SLPswap: A Bitcoin Cash Decentralized Exchange

ba.net iphone@ba.net

November 18, 2020

Abstract

A Bitcoin Cash (BCH) Simple Ledger Protocol (SLP) swap trade solution. SLPswap is a standard BCH transaction and does not have a central point of failure. It is trustless using partially signed Bitcoin transactions BIP 174. Compared to centralized exchanges, SLPswap has a unique set of difficulties and respective mitigations. As usage and liquidity increases, it enables a variety of automated, behind-the-scenes improvements to user experience. Inmediate benefits are no counterparty risk and instant zero-conf trades.

Contents

1. Introduction

Fiat currencies are consistently depreciating in value due to inflation, political biases, and other dynamic economic scenarios. As an alternative, Bitcoin and its derivatives have achieved some success as currencies.

While usage across the cryptocurrency ecosystem has grown through market cycles, volatility still hampers widespread use and adoption. To have utility, a floating currency, whether sovereign-backed or market-based, must allow users to hold it for a reasonable period of time without fear of losing purchasing power. The current reality however, is that the value of any given cryptocurrency routinely moves more than 10% in a single day due to poor liquidity, speculation, and the relatively small size of the cryptocurrency market. Some people think that a critical mass of adoption will naturally solve this problem, but that critical mass remains elusive for all cryptocurrencies.

In this paper, we describe SLPswap, a Bitcoin Cash distributed exchange solution to the volatility problem that does not have any central points of failure, has low exposure to potential programming flaws, is difficult to censor, and does not require system-wide coordination to function. The users involved in the trades do not have to take any counter-party risk and can settle instantly with zero-conf.

2. Problem description

Any currency has three fundamental functions: A store of value, a medium of exchange, and a unit of account. We believe that price stability is a gatekeeper to the mainstream adoption of cryptocurrency.

Compared to competently managed fiat currencies that have a fine tuned inflation target, the value of cryptocurrencies can swing wildly. As a result, cryptocurrency pricing of goods and services must be updated too often and becomes unreliable for users and merchants. Commerce is further hampered by frequent mismatches of expected future value. A pessimistic merchant can be reluctant to accept the cryptocurrency while an optimistic customer can be reluctant to spend.

Merchants are likely to immediately exchange received cryptocurrencies for more stable assets to avoid speculation. On the spending side, customers may “spend and replace” to compensate for optimistic sentiment. However, these measures effectively negate the low friction advantage of cryptocurrencies.

In other words, for cryptocurrencies to become more than just a playground for speculation, there is a severe need for them to be a stable store of value.

3. Existing solutions

Several broad categories of solutions to this problem have appeared.

3.1 Exchange to fiat

Many merchants prefer to exchange the cryptocurrency they exchange into fiat currencies. The exchange results in a position that is often more stable than cryptocurrencies, as well as being liquid and familiar. Examples include BitPay, local underwriting as in North Queensland, Australia, and other exchange deposit based solutions.

Fiat exchange suffers from the friction inherent to interfacing with a centrally controlled currency. It is subject to onerous regulations and processing that incur costs similar to traditional payment gateways, erode censorship-resistance and eliminate the inherent efficiency of cryptocurrencies.

3.2 Fiat-backed stablecoins

These stablecoins use a reserve fiat currency such as the US dollar, euro, among other reserve assets as collateral to give the customer an equivalent amount of crypto coins. These reserves are usually maintained by independent custodians and undergo compliance auditing. There are multiple stablecoins today that have seen various degrees of adoption such as Tether (USDT), USD Coin (USDC), TrueUSD (TUSD) and FlexCoin (FUSD).

Fiat-backed stablecoins take advantage of the current regulation landscape where use of fiat-backed instruments tends to be less regulated than direct interfaces with fiat currencies. The creation and redemption of stablecoins incurs as much or more burden as direct fiat exchange, but that complexity is managed by the issuer. The sending and receiving of stablecoins themselves receive less scrutiny, restoring some of the cryptocurrency-like properties. Furthermore, as stablecoins have a stable, liquid and familiar user experience similar to fiat currencies, they are easier to understand, trust and adopt.

