```
BIP: 199
Layer: Applications
Title: Hashed Time-Locked Contract transactions
Author: Sean Bowe <sean@z.cash>
        Daira Hopwood <daira@z.cash>
Comments-Summary: No comments yet.
Comments-URI: https://github.com/bitcoin/bips/wiki/Comments:BIP-0199
Status: Draft
Type: Standards Track
Created: 2017-03-27
License: BSD-3-Clause
         CC0-1.0
```

Abstract

This BIP describes a script for generalized off-chain contract negotiation.

Summary

A Hashed Time-Locked Contract (HTLC) is a script that permits a designated party (the "seller") to spend funds by disclosing the preimage of a hash. It also permits a second party (the "buyer") to spend the funds after a timeout is reached, in a refund situation.

The script takes the following form:

```
   OP_IF
[HASHOP]  OP_EQUALVERIFY OP_DUP OP_HASH160
OP_ELSE
[TIMEOUTOP] OP_DROP OP_DUP OP_HASH160
OP_ENDIF
OP_EQUALVERIFY
OP_CHECKSIG
```

[HASHOP] is either OP_SHA256 or OP_HASH160.

[TIMEOUTOP] is either OP_CHECKSEQUENCEVERIFY or OP_CHECKLOCKTIMEVERIFY.

Interaction

- Victor (the "buyer") and Peggy (the "seller") exchange public keys and mutually agree upon a timeout threshold. Peggy provides a hash digest. Both parties can now construct the script and P2SH address for the HTLC.
- Victor sends funds to the P2SH address.
- Either:
  - Peggy spends the funds, and in doing so, reveals the preimage to Victor in the transaction; OR
  - Victor recovers the funds after the timeout threshold.

Victor is interested in a lower timeout to reduce the amount of time that his funds are encumbered in the event that Peggy does not reveal the preimage. Peggy is interested in a higher timeout to reduce the risk that she is unable to spend the funds before the threshold, or worse, that her transaction spending the funds does not enter the blockchain before Victor's but does reveal the preimage to Victor anyway.

Motivation

In many off-chain protocols, secret disclosure is used as part of a settlement mechanism. In some others, the secrets themselves are valuable. HTLC transactions are a safe and cheap method of exchanging secrets for money over the blockchain, due to the ability to recover funds from an uncooperative counterparty, and the opportunity that the possessor of a secret has to receive the funds before such a refund can occur.

Lightning network

In the lightning network, HTLC scripts are used to perform atomic swaps between payment channels.

Alice constructs K and hashes it to produce L. She sends an HTLC payment to Bob for the preimage of L. Bob sends an HTLC payment to Carol for the same preimage and amount. Only when Alice releases the preimage K does any exchange of value occur, and because the secret is divulged for each hop, all parties are compensated. If at any point some parties become uncooperative, the process can be aborted via the refund conditions.

Zero-knowledge contingent payments

Various practical zero-knowledge proving systems exist which can be used to guarantee that a hash preimage derives valuable information. As an example, a zero-knowledge proof can be used to prove that a hash preimage acts as a decryption key for an encrypted sudoku puzzle solution. (See pay-to-sudoku for a concrete example of such a protocol.)

HTLC transactions can be used to exchange such decryption keys for money without risk, and they do not require large or expensive-to-validate transactions.

Implementation

https://github.com/bitcoin/bitcoin/pull/7601

Copyright

This document is dual licensed as BSD 3-clause, and Creative Commons CC0 1.0 Universal.