Attacks

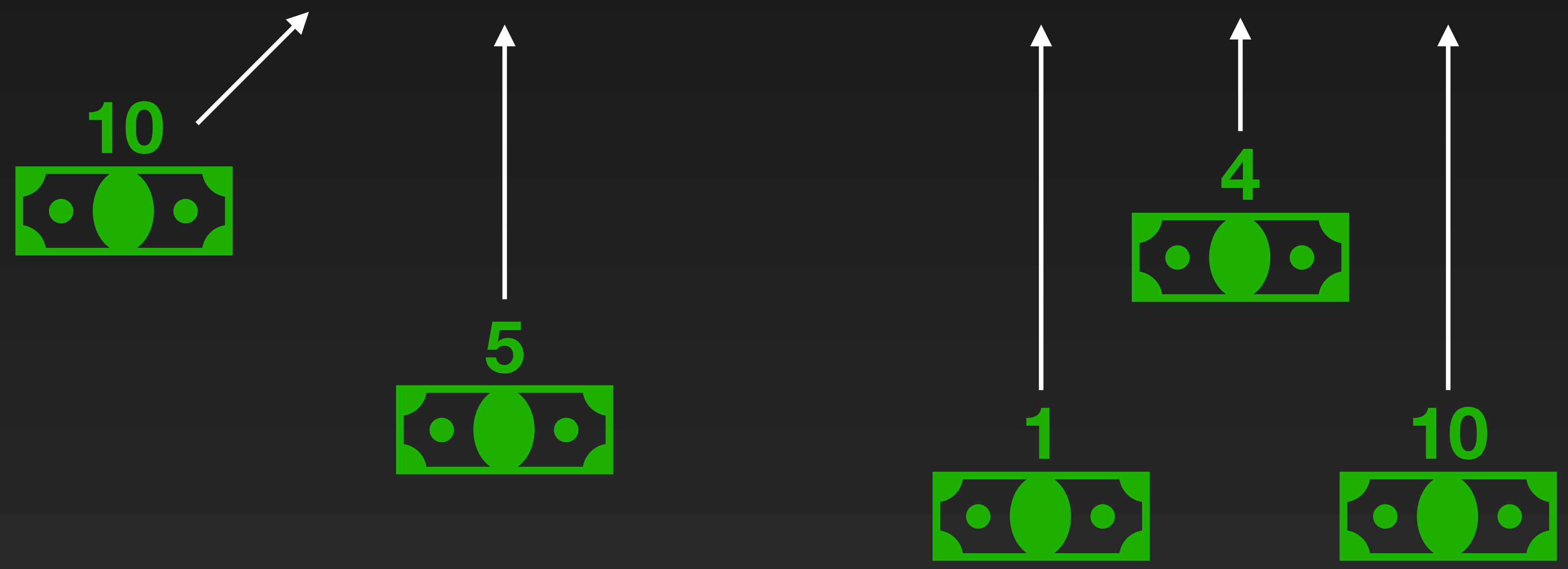
Double spend any object

- 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 X₁

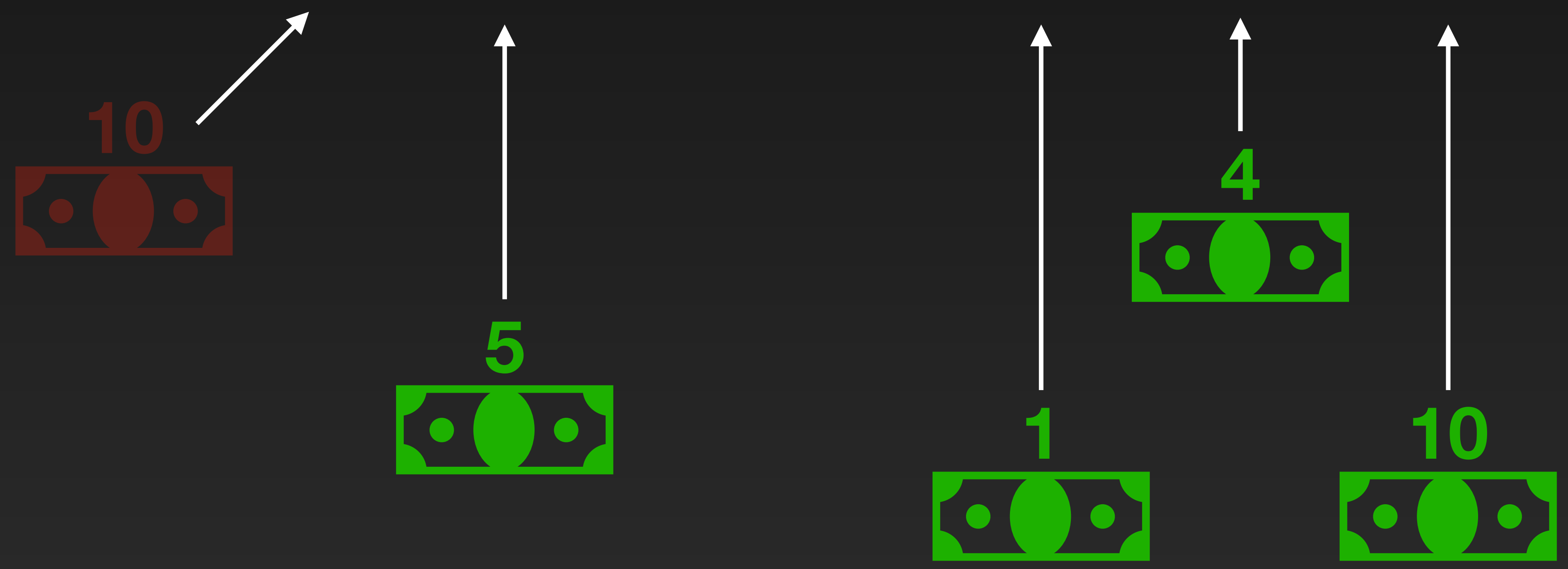
$$T(x_1, x_2) \to (y_1, y_2, y_3)$$



Attack against S-BAC

Double-spend X_1