Stablecoins do have some inherent limitations. Their value depends on their fiat currency reserve, and that reserve establishes a large custodial risk. The custodian can steal, falsify or otherwise manipulate the reserve and trigger a catastrophic loss of value throughout the stablecoin's ecosystem. The simple presence of such a risk marks a key difference between fiat-backed stablecoins and permissionless cryptocurrencies: they have clear central points of vulnerability and failure.

The regulatory advantage of stablecoins is also fragile and subject to change. Their central issuing authorities can easily be pressured into extending heavy handed scrutiny beyond redemption and creation. We have already seen an incident of direct, protocol-level blacklisting and it is reasonable to expect regulatory pressure for such measures to increase on stablecoin custodians.

3.3 Crypto-collateralized algorithmic stablecoins

To address the above shortcomings of fiat-backed stablecoins, a relatively recent development is algorithmic stablecoins such as MakerDAO's DAI and Reserve Protocol's RSV. While they differ in exact mechanisms, these algorithmic coins are typically over-collateralized by volatile crypto-assets instead of directly backed by fiat. As a result, they can be programmed to exist purely on a decentralized blockchain. There is no need for a centralized redemption gateway that forms the basis of the entire system. This mitigates the censorship and regulatory risks of fiat-backed stablecoins to a certain extent, while retaining the pleasant user experience of an easy-to-understand token representing fiat value.

Algorithmic stablecoins, however, have two primary risks associated with them. The first is the inherent risk with using volatile, illiquid assets to back "stable" value. As the underlying asset depreciates, the entire system will need to be downsized in a controlled manner. A catastrophic market downturn may result in systemic problems, such as Global Settlement in DAI, that lead to political intervention or other unexpected edge cases. This risk does not exist in fiat- backed stablecoins with a proper reserve where they simply draw down toward zero when demand falls.

Unintuitively, another risk of algorithmic stablecoins is centralization of control. Due to the need to adjust collateral policies over time, algorithmic stablecoins typically have a second layer of governance tokens, as seen in MKR of Maker- DAO and RSR of the Reserve protocol. Necessity of these governance tokens reintroduces the risk of centralized capture and control. In the worst case, poorly designed incentives can lead to apathetic holders of the governance coin, and vulnerability to sabotage by a minority of stakeholders.

Finally, all software has the potential for bugs and vulnerabilities. Any bug or vulnerability in the complex central smart contracts that control algorithmic stablecoins could have a systemic impact.

4. A decentralized exchange solution based on peer-to-peer trading

Observing the shortcomings of each approach above, we propose SLPswap, a novel, transactional solution that has no systemic dependencies or single points of failure. Easy access to various stablecoins can reduce cryptocurrency volatility and increase usage.

A Bitcoin Cash DEX, or decentralized exchange, uses partially signed bitcoin transactions. It is trustless and settles trades instantly.

Ethereum DEX roots and examples. A typical Ethereum DEX operates like a stock exchange, except it is run by a smart contract on the Ethereum blockchain that enforces rules and executes trades. Users can trade cryptocurrencies and DEXs do not require a centralized authority to operate, but they do need access to a reliable source of liquidity to service their users.

To better understand how they operate, let's compare a DEX to a centralized exchange (CEX).

Financial exchanges are where users buy and sell financial assets. Traditionally, the CEX takes orders from buyers and sellers and takes custody of their assets. DEXs do the same thing but without the custodial aspect and they can offer more in the way of security and anonymity. A user can simply interact with a smart contract directly from their crypto wallet.

Some DEXs have pools of currencies to trade or swap, whilst other DEXs use order books with Maker and Taker orders. Maker orders provide liquidity because they're not immediately matched on the order book. Whereas a Taker order is instantly matched with an order already on the books. Thus, fees for Maker orders are lower than fees for Taker orders (or they can even be zero).

How does a DEX work? While DEXs can differ in how they are designed, they are similar in how they connect buyers and sellers across a global liquidity pool. Most DEXs require the user to have at least enough ETH to cover the transaction cost of doing the trade. Some don't charge transaction fees for Maker orders but make up the difference by charging higher fees for Taker orders, while some return a portion of the trading fees to traders who willingly supply capital to their liquidity pools.

