BTDEX

BLOCKTALK DECENTRALIZED EXCHANGE

2020

BTDEX and TRT

Published 2019.12.28

BTDEX is a decentralized exchange system. It implements a unique non-custodial exchange method for cryptocurrencies and conventional fiat currencies based on BlockTalk Smart Contracts and Burstcoin on-chain encrypted messages. The **exchange method is serverless and fees are distributed** among Trade Token (TRT) holders.

Introduction

There are many requirements for a cryptocurrency exchange to be functional, most importantly: capital deposits and withdraw, order books, the exchange itself, and security. A truly decentralized exchange (DEX), must implement all these functions in a decentralized way. In regular exchanges, all these functions are centralized. Further, capital transfer is especially controlled, due to KYC (Know Your Customer) and AML (Anti-Money Laundering) regulations.

Currently there are many web-sites, platforms, and blockchains claiming to implement a DEX. However, most do not support capital deposits of conventional fiat money. Most only support single-chain atomic swaps (for instance the exchange of Ethereum-based tokens) and a few support cross-chain swaps. While cross-chain swaps will probably be essential in the future, they are impossible for conventional fiat money. Furthermore, these swaps have several requirements, hindering its application for many pairs (chains must have a common hash algorithm, hashed timelock contracts or smart contracts, etc.).

In this document the BTDEX exchange method is explained. With this method there is no need for KYC, name, ID, registry, or email. It is available in all jurisdictions, there is no central website or server. You keep custody of your funds in your own smart contract, all automated in a simple user interface. Actually, it implements a unique non-custodial exchange method for cryptocurrencies and conventional fiat money based on BlockTalk Smart Contracts and Burstcoin on-chain encrypted messages.

Cross-chain and fiat money exchange method

BTDEX implements a decentralized exchange method for cross-chain and conventional fiat money based on BlockTalk smart contracts and Burstcoin on-chain encrypted messages.

Taking as an example the exchange of BURST for USD:

1. Seller creates a smart contract holding the BURST amount being sold along with a security deposit.
2. Buyer takes the offer by also sending a security deposit to the smart contract.

3. Buyer receives an encrypted message with the bank account details to transfer USD.
4. Seller notifies the contract informing the USD amount was received and the contract automatically releases the funds, security deposits, and pays the fees.

Mediators, chosen randomly for each contract among the list of valid mediators for the specific market, help to determine the solution for occasional trade disputes. The party not following the protocol can lose the security deposit. Mediators have no control over the smart contract unless a dispute is open. During a dispute, the involved parties can agree on partial or full refunds. If there is no agreement, the mediator will have to intervene. In this case, mediator decisions are based on on-chain information and cryptographically secure submitted evidence or by more traditional methods if the former is impossible. However, it is expected that the vast majority of trades end without dispute or the parties can agree on refund terms.

The BTDEX client automatically creates and interacts with smart contracts. It also checks if the contract code of each trade is valid and if the mediators are accepted. Only valid offers are actually shown to the end user.

Besides cross-chain and conventional fiat exchange, BTDEX also supports the exchange of Burst-based tokens by atomic swap. For this case, there is no need for the mediation and there are no trading fees.

Trading fees

There are **no trading fees when exchanging Tokens for BURST**. This is accomplished by atomic swap (same-chain) and only (very small) transaction fees apply in this case.

When using BTDEX for cross-chain exchange and fiat money exchange, there are also **no trade fees for offer makers** and **only 0.25 % trading fees for offer takers**. Besides paying no fees, offer makers are rewarded with Trade Tokens (TRT).

The 0.25% fees paid by offer takers are collected in BURST and are distributed monthly among Trade Token (TRT) holders.

Trade Token (TRT)

Trade Token (TRT) is a new token with a unique distribution mechanism: **trade rewards**. For every finished BTDEX cross-chain or fiat trade, **offer makers are rewarded** with TRT in an amount numerically equal to the taker fee (0.25 %). Mediators receive the same amount, providing a return for assisting users and improving the system. TRT trade rewards are distributed weekly. Network transaction fees as well as smart contract fees apply for both offer

makers and takers. If CIP20 is activated, these smart contract fees will be reduced by a factor exceeding 100.

