University of Basel

Center for Innovative Finance

Bitcoin, Blockchain and Cryptoassets

Signature Hash Types

Prof. Dr. Fabian Schär
University of Basel

Release Ver.: (Local Release)
Version Hash: (None)
Version Date: (None)

Signature

Network participants exchange signed transaction messages.

In most cases, they sign all in- and outputs. However, in some cases, there may be a need for a more flexible approach. As such, there is the option to only sign certain in- and outputs.

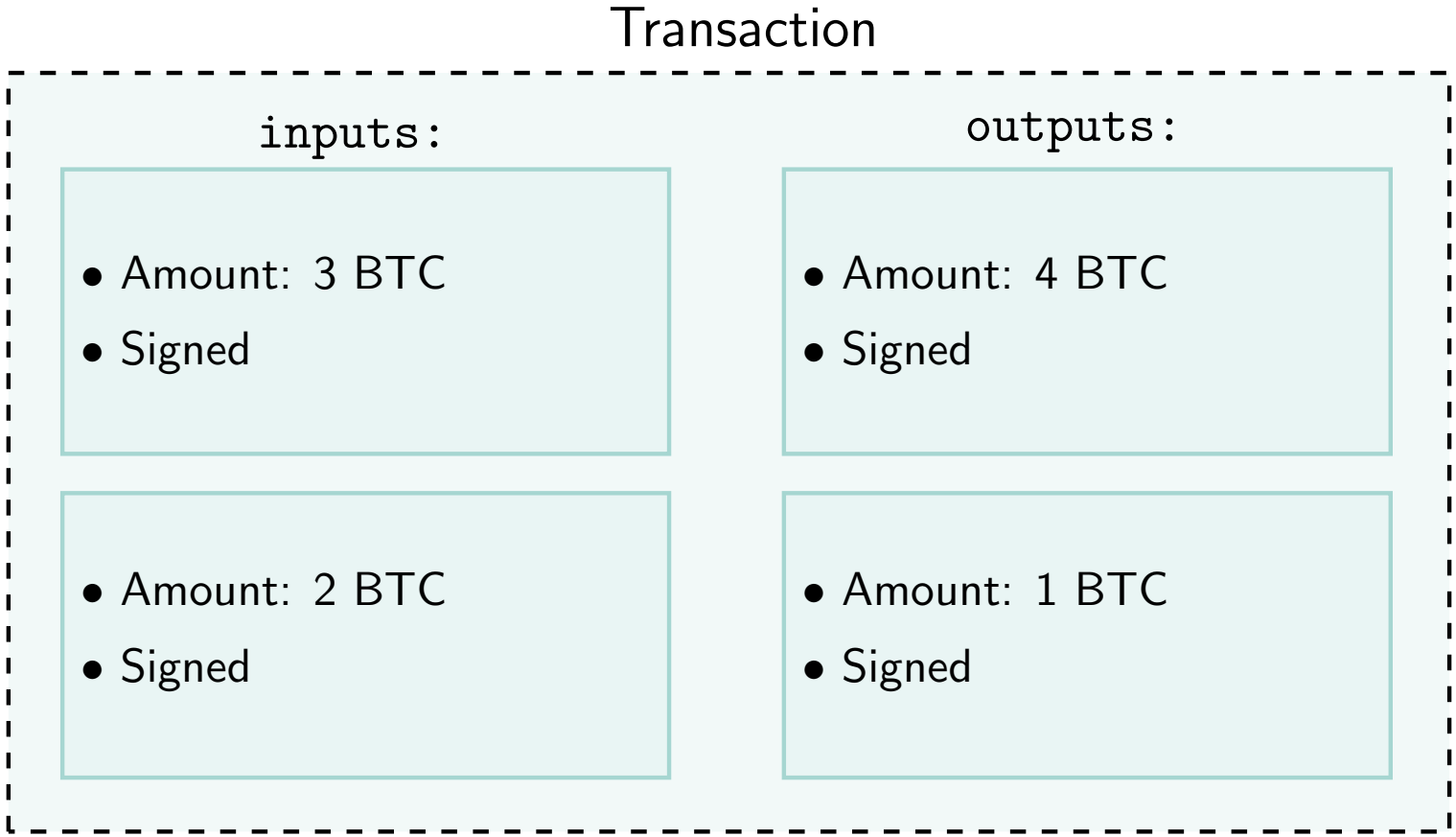
$\rightarrow$ `SIGHASH` types enable this.

