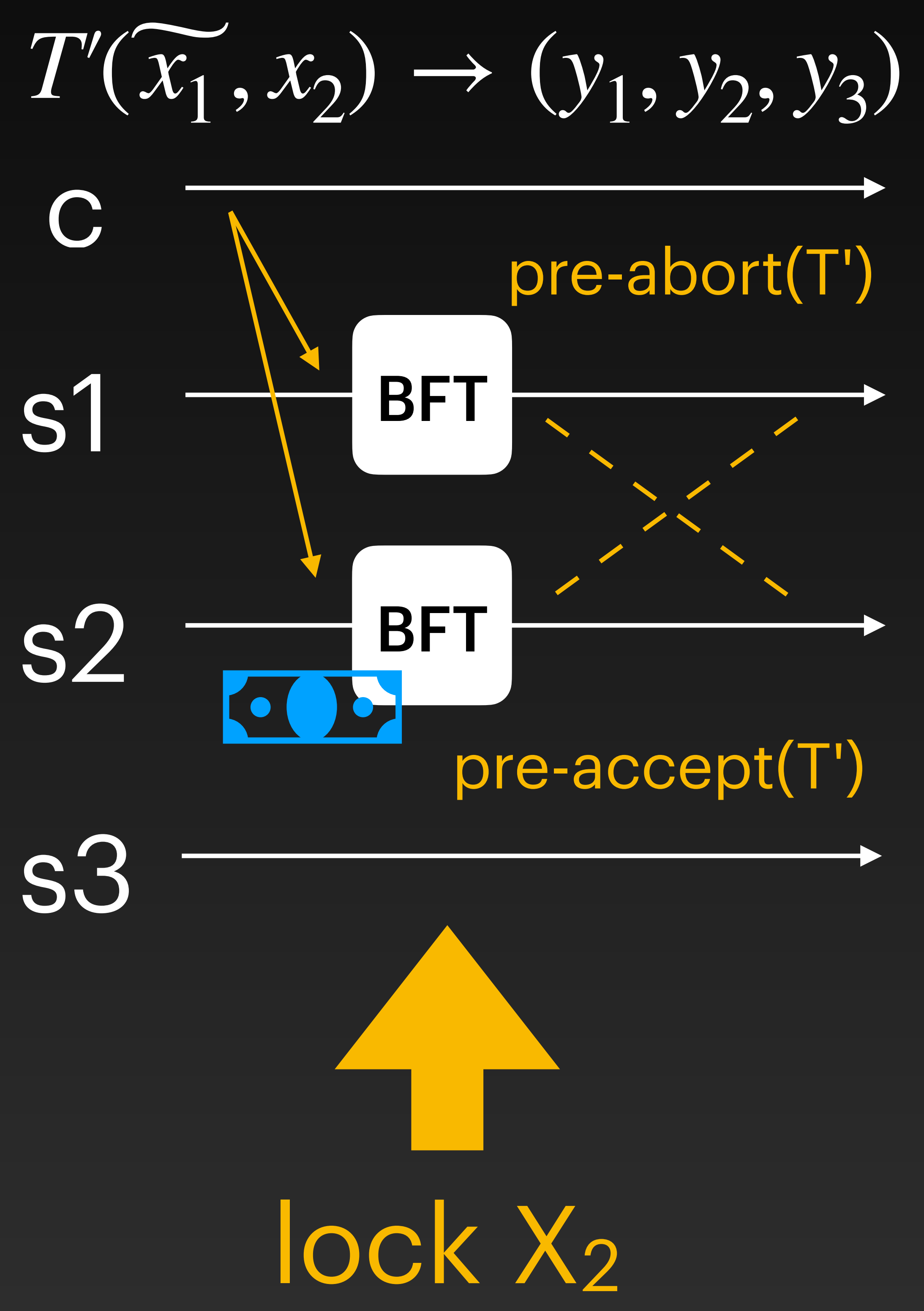
Double-spend X_1

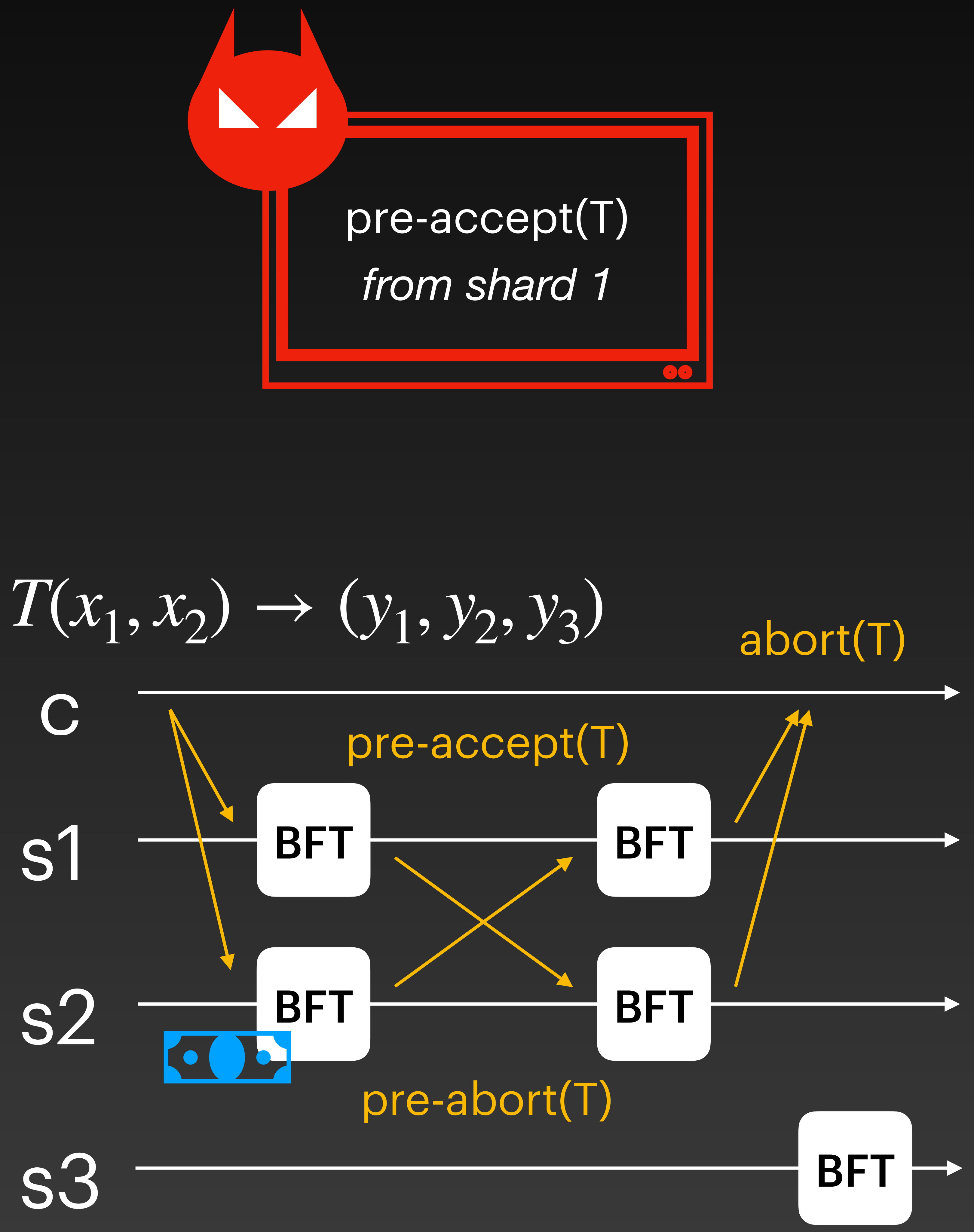




