CoinJoin Desktop App for Financial Privacy

Funded **4 months ago**

0.00 / 113.00 **BCH**

OVERVIEW

Users of Bitcoin Cash value their financial privacy. The community has built a powerful tool in the form of CashFusion, which coordinates CoinJoin transactions, in order to restore financial privacy. But over the last few months, the following problems have arisen with CashFusion:

- Many users are reporting a lack of fusion transactions. They are doing everything right, but the transaction formation is consistently failing. Despite many brilliant minds discussing it, there appears to be no clear solution.

- The protocol is complex. Despite many brilliant and well funded people making the attempt, it's only been incorporated into two wallets: Electron Cash and Pokket. And Pokket is no longer maintained.

- There is only a single server for coordinating fusions. More than one server is undesirable because that creates liquidity issues. And server hosting, in light of the recent OFAC listing of Tornado Cash, has caused the older server host to stop hosting it. A new server has been created, but the legal liability of hosting a coordination server is still problematic.

This Flipstarter campaign is not intended to criticize CashFusion. CashFusion is a valuable tool that will continue to provide value to the Bitcoin Cash community for the foreseeable future. This Flipstarter campaign seeks to compliment CashFusion by creating a second app for participating in CoinJoin transactions. It's bad for the utility of BCH if there is only a single tool for restoring financial privacy, and there is no alternative when that single tool has issues. The app funded by this Flipstarter can take some of the pressure off the CashFusion team.

THE ASK

$12,000 USD in Bitcoin Cash is sought to fund the initial development of a desktop app. This desktop app will run on Windows, Mac, and Linux. It will be a Bitcoin Cash wallet that will coordinate CoinJoin transactions, similar to CashFusion in Electron Cash. It's advantages are:

- No coordination server is used. The coordination happens peer-to-peer.

- The JavaScript libraries it uses can be easily exported to mobile wallets, web wallets, and other BCH apps.

- This protocol can easily be adapted to work with SLP tokens (or the new CashTokens protocol hitting mainnet in May 2023).

- Your privacy increases with the more rounds you participate in. Want more privacy? Send your UTXOs through more rounds.

- It's based on IPFS and the Bitcoin Cash blockchain, both of which are highly censorship resistant.

The campaign has been funded.

Celebrate! 0a7e441db…

CAMPAIGN DETAILS

This campaign is only seeking $12,000 USD in Bitcoin Cash. This is enough to fund the following 'core' goals:

- Create a desktop app that runs on Windows, Mac, and Linux. This will be created using Electron.js
- Implement the Collaborative CoinJoin protocol.
- CoinJoin BCH only (no tokens in this first iteration).

The timeline for achieving these goals is three months.

The point is to only create a minimum viable product (MVP), to simply nail down the most basic features. Once these core goals have been achieved, there will be a lot more information for the developers and the wider BCH community to consider. We'll collectively be in a much better position to understand any limitations and additional features (like making it work with tokens). Funding improvements and new features can be done through future Flipstarter campaigns. Developers will be able to fork the software and innovate.

In this first iteration, the security of the CoinJoin protocol is not expected to stand up to State or Corporate actors, but simply to prevent a merchant from beign able to find your crypto stash through a block explorer. It will be usefully secure, and be in a position to iterate and improve.

A Telegram channel will be created for developers and early adopters to solicit feedback and obtain assistance.

WHO I AM

My name is Chris Troutner. I've been an active developer in the Bitcoin Cash community since 2018. Most people in the space know me, and I'm active on Twitter. A few highlights about my career in Bitcoin Cash:

- I previously had a Flipstarter campaign of $16,000 USD funded by the BCH community to build the psf-slp-indexer. This indexer is currently running a significant amount of the SLP infrastructure on the Bitcoin Cash blockchain. It's used by companies such as Bitfinex (Tether) and Sweet.io.

- My team won the grand prize at the 2020 CoinParty Hackathon.

- I worked at Bitcoin.com from 2018 through 2020, helping them build out several tools for software developers who wish to incorporate Bitcoin Cash into their projects. After I left Bitcoin.com, I started two organizations:

- FullStack.cash sells infrastructure and freelance development to businesses building apps for Bitcoin Cash.

- The Permissionless Software Foundation is a collective of JavaScript developers. Our mission is to develop, promote, and maintain software that makes it easy for individuals to protect their privacy, circumvent censorship, and engage in economic activity.

CRITICISMS

I presented the content of this Flipstarter to the CashFusion Telegram channel to get feedback before launching it. I received the following criticisms, which I want to address here:

One criticism is that the Collaborative CoinJoin protocol is 'trusted'. By that, they mean that the one user who initiates a CoinJoin transaction learns about the other participants inputs and outputs. So you're 'trusting' that the user is not a bad actor. There are two responses to this criticism:

- Only one user learns about the inputs and outputs for that one round. Their ability to track the outputs ends when those UTXOs enter a new round (where they did not initiate the new round). Sending your UTXOs through more rounds ensure more privacy.

- This Flipstarer is only building an MVP. More important than the CoinJoin protocol is the packaging (a desktop app that runs on the major OSs) and the ability to coordinate wallets. It may be decided to replace Collaborative CoinJoin with CashShuffle, or we may find improvements to Collaborative CoinJoin and update the protocol. The point: along the way, we will inevitably find ways to improve the user experience and any security issues. This first iteration focuses more on building a modular architecture for future iteration, and less on achieving perfect security on the first try.