With this model, offer makers have negative trading fees since there is no trade fee for placing offers and there is a reward of 0.25% in TRT. This way, the amount of TRT awarded to offer makers is exactly the amount of BURST offer takers pay as trading fees. This one to one relation between paid fees in BURST and TRT rewards to offer makers might keep TRT and BURST near parity. TRT and BURST total supply are also the same: 2'158'812'800. However, TRT will initially be massively more scarce, since BURST already has more than 95 % of its total supply circulating and TRT will be slowly put in circulation through trades.

Every TRT holder is entitled to BURST trading fees monthly, coming from the 0.25 % fees paid in BURST by offer takers. The amount received is proportional to the TRT amount held. However, BURST payments only take place if the due value is 10 times higher than the current standard BURST transaction fee.

TRT holders can always choose to either sell their TRT or keep them to receive the monthly BURST dividends. One can also choose to buy circulating TRT, expecting it to rise in price or interested in the monthly earnings from trading fees. There are **no trading fees nor trade rewards** when exchanging TRT (or any other Burst-based token) for BURST, only network fees apply for this atomic swap.

TRT trade rewards are no longer distributed once all 2'158'812'800 tokens are put in circulation. However, the distribution of BURST fees to TRT holders lasts forever or as long as trades are processed via the DEX.

Security

The BTDEX reference client as well as the cross-chain/fiat smart contract are open source. Both are written in Java, made possible by the BlockTalk platform. Source codes are available at https://github.com/btdex. Users can freely inspect the source code as well as suggest improvements. Other teams or individuals can also implement other clients. Further, those more strict about security can compile the BTDEX client source code themselves.

The smart contract code and security deposits are the first layer of security. The BTDEX client always checks the actual smart contract code of each offer; only contract codes with a perfect match are accepted. Contract current balance and other internal variables are also checked to make sure the offer is valid. If any of these tests fail the offer is not shown to the end user and cannot be taken.

Security deposits are refunded when the trade is complete. Buyers are motivated to actually make the fiat/crypto deposit, otherwise they would lose their security deposit. Sellers are

motivated to signal the contract release, otherwise they might lose their security deposit. If there is an issue in any of these steps the parties open a dispute process and are assisted by a mediator. If the parties agree on terms of partial or full refunds the trade is closed. In the rare case of non-cooperating parties, a mediator has to intervene. In these cases, the party not respecting the protocol can lose the security deposit, taken as fee to be distributed to TRT holders.

In order to prevent collusion between mediators and traders, mediators must hold a large amount of TRT. As a medium term goal, this amount will actually be locked into a DAO smart contract. Then, misbehaving mediators can lose their TRT, having it confiscated by vote if found to be dishonest. Confiscated amounts are used to repair any potential damage. Initially, mediators must have at least one million TRT available to be locked. BTDEX clients constantly check and automatically refuse mediators with less than this amount on their accounts.

Special Offers with No-Deposit for Buyers

Users of decentralized exchanges often encounter various barriers to entry. For example, when using the exchange method described above, a buyer would have to make a security deposit in order to take a sell offer. This deposit is designed to protect the seller, but adds difficulty for those buyers who may not have the required BURST to make the security deposit. This problem is solved on BTDEX by offering buyers an alternative *no-deposit* exchange method.

No-deposit offers work slightly different from the usual offers explained above. Taking for example a no-deposit offer selling 1’000 BURST for USD:

1. A seller creates a no-deposit smart contract holding 10’000 BURST (which will be shown as a special sell offer of 1’000 BURST not requiring buyer security deposits).
2. A buyer takes the offer by sending a message to the smart contract (costing as low as 0.00735 BURST).
3. The BTDEX client on the seller side will see the message on the blockchain and will send to the buyer an encrypted message with the bank account details to transfer the USD.
4. The seller checks for the deposit and signals it was received. After this positive signal, the BTDEX seller client sends the 1’000 BURST to the buyer account and the trade is finished.

