Options on Decentralised Exchange - Implementation and Analysis

December 7, 2021

Abstract

The concept of centralised exchange ("CEX") has been around for many years, but as technology develops, more and more drawbacks of CEX get exposed. The presence of a central authority that controls the flow of transactions presents significant risks. For instance, it lacks transparency, may have problems with liquidity when filling large orders or can become the target of a cyberattack since it acts as the only node confirming the deals between market participants. A decentralised exchange ("DEX") can mitigate the risks that come with CEX, but it is new to the financial sector and lacks the variety of financial instruments. Therefore, in this paper, we would like to introduce how one of the major financial instruments, options, can be implemented on DEX and what it means for the ERC-20 token trading.

Contents

1 Introduction to Option Trading on CEX and DEX

Many traders wish to make more complex financial operations such as futures and options. According to the CryptoCompare exchange review, the derivative market represented 57.8% of the total volume in October 2021 [3]. Figure 1 demonstrates how the monthly volumes have increased. DEX represents a small proportion of the overall market. The most popular CEX Binance 24 hour volume is $98,792,947,271 (0:40 6 December) which is 34 times higher compared with the most popular DEX Uniswap V3 ($2,892,747,385) [4]. Similar situation in the derivative market.

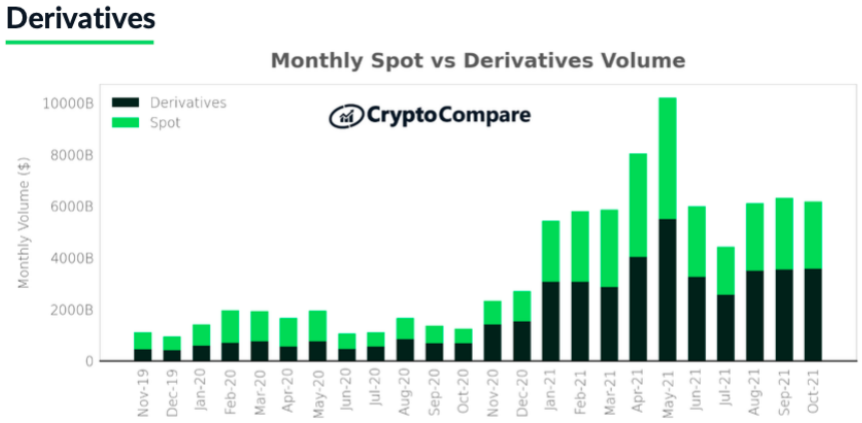

Figure 1: Monthly Volumes

DEXs have several advantages over CEXs such as privacy and anonymity. DEX does not have KYC (Know Your Customer) policies and the trader only needs to connect the wallet and sign a transaction, which means that no personal information is stored and therefore it cannot be stolen. In addition there is no verification process for listing so any ERC-20 tokens can be traded.

There are some downsides such as low liquidity which can be solved by using Automated Market Maker (AMM). However, AMMs are often accompanied by high slippage and divergence losses especially for high volumes traded [1]. Other DEX disadvantages are lower efficiency due to scalability issues and possible security issues related to smart contracts [2]. We will expand on the notion of smart contract risks in section 3.4.

In the first 20 derivative exchanges by trade volume in BTC over 24 hours, representing 98,4%, there is only 1 DEX [5].

Name	**Open interest BTC**	**Trade volume 24h BTC**	**Number of perpetual pairs**	**Number of futures pairs and CEX/DEX**	**DEX or CEX**
Binance	186,614	1,457,909	168	54	CEX
Prime XBT	80,169	956,111	21	-	CEX
OKEx	80,930	450,898	163	1,888	CEX
FTX	148,174	311,677	172	627	CEX
CoinTiger	-	230,370	62	-	CEX
CoinFLEX	8,100	155,221	31	29	CEX
Bybit	65,119	148,400	92	4	CEX
Huobi	18,183	112,040	198	56	CEX
Bitget	56,920	96,098	34	-	CEX
Hopex	20,122	70,907	11	-	CEX
Phemex	22,259	62,460	40	-	CEX
KuCoin	32,667	56,983	79	8	CEX
Gate.io	42,429	55,452	199	-	CEX
Bitforex	2,784	50,454	13	-	CEX
dYdX	19,042	**40,209**	**28**	**-**	**DEX**
BTSE	18,518	26,377	15	141	CEX
Deribit	34,654	26,312	2	105	CEX
BigONE	106	25,101	8	-	CEX
AAX	3,533	24,206	16	-	CEX
BitMEX	13,838	23,306	40	89	CEX