SIGHASH Types Overview

There are three base `SIGHASH` types plus the `ANYONECANPAY` modifier:

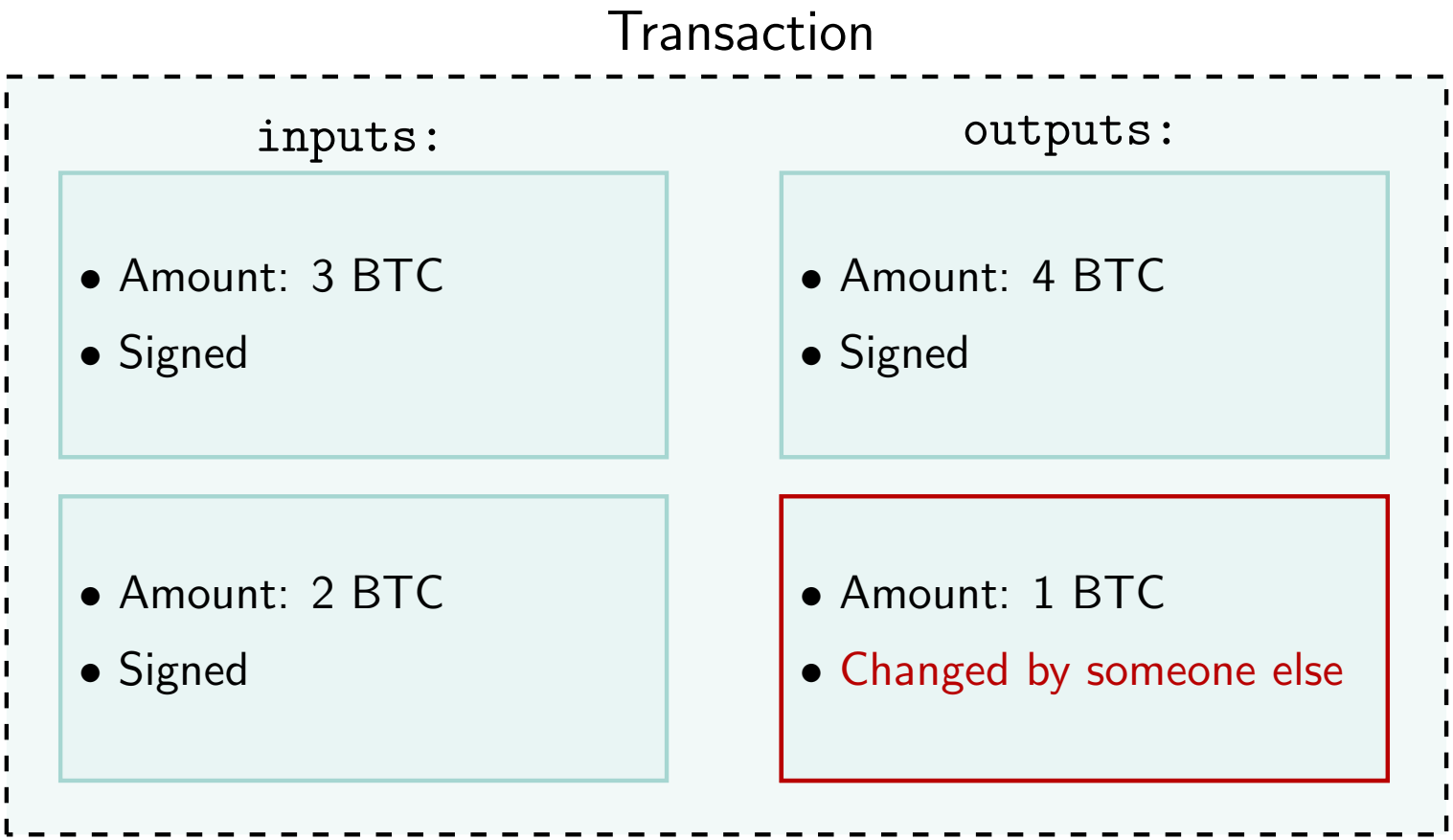
	All inputs	Only your input
All outputs	`SIGHASH_ALL`	`SIGHASH_ALL|SIGHASH_ANYONECANPAY`
Single output	`SIGHASH_SINGLE`	`SIGHASH_SINGLE|SIGHASH_ANYONECANPAY`
No outputs	`SIGHASH_NONE`	`SIGHASH_NONE|SIGHASH_ANYONECANPAY`

