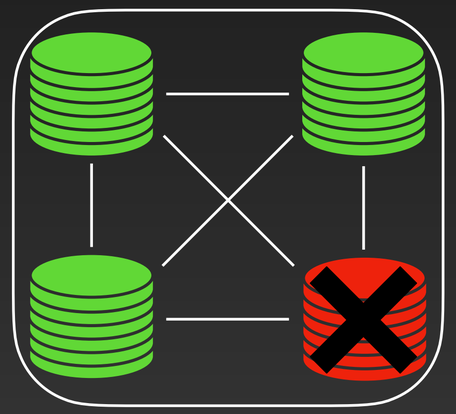
Byzcuit

Fix issue 1

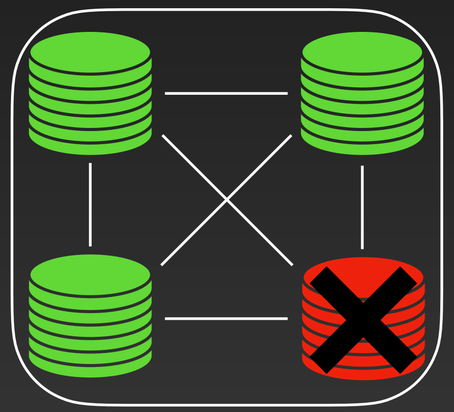
Add sequence numbers per object

X_1, S_{x1}



Shard 1

X_2, S_{x2}



Shard 2