Table 1: Exchange Volume list 5-6 December

The biggest DEX by volume is dYdX, and it does not have options available on its platform for users to trade. In general the volume of options traded on DEXs is significantly smaller than the volume of options traded on CEXs. For example, $586,475,000 is the total cumulative options trading volume in Hegic since February 20, 2020 [6].

DEX	**Option Type**	**Cash/Physical settlement**	**Collateralision**
Opyn V2 [7]	European options	Cash settled	Partially collateralised
Hegic [6]	American options	cash-settled	Fully collateralised
Siren [8]	American options	Physical settlement	Fully collateralised

Table 2: Comparing DEX

Table 2 compares three popular DEXs to trade options. DEX users are usually required to post 100%(fully collateralised) of the maximum loss as collateral. In contrast, CEX users only need to collateral a small fraction, which

is another limitation and the possible explanation why the volumes are so low [9].

2 Key Potential with DEX

The crypto market is currently in a stage where new tokens are introduced daily. It is frequently challenging to distinguish tokens with profit potential from tokens without one or tokens designed with malicious intent. Since the Ethereum blockchain enabled the creation of ERC-20 tokens via smart contracts, it has become even more difficult for investors to find value without taking significant risks.

Furthermore, most tokens are traded on DEXs, making it an ideal marketplace for introducing options. The options will be ERC-20 tokenised smart contracts that function as a derivative of the underlying token. The availability of such an instrument will attract more risk-averse investors who will be able to hedge their risks. In contrast, risk-tolerant investors will have a financial instrument with high volatility that will allow for high-risk-high-reward trading.

3 Option Smart Contract Implementation based on dYdX and Chainlink methods

We explored the implementation of two different approaches for DEX Options:

1. Chainlink using their price feed [23]
2. dYdX using 0x exchange and custom proxy authentication [10][11]

Our prototypes focused solely on the options blockchain functionalities (write, buy, exercise, retrieve and cancel) and thus isolated the Chainlink price feed, 0x exchange and proxy. Moreover, we reused our ERC-20 token implementation as the underlying asset and used ether payments as the base token for the sake of making both implementations more coherent and easier to compare. An American covered option approach was followed, meaning that an option can be exercised at any time before expiry and the underlying gets put up as collateral to guarantee that it can be collected at a future date. The implementations follow a "call" option, but "put" can be done simply by switching the underlying and base token and inverting the strike price. A powerful feature is that all values are transferred through the contract without any trusted party.

3.1 Chainlink

When the smart contract is created, an empty list of written options gets initialised.

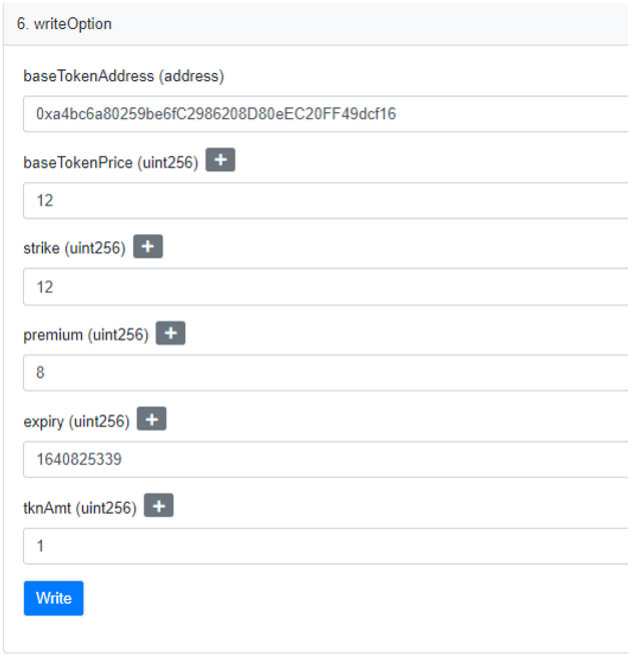

Figure 2: Writer can execute a write call by specifying the underlying token, strike price, premium and expiry. At this point, his underlying asset gets stored as collateral, and the list of options gets populated.

