

ADDITIONAL INFORMATION

How does Hashed Time-Locked Contracts (HTLC) for cross-border payments work?

Cross-border payments generally involve a set of actions (updating the records of ownership of assets being transferred at separate settlement systems in multiple financial institutions) that are not tightly synchronised, creating the possibility that one action will succeed and another fail. This could leave the payment inconsistent, creating a risk that one party will gain at another's expense.

This specific risk may be eliminated by ensuring that all actions succeed or the payment, in its entirety, is cancelled. One way to accomplish this is to employ a trusted third party acting as escrow to the transacting parties; this third party will ensure commitment of the whole transaction or nothing.

Another way is to provide a technology-based means of ensuring this commitment without a trusted third party.

The Jasper-Ubin project uses Hashed Time-Locked Contracts (HTLC) to realise this all-or-nothing guarantee through an atomic transaction for a Canadian Dollar (CAD) – Singapore Dollar (SGD) payment across two distributed ledger technology (DLT) platforms.

HTLC synchronise all the actions making up a payment, so that either they all happen, or none happen. This is achieved through the use of smart contracts¹ on the two DLT platforms to lock or encumber the assets to be transferred, complete transactions on both platforms when a common secret is used, or release the locked or encumbered asset on both platforms back to their original owners if the common secret is not used within the pre-agreed time period, i.e. upon timeout.

In a Payment versus Payment (PvP) scenario, the actions refer to the transfer of CAD and the transfer of SGD on the two platforms. As prior actions are rolled back if any particular action fails, transacting parties would be left whole, even if there is a failure with the other transacting party or DLT platform.

¹ Smart contracts are self-executing computer programs that perform predefined tasks based on a predefined set of criteria or conditions. Smart contracts cannot be altered once deployed, which ensures the faithful completion of contractual terms.