Are DEXs Risky? There is always a risk anytime you use a CEX because you first have to deposit your funds. CEXs hold millions of dollars in deposits and thus are constantly targeted by hackers looking for big money heists. The big risk in a CEX, therefore, is that of custody, which a user forfeits the entire time their deposit is being held.

Hackers have made off with millions of dollars as well as reams of user data by cracking into CEXs over the years, the most infamous being the Mt. Gox hack in 2014. That exploit gave Bitcoin a black eye from a security reputation standpoint, and opened the door for gold-shilling naysayers like Peter Schiff to boast, “I told you so!” It is this lack of security that has tarnished the image of crypto exchanges and hampered them from becoming potential competitors to conventional exchanges.

Hopefully, DEXs can change all that because the assets are only transferred at transaction time naturally making them more secure. So DEXs can offer non-custodial solutions that bigger CEXs like Coinbase or Binance cannot. Even though they are still the 800-pound gorillas in the room, DEXs are poised to compete with them due to improvements being made in usability, liquidity, and security.

4.1 DEX trading advantages

Pseudo-anonymous: No lengthy forms, background info, or ID is required to participate.

Automatic: So long as there is sufficient liquidity, DEX trading is instant.

Non-custodial: You don’t have to turn over your funds to 3rd party control.

Lower cost: Minimal trading fees.

So, as long as a user can keep their private keys in check, using a DEX should mitigate the risk of getting hacked.

4.2 Partially signed Bitcoin transactions (PSBT)

You may be familiar with the concept of a multi-signature, or multisig, system? In this type of system two or more people must sign a transaction in order for it to be valid.

Multisig payments had one limitation, though: the act of signing must be simultaneous. Everyone who agrees with a transaction must sign it at once before it is broadcast to the network.

Now imagine that there was a protocol such that a Bitcoin transaction that required multiple signatures was created but this transaction did not have to be built at once.

One user could sign today, another user could examine the TX and decide whether to sign later on and so forth. This can be achieved without a trusted intermediary.

That is what PSBT achieves. BIP 174 was proposed in mid 2017 to address exactly this scenario – and this system is already available in the current Bitcoin Cash Here's a simple example scenario that illustrates how PSBT works.

To make a group payment, one of the group members creates a PSBT and adds unspent outputs, both his and other's and the desired target output (who will receive the payment).

Other users whose inputs are included in the PSBT receive the transaction by email or chat. The user analyzes the inputs, outputs and amounts and decides whether it's correct or not. If there is agreement, the user then adds his signature to the PSBT.

Once every participant has added their signature, the PSBT is complete. It is then compiled into a regular multisig Bitcoin transaction just as if it had been signed simultaneously. The TX is transmitted and mined like any other transaction.

That is how PSBT's work. Fully decentralized – no single entity needs to be relied on or trusted to coordinate and distribute funds.