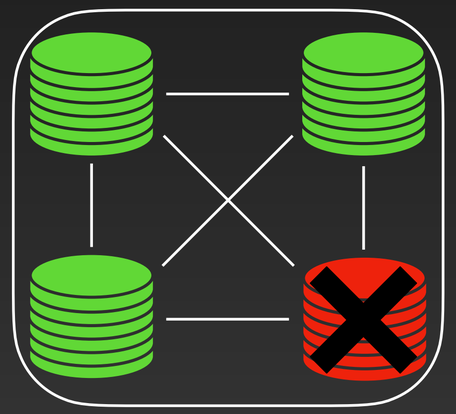
Shard 3

Byzcuit

Fix issue 2

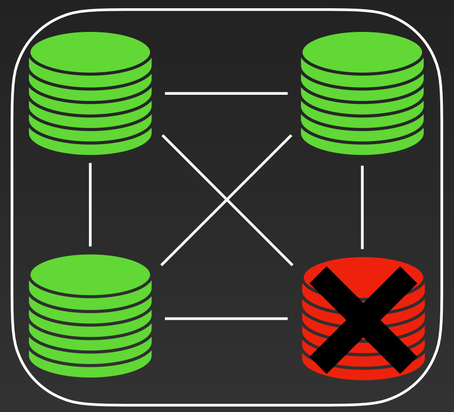
Dummy objects for output shards

X_1, S_{x1}



