

Particl - Making Litecoin Invisible with BasicSwap



(BSX) BasicSwap v0.13.0 - (GUI) v.3.0.0

Welcome to BasicSwap DEX

Swap cryptocurrencies in <u>total privacy</u> with no middlemen, fees, or restrictions.

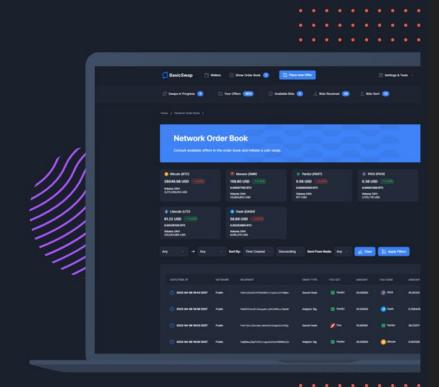


Manage your cryptocurrency wallets.

Start Trading

Browse available swap offers placed by others.

Learn how to use BasicSwap with the Particl Academy.



The History of BasicSwapDex



- Particl Project [2017] Privacy ecosystem and dApps
 - Particl Marketplace [2019] eBay-style decentralized marketplace
- BasicSwap DEX [2020] Atomic swap DEX
 - [2023] First DEX with fully decentralised distributed order book.
 - [2024] First implementation bidirectional XMR atomic swaps.
 - [2024] First to implement LTC MWEB atomic swap support.

Features



What's BasicSwap?

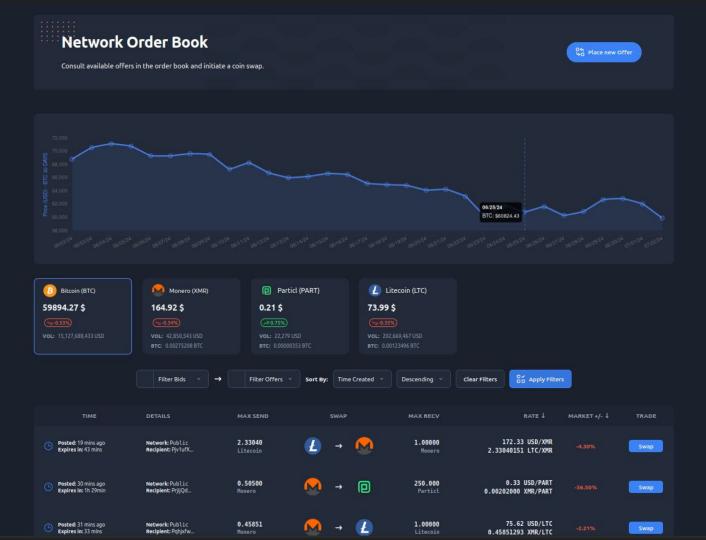
- A non-custodial wallet with swap functionalities;
- No intermediaries (utilizes atomic swaps);
- Open source, released under the MIT license;
- An interface for making and taking atomic swaps;
- No accounts, no KYC,
- Resistant to chain analysis.

Common misunderstandings



What's BasicSwap?

- Not an AMM Dex uses a distributed order book; no rugpull risk!
- No intermediary tokens or wrapped assets;
- Not monetized;
- Not a website (but you could build a website around it);
- Highly private E2EE, direct P2P swaps;
- 100% decentralized.



Wallets

Total Assets: O

\$3.61 USD



Change Password





Particl (PART)

Version: 23000300 Updating...

Balance:	16.99899600 PART
PART USD value:	\$3.61
Blind Balance:	0.0 PART
Blind USD value:	\$0.00
Anon Balance:	0.0 PART
Anon USD value:	\$0.00
Blocks:	1704999
Last Updated:	2024-06-08 08:19 +0000
Expected Seed:	True
m. d. d. d.	400.000



Balance:

0.00000000 BTC

Bitcoin (BTC)

Version: 230000 Updating...

Blockchain	99.99%
Expected Seed:	True
Last Updated:	2024-06-08 08:19 +0000
Blocks:	846980
BTC USD value:	\$0.00

The order book/blockchain is currently syncing, offers will only display once the network has fully 100% synced. Please wait until the process completes.



Litecoin (LTC)

Version: 210300 Updating...

Blockchain	98.55%
Expected Seed:	True
Last Updated:	2024-06-08 08:19 +0000
Blocks:	2679096
MWEB USD value:	\$0.00
MWEB Balance:	0.0 LTC
LTC USD value:	\$0.00
Balance:	0.00000000 LTC

The order book/blockchain is currently syncing, offers will only display once the network has fully 100% synced. Please wait until the process completes.

Why Litecoin?



