Conditional off-chain Ether and Token payments for offline participants without on-chain checkpointing.

FTLC is an alteration of the Hashed-Timelocked-Contracts (HTLC) deployed to the Lightning and Raiden network. FTLCs potentially enhance the user experience of “layer2” scalable cryptocurrency payments by allowing an online party to initiate and complete a payment to an offline party. In HTLC networks like Lightning, both the sender and recipient of a payment must be online to coordinate the off-chain payment. This is due to the way that the receiver of a HTLC payment must share the pre-image between intermediaries. FTLCs are inspired by Plasma-Debit where an operator is allowed to checkpoint the state of their “channels or merkle leaves” on the parent chain, however this construct attempts to achieve this with no need to checkpoint plasma blocks or data to the main chain.

FTLCs are called “forward-time locked” rather than “hashed-time locked” as with Lightning or Raiden. This implies that the payment initiator contract does not rely on a pre-image of a hash to move funds from initiator to hub, rather it relies on some proof that the hub updated their channel to reflect the payment before the initiators FTLC timeout.

Ledger Channel:

Assume a simple payment network with one intimidiary (Ingrid) containing { Alice (sender), Ingrid, Bob (receiver) }.

Between {Alice/Ingrid} and {Bob/Ingrid} we deploy a ledger channel that tracks normal bidirectional payment state updates and special single signed additive payment updates. The rules for re-entering this channel’s state to the main chain will vary from normal channels. There will be one type of transaction that will be allowed to build on the normal double signed ledger channels that increase the receivers balance. Since the consensus mechanism of normal channels is now broken for these types of state updates, the main chain contract must also verify that the deposit bond or receiving capacity is valid. This is similar to “Force-Move-Games” from Magmo. The contract may also attempt to punish incorrectly signed updates. Alice needs verify that the forwarded payment is valid off-chain and if it is not she must challenge to undo her payment to Ingrid.

Forward Proof:

The proof of forwarding that Ingrid creates comes in the form of the single signed state update on the receiving channel. In order to prevent double spending on Ingrid’s behalf, we require that an identifier be supplied by Alice and attach this to the state update from Ingrid. Ingrid_Sig({ID, Bob_Balance}). If an identifier is not supplied then Ingrid may use old payments as proof in challenges initiated by Alice to Bob. If an identifier is supplied then Alice’s challenge will need to be supplied the specific update for that FTLC that proves transfer and that the transaction was constructed properly (Ingrid had enough collateral).

Basic Protocol:

1 Alice signs channel update to Ingrid with a conditional FTLC. This state transition moves the conditional funds to Ingrid’s balance with a timestamp and TX_ID.

1(a) Igrid approves the conditions (checks that Bob has enough receiving capacity and that she is able to sign an update to complete the FTLC. Move on to step 2.

1(b) Ingrid rejects the FTLC and nothing happens. Either party may exit per normal state channels rules.

2 Alice waits as Ingrid is now responsible for completing the payment to Bob.

2(a) Ingrid generates a single signed state update with Bob with the same amount moving from Ingrid’s balance to Bob’s balance as was moved from Alice to Ingrid with the FTLC ID and incremented channel sequence. Moves to step 3.

2(b) Ingrid does not sign a state update to Bob within FTLC timeout, Alice must then go to chain and settle the latest state of their channel that reflects the active FTLC, then she may exit with state that nullifies the transaction after a second timeout to prove that nobody has evidence that Ingrid produced a valid forward proof for the FTLC.

3 Alice and Ingrid may settle the FTLC offchain.

3(a) Once Alice witnesses this state update, she may sign an update with Ingrid that nullifies the FTLC and leaves the balance transfer permanently on the channel.

3(b) Alice does not sign a channel update, then Ingrid may bring the state channel on-chain and prove the latest double signed state reflecting the FTLC, after which she may then prove her payment was forwarded by supplying to the contract the proof that Bob’s balance has irrevocably incremented in a single signed state channel. This needs to be done before the timeout or Ingrid will lose the transaction.