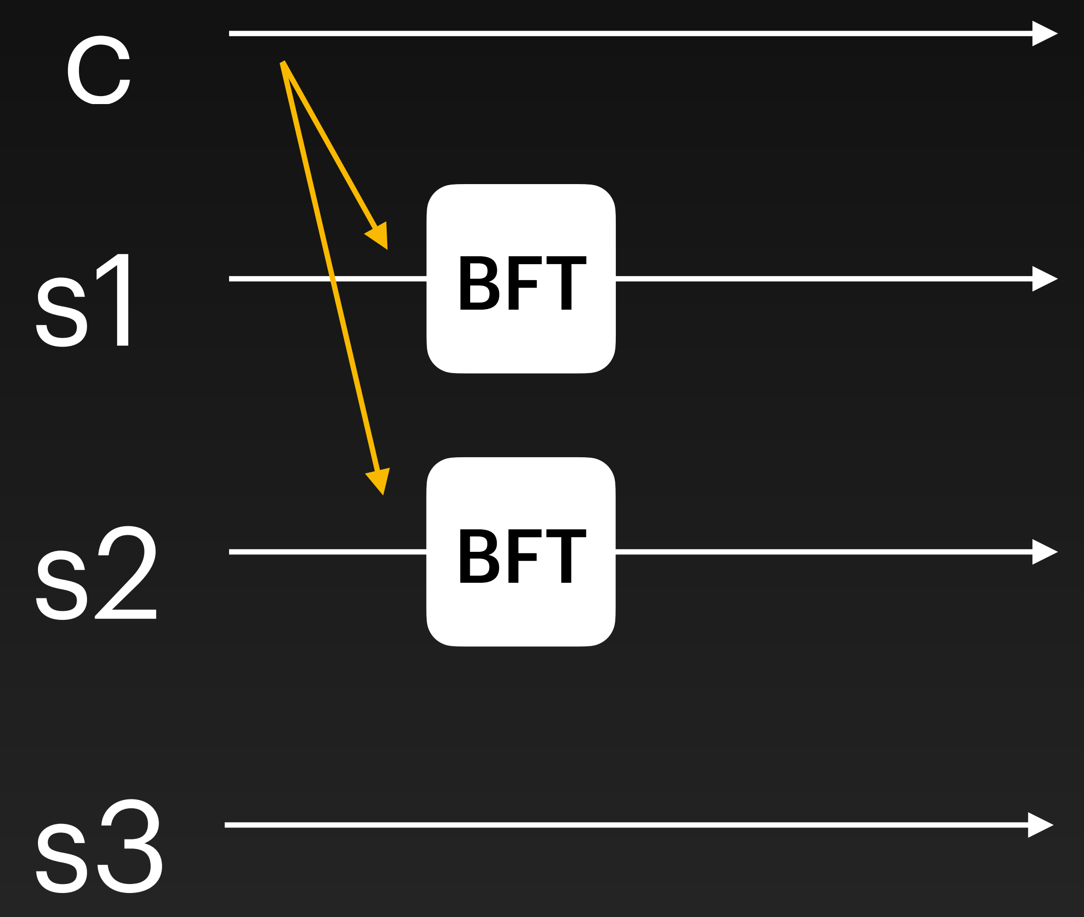
$$T'(\widetilde{x_1}, x_2) \rightarrow (y_1, y_2, y_3)$$



Attack against S-BAC

Double-spend X₁

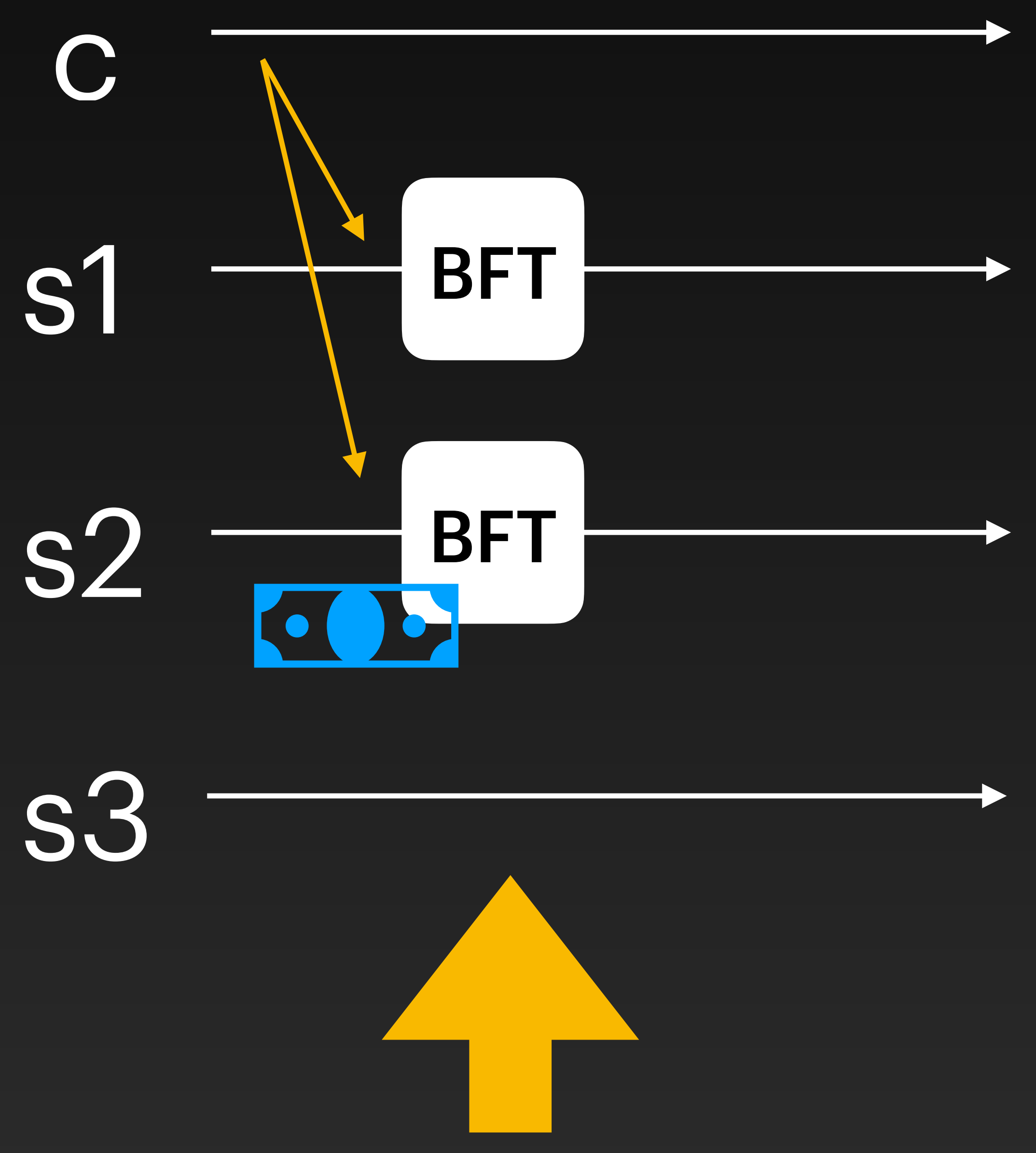
$T'(\widetilde{x_1}, x_2) \rightarrow (y_1, y_2, y_3)$