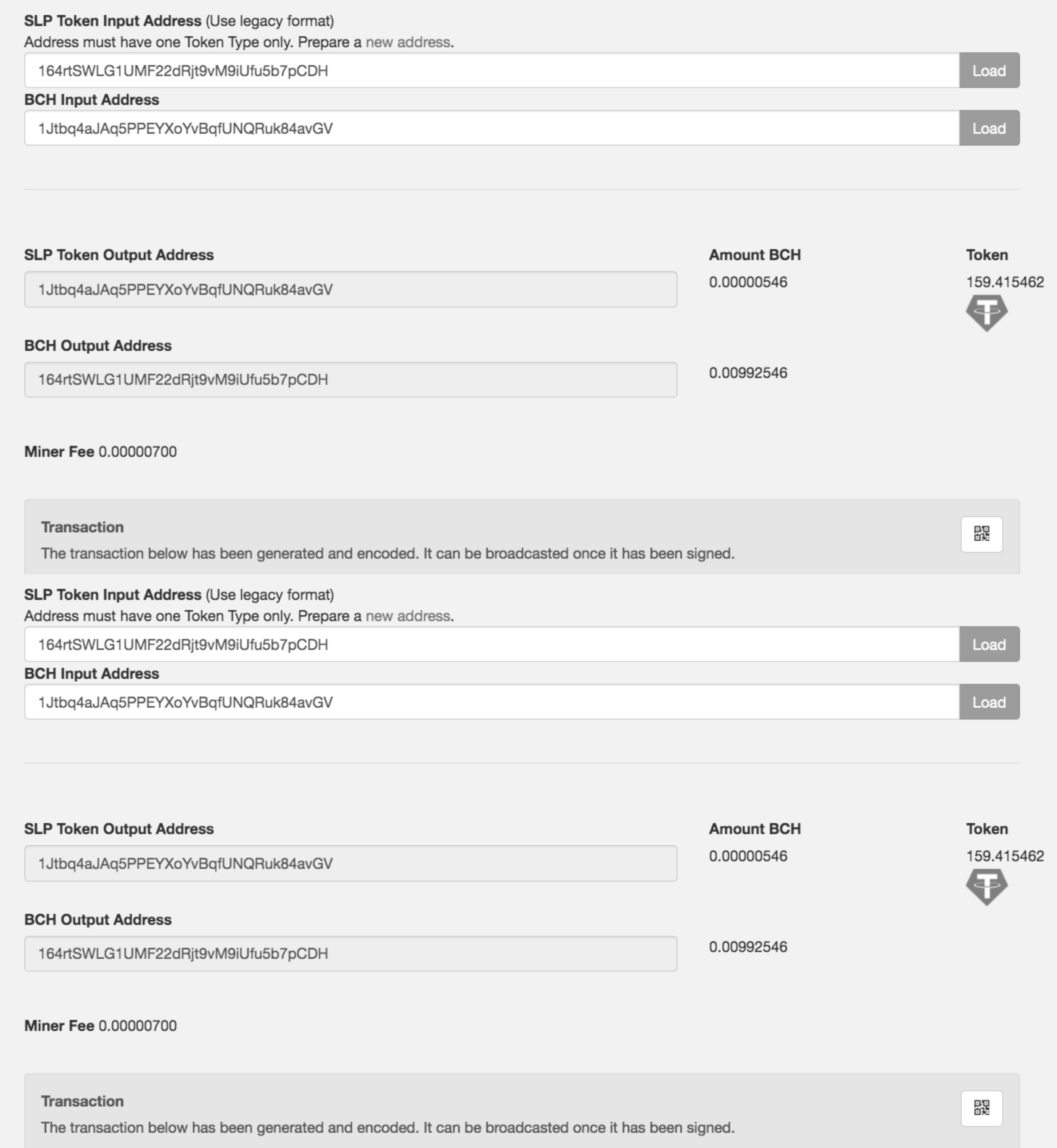
Users must only know each others's Bitcoin addresses. This is a requirement for all Bitcoin payment processing anyway. So the only manual coordination that is needed between users is to know each others' addresses. For which they can coordinate via email or chat.

4.3 Swap transaction building

To make a trading swap, the input SLP address must have one token type only. Prepare a new address with the exact token amount to swap.

Then, fill the input SLP addr, the input BCH addr, press "Load". Check the token and bch amounts.

Press "Generate Swap Tx" and your transaction is ready!



SLP Token Input Address (Use legacy format)
Address must have one Token Type only. Prepare a new address.

164rtSWLG1UMF22dRjt9vM9iUfu5b7pCDH

BCH Input Address

1Jtbq4aJAq5PPEYXoYvBqfUNQRuk84avGV

	Amount BCH	**Token**
SLP Token Output Address 1Jtbq4aJAq5PPEYXoYvBqfUNQRuk84avGV	0.00000546	159.415462
BCH Output Address 164rtSWLG1UMF22dRjt9vM9iUfu5b7pCDH	0.00992546	

Miner Fee 0.00000700

Transaction
The transaction below has been generated and encoded. It can be broadcasted once it has been signed.

SLP Token Input Address (Use legacy format)
Address must have one Token Type only. Prepare a new address.

