NebliDex

The World’s First Neblio Blockchain Decentralized Exchange

Last Updated:May 26th 2019

Background

NebliDex is a novel cryptocurrency exchange powered by the Neblio blockchain and with support of the NTP1 protocol. This exchange allows users to trade NEBL for other cryptocurrencies on other blockchains via a trust-less platform and in an automated fashion. Unlike traditional centralized platforms such as Binance and Kucoin, NebliDex is decentralized which means there are no central servers that hold on to your NEBL. You retain full control of your wallet at all times. Cryptocurrency exchanges are required to buy and sell NEBL to other users. While direct sale is possible, it engenders risk as one party may fail to deliver their part of a transaction and because most cryptocurrency transactions are irreversible, a significant loss of funds for the other party may result. Exchanges serve as the third party mediator that removes most of this risk and allow users to trade with many other parties in one place.

Why Decentralized?

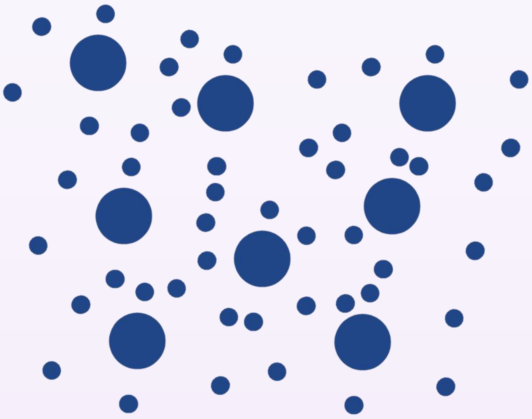
Decentralized exchanges represent a shift in the current cryptocurrency sale market. While the bulk of cryptocurrency transactions take place on centralized exchanges, these type of exchanges are falling out of favor due to major limitations:

- The account owner does not possess the private keys for the coins in his/her account.
- If the exchange goes down, there is no way to move funds out of the account wallet due to the reason above.
- The exchange owner can impose and enforce actions that may lock out funds and slow down trading.
- Centralized exchanges are major targets for hackers and funds have been stolen and will probably be stolen in the future.
- DDOS attacks can cripple an exchange and bring trading to a halt.
- The exchange owner can charge whatever he/she wants for trading fees and you must pay it to continue trading.

As you can imagine, with decentralized exchanges, you do not have to deal with the pitfalls mentioned above; however, there are issues with decentralized exchanges currently that limit their use such as low volumes, non-intuitive user interfaces, manual and slow trades and dealing with arbitrators. NebliDex is designed to address these issues. NebliDex is created to provide traders with a centralized feeling but via a decentralized system. This allows its users to:

- Trade without concern for downtime and fear of losing your wallet and coins.
- Create buy or sell orders that can be filled automatically when manually matched.
- Perform a market trade that is executed automatically and quickly via an automated counter-party between traders.
- Avoid waiting for someone else to clear the payment and avoid getting human mediators and arbitrators involved.
- Have peace of mind knowing that even the order book and the charts are decentralized so there is no downtime if a website goes off-line.
- Utilize cutting edge atomic swap trading technology.

How it Works



A graphical display of the decentralized system based on a Critical Node and Trader Node model.

The NebliDex cryptocurrency exchange is composed of two types of nodes: The Trader Node (TN) and the Critical Node (CN). These nodes interact with each other to make trades on the platform work quickly and automatically. The TN comprises most of the platform as any person who downloads the NebliDex client software will become a TN by default. CNs, by the name implies, are critical for the function and operation of the decentralized exchange. Not every person who downloads the client software can become a CN. The requirement for becoming a CN is to possess a certain amount of NebliDex proprietary platform tokens which will be discussed further down. Individuals who are CNs can also trade like a TN but not at the same time.

Here is a breakdown of what a Trader Node can do:

- Trade freely on the platform with others.
- Create buy and sell orders that are broadcast across the NebliDex.
- Perform market trades with other users.
- Get a list of all CNs from a DNS seed or a CN.