Attack against S-BAC

Double-spend X₁

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

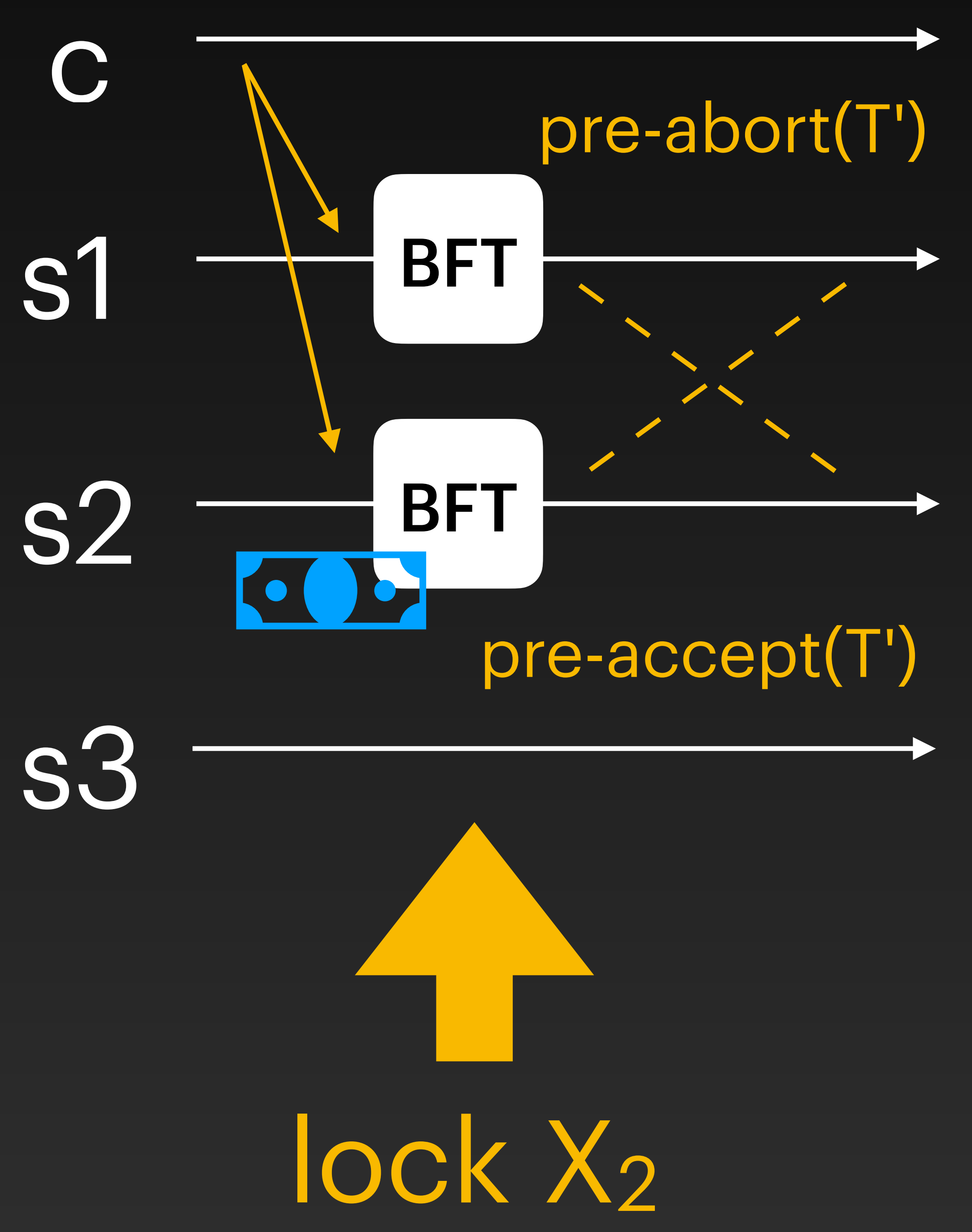


lock X₂

Attack against S-BAC

Double-spend X₁

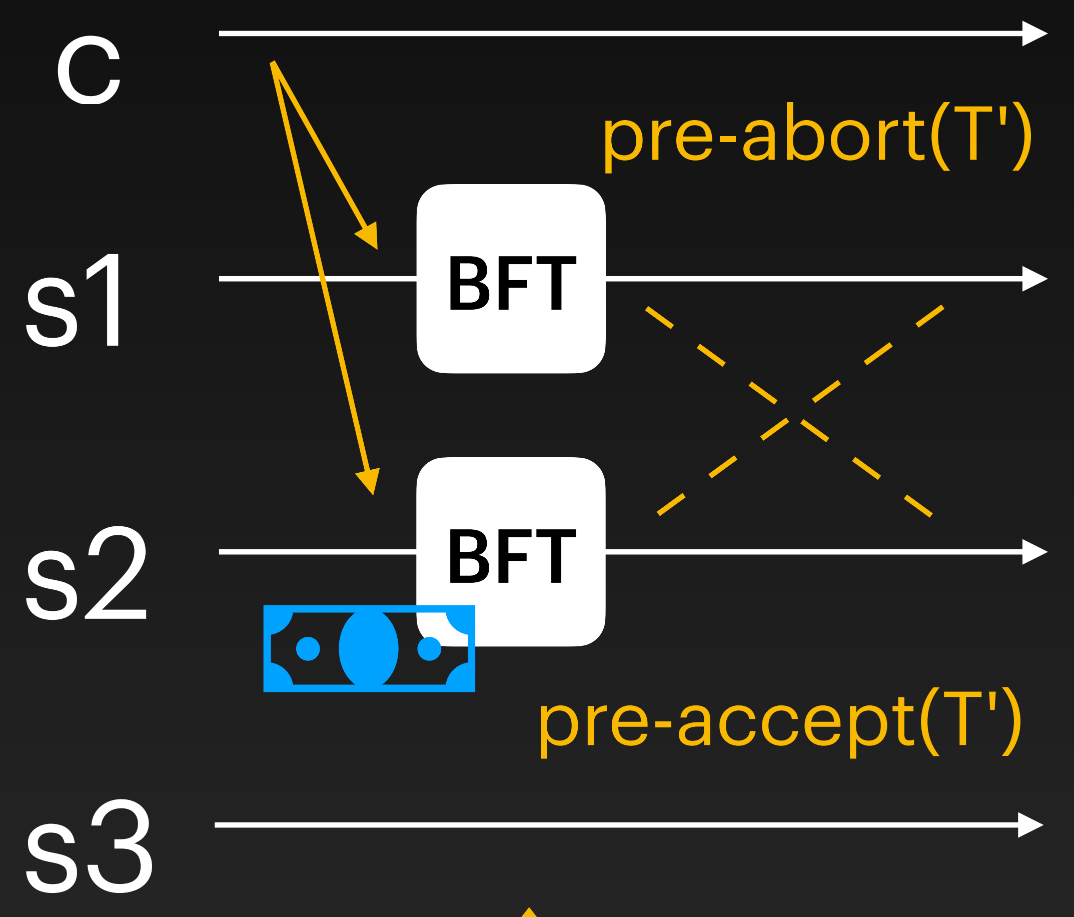
$T'(\widetilde{x_1}, x_2) \rightarrow (y_1, y_2, y_3)$