- Faster block time than other blockchains;
- Low TX fees;
- Solid liquidity;
- High non-speculative usage.

These qualities make Litecoin the most popular pairing on our platform!

A Problem: Litecoin and Privacy



Default Litecoin is public and traceable.

 Many users want financial privacy - no one wants their data exposed in a way which could be used against them.

 Litecoin offers privacy via MWEB transactions which are fast, cheap and scalable, but adoption remains poor.

Our Solution

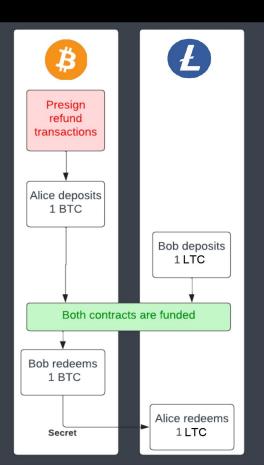


- LTC Adaptor Signature atomic swap pairs provide an opportunity to on-ramp and off-ramp Litecoin privately;
- Non-custodial, decentralised and open-source architecture contributes to the safety and privacy of your transactions;
- MWEB integration into BasicSwap pushes this even further.

What is an Atomic Swap?



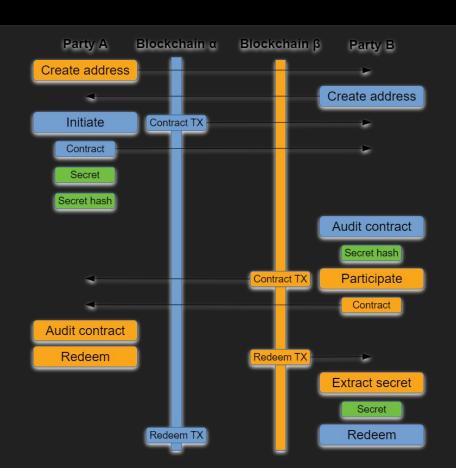
A direct peer-to-peer trustless swap of two cryptocurrencies, done by executing two linked conditional smart contracts on two synchronized blockchains.



How does it work? - Atomic Swaps (HTLC)



- Bob owns BTC, Sally owns LTC.
- Bob creates a private secret (s)
- A public hash (h) is derived from (s).
- Bob creates a contract to transfer his BTC to Sally when secret (s) is used.
- Sally creates a contract to transfer her LTC to Bob locking funds using the same (h).
- Since both contracts use the same (h) and Bob knows (s), he uses (s) on the LTC contract revealing the (s) on the BTC contract to Sally.
- Sally uses (s) and the LTC-BTC swap completes!



How it Works: Adaptor Signature-based Atomic Swaps



Atomic Swaps mean:

- No third-parties, arbiters, or central authorities necessary
- Very few moving parts
- No conflict resolution needed Time limit & refund conditions built in
- No public swap history, no public balances, no need for permanent data
- No chain of custody

How it Works: Adaptor Signature-based Atomic Swaps



The problem with traditional (HTLC) Atomic Swaps

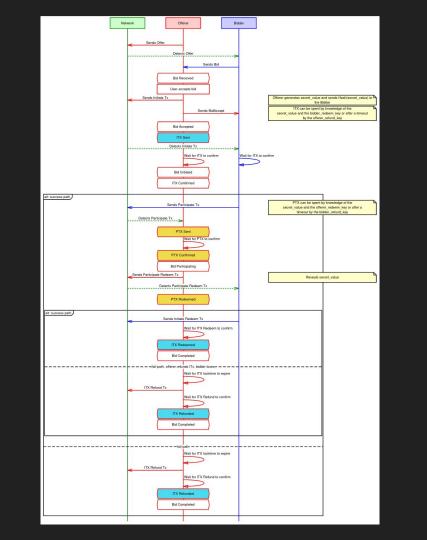
- They require programmable outputs *for both coins* (impossible with many privacy coins which lack this feature, incl. LTC MWEB)
- HTLC swaps produce timestamps on both blockchains (rendering the act of swapping vulnerable to chain analysis)

How it Works: Adaptor Signature-based Atomic Swaps



Adaptor Signatures - Private LTC Atomic Swaps:

- Adaptor signature swaps are an implementation of scriptless scripts.
- This allows us to swap cryptocurrency assets that lack programmable inputs.
- The principle is that **the sum of public keys will match the public key for the sum of private keys**. So when one side shares their half of a private key signing a tx, the other party can derive the other half and complete the swap.
- Messages to initiate, participate and redeem tx are transmitted off-chain on the SMSG network, removing detectable timestamps & further preserving privacy.