Again, all steps are handled by the BTDEX client user interface. The main difference from usual trades is that a single no-deposit smart contract can be used indefinitely by the seller. The BTDEX client checks how many buy orders are still open and only lists special no-deposit orders for which less than 80% of its amount is currently being traded. As usual, in case of disputes the mediation system takes place. A seller of a special no-deposit offer cannot withdraw the funds if a dispute is open. Further, the seller of these special offers can only withdraw their funds after 72 h due to a time lock programmed in the smart contract. Buy offers

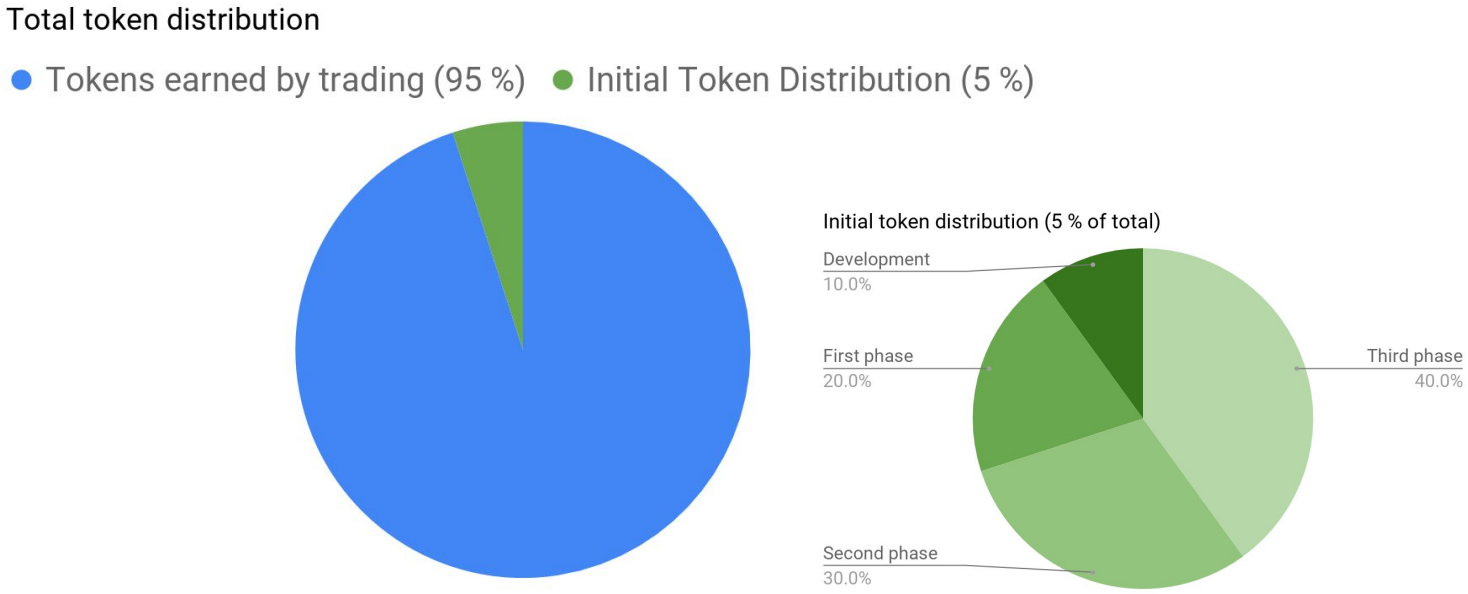
registered on the blockchain but not paid by the buyers are automatically disregarded by the BTDEX client after 48 h.

Regarding fees, **no-deposit sell trades are feeless for both offer makers and takers**, only small transaction fees apply to send the messages. There is a one time 1% fee for offer makers when they withdraw the funds from a special no-deposit smart contract. Similarly to usual trades, this 1% BURST fee is also compensated with the same amount in TRT for the offer maker and mediators.