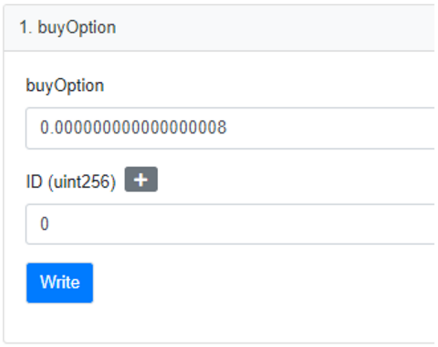

Figure 3: Buyer can see the written option in the list and execute a buy call by specifying the option ID and the premium payment in ether.

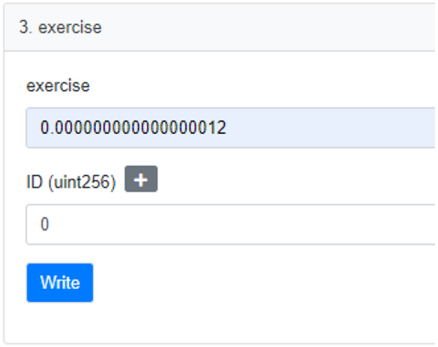

Figure 4: Buyer can do an exercise call to get the underlying token by selecting the option ID and paying the strike price, which gets sent directly to the writer.

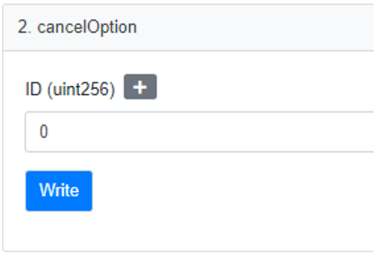

Figure 5: Writer is allowed to cancel his written option at any time if there is no buyer.

Figure 6: Writer is allowed to retrieve his underlying if the option hasn't been exercised before expiry.

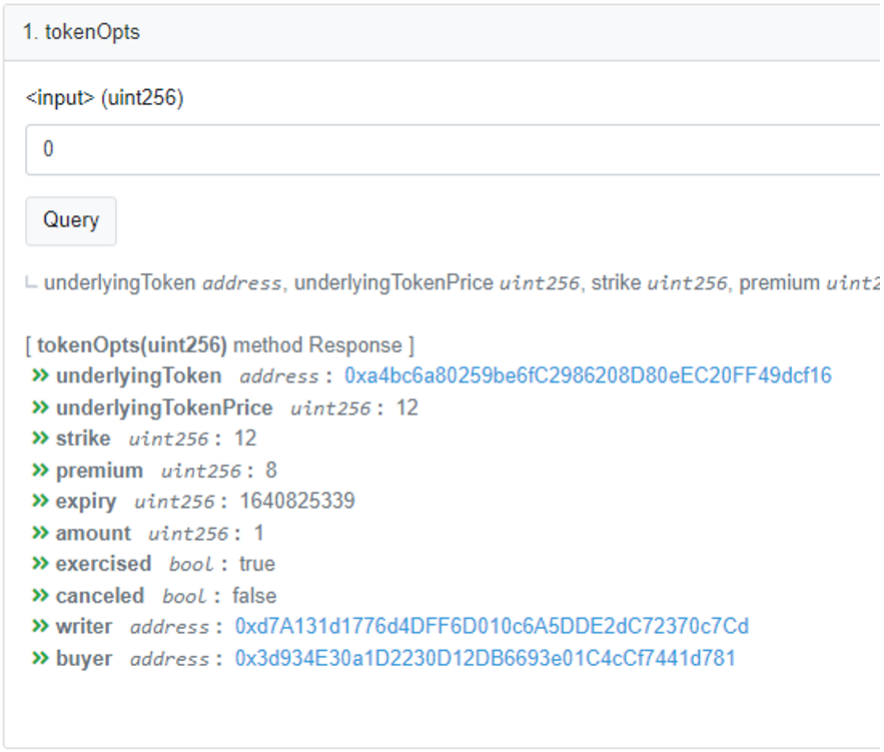

Figure 7: The entries from the option list never get removed as it is an expensive operation. Using a linked list could be an alternative, but we don't get direct access to the options. As a result, we never remove options but rather mark them cancelled or exercised. Thus, trading space for speed and low complexity gives us gas efficiency with O(1) operations.