The SMSG Network: Privacy from the Ground Up



SMSG (Secure Messaging) - Enabling MWEB Atomic Swaps:

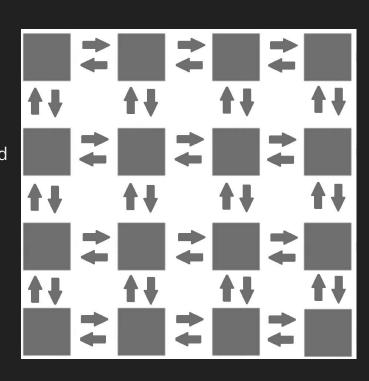
- A P2P, fully end to end encrypted, data relay, storage and messaging mixnet layer supporting off chain smart contract execution and settlement for cryptocurrencies.
- The foundation on which the fully decentralised, distributed order book of BasicSwap is built and enables orders to be placed, stored, communicated, executed and completed.
- The means through which we enable bidirectional MWEB atomic swaps (by offloading aspects of the swap contract off-chain).

The SMSG Network: Privacy from the Ground Up



SMSG (Secure Messaging) - P2P data layer BSX is built on.

- A mixnet of interconnected nodes
- E2EE messaging, storage and relay between nodes
- Censorship-proof
- Resistant to active and passive analysis



- Off-chain smart contract
 execution for any blockchain
- Orchestrate atomic swaps
- Enables fully decentralized orderbook
- No native token
- Open Source

	Filter Bids -	→ Filter Offers	Sort By: Time Created	Descending *	Clear Filters 00 Apply Filter	ers	
TIME	DETAILS	MAX SEND	SWAP	MAX RECV	RATE I	MARKET +/- ↓	TRADE
Posted: 0 mins ago Expires in: 59 mins	Network: Public Recipient: PZYgPTe_	0.07173 Decred	8 - 8	0.00600 Nonero	159.24 USD/XMR 11.9555050 DCR/XMR	-1.05%	Edit
Posted: 21 mins ago Expires in: 41 mins	Network: Public Recipient: Publicij	2.39650 Literoin	Ø →	1.99999 Monero	164.66 USD/XMR 2.39650204 LTC/XMR	+3.79%	Swap
Posted: 22 mins ago Expires in: 37 mins	Network: Public Recipient: PehEZPh	1.24000 Manero	⊘ → 0	0.00200 Bitcoin	98220.40 USD/BTC 628.800000 XMR/BTC	+40.93%	Swap
Posted: 26 mins ago Expires in: 34 mins	Network: Public Recipient: Puvil5TY_	8.44398 Honero	Ø → Ø	1.00000 Litecoin	78.32 USD/LTC 6.44398819 XMR/LTC	+2.29%	Swap
Posted: 27 mins ago Expires in: 32 mins	Network: Public Recipient: Pe54VJH	1.00000 Manero	Ø → 0	0.00100 Bitcoin	158420.00 USD/BTC 1000.00000 XMR/BTC	+63,38%	Swap
Posted: 28 mins ago Expires in: 36 mins	Network: Public Recipient: Plaforng	8.44825 Manero	⊘ → ②	1.0000 Litecoin	71.00 USD/LTC 0.44825215 XMR/LTC	+3.23%	Swap
Posted: 29 mins ago Expires in: 34 mins	Network: Public Recipient: PvoDKDz	2.41886 Litecoin	() - ()	1.0000 Monero	165.65 USD/XMR 2.41086326 LTC/XMR	1436%	Swap
Posted: 34 mins ago	Network: Public	0.29768	(a) → (a)	200.000	8.18 USD/WOW	+38.92%	Swap

Expires in: 25 mins

Recipient: PlanYsV...

O DOLLEDOAL LTC (MON)

Our Vision for MWEB on BSX



- Finalize Integration
 - Recently integrated MWEB balances & in-wallet LTC-to-MWEB conversions
 - Preparing for full MWEB swaps (viewkeys)
- An open-source swap hub for MWEB
- Add high-level privacy options for swappers

BasicSwap DEX



What's ahead?

- Open Source Integrations & web framework
- Integration into Particl Marketplace for wider eCommerce use
- Full MWEB support
- Wallet integrations
- More coins!

BasicSwap DEX



In Summary

- Atomic swap-based DEX utilizing fully decentralized distributed orderbook.
- No third party fees, no intermediaries, no rugpull risks.
- Very, very private! Resistant to chain analysis.
- Soon supporting LTC Mimblewimble atomic swaps!
- Always open source.



basicswapdex.com

github.com/basicswap/basicswap

basicswapdex.com github.com/basicswap/basicswap