TRT Initial distribution

Regarding the requirement for mediators to hold a large amount of TRT: one can only hold or lock a large amount of TRT if there is enough in circulation. The issue is, TRT is distributed along trades which in turn require mediators. In order to solve this infinite regress dilemma, a small fraction of the total supply needs to be distributed before the mediation system becomes operational. After that, all remaining TRT will be distributed as trading rewards. Initially, mediators must have at least one million TRT available to be locked.

Initial token distribution will amount to 5% of total supply, as follows:



Initial token distribution will consist of 4 parts:

1. 10% (0.5 % of total) development fund 10’794’064 TRT
2. 20% (1.0 % of total) first phase 21’588’128 TRT
3. 30% (1.5 % of total) second phase 32’382’192 TRT
4. 40% (2.0 % of total) third phase 43’176’256 TRT

Thus, the total amount of tokens distributed in open market is 97'146'576 TRT. This creates the possibility to have up to 97 BTDEX mediators right after the initial distribution. However, before the DAO smart contract is implemented, only contributors of the project would be eligible to be mediators.

The development fund will be controlled by the founding team and used for future project needs. The first phase of initial token distribution (ITD) will be sold in open market as a sell order with a price of 0.1 BURST each. This sell order will be placed only after public announcement. Everyone can participate in this ITD, no KYC or registration is needed, just download and run the BTDEX client. After the first phase is finished, the second phase takes place under the same terms, but TRT token price will be 0.2 BURST. After all second phase tokens are sold the third (and last) phase starts, with a price of 0.3 BURST.

Short-Term Roadmap

1. Cross-chain/fiat exchange smart contract initial design 2019 Q3✔
2. BTDEX reference client implementing a wallet and token exchange 2019 Q4✔
3. Private tests on testnet 2019 Q4✔
4. Alpha release on testnet for the general public with GPL3 source code 2019 Q4✔
5. Main net release and TRT initial distribution 2020 Q1
6. Cross-chain exchange for main cryptocurrencies (BTC, LTC, ETH, XMR) 2020 Q2
7. Conventional fiat money markets (USD, EUR, BRL) 2020 Q3
8. Add more cryptocurrencies and conventional fiat money exchange 2020 Q4

Long-Term

Ideally, all trades should be accomplished by atomic-swaps. In this case there is no need for a mediation system. However, cross-chain atomic swaps have several requirements on both chains (they must have a common hash algorithm, hashed timelock contracts, smart contracts, etc.) and are impossible with conventional fiat money. Further, they require off-chain communication between peers, multi-chain wallets, etc.

In the long-term, as adoption of cryptocurrencies and/or stable coins advances, the BTDEX client will introduce cross-chain atomic swaps. As more atomic swaps are included, the mediation system becomes less important. As a consequence, there will be a gradual reduction in TRT trade rewards as only offer makers will still receive the rewards, not mediators. However, even with cross-chain atomic swaps, trades still need to wait for block confirmations. In order to fix this, lightning network (or side chain) methods should be pursued.

Founding team

Developers

Ohager - “code punk”, BAT member, leaning to front-end.
JJos - “master of smart contracts”, BAT member, creator of BlockTalk (Burst smart contract compiler), leaning to back-end.

Public relations

FrankTheTank - BMF founder, DEX enthusiast
Shefas - BMF member, BlockPlay founder.
Ryanw - BMF member

Disclaimer

BTDEX is not a company or organization, it is a software package with source code available under GLP3 license. As such, it is provided with no warranty. BTDEX founding team (hereafter just team) provides only software and is not responsible for trades that occur in the decentralized exchange or mediators activity. TRT and BURST are not based on any physical commodity or any government-issued currency, so the team is not responsible for their price. Every BTDEX user is responsible for his decisions and it is a user's responsibility to pay taxes or comply with local regulations. Every blockchain transaction is final and cannot be reverted or changed by the team or any other party.