3.2 dYdX

There are two smart contracts in place – Creator.sol and Options.sol.

Figure 8: Creator.sol is responsible for creating different types of Options.sol. A type refers to a given underlying token, base token, strike price, premium and expiry. Creating a new type can be done by anyone and only opens it up for sale without issuing any options.

Each Options.sol contract is able to issue new options of its type before the expiration date. It also implements the ERC-20 interface to allow issued options to be publicly traded on an exchange.

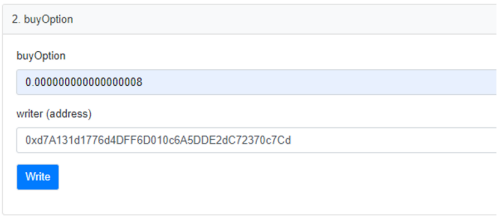

Figure 9: Issuing and buying an option is done in a single transaction. This happens when the buyer makes a buy call with a specified writer. The writer is required to have given approval to the Options.sol address to do transferFrom of his underlying token.

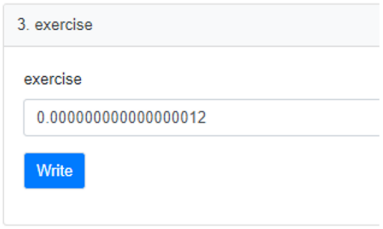

Figure 10: Before the option expires, any buyers can exercise the amount they own by paying the strike price that's globally specified in the deployed Options.sol.

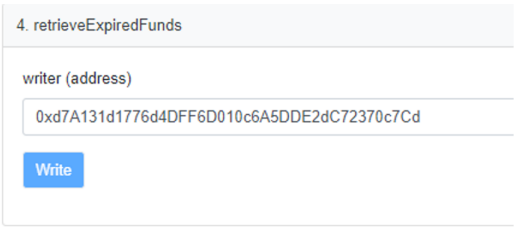

Figure 11: Writers can withdraw a proportion of the underlying and base token held by the deployed Options.sol only after expiration. This process obeys equation (1).

$$\text{Writer Token Return} = \frac{\text{Options Written}}{\text{Total Options Written}} * (\text{Total Tokens Held}) \quad (1)$$

Example:

- 5 writers issue an option to 5 buyers, each giving 1 underlying token for 12 strike price
- 2 buyers exercise the option
- After expiry, Options.sol inventory has 3 underlying and 24 base tokens
- Each writer receives 1/3 underlying and 4 base

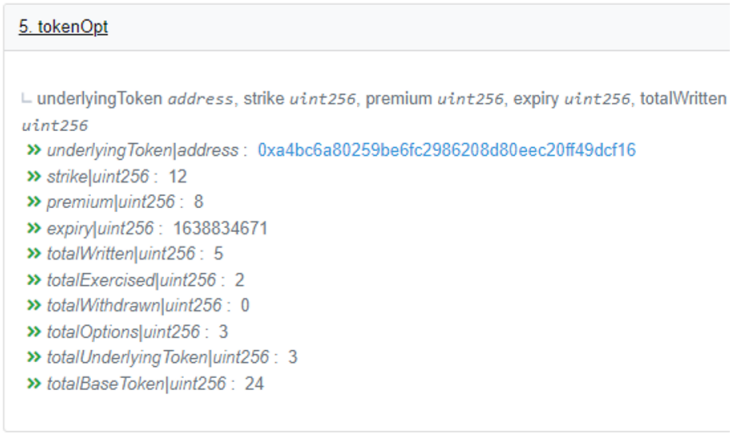

Figure 12: Token Option output for the example above.