Here is a breakdown of what a Critical Node can do:

- Everything a Trader Node can do.
- Validate transactions from Trader Nodes.
- Serve as a counter-party for both the buyer and the seller. This is done automatically without human intervention.
- Broadcast transactions to the corresponding blockchain for permanent entry.
- Transmit a list of all the CNs to a TN that is requesting it.
- Transmit market data to a TN such as the order book and chart information.

Creating Buy And Sell Orders on NebliDex:

When a person is creating a buy or sell order from a TN, that information is broadcasted to a randomly selected CN that will rebroadcast that information to all its linked TNs and all its linked CNs so that every node on the exchange knows about the existence of the order. The rebroadcasting will stop once the CN confirms that every linked node is already aware of the order. TNs do not rebroadcast orders.

Making Market Trades on NebliDex:

When a person (Person A) sees an order that they would like to fill (ie. He/she wants to purchase 20 Neblio from a person selling it for 1 LTC) from Person B, a request will be sent to a randomly selected CN that will forward this request to Person B by broadcasting to other CNs. Person B will receive this request and either confirm or reject the trade request.

Once Person B accepts the request, either Person A or Person B will query a randomly selected CN for information on a CN that can be used for transaction validation. The CN will use a modified weighted average algorithm (fig.A) to find a CN that can be used for transaction validation and transmit this information indirectly to Person A. Person A will create an atomic swap contract to Person B, a signed fee transaction to the validator, and a signed payment transaction to the contract then transmit this information to the validating CN. The CN will confirm the validity of the contract and its fee funds before forwarding contract information to Person B. When Person B receives the validating CN information, he/she creates a duplicate contract to confirm its authenticity and then create its own atomic swap contract and signed fee transaction to the validator that is forwarded to the CN. The CN will confirm the validity of the contract and its fee funds before forwarding contract information to Person A. When Person A receives Person B's contract, Person A will then duplicate the contract to check its authenticity then inform the validating CN that is approves it. At this point, the validating CN will broadcast the fee transactions from Person A and Person B and broadcast the payment transaction from Person A. At this point, the work of the validator is done and the validator is paid for relaying important trade information. The traders will then monitor their respective contracts for spending transactions. Once Person B confirms the correct balance (including blockchain fees) in Person A's contract, Person B will submit payment to its contract. When Person A confirms the correct balance in Person B's contract, Person A redeems the balance from Person B's contract and in the process, reveals a secret for unlocking its own contract. Person B sees the spending transaction, extracts the secret then redeems the balance from Person A's contract thus completing the trade. This process in its entirety is automated and depending on the blockchain's block rates, can be relatively quick to complete without any human intervention.

Fig. A

$$Validating\_Chance\_Percentage = \left(0.5 \times \frac{1}{Total\_Network\_Nodes} + 0.5 \times \frac{My\_NDEX}{Total\_Network\_NDEX}\right) \times 100$$

New validator selection formula

What is a NebliDex platform token?

NebliDex has its own token that is used on the platform by both TNs and CNs and its function is critical to the operation of NebliDex. This token is called the **NebliDex token** (symbol: NDEX) and is built on the Neblio blockchain using NTP1 (Neblio Token Protocol 1). There is a limited supply of these tokens and the full amount will be distributed to interested parties prior to the platform launch. NebliDex tokens are used by the NebliDex exchange to determine who can be a Critical Node. They are also used by NebliDex to complete a trade. Critical Nodes must have a certain amount of NebliDex tokens in their wallet in order to be considered a CN. As mentioned earlier, part of a CNs job is to validate transactions. For each validation, a CN is rewarded with a certain amount of NebliDex tokens from both the buyer and the seller for facilitating the transaction. CNs with a higher number of tokens have a higher chance of being chosen for transaction validation by the TNs. TNs are required to have a few NebliDex tokens in their wallets before asking for a trade (with the exception of the NDEX/NEBL pair in which only the seller is required to hold the token). This reward method incentivises the CN to validate a transaction. NebliDex tokens will be available for purchase prior to launch at a discounted rate. After launch, NebliDex tokens can be purchased on the platform at market rate and possibly on other exchanges as well.