164rtSWLG1UMF22dRjt9vM9iUfu5b7pCDH

BCH Input Address

1Jtbq4aJAq5PPEYXoYvBqfUNQRuk84avGV

SLP Token Output Address 1Jtbq4aJAq5PPEYXoYvBqfUNQRuk84avGV **Amount BCH** 0.00000546 **Token** 159.415462

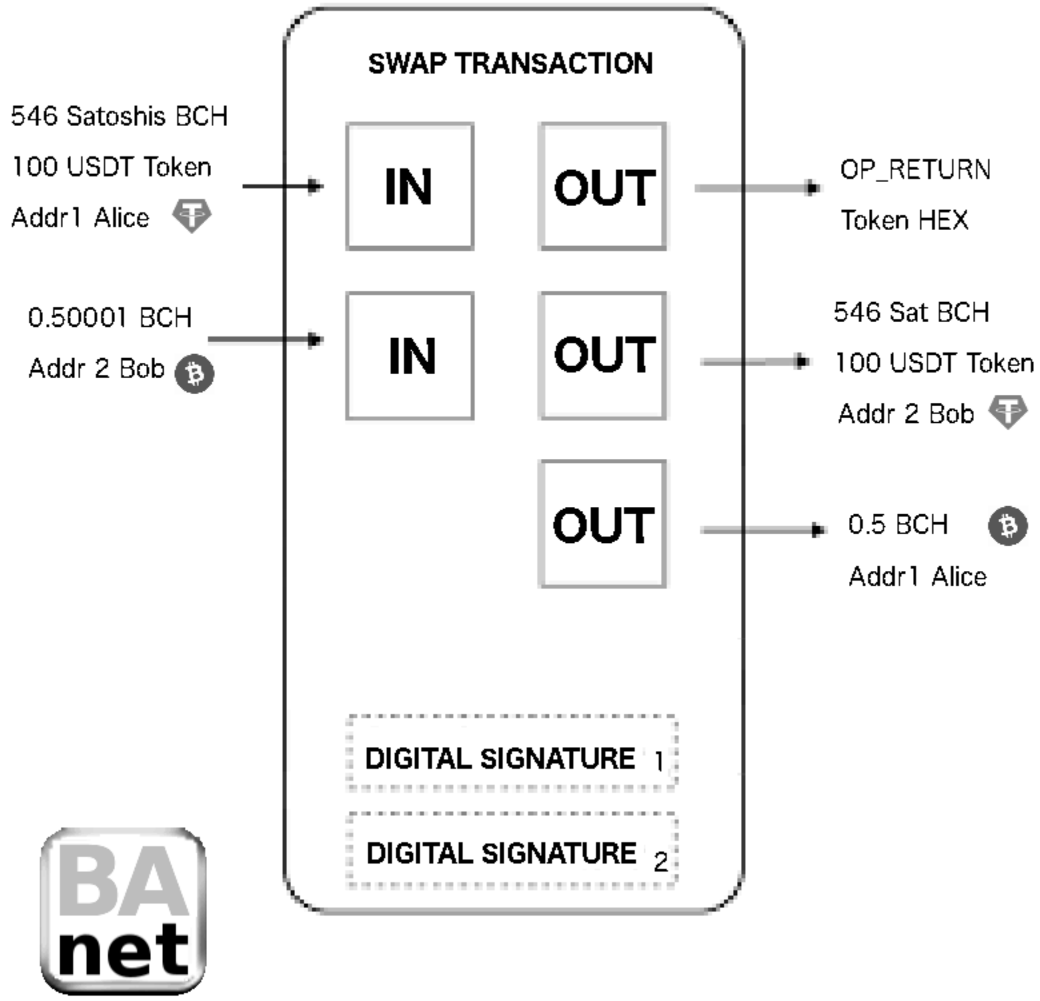
BCH Output Address 164rtSWLG1UMF22dRjt9vM9iUfu5b7pCDH 0.00992546