3.3 Differences

Chainlink	dYdX
Writer loses his underlying as soon as he writes the option	Writer loses his underlying only when the buyer buys it
Writer and buyer find each other through the smart contract list	Writer and buyer find each other off-chain
Writer receives his funds as soon as the buyer exercises the option	Writer receives his funds as soon as the buyer exercises the option Writer receives his funds only when the option expires
Writer receives the exact amount of ether when his option is exercised	Funds from exercised options are stored in the smart contract pool and are proportionally allocated to all writers after expiry
Options cannot be traded and buyers do not receive the address of the option in their wallet	Every type of option has its own address and can be traded like any ERC-20 token
All options are under one address which could be prone to attacks	Multiple addresses which decreases the chance of corrupting all options

Table 3: Differences between Chainlink and dYdX

3.4 Mechanisms to Avoid Smart Contract Risks and Exploitation on DEX

According to a report in April 2021 by Messari, a research company for the crypto industry, DeFi protocols have lost about $284.9 million to hacks and other exploit attacks since 2019 [12].

There are two critical mechanisms in both dYdX and Chainlink approaches that avoid the exploitation of DEXs.

First, in both dYdX and Chainlink prototypes, we ensure that each option's blockchain functionality (write, buy, exercise, retrieve, or cancel) is executed atomically in a single blockchain transaction. Either all the involved steps happen, or none of them happens. Figure 8 illustrates the on-chain issuance of an option on dYdX.

Second, despite simplifying the option contract prototypes, it is key to highlight how dYdX and Chainlink involve decentralised oracles in broadcasting orders placed across public or private order books. Getting price feed from a single DEX may induce price manipulation due to flash loan attacks [13]. Blockchain oracle mechanisms using a centralised entity to deliver data to a smart contract introduce a single point of failure. If the single oracle goes offline, then the smart contract will not have access to the data required for execution or will execute improperly based on stale data [14].

dYdX leverages a hybrid approach pioneered by 0x protocol [10]. 0x fea-

tures an off-chain relay together with an on-chain settlement [15]. The off-chain relays broadcast orders placed across order books (This is the future work to be completed under Figure 9). Chainlink offers similar off-chain connectivity - Decentralised Oracle Networks (DONs) [16]. It provides a layer offering smart contracts to extensive off-chain computing resources. However, relays would not be able to execute a trade alone. The on-chain smart contract would require the option writer's signature to ensure an order is legitimate to complete the exchange of quote token premium and base token. These hybrid approaches minimise the potential risk of oracle manipulation, and additionally, off-chain relay helps resolve the problems of blockchain bloat and high gas fee on ethereum.

Finally, we are encouraged to conduct further work and research to protect investors by minimising the risks arising from DEXs. Potentials have smart contract code audits by Consensys and Peckshield [17], and smart contract coverage offered by the decentralised insurance industry, Nexus Mutual [18] and Unslashed Finance [19], in the event of a smart contract bug or exploit arising from risk-free arbitrage.

4 Conclusions and Discussions

The work highlighted the value of options trading for investors and compared the differences between centralised and decentralised exchanges. Our theoretical concept aimed to prototype the implementation of option functionalities - write, buy, exercise, retrieve, and cancel, on DEXs. We gave a detailed technical perspective on how an option smart contract function must be completed in a single transaction atomically. The concept provided the basis to implement option smart contracts on dYdX and Chainlink respectively, with future work and research in connection with off-chain decentralized oracles for orders placed across public or private order books.

Moreover, DEXs can be improved by finding the optimum balance between AMM and the order-book approaches by potentially adapting the dYdX hybrid model. Currently, the issues with these are the gas fees and liquidity optimisation. Uniswap V3 attempted to solve both by introducing AMM where liquidity can be provided to increments of the liquidity curve, therefore improving liquidity at the relevant price action. However, it further can be tested how the hybrid approach that consists of systems like Uniswap V3 and order-book can be implemented and optimised.

Additional improvements can be made to mitigate financial risks associated with options on DEX. One will be to construct a volatility model for the underlying token pairs on DEX that considers the liquidity pool mechanism. By constructing such a model, the options can be more accurately priced, further reducing the financial risks associated with mispricing the options. Option exercise mechanisms on DEX is another development area as a secure mechanism must be developed, such as taking collateral or freezing cash at stake, to avoid the default of the underwriter upon option exercise.

