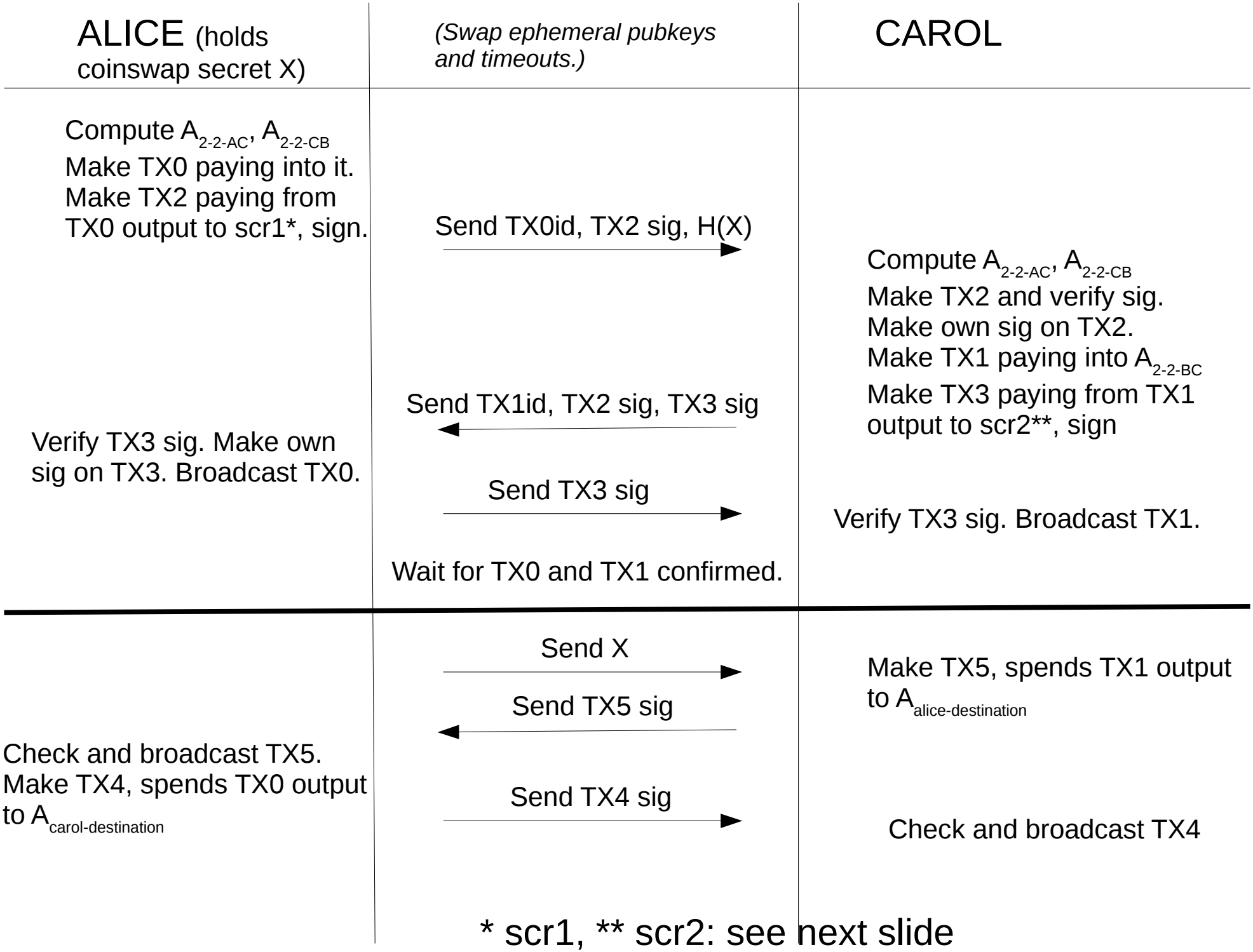


* scr1, ** scr2: see next slide

TODO: probably replace CLTV with CSV

Scr1: scriptPubKey for hash locked/time locked output that will be paid to Alice/Bob in cooperative case. It is a standard P2SH pubkey for the following redeem script:

```
OP_IF OP_HASH160 H(X) OP_EQUALVERIFY <carol_pubkey>  OP_CHECKSIG
OP_ELSE <locktime-0> OP_CLTV OP_DROP <alice_pubkey> OP_CHECKSIG
OP_ENDIF
```

In English: *pay to Carol if she has the preimage of the hash at any time, or pay to Alice/Bob anytime after locktime-0.*

The scriptSig for redeeming this output by Carol would be:

```
signature_carol X OP_TRUE <redeem script>
```