SIGHASH_ALL



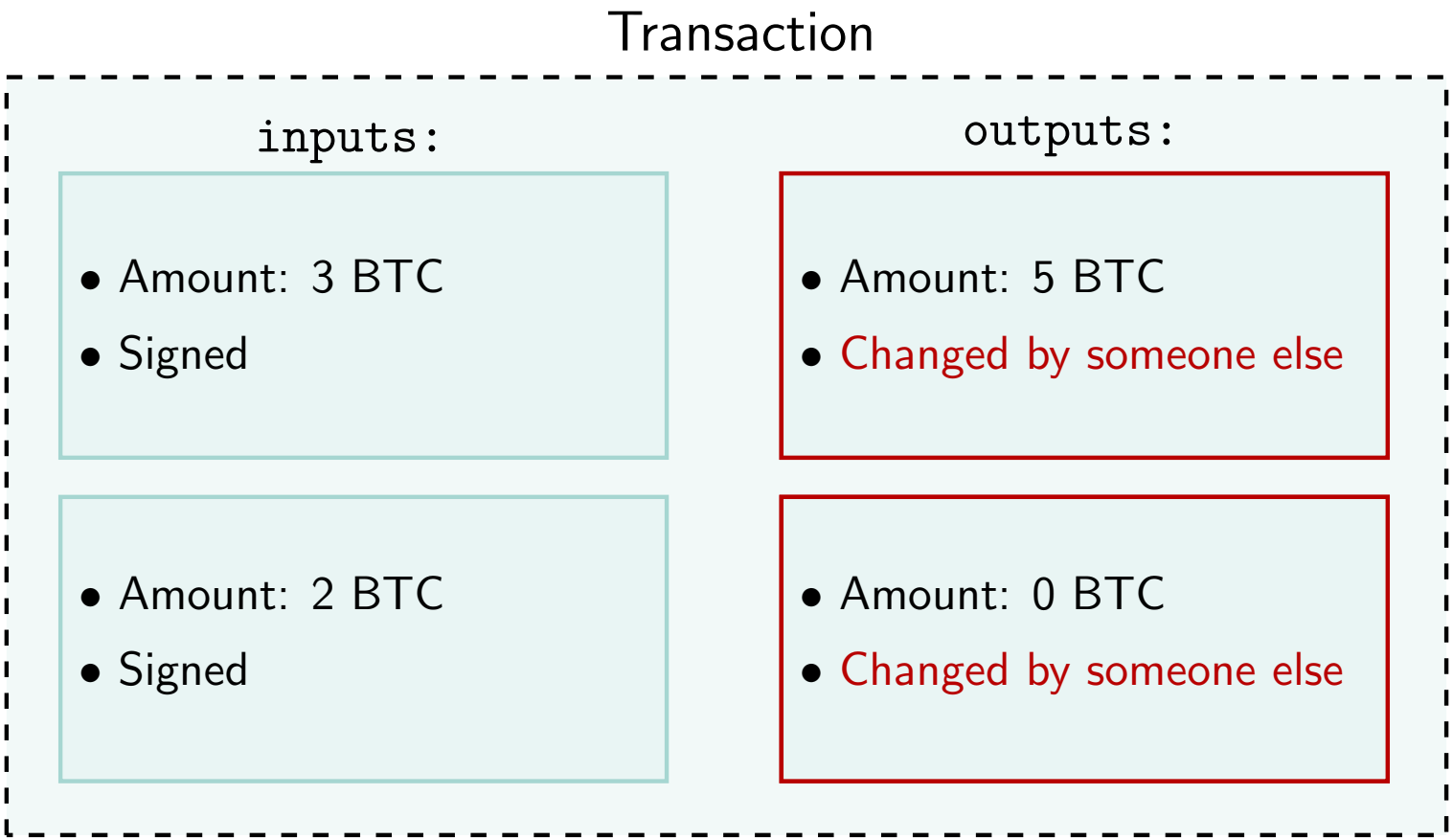
- Default value
- Signs all inputs and outputs.
- Modified inputs or outputs invalidate the signature.