A second criticism received was that the CashFusion team is working on a peer-to-peer (p2p) protocol for removing the need for the central server in CashFusion. It is really up to the BCH community and those who donate to this Flipstarter to answer that criticism. Here is my thought process:

Electron Cash is written in Python, and time has shown that only a handful of people contribute consistently to it. This new CoinJoin wallet will be written in JavaScript, and the development will be done completely in parallel to the Electron Cash and CashFusion teams. I think it would be a healthy move for the BCH community to fund parallel development teams, so that they are not too dependent on either one. I'll know if other people in the BCH ecosystem echo this attitude, if this Flipstarter gets funded.

1 recipients

Chris Troutner *113 BCH*

<> Track Delivery

Development Status

61 contributors

22%	**zveda**	25.00 BCH

15%	**Renegade** “Can I persuade you to write it in ReScript or TS?”	17.00 BCH
13%	**majamalu** “thank you!”	15.06 BCH
11%	**Anonymous** “We are all Satoshi”	12.05 BCH
10%	**Anonymous** “Privacy is a human right. Financial privacy is a subset of privacy.”	11.31 BCH
3%	**Anonymous**	3.35 BCH
3%	**Brad** “I want more privacy!”	3.28 BCH
2%	**Anonymous** “Great idea!”	2.33 BCH
2%	**Anonymous**	2.26 BCH

2%	**Ekliptor** “BCH devs need funding”	1.99 BCH
2%	**Sunny Gahani** “Keep up the good work, Chris!”	1.78 BCH
2%	**bitcoincashautist**	1.76 BCH
1%	**Omar**	1.41 BCH
1%	**Shadow Of Harbringer** “This is Leet™”	1.34 BCH
1%	**ErdoganTalk** “Economics Writer”	1.26 BCH
1%	**psiconautasmart** “Privacy is CRITICAL for P2P CASH, we need more options!”	1.00 BCH
1%	**@_minisatoshi** “Continue spreading economic freedom to the world!”	1.00 BCH

1%	Anonymous	1.00 BCH
1%	**Bitcoin Jason** "You are, I am, We are ALL Satoshi!! Let's Do Our Part!!"	1.00 BCH
1%	Anonymous	1.00 BCH
1%	**KeepBitcoinFree.org** "This is an important step forward in privacy for Bitcoin (Cash). The PSF team can make it happen if we fund them."	0.87 BCH
1%	**doramas89** "Funding Chris' work no matter what he choses to build, and so should all!"	0.74 BCH
0%	Anonymous	0.56 BCH
0%	**Sydwell** "Bitcoin Cash for the win!"	0.50 BCH
0%	**Joemar Taganna / Paytaca** "I love that this is going to be more portable to mobile wallets. Go Chris!"	0.45 BCH

0%	**Blockstream** “Need that privacy”	0.44 BCH
0%	Anonymous	0.27 BCH
0%	**Remora_101**	0.26 BCH
0%	**Pantera**	0.25 BCH
0%	**Dave BCH 11011 Holland**	0.25 BCH
0%	**Bitcoin Collab** “Bitcoin Payment Module - Bitcoin Cash Register - Bitcoin Smart Lock”	0.23 BCH
0%	Anonymous	0.22 BCH
0%	**Individual Sovereignty**	0.21 BCH

0%	**Borracho.bch**	“Privacy matters! Its awesome to see Chris trying to bring more greatness to the BCH community. ”	0.20 BCH
0%	**Bitcoin Out Loud**	“Good luck!”	0.19 BCH
0%	**Steve2048**	“Thanks for taking care of our privacy!”	0.18 BCH
0%	**hero462**		0.17 BCH
0%	**lugaxker**	“Privacy is necessary for an open society in the electronic age.”	0.17 BCH
0%	**Anonymous**		0.10 BCH
0%	**Bros > Wham**		0.10 BCH
0%	**Anonymous**		0.09 BCH

0%	**BCHisFuture** “Let's do our part”	0.09 BCH
0%	**SBF** “I'm broke hence the small amount. Borrowed from Caroline. YOLO”	0.08 BCH
0%	**Anonymous**	0.06 BCH
0%	**Anonymous** “Privacy FTW”	0.03 BCH
0%	**Chainalysis** “Make Orwell fiction again.”	0.03 BCH
0%	**Anonymous**	0.03 BCH
0%	**bChad**	0.01 BCH
0%	**devperate** “a bet on competition”	0.01 BCH

0%	**Chris Troutner** “Donating on a livestream!”	0.01 BCH
0%	**CryptoShirts.plus** “https://cryptoshirts.plus”	0.01 BCH
0%	**GeneralAkAbA** “Never back down.”	0.01 BCH
0%	**Poor guy** “Its not too much but its coming from my heart, love your work, thanks”	0.01 BCH
0%	**Anonymous**	0.01 BCH
0%	**Anonymous**	0.00 BCH
0%	**Anonymous**	0.00 BCH
0%	**Strange**	0.00 BCH

0%	Anonymous	0.00 BCH
0%	Anonymous	0.00 BCH
0%	Anonymous “min”	0.00 BCH
0%	**test**	0.00 BCH

How to contribute to this campaign Common questions

Powered by Flipstarter