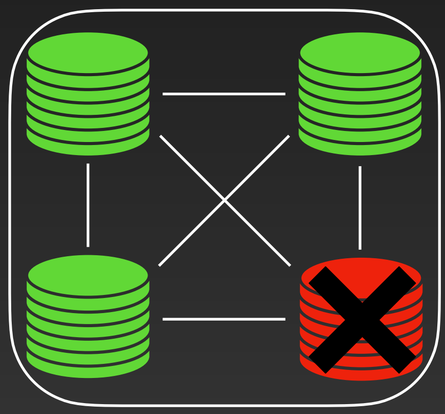
Shard 1

X_2, S_{x2}



Shard 2

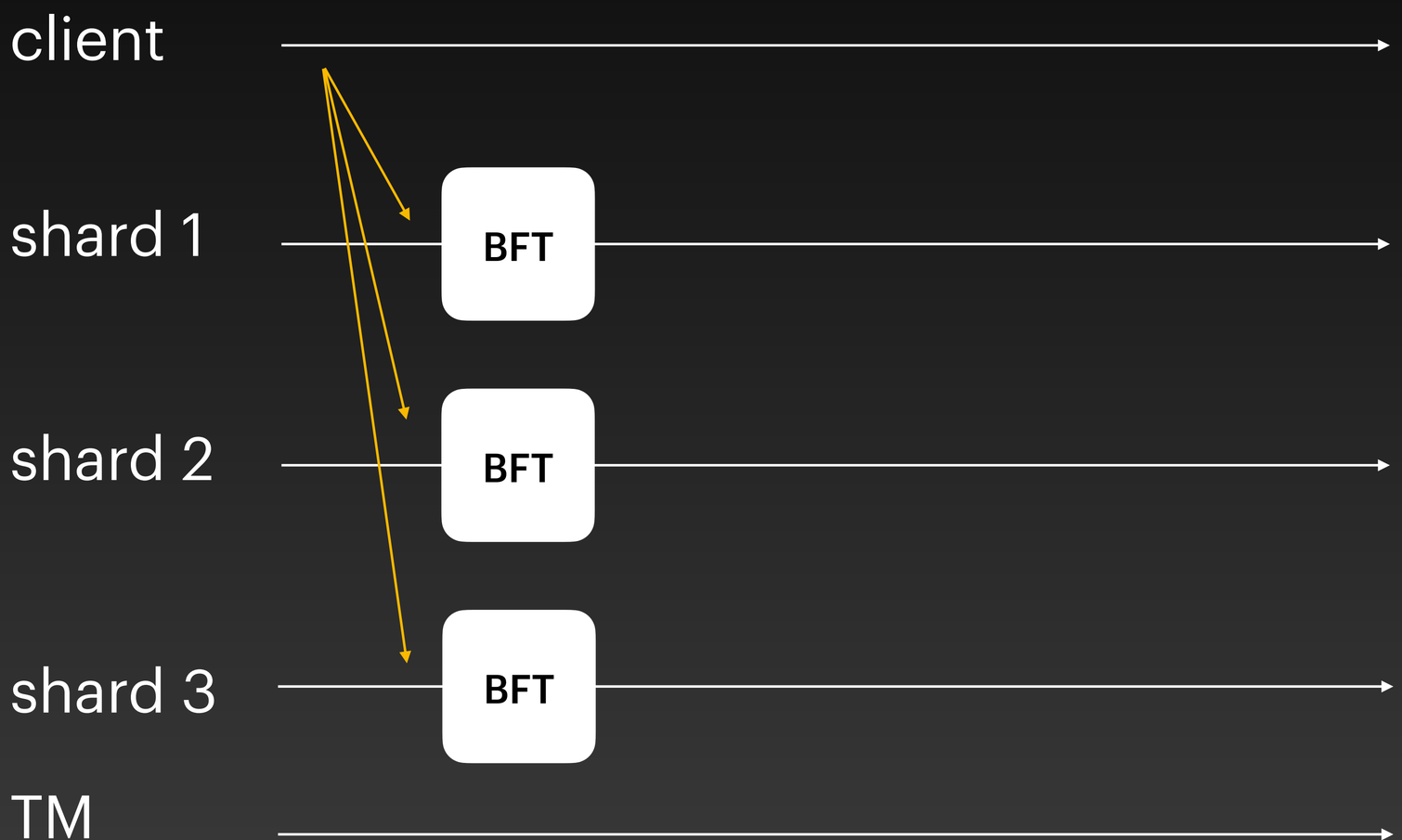
$D3, S_{D3}$



Shard 3

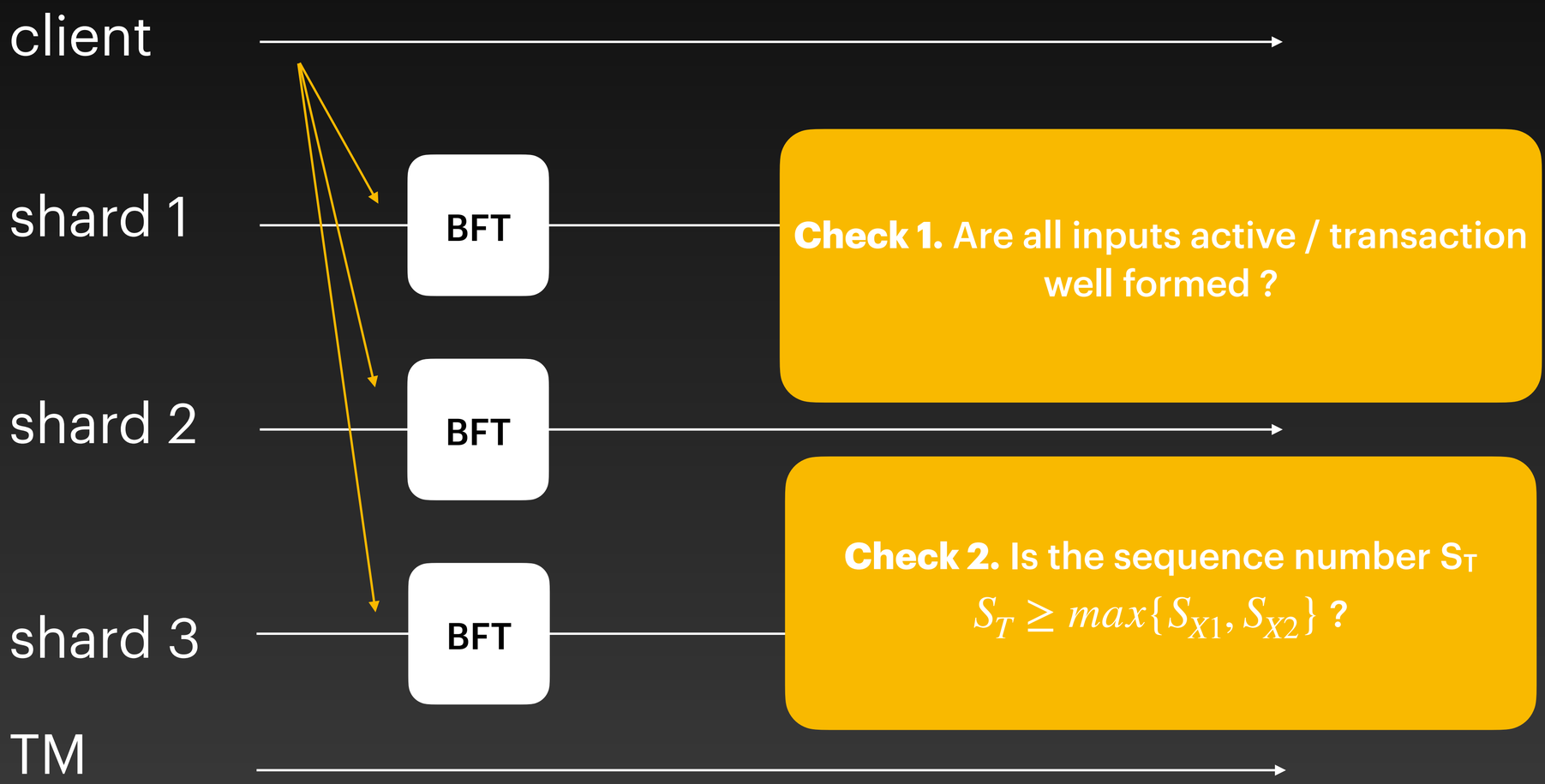
Byzcuit