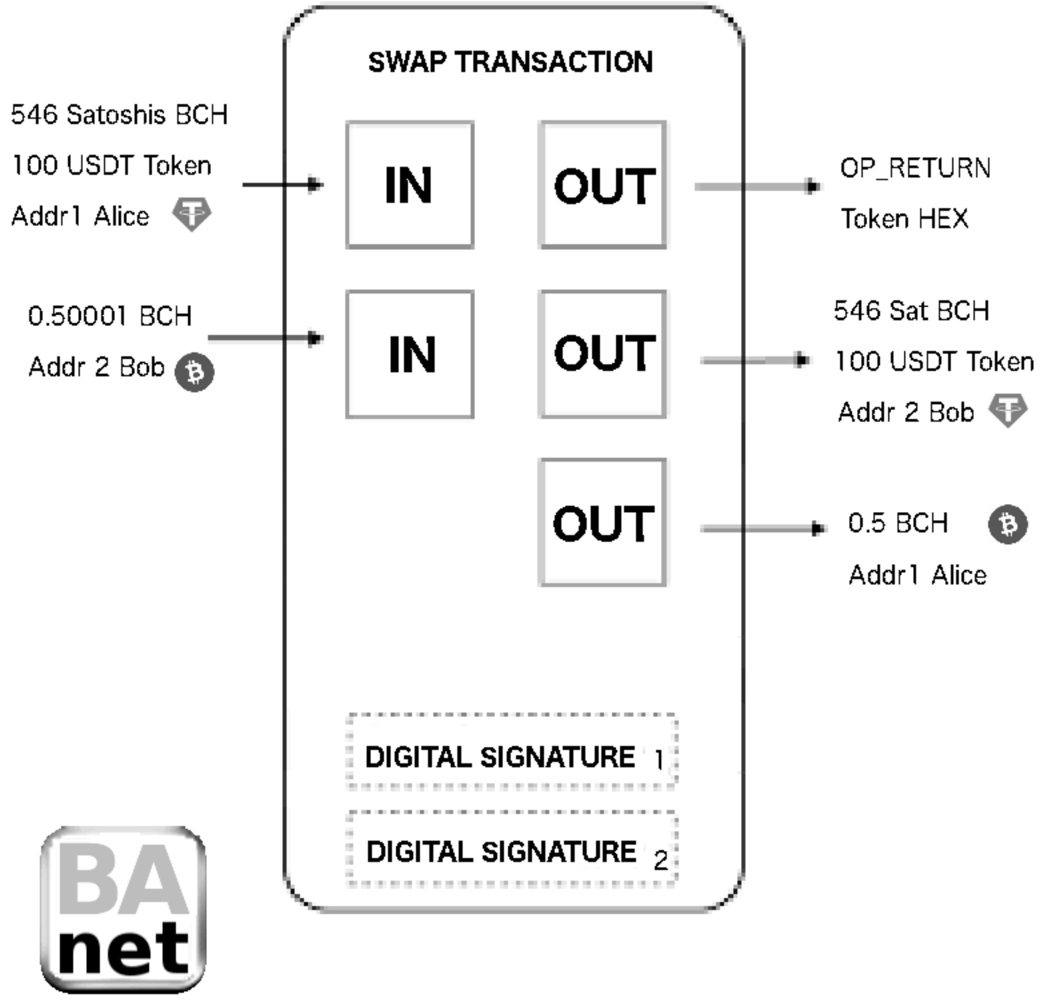
Miner Fee 0.00000700

Transaction
The transaction below has been generated and encoded. It can be broadcasted once it has been signed.

Sign your hex transaction. Send it to your conterparty for the 2nd signature.

Trade in seconds! Using the swap webapp or offline apps for any OS or mobile.





4.3.1 Posted bid, offers, swap trades

1. Post your BID or OFFERS including your input address, and price.

2. Buyer can then create the swap transaction, locking-in all inputs and price.

3. Seller receives the signed swap to verify and add the 2nd signature. Swap is done!

4.3.2 Providing swap liquidity, staking

By posting your input address and price you are providing liquidity, and you can choose your own trade profit percentage. For example you can set a price of coinmarketcap +1%
You control your own liquidity pool and your trade margins.
You can create new trading pairs with your own tokens.

4.3.3 Business automated market maker (AMM)

A bot can automate the checking of valid received swaps. Once a valid swap is received from its own address pool and the price is within limits, the swap is signed and broadcasted.

Make a market for any trading pair, or for your own business reward tokens.

4.3.4 Custom exchange offline apps

Promote your Exchange or OTC desk with your own branded offline apps. Non-custodial, and equivalent to Binance Safepal, or Coinbase cold wallet solution.

Maximum security, private keys never touch the Internet. Bitcoin cold storage.

