1 State of a channel

Consider a channel between *Alice* and *Bob*. Both parties hold some data locally that correspond to ownership of some funds in the channel. Here we define a concise way of representing this data.

What *Alice* has to hold, specific for this channel:

- keys:
  - local funding secret key
  - remote funding public key
  - local {payment, htlc, delayed_payment, revocation}_basepoint_secret
  - remote {payment, htlc, delayed_payment, revocation}_basepoint
  - seed (for local per_commitment_secrets)
  - remote per_commitment_secret$_{1,\dots,m-1}$
  - remote per_commitment_point$_{m,m+1}$
- *Alice*'s coins
- *Bob*'s coins
- every HTLC that is included in the latest irrevocably committed (local or remote) commitment:
  - direction (*Alice* → *Bob* or *Bob* → *Alice*)
  - hash
  - preimage (or $\perp$ if still unresolved)
  - coins
  - Is it included in local commitment$_n$?
  - HTLC number
- signatures:
  - signature of local commitment$_n$ with secret key corresponding to remote funding public key
  - for every HTLC included in local commitment$_n$, one signature of HTLC-Timeout if outgoing, HTLC-Success if incoming with secret key corresponding to remote htlc_pubkey$_n$ (= htlc_basepoint + $\mathcal{H}$(remote per_commitment_point$_n$ ||remote htlc_basepoint) $\cdot G$)

The rest of the things used in the protocol can be derived by the above.

Representation of a channel's state (from the point of view of *Alice*):

- *Alice*'s coins c_{Alice}
- *Bob*'s coins c_{Bob}
- list of (coins, state $\in$ {proposed, committed}) preimage, whether we have a signature), `HTLCs`

- negative coins are outgoing, positive are incoming
- HTLCs can either be simply proposed (not in an irrevocably committed remote transaction) or committed (the opposite). After the preimage is supplied (no matter the direction), the HTLC is considered settled and is discarded.

I.e. $\text{State}_{Alice,pchid} = (c_{Alice}, c_{Bob}, ((c_1, \text{state}_1), \dots, (c_k, \text{state}_k)))$

E.g. $\text{State}_{Alice,pchid} = (4, 5, ((0.1, \text{proposed}), (-0.2, \text{signed})))$

We do not include in the state elements whose contents are irrelevant (e.g. sigs, keys, hashes).