$$\{S_T, T(x_1, x_2, d_3) \rightarrow (y_1, y_2, y_3)\}$$



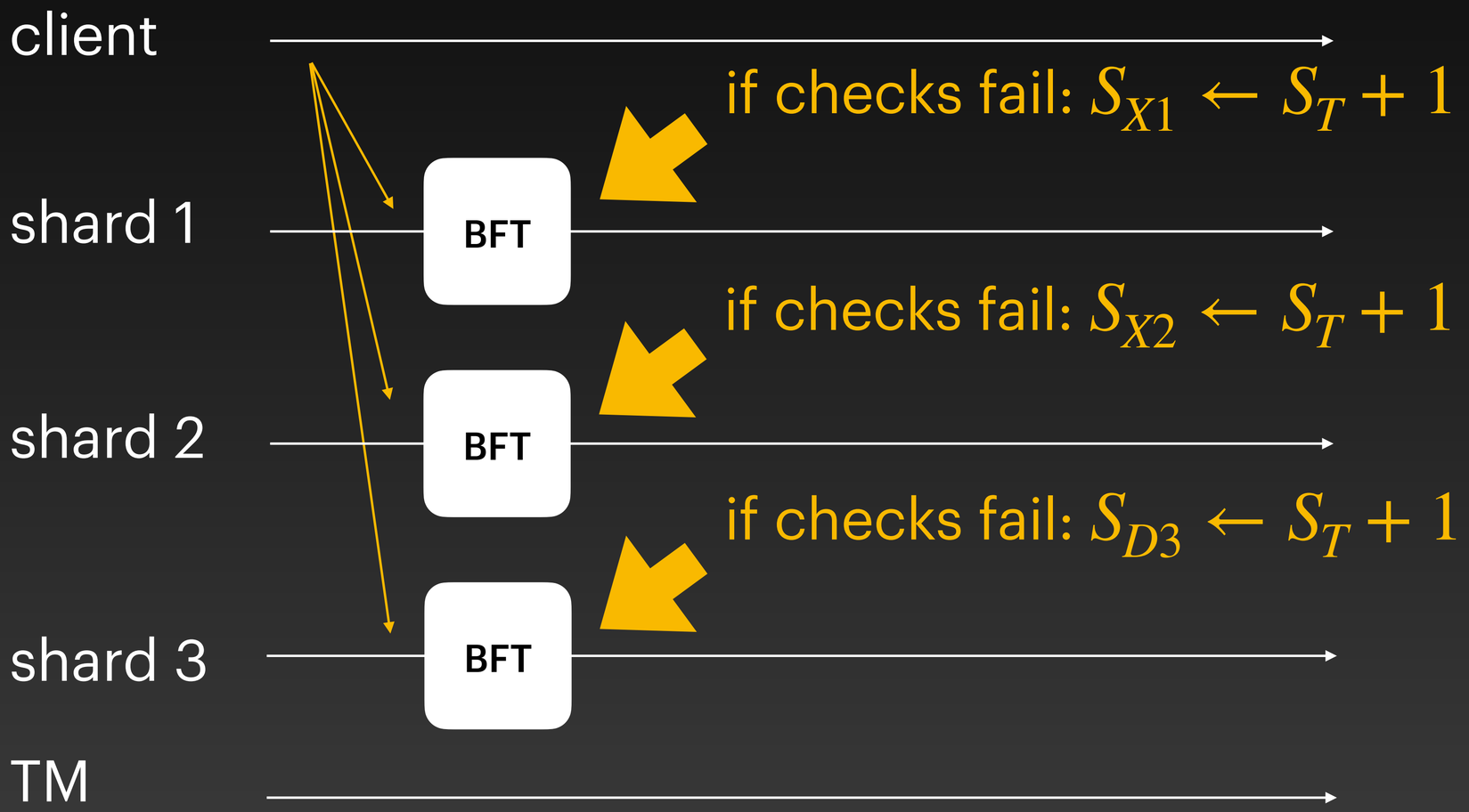
Byzcuit

$$\{S_T, T(x_1, x_2, d_3) \rightarrow (y_1, y_2, y_3)\}$$



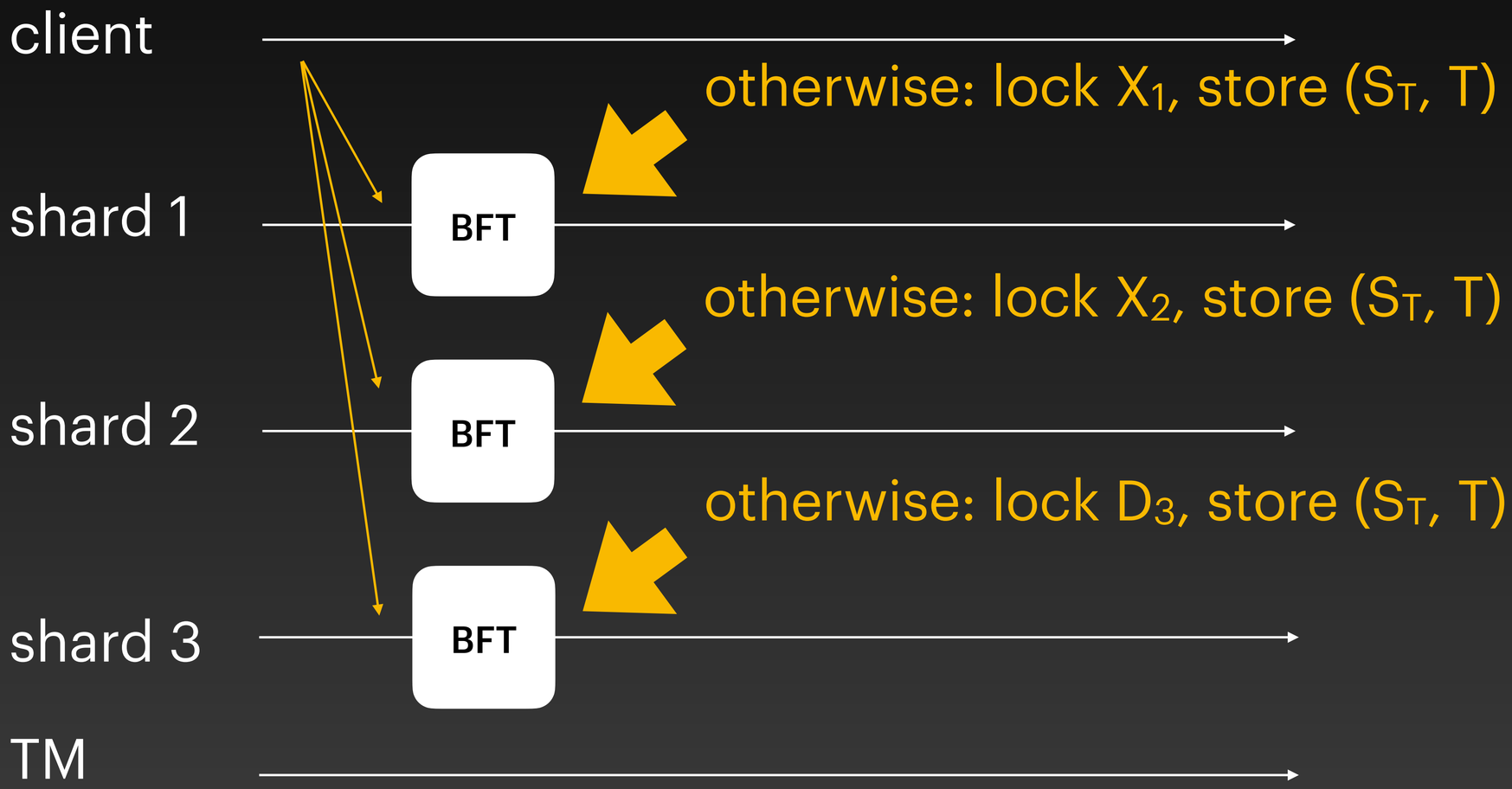
