# #

HTLC

#

Concepts

Hash Time Locked Contract (HTLC)open in new windowis a protocol intended for cross-chain atomic swaps. It performs a P2P swap in a decentralized form. HTLC can guarantee that all swap processes among participating parties take place or nothing is done. Leveraging the HTLC on IRIS Hub, users can implement cross-chain asset swaps with Bitcoin, Ethereum, LTC and all other chains which support HTLC.

#

Interaction Process

Supposed that Alice swaps BTC for IRIS with Bob. The atomic swap process between Alice and Bob can be divided into following steps.

#

step 0

Alice and Bob reach an agreement on the swap by an off-chain procedure, which is completed commonly on an exchange platform. Let Alice be a maker and Bob be a taker. The agreement includes the exchange rate between BTC and IRIS, the each other's address on the counterparty chain and a unique hash lock generated from a secret, and an appropriate time span.

#

step 1

Afterwards, the secret holder, Bob sends an HTLC transaction which commits to transfer IRIS of the specified amount to Alice(the maker) with the negotiated hash lock on IRIS Hub.

#

step 2

An event is emitted on IRIS Hub which indicates that Bob has created an HTLC. Alice is informed of this event by monitor tools (usually wallets) or the platform. The HTLC initiating transaction with the same hash lock will be sent to Bitcoin by Alice once the event is validated against the agreement. Particularly the HTLC will be locked by an quite smaller time span than the one provided by Bob.

#

step 3

Bob is informed of and confirms the event on Bitcoin. Then Bob claims the HTLC-locked BTC with the owned secret before the time span set by Alice on Bitcoin.

#

step 4

The secret will be disclosed while the HTLC is claimed successfully by Bob on Bitcoin. Alice will perfom the same claim to the locked IRIS with the secret before the expiration time on IRIS Hub.

#

IRIShub HTLC Specification

#

Create HTLC message

Field Type Description receiver Address recipient address receiverOnOtherChain string the claim receiving address on the other chain (less than 128 characters) amount Coins tokens to be swapped out hashLock string sha256 hashed value in hexadecimal form, used to generated by a random secret and timestamp (if provided) timestamp uint64 timestamp in seconds used to generate the hash lock together with secret, if provided timeLock uint64 time span after which the HTLC expired ranged between 50 and 25480 (greater than 5 minitues, less than 48 hours) transfer bool whether it is an HTLT transaction

#

Claim HTLC message

Filed Type Description hashLock string the hash lock identifying the HTLC to be claimed secret string a random number which generates the hash lock together with timestamp (if provided), being of 32 bytes in hexadecimal form

#

Actions

- Create HTLC
- Claim HTLC
- Query HTLC