SIGHASH_SINGLE



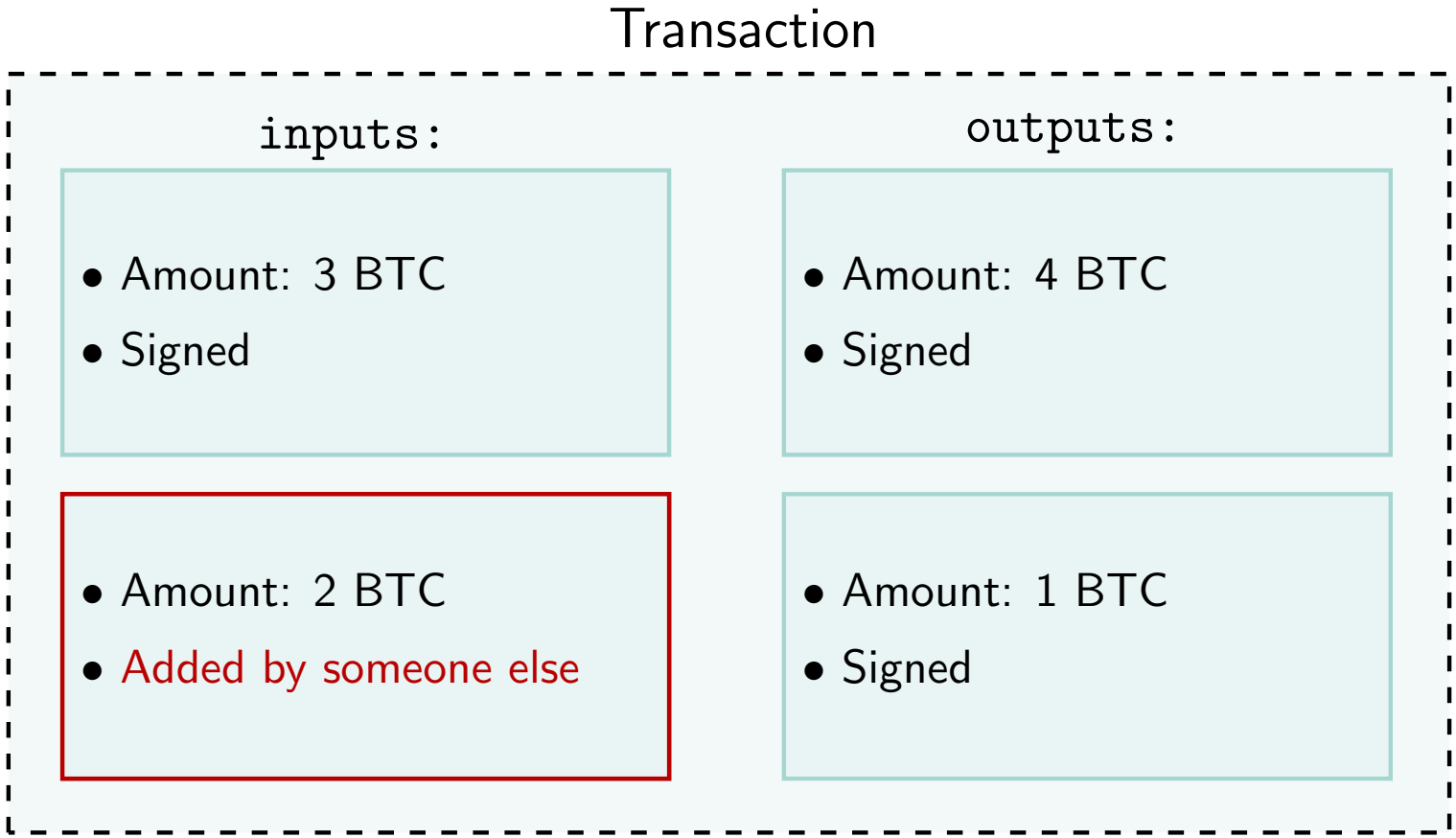
- Signs all inputs and *one* output only.
- Modified inputs or the modification of the signed output invalidate the signature.
- Other people can change any of the unsigned outputs.