Byzcuit

$$\{S_T, T(x_1, x_2, d_3) \rightarrow (y_1, y_2, y_3)\}$$



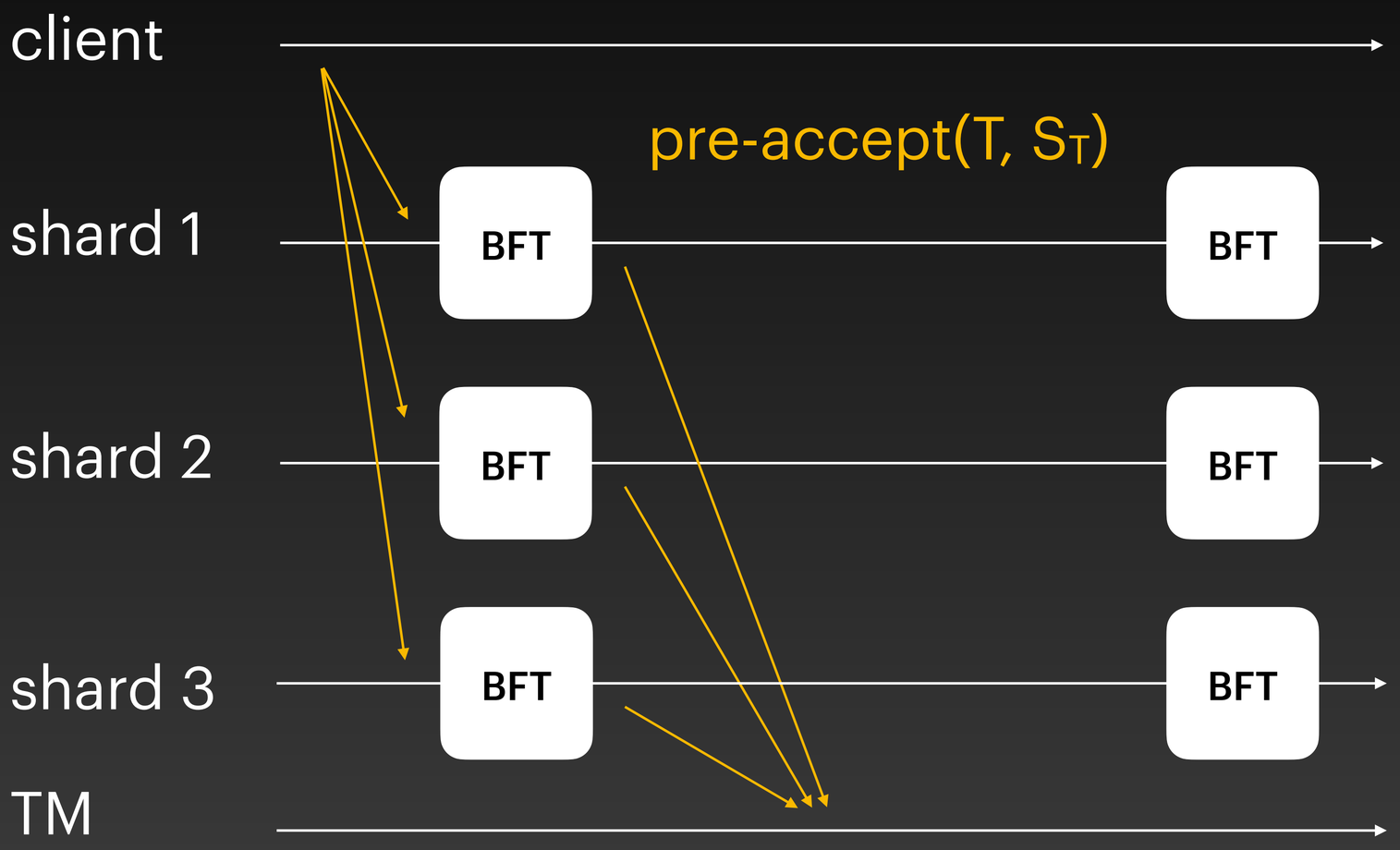
Byzcuit

$$\{S_T, T(x_1, x_2, d_3) \rightarrow (y_1, y_2, y_3)\}$$



