

Counterparty Token Distribution Solutions

A survey of what's available now and what might be possible in the future.

Short Term Solutions

Individual Sends - The Current State of the art in Counterparty asset sends

The cheapest send involves sending tokens to 1 user at a time with primed UTXOs and minimal fees:

Bitcoin dust: 0.00005430

Transaction Size: 231 bytes

Fee: 0.00007500 (at 32.5 sathoshis per byte)

Total cost per send: 0.00012930 BTC (\$0.142)

Example from a recent FoldingCoin distribution using Tokenly Bitsplit:

<https://www.blocktrail.com/BTC/tx/303e084558793ca01898e508d14c07e69461982f057c9f75994dfa0422f670ee>

<https://counterpartychain.io/transaction/303e084558793ca01898e508d14c07e69461982f057c9f75994dfa0422f670ee>

Enhanced sends with CIP-9 - The short term future

Enhanced sends still deliver 1 token at a time. But they do not require a recipient UTXO and therefore save the BTC dust cost.

Projected Timeline: June 1

Bitcoin dust: none!

Transaction Size: 227 bytes

Fee: 0.00007264 (at 32 sathoshis per byte)

Total cost per send: 0.00007264 BTC (\$0.080)

Enhanced sends (CIP-9) and Multisends (CIP-xx) - The slightly less short term future

Enhanced multisends combine enhanced sends with multiple destinations. The asset name is only specified once, so only the quantity and recipient are specified for each recipient.

Projected Timeline: July 1 (maybe June 1)

Bitcoin dust: none! (* see caveat below)

Encoding efficiency is: 62 out of every 102 bytes (1.645161291x the size, not including padding)

Example recipients per send: 40

Transaction Size: 2156 bytes (150 bytes for setup and then 29 bytes per recipient = 1310 bytes * 1.645161291 for encoding)

Fee: 0.00069000 (at 32 satoshis per byte)

Total cost per send: 0.00001725 BTC (\$0.019)

Other notes:

- **Important:** You will need to send temporary BTC dust to each of the multisig outputs, but this dust can be eventually redeemed with a specially formulated transaction.
- Priming transactions are not needed for optimal fee usage
- We lose 40 out of every 102 bytes (approx 39%) due to the multisig encoding scheme

P2SH data embedding (CIP-6) - The medium term future

Timeline: Late 2017

A more efficient version of multisends which does not lose 39% of data and does not require multisig dust. This works out to cost about **\$0.012 per send**

The Glorious Future

Payment Channels

Pros:

- Very cheap to send
- instant receives
- most, if not all, of the work has already been done on this

Cons:

- One payment channel must be created for every potential recipient
- Without segwit, transaction malleability can cause nuisance problems.
- New technology that is unproven in practice.
- No wallet support.

A token lightning network

Pros:

- Very cheap to send
- instant receives
- Can outsource "bank" duties to 3rd party hubs (like exchanges)

Cons:

- Requires segwit to be practical (theoretically possible without it)
- No work has been done yet for a token implementation. May requires significant engineering to overcome some of the complexity (and may not be possible at all)
- Still a hub and spoke system - someone has to serve as a bank
- Needs wallet and infrastructure developed to support it

More radical and theoretical solutions:

Centralized Database Solutions

Pros:

- Super cheap
- instant receives
- easy to implement

Cons:

- Central point of control and failure - vulnerable to hacks and corruption (can be mitigated with multisig)
- Custodial control and potential regulatory obligations
- less transparency

Off-chain Scaling with Distributed Storage

Embed a data hash in a transaction and store the data in a distributed data store (Storj, IPFS, etc.)

Pros:

- Much cheaper (Approaches free for large multisends)
- Maintains decentralization

Cons:

- Requires a radical change to Counterparty code (and philosophy)
- Requires all Counterparty servers to run a distributed storage client (Storj or IPFS)
- Opens new protocol-level attack vectors (DOS attacks)

Appendix A - Costs Chart

Solution	Dust BTC	TX Size	Rate	Fee	Total BTC	Total USD
Individual Sends	0.00005430	231	32.5	0.00007500	0.00012930	\$0.142
Enhanced Sends (CIP-9)	0	227	32.0	0.00007264	0.00007264	\$0.080
Multisends	0*	53.9	32.0	0.00001725	0.00001725	\$0.019
Multisends w/ P2SH	0	32.8	32.0	0.00001048	0.00001048	\$0.012

*requires multisig dust which can be redeemed. Redemption will require payment of some fees.

USD amounts are based on a BTC price of \$1100 USD/BTC

<https://docs.google.com/spreadsheets/d/1OqvFe1KQx1sof6NxsK1pmGOzO4SOAxXe9jfk9LSZiWw/edit#gid=0>