BUIP149: Delimited OP_RETURNs

Submitted by: Jonathan Silverblood
Date: 2020/06/27

Status: DRAFT PROPOSAL

Summary

The purpose of this BUIP is to get a commitment from Bitcoin Unlimited to support a proposal to change how OP_RETURN functions within Bitcoin Cash.

Proposals

I propose that we raise the OP_RETURN size limitation and rework the OP_RETURN opcode, so that instead of being used only as the first opcode of an OP_RETURN output, it:

- Can be used more than once within an OP_RETURN output.
- Every time it is used it acts as a delimiter that makes the following push operations semantically grouped.
- Every time it is used, it limits how much data can be pushed after it.

This means that old OP_RETURN transactions will be parsed exactly the same as new ones (since the old only have one OP_RETURN opcode), which makes the old transactions forward-compatible. This also means that it becomes possible to use more than one OP_RETURN based protocol within a single transaction. By also having a limitation on how much data can be pushed, we can structurally prevent a situation where some protocol would make itself incompatible with any other by accident.

I propose that we raise the OP_RETURN size limitation to 512b or 1024b and that we make the max size between OP_RETURNS either 255b or 511b respectively, to guarantee that any two protocols will always work together.

The numbers are provided as an example for discussion and to set a ballpark of what the expectations are, but should not be seen as a requirement for this proposal.

Motivation

By commiting to support this change of OP_RETURN functionality, Bitcoin Unlimited would send a signal to other node software developers that this is something that is possible to change under consensus and would help start the necessary discussions in the community.

Background

With the expanse of OP_RETURN based protocols and the widespread adoption of SLP tokens there is a need to enable cross-protocol collaboration. We cannot predict all possible usecases for this feature, but there is already several protocols that either see a benefit to this (CashIntents with SLP) or that are working around current limitations in awkward ways (SLP and SLPDEX).

Budget
None