SIGHASH_NONE



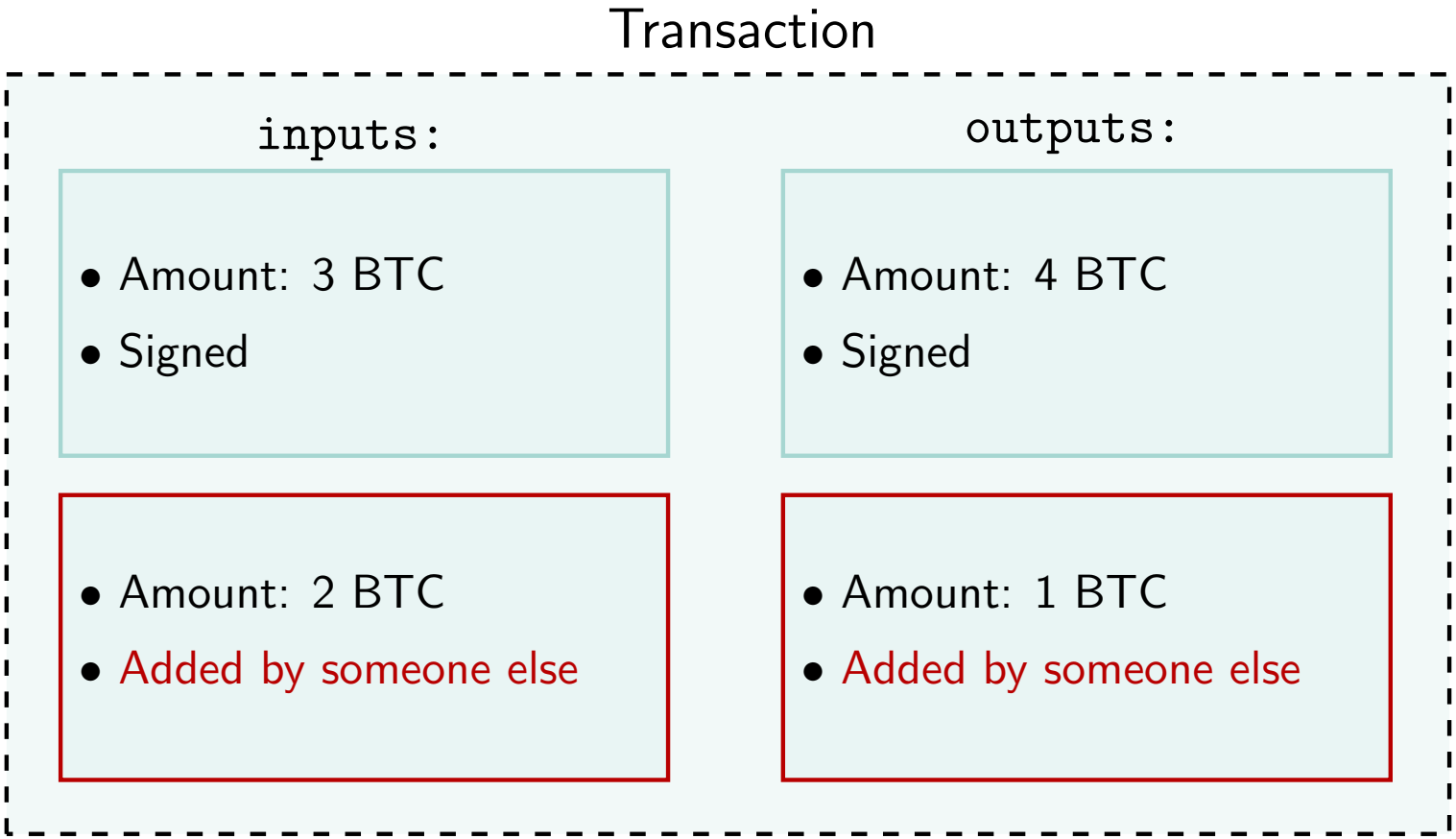
- Signs all inputs but *none* of the outputs.
- Anyone can freely modify the unlocking conditions.