Attack against S-BAC

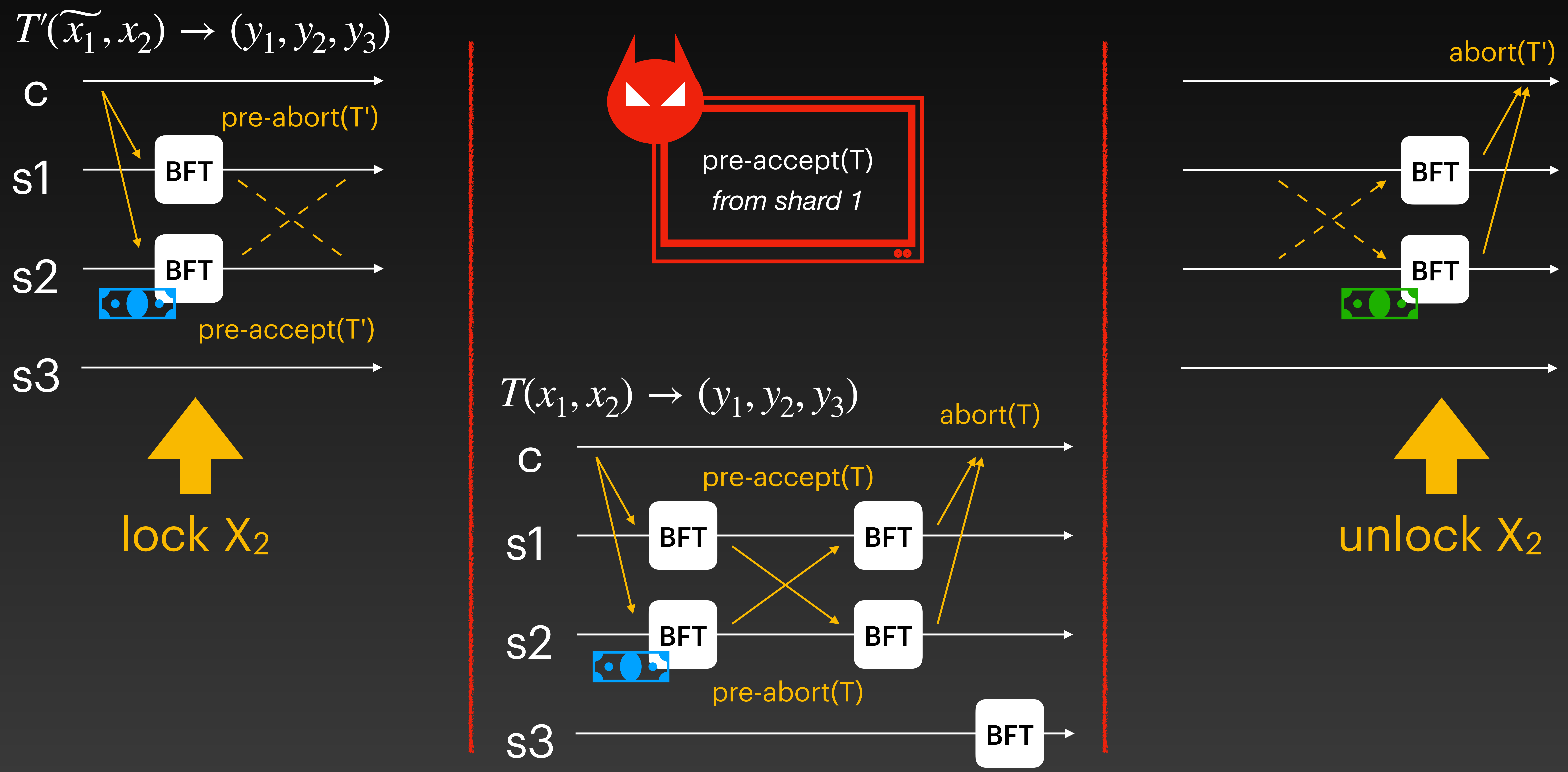
Double-spend X_1





Attack against S-BAC