Attack against S-BAC

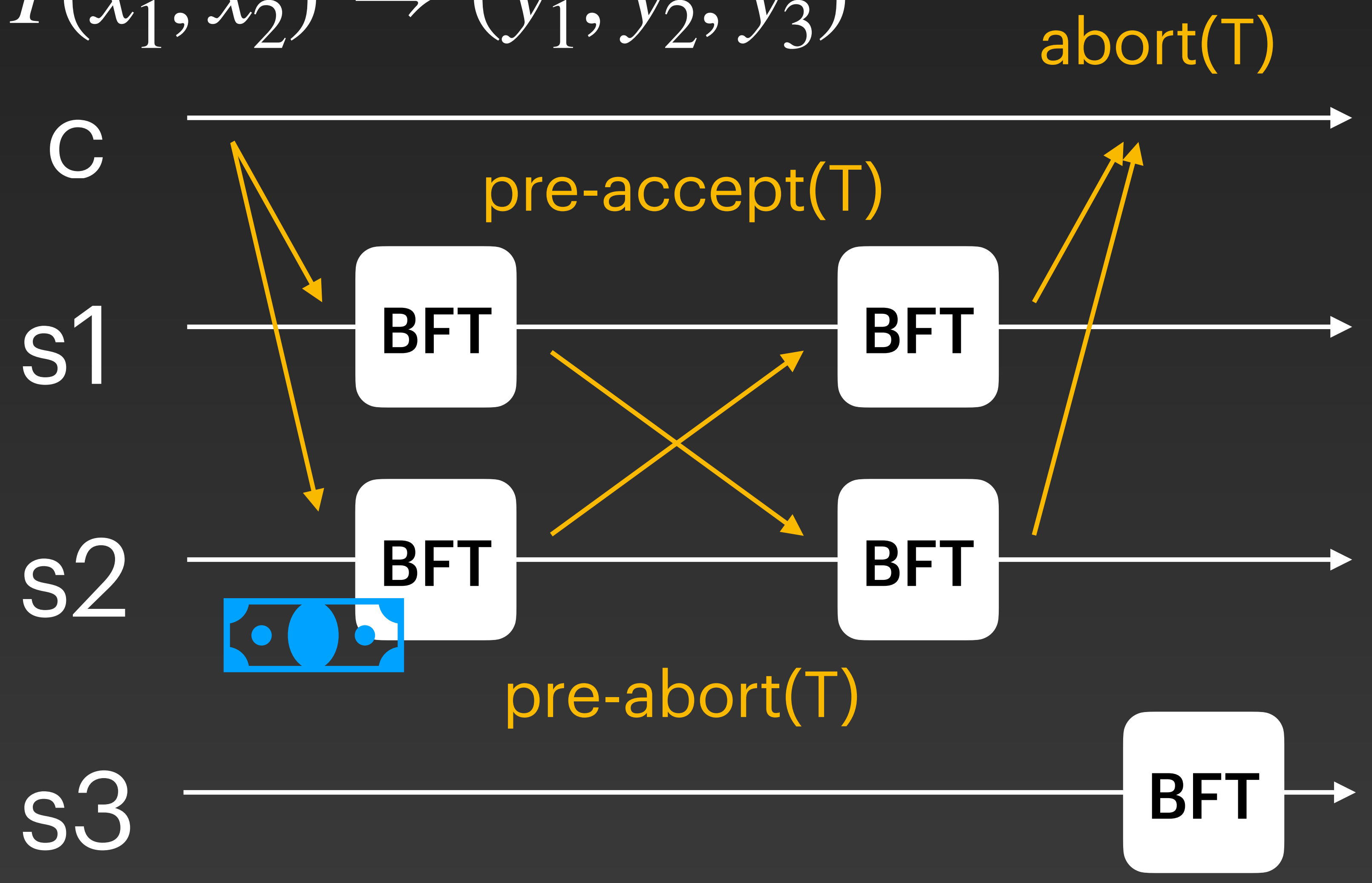
Double-spend X_1

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



lock X_2

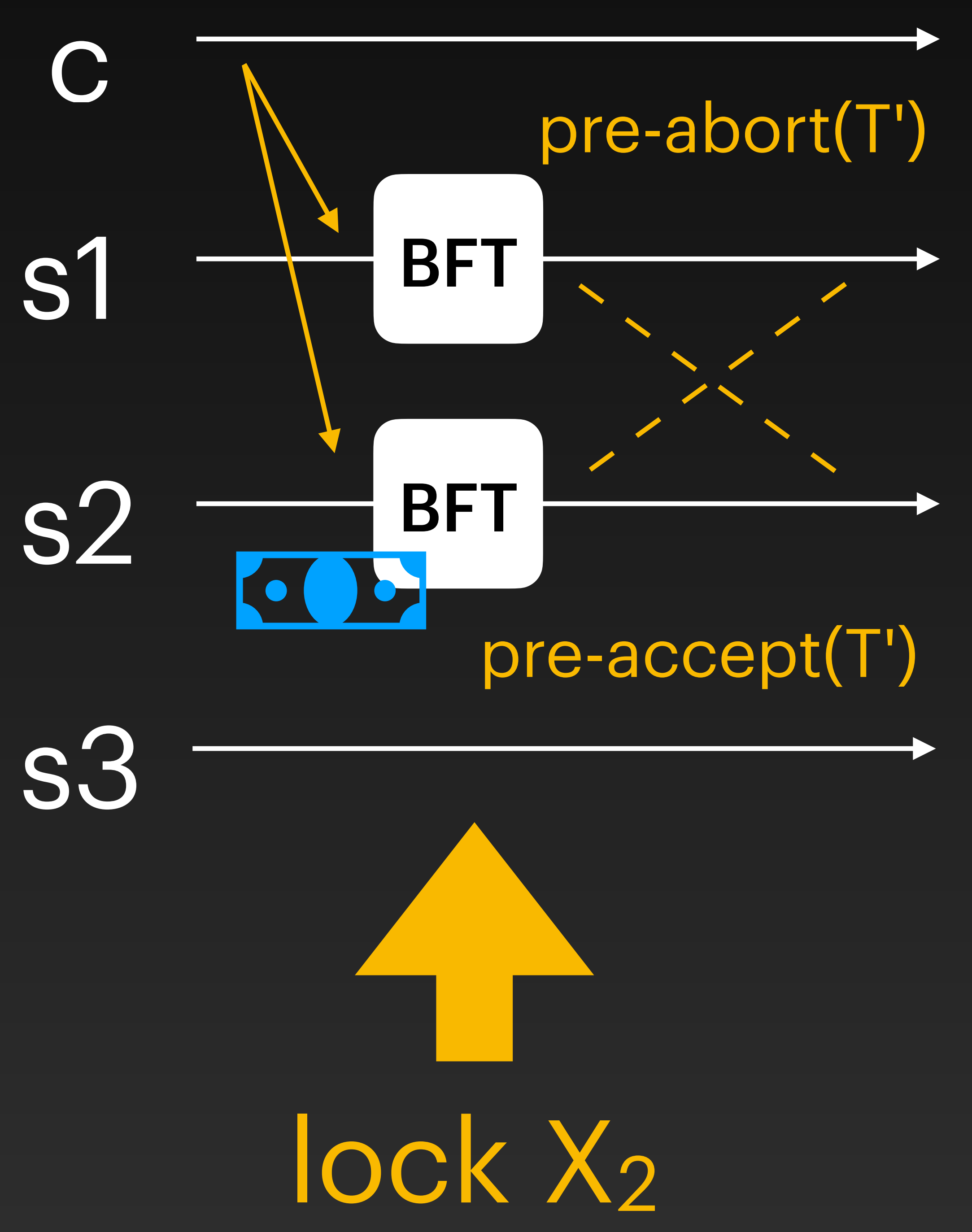
$T(x_1, x_2) \rightarrow (y_1, y_2, y_3)$



