BUIP082: opt-in malleability fix
Submitted on 25th December 2017 by torusJKL

Background
Malleability is not an issue when working only with confirmed tx.
But if an application wants to reference an unconfirmed tx based on its tx id it could fail if said id is changed (malleate).

Motivation
Allow applications to use unconfirmed tx based on a non-malleable id.
This could open up Bitcoin Cash to new technology we do not know of today.

Goal
The solution will make tx non-malleable by the 1st party.
It should be opt-in and mustn't require existing inputs to be moved first (e.g. with SegWit where the tx has to originate from a SegWit address).

Task
1) The Bitcoin Unlimited lead developer shall engage in the discussion with other consensus implementations and propose a solution.
The solution can be already proposed by others or be a new one.

2) Writing of a specification and a pull request to the BitcoinCash repo such that other develops can implement the solution in their software.

3) Development of the malleability fix for BUCash.

Timetable
The malleability fix 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 an opt-in malleability fix for Bitcoin Cash.

References
Malleability fix proposal
Malleability Fix SIGHASH_ANYOUTPUT
Start differenciating txid and txhash