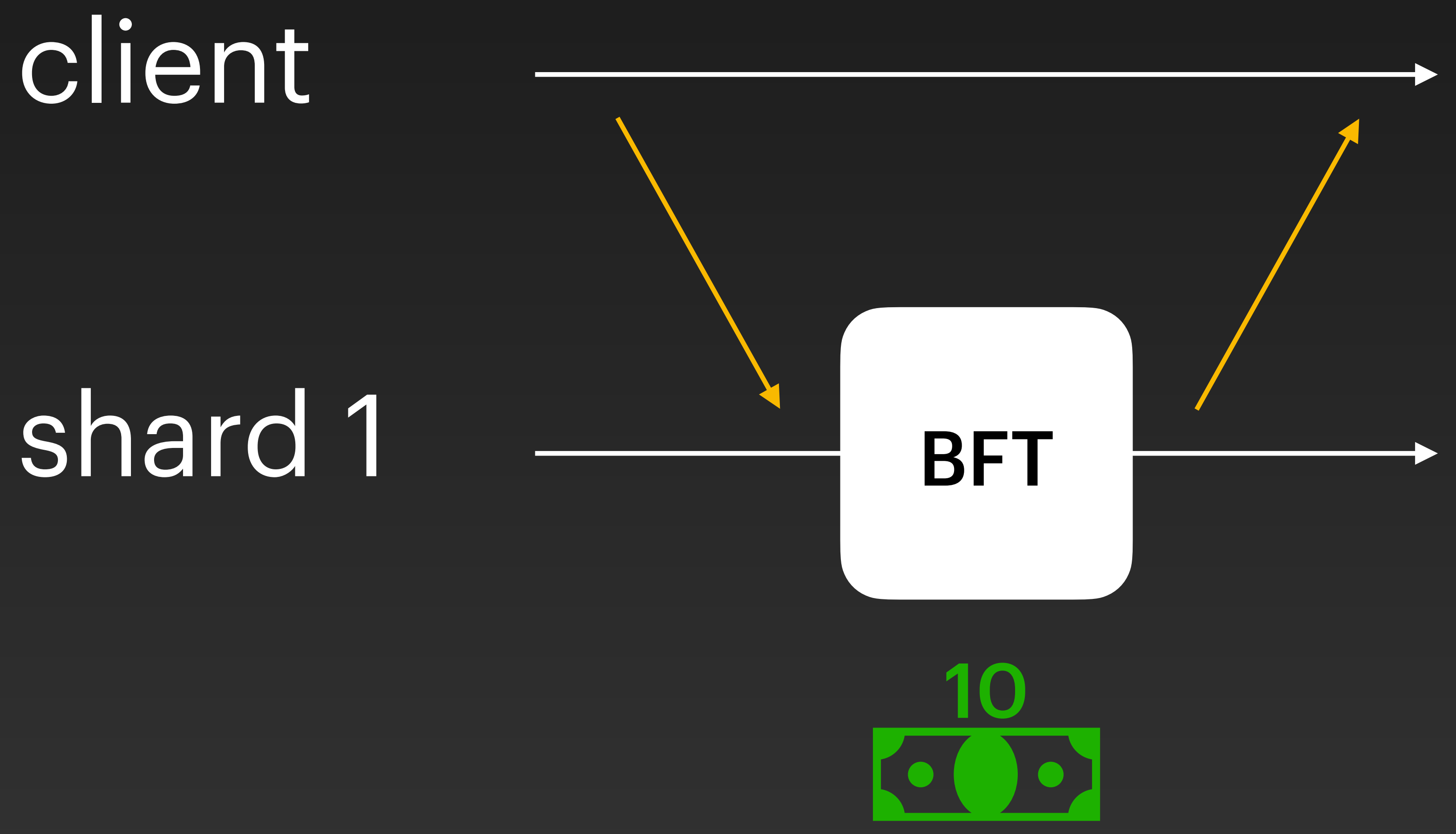
Double-spend X_1



Attack against S-BAC