Attack against S-BAC

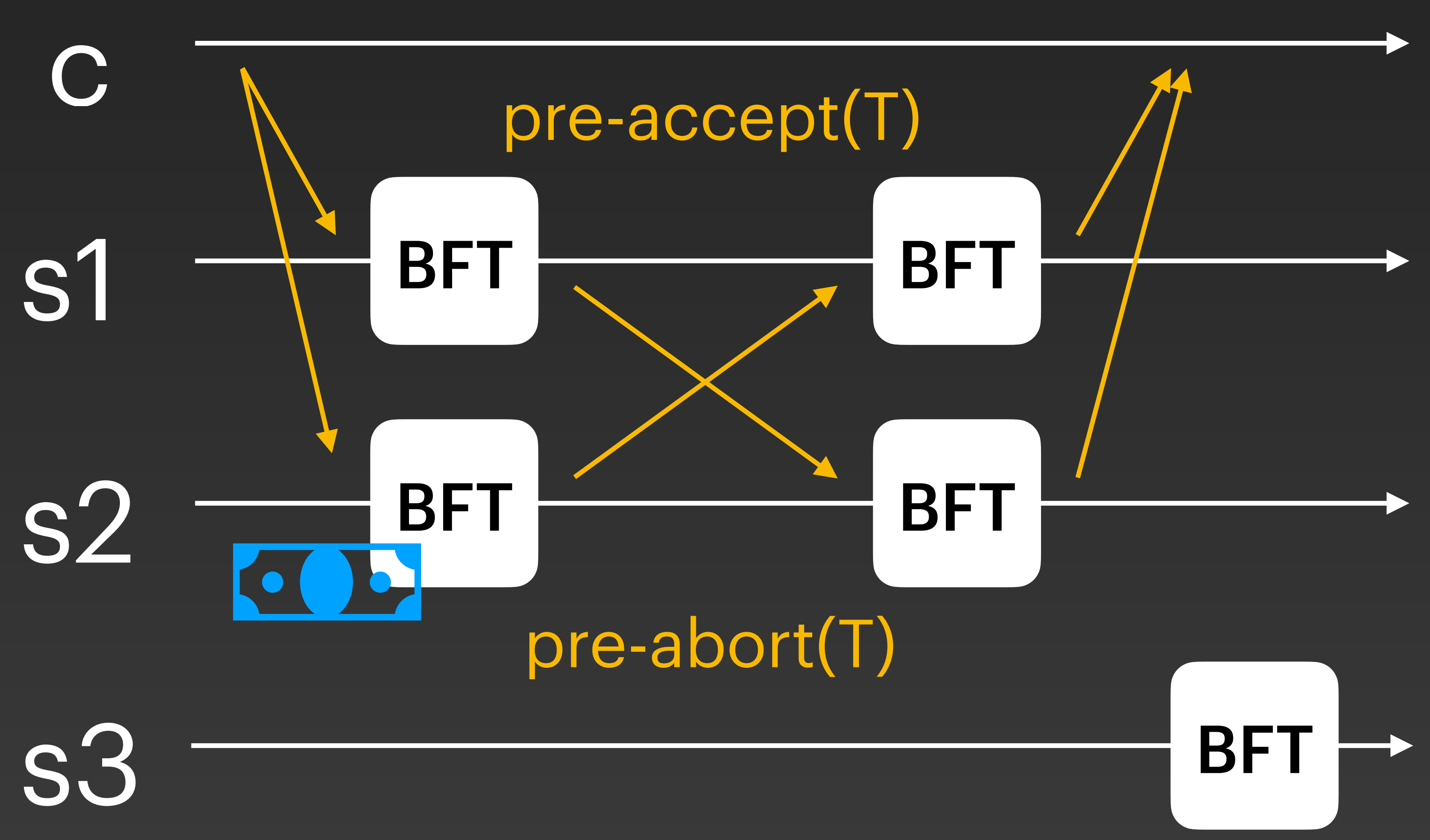
Double-spend X₁

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



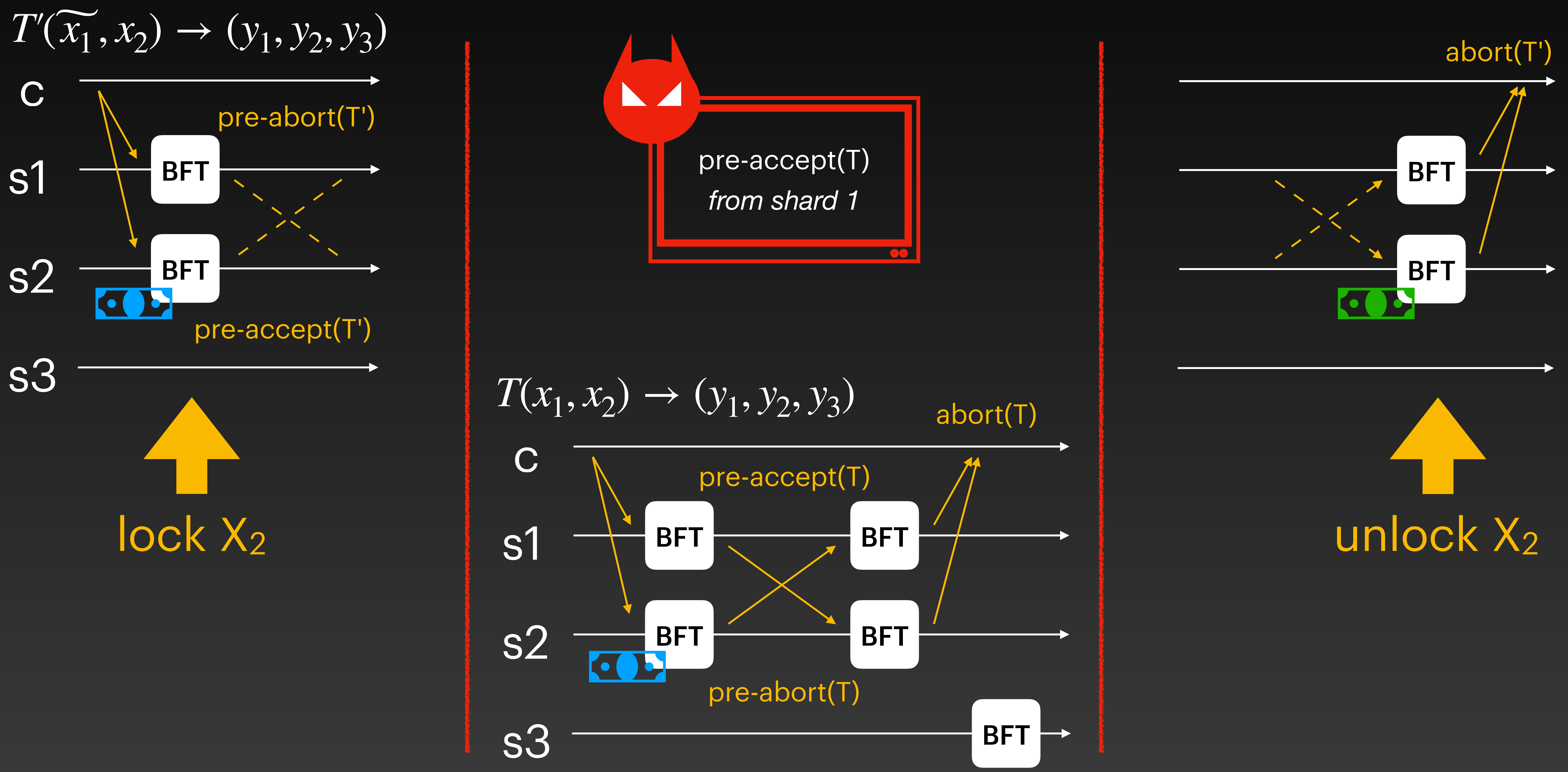
pre-accept(T)
from shard 1

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