Supported Currency Pairs

NebliDex currently supports the following currency pairs:

- NEBL/LTC
- NEBL/BTC
- NDEX/NEBL
- NDEX/BTC
- NDEX/LTC
- TRIF/NEBL
- NTD/NEBL

- TGL/NEBL
- NCC/NEBL
- NAUTO/NEBL
- IMBA/NEBL

More pairs will be added as the platform grows.

Technical Description for a New User Account

This is a technical description of how the platform will function for a new user to NebliDex broken down into steps.

1. A new user downloads the client application from the official NebliDex website. Initially, the application will be designed in C# for the Windows platform but will be ported to MacOS and Linux eventually. Currently, NebliDex exists on Windows, Mac and Linux. The zip file will contain the application and any accessory files. There are no install files or files to compile. Alternatively, the user can opt to compile the source code directly to run.
2. When the application is opened for the first time, three wallets are created. One for each currency. Each of these wallets will have HD master key in which addresses will be created from. The wallets can be saved to a backup file if desired. NebliDex tokens are stored in the Neblio wallet.
3. The client will first need to find Critical Nodes in order to download the order sheet and the charts. It will first use a DNS seed to obtain a list of all the CNs. This can be manually altered to another DNS seed website or a direct IP address to a CN can be selected as well.
4. Once the client obtains a list of all CNs, it will query multiple CNs for a list of all the CNs and using consensus model, it will pick the list that is most prevalent. In theory, they should all be the same. This list will be saved to the computer for future use. The client will then select a random CN to obtain information about the platform, such as open orders, chart information and recently completed trades. If a particular CN is down, the

client will remove the CN from its list and try another CN until all the CNs are down, at which point it will report system down.

5. Once the client receives trade information from the CN, the CN will share platform information with the client as long as the client sends a “keep-alive” ping every minute. Without this ping, the CN will assume the client has disconnected and stop sending it messages. The “keep-alive” ping contains information about the client as well. If the client tries to ping and is unsuccessful, it will remove that CN from its list and attempt to connect to another CN.
6. Before trades can be made, the user must fund his/her NebliDex account. Once funded, the user can start trading. In order to create an order, the user will need to go to the desired pair and create a sell or buy order at a certain price point and the amount. The order will be broadcasted across the network with an order specific ID hash that represents the order. The CN used to connect to the network is the first broadcast; however, if this CN goes down, the client will try another CN on the network and use that one as its default. The CN will first validate the order to make sure that the user does in fact have spendable funds, then it will rebroadcast this order to all its connected TNs and to all the CNs. In a short time, everyone on the network will be aware of this order. The same process happens when the order is canceled. The order is stored on the CNs order database until it is filled.
7. Open orders can sit on the market for an indefinite period of time. The only requirement is that the user keeps the client open during this time otherwise the order will automatically close if the CN does not receive the ping. The client will be designed to run in the background if the user wants to minimize it.
8. When another person decides to fill your order, that person will contact a CN to make the request. Partial fills are allowed by the system. That process will be carried out as mentioned earlier in this document until the order is completed. When a CN validates a transaction, it will look directly at blockchain to determine whether a specific address can spend funds.

9. Once this process is completed, a client is free to trade again or withdraw funds from NebliDex.
10. Any client has the ability to become a Critical Node once there are a certain number of NebliDex tokens in the Neblio wallet. Becoming a CN is as easy as selecting an option in the menu. When this request is made, a signed message with your public key is broadcasted to all the CNs. The other CNs will validate this message against your address to make sure you are the address owner and check it in the Neblio blockchain to make sure you have a sufficient amount of NebliDex tokens. If you meet the criteria, you will be added to a list of CNs. An important point to remember is that you cannot validate your own transactions. The other CNs will prevent you. You also cannot trade while in CN mode.

Attack Vectors & Mitigation Methods

To address potential concerns with using this platform, here is a list of possible attack vectors from a malicious user or users and ways that the NebliDex system prevents these attacks.

A malicious user signs a transaction that doesn't have enough unspent TXOUTS and sends it to the CN to be validated.