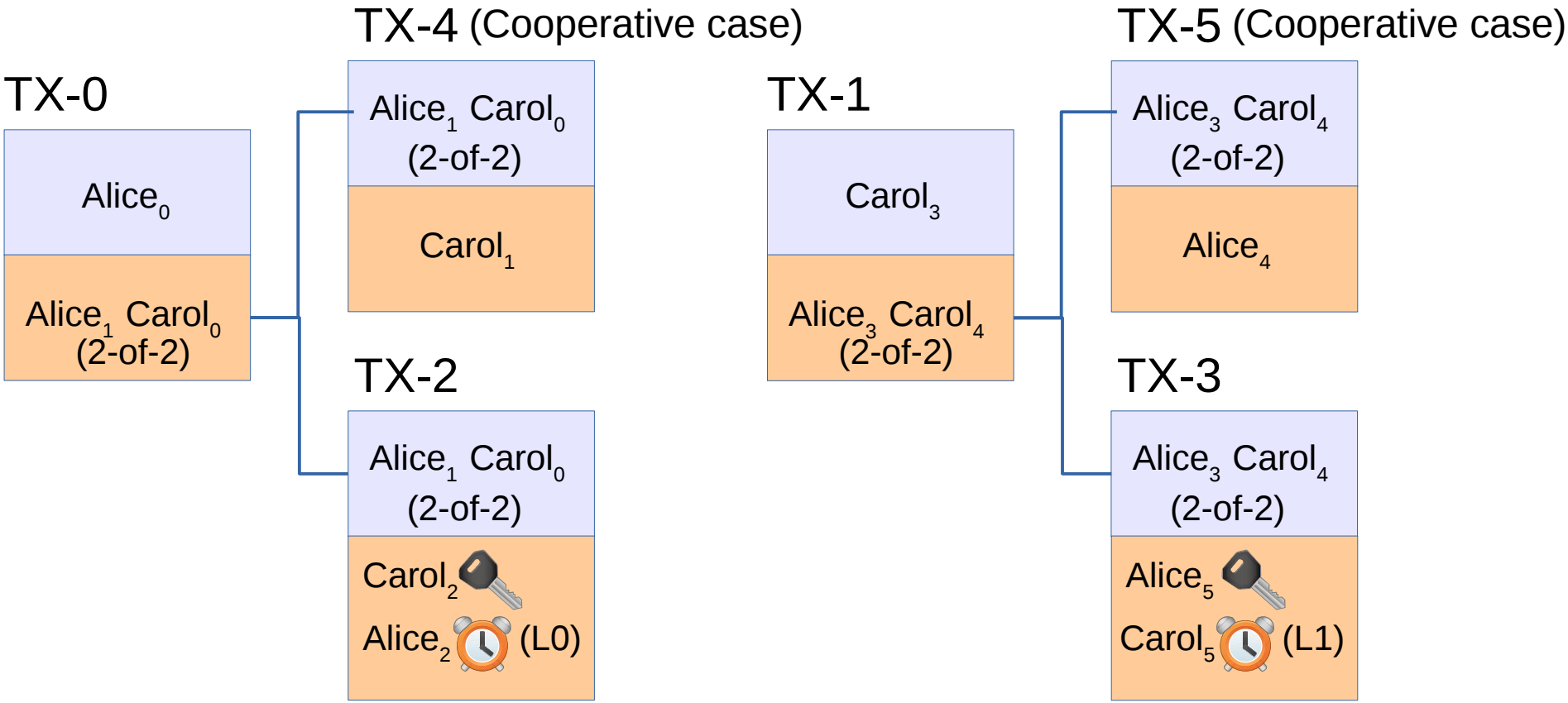
The scriptSig for redeeming this output by Alice would be:

```
signature_alice OP_FALSE <redeem script>
```

Scr2: scriptPubKey for hash locked/time locked output that will be Paid to Carol in cooperative case. Simply the mirror image case:

```
OP_IF OP_HASH160 H(X) OP_EQUALVERIFY <alice_pubkey>  OP_CHECKSIG
OP_ELSE <locktime-1> OP_CLTV OP_DROP <carol_pubkey> OP_CHECKSIG
OP_ENDIF
```

`locktime-0` must be **after** `locktime-1`.



=transaction input

=transaction output

Subscripts refer to different ephemeral pubkeys. TX2 and TX3 outputs can be spent if counterparty fails to follow protocol, either by revealing the hash preimage (which atomically releases the other), or by spending after timeout. L1 < L0, so Alice cannot back out before Carol (this is to account for the fact that Alice holds the secret initially).