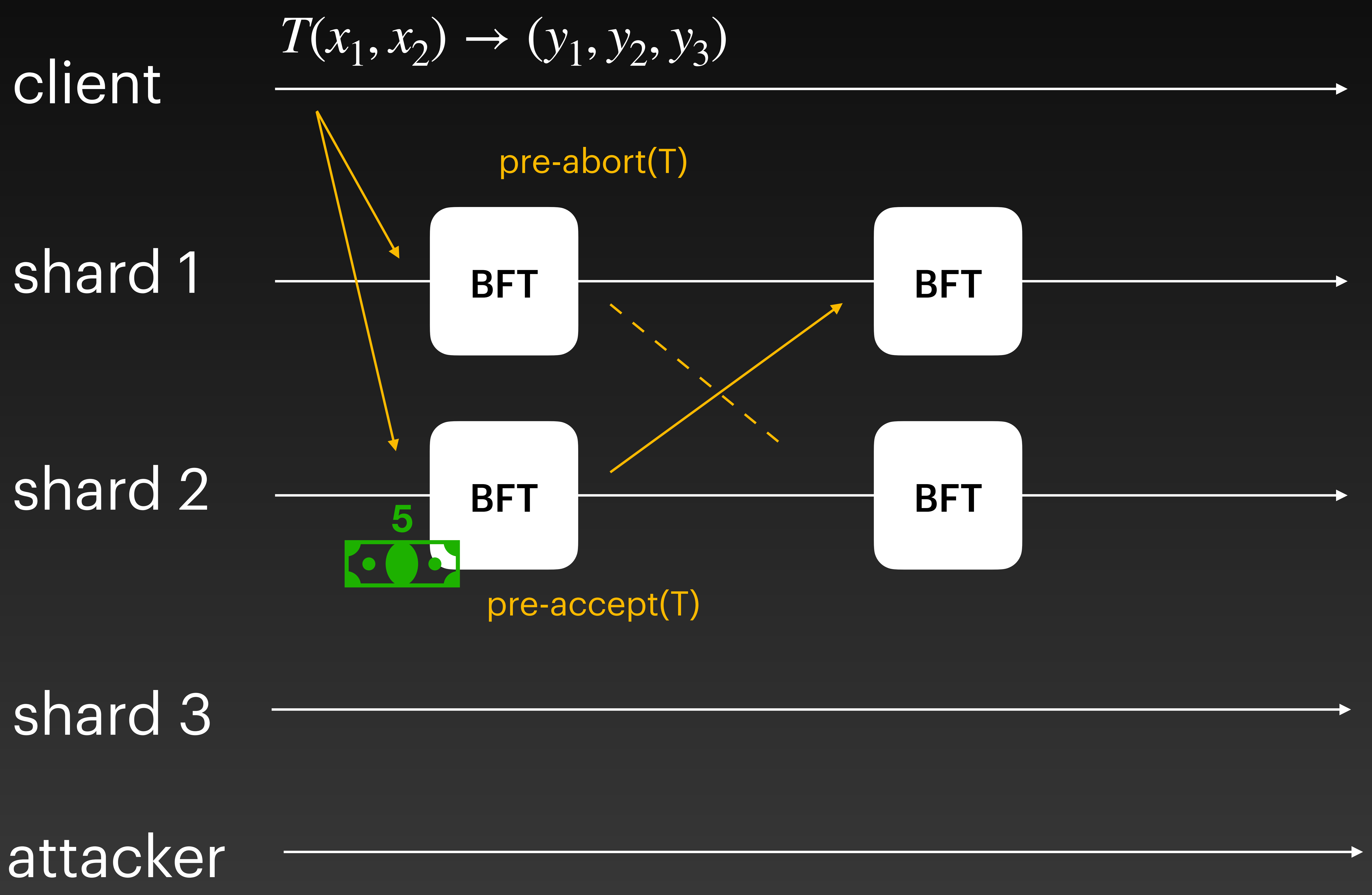
Double-spend X_1

$$T^*(x_1) \rightarrow (y_*)$$



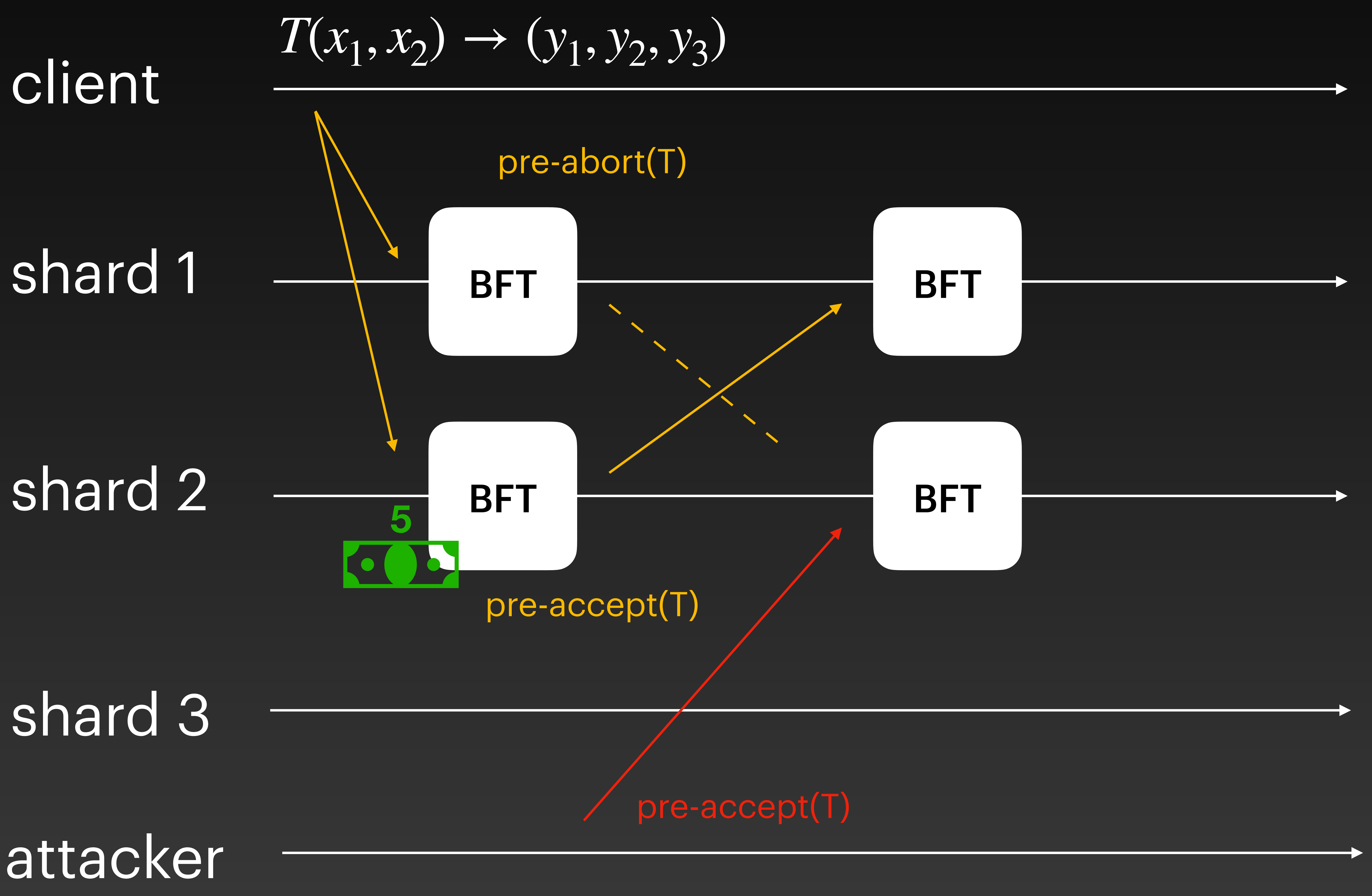