As mentioned earlier, before a transaction is broadcasted unto the blockchain, the CN will decode the transaction received and check the address to make sure it has enough unspent TXOUTs to complete this transaction. The TXOUTS must have more than a certain amount of confirmations on the blockchain as well in order to be spent. The CN will also verify that the to address matches the other party's receive address. In addition, because of the use of atomic swaps, it will not be possible to spoof balances that do not exist.

A malicious user tries to double spend by requesting more than one trade simultaneously.

This will cause two different CNs to request signed transactions from an order creator. When a CN receives an order request, it broadcasts that status to all the CNs in NebliDex as a pending order being filled. When the next CN begins to validate the order and sees more than one pending order being filled with the same request address, it will cancel the order and place that request address in a cool-down period that prevents trading for a period of time. Any other order processed during this cool-down period for this request address will be automatically canceled.

A malicious user acquires a Critical Node and breaks the NebliDex protocol with modified code.

Due to the requirements of becoming a CN on the NebliDex exchange, it would be disadvantageous for a malicious user to attempt to break the exchange. Since this platform is based on the assumption that CNs follow protocol, a loss of trust will directly result in a loss of value for the platform token NDEX. The malicious user will only in the long run lose money by altering the platform if it behaves in a way that is unexpected. NebliDex is designed not to depend too much on one specific CN as CN selection is random. In addition, because there are no custodial accounts due to the use of atomic swaps, it is not possible for a malicious CN to steal funds. The requirements to become a CN would be too burdensome for most malicious users.

A malicious user tries to spoof themself as a CN to other TNs.

Every message received by a CN is checked against a list of authorized CNs before it is processed. TNs also do not have a means of communicating with each other as all messages must go through a CN and TNs cannot accept inbound connections.

A malicious user attempts to spam the network with repeated calls and slow it to a crawl.

CNs will employ throttling to limit the effectiveness of a spam attack.

A malicious user attempts to overflow the network with multiple connections to a particular CN.
CNs limit the amount of connections per IP address to mitigate this vector.

A malicious user monitors my local network and intercepts my signed transaction then broadcasts it before it gets to the CN.
Transaction messages from TNs to CNs are encrypted in a way that they can only be decrypted by the CN.

A malicious user tries to cancel a transaction by broadcasting another transaction to the blockchain with a higher fee to themself after sending the transaction to the CN.
This is a hard to prevent attack vector is eliminated with the use of HTLC (hash time-locked contract) atomic swaps.

How can I get involved?

Become a Critical Node when the platform opens! Get NebliDex tokens and become a part of the NebliDex decentralized cryptocurrency exchange. NebliDex is the world's first exchange for the Neblio blockchain and is designed to rival some of the best centralized exchanges without risk for fund loss.

Token Distribution Information

NebliDex tokens (NDEX) are crucial to the liquidity and function of the NebliDex. There was a combination of an airdrop (token giveaway) and a token sale for the initial distribution of NDEX tokens. This created the market and the initial Critical Nodes. The airdrop and the token sale has been completed and the results of the token sale are available at NebliDex.xyz

Total Tokens Created:	105,000,000 NDEX
Dev Team:	5,000,000 NDEX
Airdrop:	1,000,000 NDEX
Token Sale:	99,000,000 NDEX*
Price Per NDEX:	0.005 NEBL

*The top 25 buyers during the token sale received an additional 25% of what they bought. 10% of the unsold tokens will be retained by the Dev Team to maintain market liquidity and all remaining tokens after that will be distributed proportionally among all buyers in the token sale. For example, if a buyer’s purchase and bonus, if eligible, accounts for 5% of all tokens sold, that person will receive 5% of all unsold tokens remaining if there are any. To be clear, the top 25 bonus counts towards the percentage bought.

Restrictions: There was a hard cap of 1,500,000 NDEX tokens per person during the token sale and citizens of certain countries were not allowed to participate (including major markets: USA, South Korea and China) due to country restrictions. Each buyer was subject to KYC (Know-Your-Customer) requirements and was prepared to present documentation confirming his/her identity in order to receive his/her tokens.