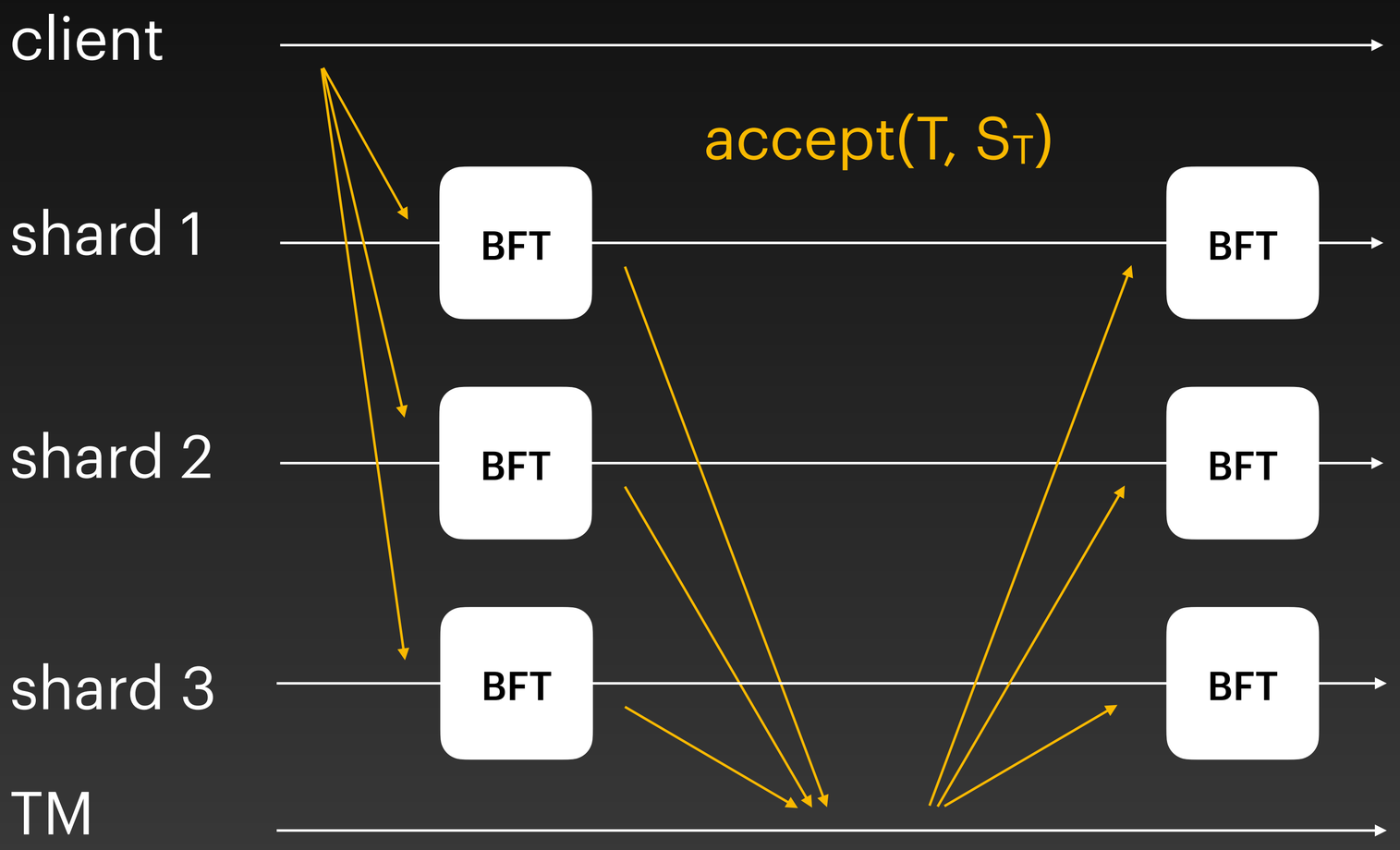
Byzcuit

$$\{S_T, T(x_1, x_2, d_3) \rightarrow (y_1, y_2, y_3)\}$$



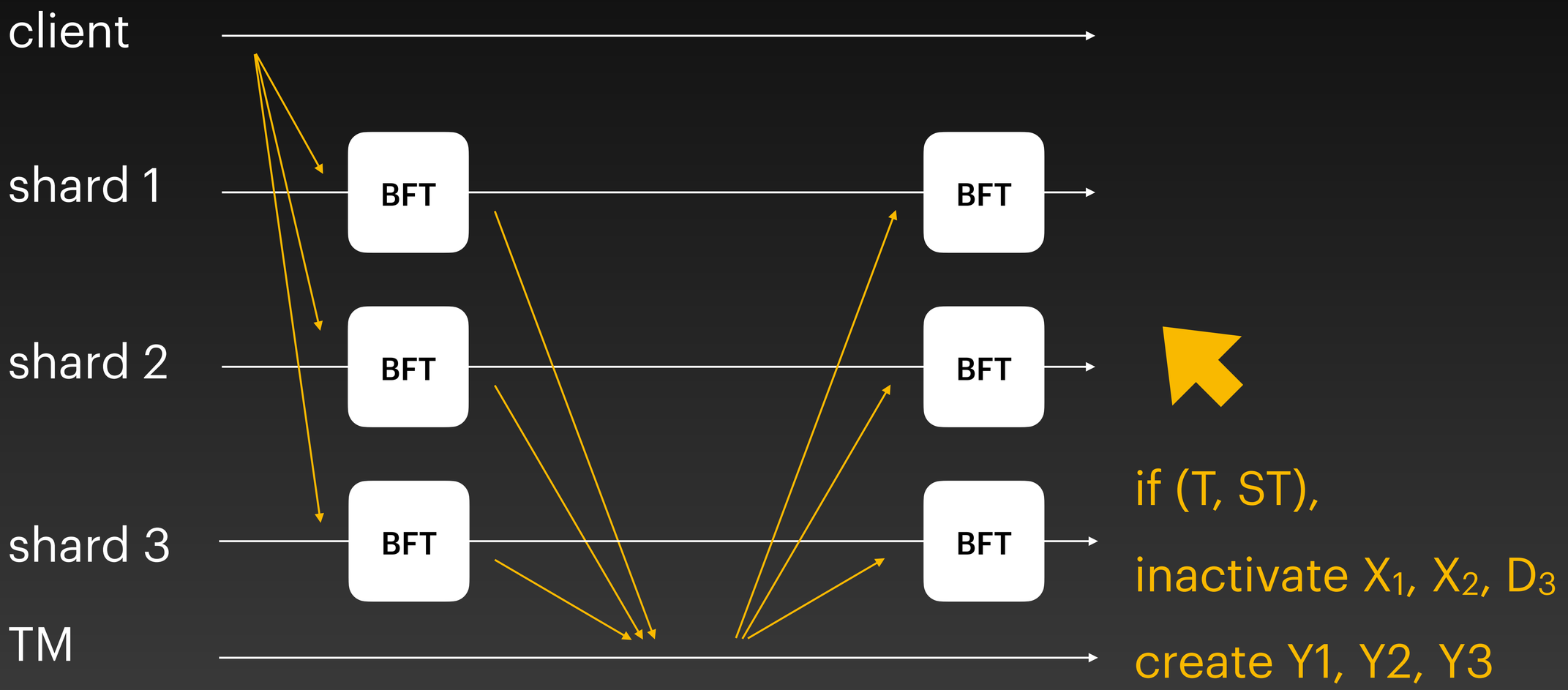
Byzcuit

$$\{S_T, T(x_1, x_2, d_3) \rightarrow (y_1, y_2, y_3)\}$$



Byzcuit

$$\{S_T, T(x_1, x_2, d_3) \rightarrow (y_1, y_2, y_3)\}$$



Why is Byzcuit secure?

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

Sequence numbers:

act as session ID

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

Dummy objects:

all shards experience the first phase of the protocol