5. Swap fees and liquidity rewards

Tipical centralized exchanges fees range from 1.1% to as high as 2%. Swap fees are embedded in the swap trading library, currently they are set to 0.50% and will be reduced over time to 0.35%

Liquidity providers can add orderbook fees for the bid and ask trading spreads. Providers can choose their own profit margins. They can stake any token or BCH. There is no danger or impermanent loss, as in Uniswap.

Exchanges have the option to include a reward token. The token can account for a part of the swap fee, and be exchanged for BCH. The reward token can also be staked for protocol governance voting and receiving a dividend from swap fees.

The SLPswap library can be used in Exchanges, OTC trading desks and wallets. The pure javascript implementation with no Node or any external dependencies allows easy embedding anywhere. Web apps, offline apps and native apps.

Several third-party implementations are in production use today.

6. Impact on the Bitcoin Cash ecosystem

We expect SLPswap over time to build liquidity, volume and adoption, and become a significant part of the Bitcoin Cash ecosystem. Once sufficient volume is achieved, we expect it to have the following effects:

6.1 Merchant adoption

SLPswap allows merchants to seek currency stability at low cost or even profit, while simultaneously retaining all the benefits of Bitcoin Cash. Wider adoption by merchants will strengthen the permissionless nature of the ecosystem.

6.2 Mitigating crypto-holding risk

Allowing easy access to stablecoins, without relying on a custodial solution. Users of SLPswap take no counter-party risk and can trade instantly with zero-conf settlement.

6.3 Increased demand and utility for Bitcoin Cash

In addition to simple upward price pressure, we expect widespread use of Bitcoin Cash-denominated SLPswap trades to increase demand for Bitcoin Cash as collateral, directly impacting long term viability as peer-to-peer electronic cash.

This effect should be especially apparent in trading against other speculative assets such as precious metals and alternative cryptocurrencies, where Bitcoin Cash absorbs speculative demand from their overall spot markets.

7. Market difficulties and mitigations

7.1 Centralization pressure

The design of SLPswap does not involve a central, systemic point of failure. Centralization pressure will exist on various parts of SLPswap and we expect it to ease as adoption and diversity rises, as described below. Failure of the ecosystem to diversify may result in a system that is more fragile than expected.

7.2 Liquidity pressure

SLPswap trades can be constructed ad-hoc between any two willing parties. However, finding a willing counterparty at a desired set of parameters, in a timely fashion, and at a reasonable premium is essential for SLPswap to have significant utility at scale. If matchmaking activity is concentrated in the hands of few centralized exchanges, they can censor and otherwise impose non-optimal conditions on SLPswap users.

As SLPswap is not fundamentally tied to any outlet, we expect that censorship and non-optimal conditions will be countered as liquidity flees either to other exchanges, decentralized setups or ad-hoc bazaars. Federation between exchanges can further discourage these pressures from rising in the first place.

7.3 Regulatory pressure

Regulatory pressure is a common concern for all cryptocurrency activities including swaps and trading. Regulatory bodies can attempt to impose reporting and tracking burdens, reducing the number of exchanges that can comply. The non-custodial nature of SLPswap should afford it an edge over custodial solutions when it comes to regulatory pressure.

Assuming liquidity is sufficiently distributed, there are only limited ways regulatory bodies can censor the system as a whole. Even at exchanges where regulatory bodies apply pressure, they can censor but not compromise funds.

8. Conclusion

We have described a new swap trading trustless solution for Bitcoin Cash.

Exchanges and over the counter (OTC) services can provide convenience, liquidity and other benefits but are not strictly necessary. SLPswap takes advantage of the most fundamental building blocks of Bitcoin Cash and we expect usage to increase overall utility.

Any two users can trade using SLPswap with no counterparty risk and enjoy instant zero-conf settlement.

1. Add a DEX to your Exchange or OTC Desk , BA.net White-Label DEX

2. Third-party library implementation, Live , Bitcointalk.org

3. Partial Signatures PSBT BIP 174 Andrew Chow, GitHub.com

4. Bitcoin PSBT, Definitions

5. Bitcoin PSBT, Documentation

6. Multisig Transactions, Documentation

7. Offline Transactions, BCH Offline Wallet , GitHub.com

8. General Protocols, AnyHedge, Whitepaper

9. Contact us, t.me/banet1 , r/SLPswap , iphone@ba.net