Attack against S-BAC

Double-spend X1



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

lock X2

pre-accept(T)
from shard 1

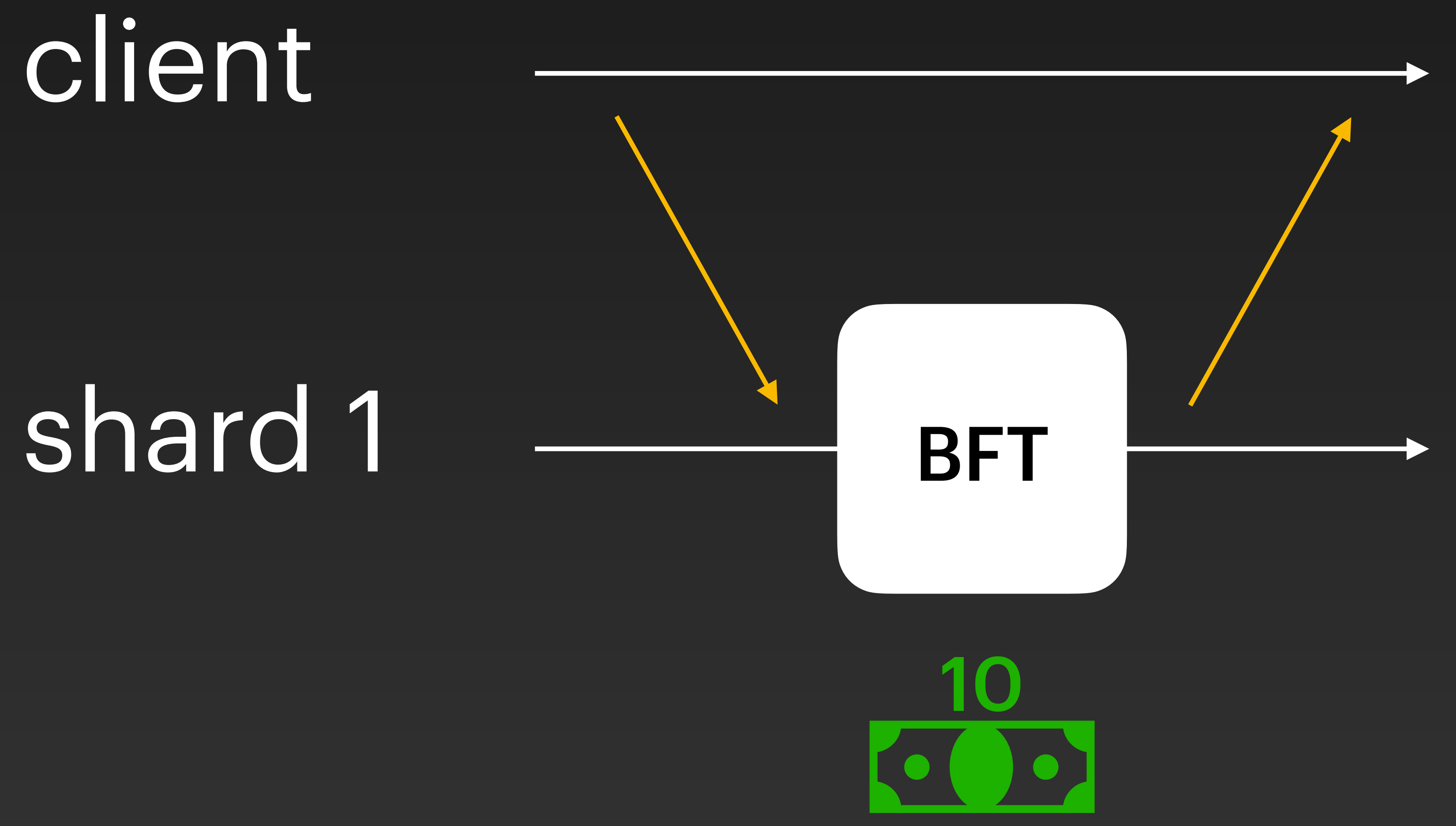
$T(x_1, x_2) \rightarrow (y_1, y_2, y_3)$