SIGHASH_ALL|SIGHASH_ANYONECANPAY



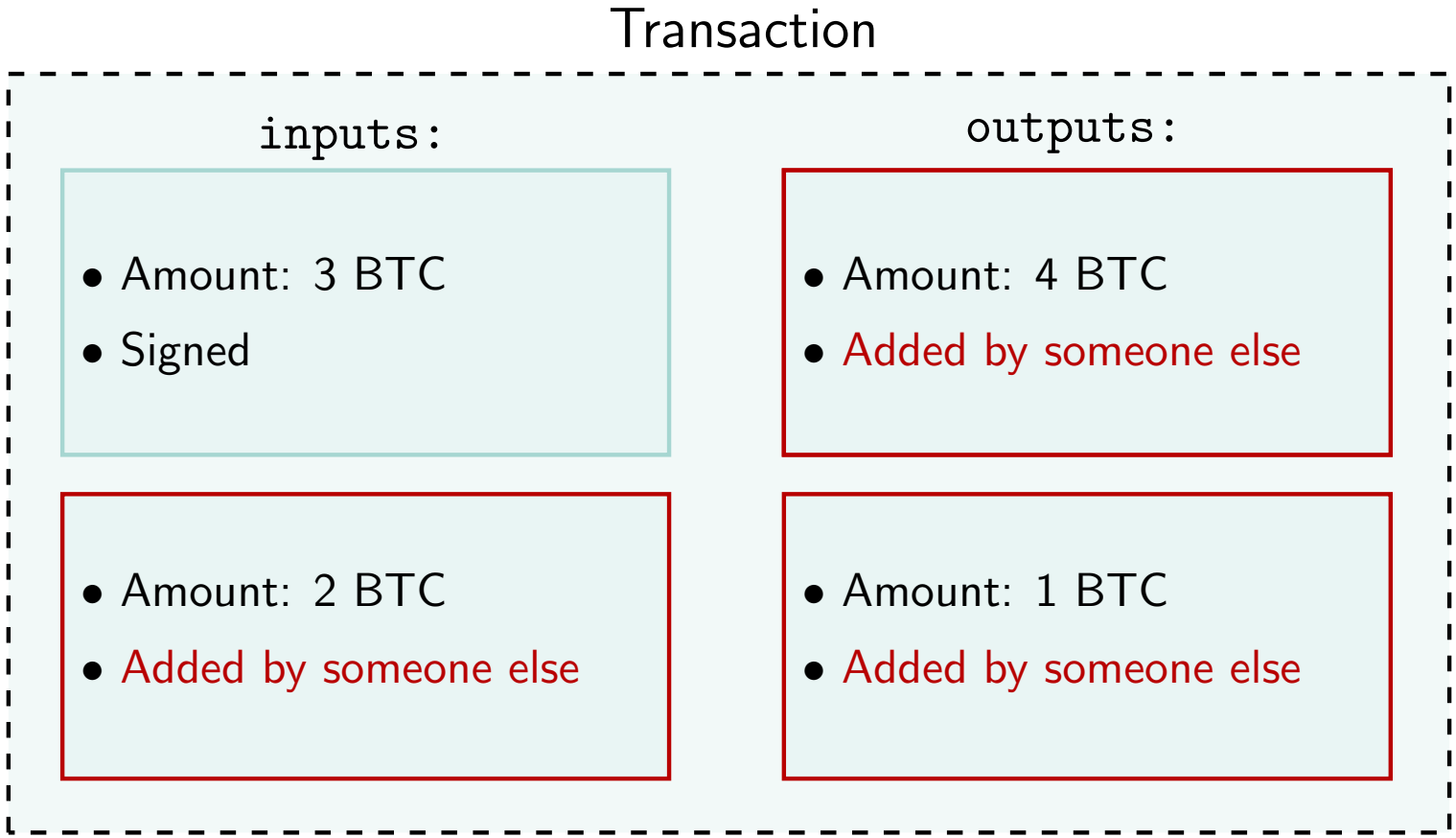
- Signs only the signer's inputs and all outputs.
- Anyone can add or remove other inputs.
- E.g. crowdfunding campaign

SIGHASH_SINGLE|SIGHASH_ANYONECANPAY



- Signs only the signer's input and *one* output.
- Other people are free to add or remove additional inputs and outputs.
- Any change to the signer's part of the transaction will invalidate the signature.

SIGHASH_NONE|SIGHASH_ANYONECANPAY



- Signs only the signer's inputs and no outputs.
- Anyone can add or remove other inputs and outputs.
- Anyone can use the signed input in any way.