Attack against S-BAC

Double-spend X_1



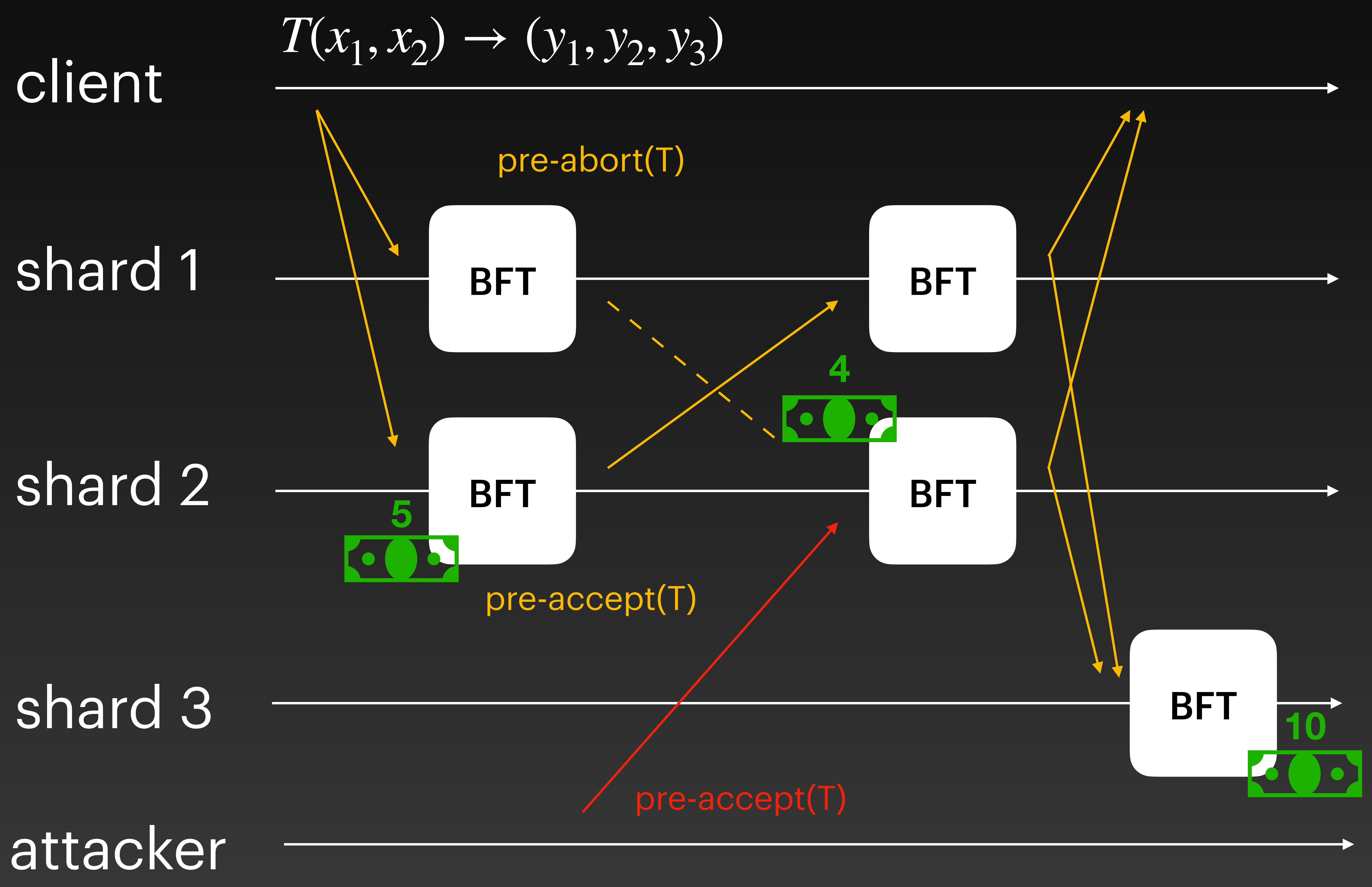
Attack against S-BAC

Double-spend X_1



Attack against S-BAC

Double-spend X_1



Attack against S-BAC

Double-spend X_1

Before attack

X_1 10

X_2 5

After attack

Y_* 10

Y_2 4

Y_3 10

Byzcuit

S-BAC + Atomix