BUIP088: Double spend proof creation and forwarding
Submitted on 29th March 2018 by torusJKL

Background

A double spend can happen within the time from the initial broadcast until the transaction is included in a block.
Although this is on average within 10 minutes at the point of sale we need to know that a unconfirmed transaction is as safe as possible within seconds.

Currently double spend proofs are not communicated thus a merchant might not know that there is a high chance of him not receiving his transaction.
In order to detect double spends a double spend proof needs to be created and forwarded by the nodes.

Motivation

By receiving double spend proofs sellers learn about attempts to defraud them faster and can take appropriate steps.
This will make 0-conf transaction on Bitcoin Cash more safe and will give it broader acceptance.

With merchant software going in the direction of receiving the tx directly from the customer at the POS there is no need to receive the whole double spend tx and a proof of double spend inputs is enough to flag a payment.

Goal

The goal of the implementation is that any node that has access to both transactions can create the proof.
And that any other node (even with none of those transactions in the mempool) can validate and forward it.

Task

1) Create specifications for the double spend proof implementation and submit a pull request to the BitcoinCash repo so that others can implement it in their software

2) Develop a double spend proof mechanics based on only sending the minimal part of the transaction (e.g. only the inputs) that is needed to detect a double spend with the following properties:
2a) the proofs are stand-alone evidence of the respend
2b) the proofs are verifiable so that they can't be faked by a 3rd party

3) Add a double spend visualization in the wallet GUI

Timeline

The double spend proof should be developed and to be implemented for BUCash with the aim of being ready for inclusion in the scheduled November 2018 protocol upgrade.

Caveats

The lead developer will have discretion and flexibility to modify details specified in this BUIP, while keeping within the spirit of the BUIP with the goal of advancing 0-conf tx security on Bitcoin Cash.

References

Comment by Tom Zander describing that only some hashes need to be communicated