

ALICE (holds coinswap secret X)	(Swap ephemeral pubkeys, $H(X)$ and timeouts.)	CAROL
<p>Compute 2-2-A1C0*, 2-2-A3C4**</p> <p>Make TX0 paying into 2-2-A1C0. Make TX2 paying from TX0 output to scr1*, sign.</p>	<p>Send TX0id, TX2 sig, <math>H(X)</math></p>	<p>Compute 2-2-A1C0, 2-2-A3C4 Make TX2 and verify sig. Make own sig on TX2. Make TX1 paying into 2-2-A3C4 Make TX3 paying from TX1 output to scr2**, sign</p>
<p>Verify TX3 sig. Make own sig on TX3. Broadcast TX0.</p>	<p>Send TX1id, TX2 sig, TX3 sig</p> <p>Send TX3 sig</p> <p>Wait for TX0 and TX1 confirmed.</p>	<p>Verify TX3 sig. Broadcast TX1.</p>
<p>Check and broadcast TX5. Make TX4, spends TX0 output to A<sub>carol-destination</sub></p>	<p>Send X</p> <p>Send TX5 sig</p> <p>Send TX4 sig</p>	<p>Make TX5, spends TX1 output to A<sub>alice-destination</sub></p> <p>Check and broadcast TX4</p>

\* TX0 destination address (see third slide)

\*\* TX1 destination address (see third slide)

\*\*\* scr1, \*\*\*\* scr2: custom scriptpubkeys (see second slide)

**Scr1:** scriptPubKey for hash locked/time locked output that will be NOT be paid to Alice/Bob in cooperative case. It is a standard P2SH pubkey for the following redeem script:

```
OP_DEPTH 2 OP_EQUAL OP_IF
    OP_HASH160 <digest> OP_EQUALVERIFY <carol_pubkey> OP_CHECKSIG
    OP_ELSE
        <L0> OP_CHECKLOCKTIMEVERIFY OP_DROP <alice_pubkey> OP_CHECKSIG
    OP_ENDIF
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:

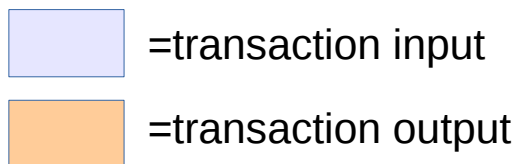
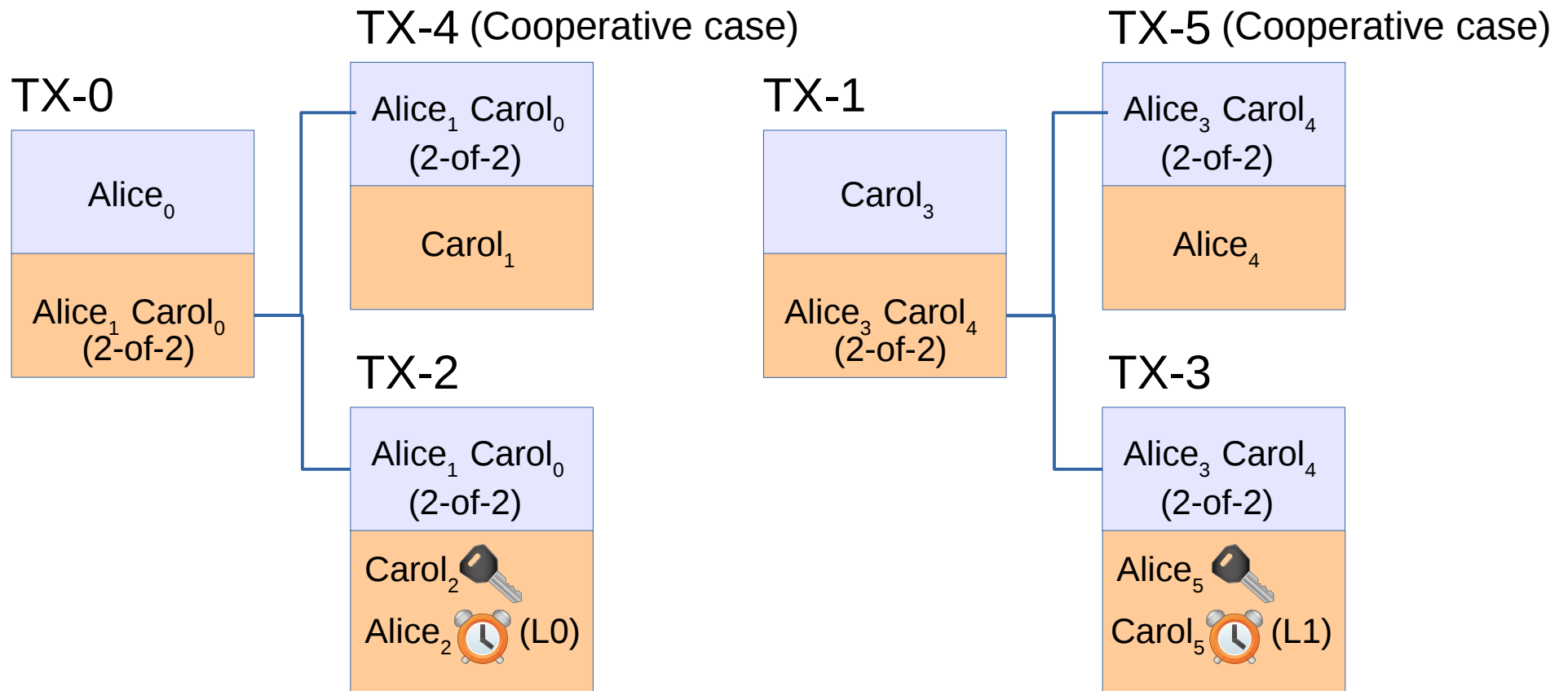
```
signature_alice OP_FALSE <redeem script>
```

---

**Scr2:** scriptPubKey for hash locked/time locked output that will NOT be paid to Carol in cooperative case. Simply the mirror image case:

```
OP_DEPTH 2 OP_EQUAL OP_IF
    OP_HASH160 <digest> OP_EQUALVERIFY <alice_pubkey> OP_CHECKSIG
    OP_ELSE
        <L1> OP_CHECKLOCKTIMEVERIFY OP_DROP <carol_pubkey> OP_CHECKSIG
    OP_ENDIF
OP_ENDIF
```

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



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).