BUIP092: Workshop on Instant Transactions for Bitcoin

Submitted: 6 August 2018
8 August 2018 revisions in blue

Purpose

To request Bitcoin Unlimited (BU) membership approval to allocate BU funds to sponsor a multi-day developer workshop dedicated to improving instant transactions for Bitcoin Cash.

Location & Date

Location: Gargnano (Lake Garda), Italy
Date: 16 - 19 October, 2018

Workshop Description

A collaborative and highly-technical three-day workshop with the goal of improving instant transactions for Bitcoin Cash. Attendance will be limited to active developers, researchers, and key stakeholders. (15 to 30 participants.)

The workshop's main focus is to develop strategies for improving instant transactions that can be implemented over the short term (addressing the synced double-spend problem). Examples include double-spend relay, super-standard transactions, and double-spend proofs. A secondary focus will be on longer-term ideas to address the RBF double-spend problem, such as those based on pre-consensus techniques.

The workshop will include round-table discussions, working groups, and technical presentations.

Tentative Schedule:

Day 1: Defining the problem

- How can double-spends of instant transactions be carried out today?
- Statistics on 0-conf double-spends

Day 2: Exploring solutions

- Double-spend relay vs. double-spend proofs
- Super-stand transactions
- Pre-consensus

Day 3: Forging a path forward

- Coordinating between node implementation (ABC, BU, XT, Flowee the Hub), SPV wallets, businesses, and miners
- Best practices when accepting instant transactions and understanding risk level

Inclusiveness

This workshop hopes to encourage new developers to get involved and there will be an open call for proposals to present. Depending on demand, a small number of public tickets may be available.

Budget

The workshop organizers seek up to $50k of BU funds to sponsor the event.

These funds will be used to pay for the meeting rooms, A/V requirements, and catering. The funds will also be used, on a case-by-case basis, to pay travel and accomodation costs for workshop participants who do not have external sources of funding (e.g., developers).

NOTE: Workshop organizers are seeking additional sponsors, with the goal of reducing BU's direct costs to $30k. Please contact us if you would like to be a sponsor for this event.

Workshop Output

Presentations made during the event will be recorded and published on Youtube. These videos will be useful for educating the broader community about instant transactions, their risk level, and how those risks may be mitigated.

Live streaming of the presentations is a possibility.

Benefits

1. Eliminating the (fixable) vulnerabilities of instant transactions is low-hanging fruit that will greatly improve BCH's function as digital cash.

2. Educating the public on best-practices when accepting instant transactions, and understanding their risk levels, will encourage greater use of instant BCH transactions for payments.

3. Sponsoring the workshop will further establish Bitcoin Unlimited as a center of excellence for Bitcoin research and full-node software development.