DiffEx: Smart Contract Based Platform for ERC20 Options Contracts

Author: DiffEx Developers

support@diffex.io

May 1 2021

1 Abstract

DiffEx is a DApp (Decentralized Application) platform for writing, buying, selling, and executing options contracts for ERC20 tokens. Each options contract is either a covered call, or an Ether secured put. Each contract also has a strike price (the price per underlying token paid on execution denominated in Ether) and expiry (block number after which the option cannot be executed). The DiffEx smart contract handles balances, option writing and execution, as well as order execution. When DiffEx is launched on the mainnet, the DFX token will be able to be staked to reduce fees paid per transaction.

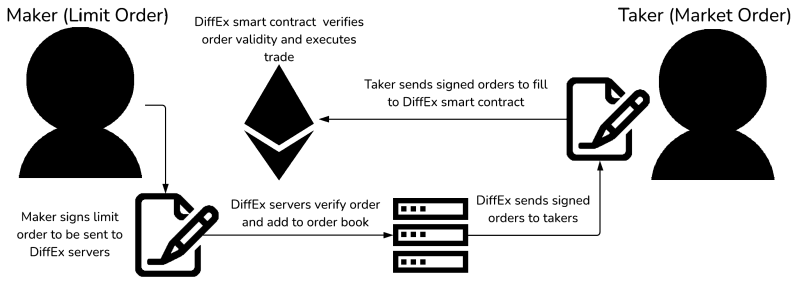
2 Introduction

In the ever-expanding world of decentralized finance and smart contract token exchanges, there is a notable lack of a decentralized options exchange for ERC20 tokens. DiffEx seeks to fill that void by offering a way for users and institutions alike to hedge their positions in ERC20 tokens and Ether, increase exposure, and earn passive income on their holdings. DiffEx accomplishes this by allowing users to create, sell, buy, and execute call and put options for ERC20 tokens, all through a decentralized smart contract. A call option gives the holder the ability to buy 100 of the underlying ERC20 token from the option writer at the strike price. A put option gives the holder the ability to sell 100 of the underlying ERC20 token to the option writer at the strike price. To write a covered call, the writer must have 100 of the underlying ERC20 token, and for an Ether secured put the writer must have 100 * strike price Ether. After writing, the writer can sell these options on the DiffEx exchange to a buyer, who can then execute the option any time before the expiration block.

3 Technical Overview

DiffEx works by storing all trading logic and balances state in an Ethereum smart contract, along with an off-chain orderbook for decreased trading costs

and increased speed. When a user wishes to deposit or withdraw Ether or ERC20 tokens, write or execute an option, or execute a market order, they must call the smart contract. To post a limit order, the DiffEx API must be given the order's hash, signed with the private key of the market maker. To fill an order from the order book, the taker sends the signed order to the smart contract, which then verifies the order's validity and executes the order.



4 Utility Token

To fund further development and liquidity for DiffEx, a utility fee token may be created. The contract will allow the token to be staked, reducing the fees paid by traders proportional to the amount staked and the time it has been staked for.

5 Conclusion

Options contracts are an integral part of the financial industry outside of cryptocurrency, and there is currently no smart contract-based solution to trade options contracts for ERC20 tokens. Because of this, DiffEx could provide significant utility to retail and institutional cryptocurrency owners and traders.