unlock X2

Attack against S-BAC

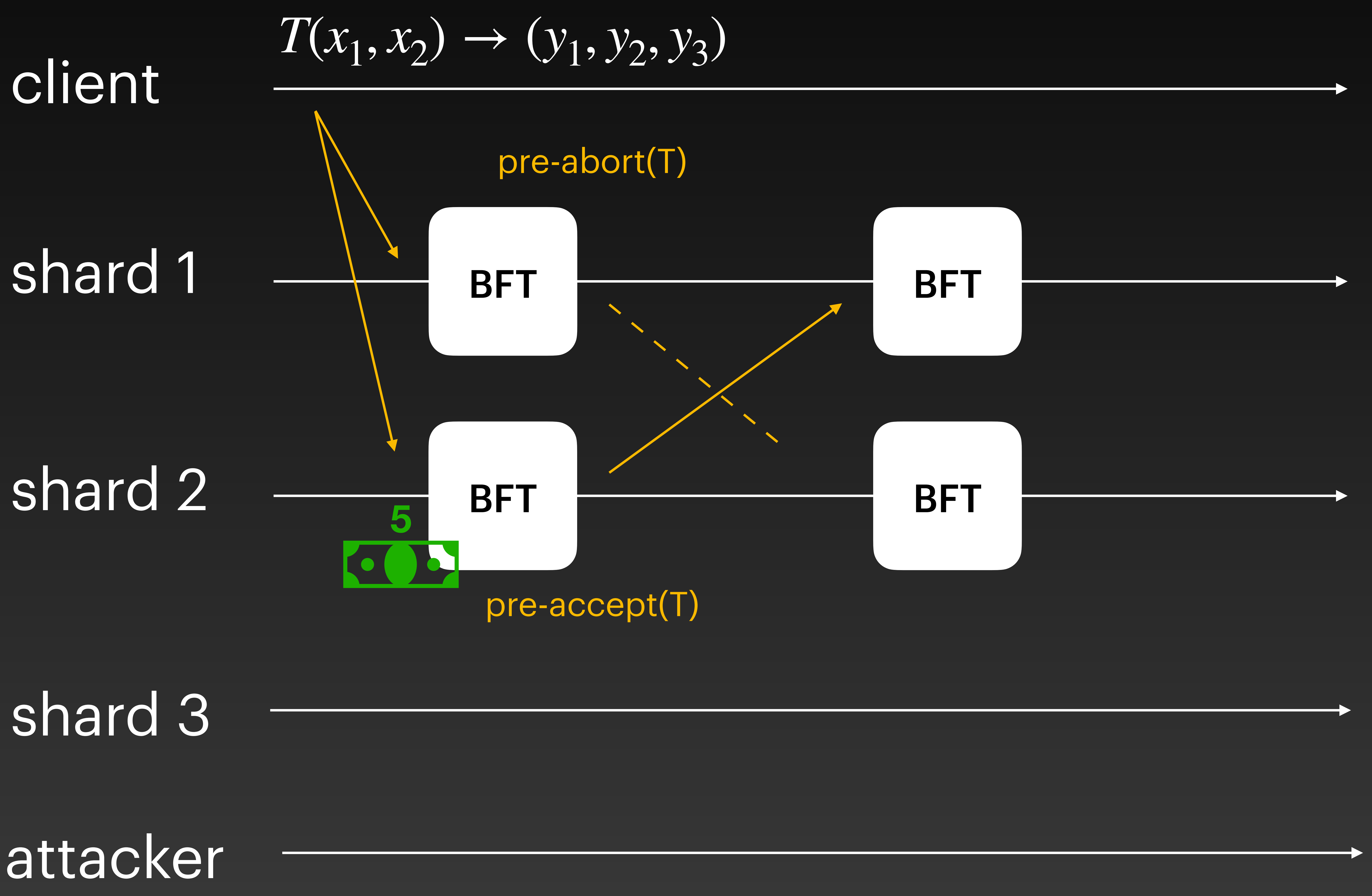
Double-spend X$_1$

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



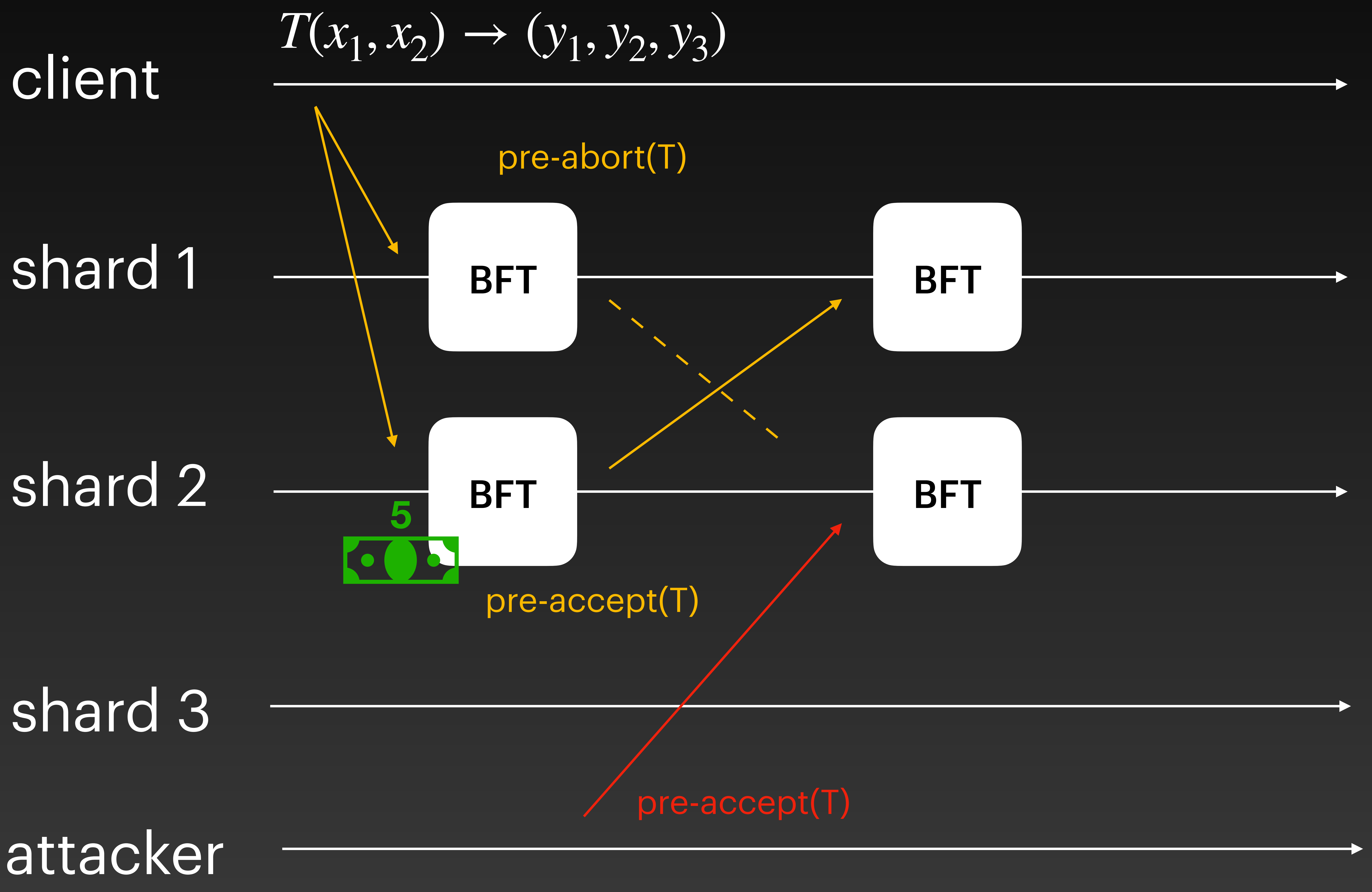
Attack against S-BAC

Double-spend X1



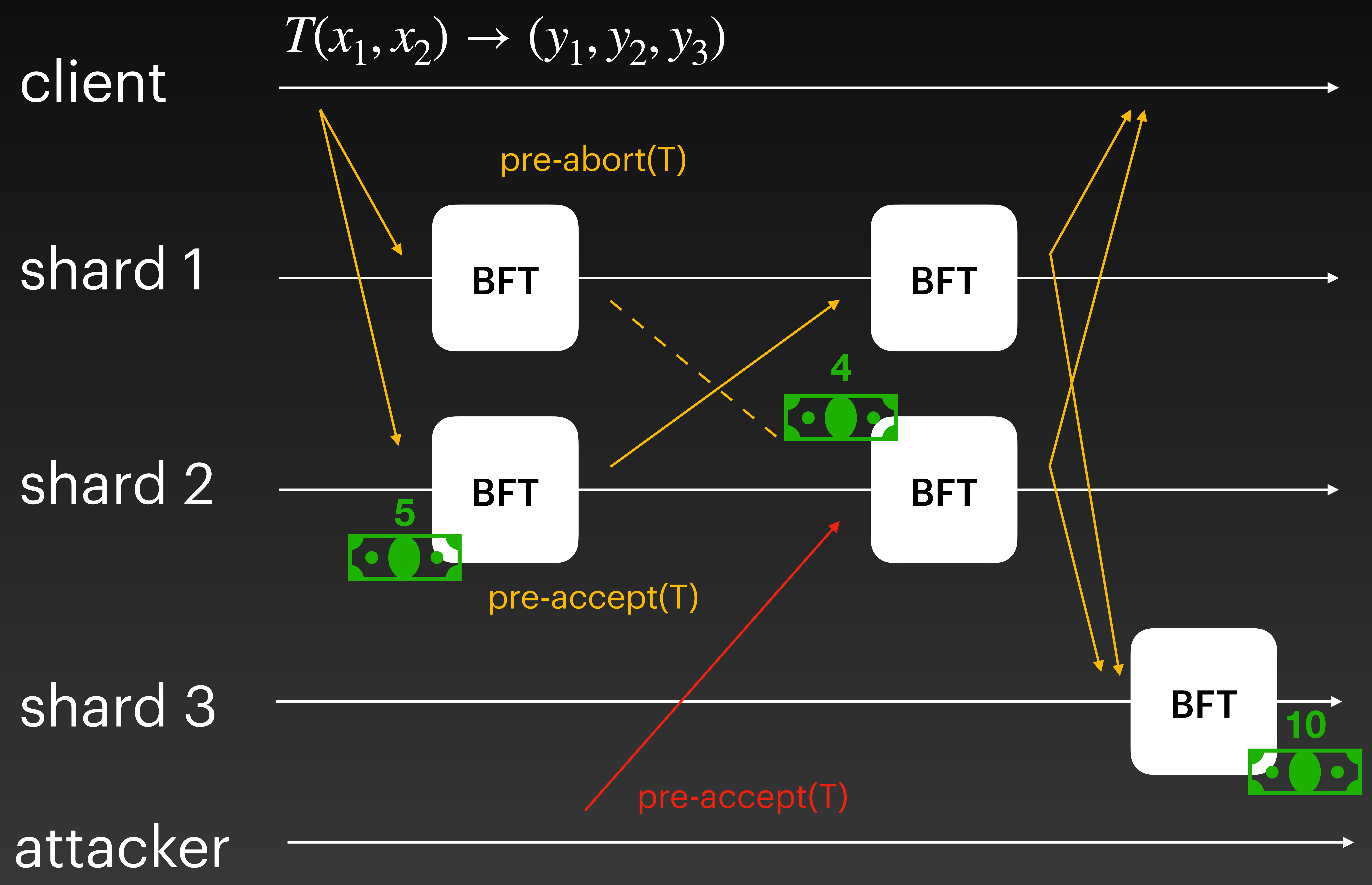
Attack against S-BAC

Double-spend X1



Attack against S-BAC

Double-spend X₁



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 💵

What causes these issues?

Issue 1. Input shards cannot associate protocol messages to a specific protocol execution.

Issue 2. Output shards (that are not also input shards) do not experience the first phase of the protocol