Appendices

A Smart Contract Links

- Deployed Chainlink Contract
- Deployed Creator.sol

  getCoveredOption parameters: 0xa4bc6a80259be6fC2986208D80eEC20FF49dcf16, 12, 8, 1638834671
- Deployed Options.sol (already expired)
- Source Code and README file

B Use Cases

B.1 Example 1

Options can be used to provide additional leverage in speculation. For example, suppose the price of TOKEN is 100 wei, and a buyer who has 1000 wei believes it will go up. Buying 10 TOKENs will yield him 100 wei profit (10%) if the price rises to 110. Suppose instead that the buyer had purchased call options with 100 strike and 2 premium. He could afford 500 of these options (1000 wei balance / 2 wei premium). If the price again rose to 110, the buyer can exercise the options which will yield him (10 - 2) * 500 = 4000 wei of return. This shows how with the same amount of capital investors can achieve much larger returns.

B.2 Example 2

Options can also be used to hedge or reduce risk. If an investor is long on 100 TOKENs trading at 100 wei each, the investor could purchase a put option with 90 wei strike for 2 premium. Such an option would ensure that he cannot lose more than 10% with only a 2% fee which is a great risk reduction considering the cryptocurrency volatility.

B.3 Example 3

Another use case would be the employment of options as market oracles of volatility and risk [20]. Similar to the VIX index in traditional finance [21], one can derive the implied volatility of the underlying asset using the Black-Scholes equation with already computed option prices. The options will be an important early warning in DeFi in case their prices start to drastically increase. Further, option prices can be used to assess probability that an asset will reach certain strike prices in a specific time.

B.4 Example 4

Options can also be useful to insure a risk-averse investor who deposits on the Compound platform [20]. After depositing 1 USDC there, the fund owner receives 1 cUSDC contract. The fund owner can earn interest on the cUSDC [22]. He can retrieve his USDC plus interest whenever he chooses, but if an adverse event occurs (e.g hack, flash crash in market value), the cUSDC will not be redeemable for the deposited USDC. The depositor can protect themselves by purchasing a put with underlying cUSDC with strike 0.99 USDC. If USDC drops dramatically, the investor can exercise the option to avoid significant losses.

References

[1] Jiahua Xu, Krzysztof Paruch, Simon Cousaert, Yebo Feng, *SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols*, 2021. Link

[2] Tomas Krupa, Michal Ries, Ivan Kotuliak, Kristian Kostal, *Security Issues of Smart Contracts in Ethereum Platforms*, 2020. Link

[3] CryptoCompare, *Exchange Review November 2021*, 2021. Link

[4] CoinMarketCap, *Top Cryptocurrency Decentralized Exchanges*. Link

[5] *CoinGecko API Documentation*. Link

[6] *Hegic*. Link

[7] Opyn, *Opyn v2 Introduction*. Link

[8] *SIREN Whitepaper*, 2021. Link

[9] Zubin Kotcha, *Partially Collaterized Options - Now in DeFi*, 2021. Link

[10] Antonio Juliano, *dYdX: A Standard for Decentralized Margin Trading and Derivatives*, 2017. Link

[11] *An open protocol for decentralized derivatives built on the Ethereum blockchain*. Link

[12] Osato Avan-Nomayo, *DeFi hacks and exploits total $285M since 2019, Messari reports*, 2021. Link

[13] Kaihua Qin, Liyi Zhou, Benjamin Livshits, Arthur Gervais, *Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit*. Link

[14] Chainlink, *What Is a Blockchain Oracle*? Link

[15] *0x Protocol*. Link

[16] *Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks*, 2021. Link

[17] *Perpetual Protocol*. Link

[18] *Smart Contract Cover*. Link

[19] *Unslashed Finance Documentation*. Link

[20] Zubin Koticha, *Convexity Protocol: Building a Generalized Liquid Options Protocol in DeFi*, 2019. Link

[21] *Cboe VIX White Paper: Cboe Volatility Index*. Link

[22] Robert Leshner, Geoffrey Hayes, *Compound: The Money Market Protocol*, 2019. Link

[23] *Build a DeFi Call Option Exchange With Chainlink Price Feed*, 2020. Link