Convexity Protocol

Building a Generalized Liquid Options Protocol in DeFi

Zubin Koticha
Opyn
WORKING DRAFT

November 12, 2019 Draft

Abstract

In this paper, we propose a generalized noncustodial options protocol for Decentralized Finance (DeFi). By depositing crypto-collateral (e.g. ERC20s or ETH), and specifying certain key parameters (e.g. underlying asset, strike price, expiry date, etc.), options writers are able to mint arbitrary fungible ERC20 option tokens called *oTokens*. Selling those minted oTokens allows writers to earn premiums, thereby generating revenue on their collateral. Buyers can then purchase these oTokens, which trade on exchanges such as 0x or Uniswap, ensuring market liquidity. Beyond the primitive of fungible, freely tradable ERC20 option contracts enabled by this framework, this paper considers initial use cases for DeFi options, in particular focusing on protective put strategies for deposit insurance (e.g. protecting users of tokenized money markets like Compound against hacks and liquidity crises), as well as protection against stablecoins like DAI crashing in value. This paper also considers cases wherein option sellers wishing to offer protection can do so using a collateral type (such as ETH) which is different than the asset (such as USD) in which the strike price is denominated. Thereby, this protocol allows DeFi users for the first time to earn significant premiums on their ETH holdings by posting ETH as collateral in options selling. These oToken primitives allow users to hedge risks, create leverage, buy insurance, and make bets on volatility. These oTokens will also serve as oracles of volatility and risk in DeFi.

1 Introduction

1.1 Motivation

Decentralized finance (DeFi) has experienced an explosion of interest and activity recently. More than $1.5 billion worth of cryptoassets have been deposited in Ethereum DeFi applications since December 2017 at a rate that continues to accelerate. Many users have been drawn to DeFi due to the high USD-denominated yields offered on DeFi lending platforms, touting these as superior to the low interest-rate FDIC-insured accounts in which many Americans have their savings. In truth, it is well accepted in finance that high yields reflect significant risk inherent in using such protocols [6], such as smart contract hacks, hard forks, flash crashes in the price of collateral, and liquidity crises in DeFi. Indeed, hundreds of millions of dollars have already been lost in smart contract hacks [10].

1.2 Options

Though derivatives markets comprise some of the most liquid markets in all of traditional finance, true derivatives markets are missing in DeFi. Options are amongst the most widely

traded of derivative assets in traditional finance, with yearly exchange volume of more than $635 trillion (not including OTC options trading) [1]. Liquid options markets provide market participants with access to hedging, leverage, and financial insurance, making the development of such markets a prerequisite to DeFi's maturation.

Beyond just being an important financial primitive, options can effectively address many of the risks mentioned in 1.1 through strategies such as protective puts. We explore this protective potential throughout the rest of the paper.

1.2.1 Plain Vanilla Options

At a high level, an option is an asset that gives its owner (buyer) the right to buy or sell a specific asset from the option writer (seller) at a specific price at or before the option expiry. [1]

Let's go through some examples with Alice, who will take the role of the options seller for the remainder of the paper, and Bob, who will be the options buyer.

1.2.2 An Example Option Series

Bob wants the right (the *option*), but not the obligation, to sell 1 DAI for 1 USDC before 11:59 PM on Dec 31, 2019. Alice is willing to take on that obligation to purchase that 1 DAI in exchange for 1 USDC at Bob's request. Since Bob gains a right and gives Alice an obligation, he must compensate her by paying her, say, .10 USDC. Fast forward to 10:00 PM on Nov 29, 2019. Bob has 1 DAI. If Bob wants to sell his 1 DAI, then Alice must purchase it for 1 USDC. If Bob does not want to sell his 1 DAI, he will hold on to his 1 DAI and Alice will keep her 1 USDC.

Let's break the above scenario down, to understand some basic options terminology.

- Bob is the option *owner* (or buyer). He is *long* the option
- Alice is the option *writer* (or seller). She is *short* the option
- DAI, the asset that Bob has the right to sell, is called the *underlying asset*
- USDC, the asset that Bob receives if he exercises, is called the *strike asset*
- 1 USDC, the price at which Bob wants to sell DAI, is called the *strike price*
- We call this option a DAI:USDC option and will use this format (underlying asset:strike asset) to refer to option pairs throughout the paper
- .10 USDC, the sum that Bob pays Alice for the option, is the option *price* or *premium*
- If Bob sells his 1 DAI to Alice for 1 USDC on Nov 29, 2019, that is known as *exercise* of the option
- Because Bob can exercise his option anytime before (or exactly at) 11:59 PM on Dec, 31, 2019, this type of option is known as an *American* option. If instead, Bob could only exercise his option exactly at the time of expiry, and not before or after that time, this type of option would be known as a *European* option
- Because Bob has the right to *sell* DAI, this is called a *put* option. If instead, Bob had the right to buy DAI from Alice, this would be called a *call* option [2]

[1] Note that the owner of the option contract has the right (the*option*) to buy/sell the specified asset, but not the obligation to do so.

[2] Note that an option to sell DAI to buy USDC is the same as an option to buy USDC to sell DAI (*i.e.* a put on DAI:USDC is the same as a call on USDC:DAI). We discuss this in Section 9.

The specification of a combination of *all* the above parameters together creates a unique option *series*. Given the number of parameters, as well as the possible ranges each parameter can take, an infinite number of different option series can exist.

In the example above, if the price of 1 DAI (the underlying asset) falls below the strike price of 1 USDC, the put option is said to be *in the money*, meaning that, if Bob were to exercise his option, the exercise would be profitable. Alternatively, if the price of 1 DAI is exactly 1 USDC, the put is *at the money*. If, for some strange reason, 1 DAI's value is greater than 1 USDC, the put option is *out of the money*, since Bob would lose money were he to exercise it.

1.3 Related Prior Work

The most notable prior attempt for options in DeFi is dYdX. While dYdX is now a thriving lending and margin trading marketplace, the original dYdX whitepaper considered ERC20 options markets [2]. However, there were a number of drawbacks with the proposed model, and it was never built. dYdX placed a number of restrictions on sellers. First, writing and selling options relied solely on orderbook liquidity on 0x, and as such minting and selling options was executed in a p2p manner, which is a significant barrier to liquidity [7]. It would not have been possible for sellers to write and sell their options on Unsiwap or any other DEXes, for example. Also, the proposal required writers to accept premiums in only the strike currency, rather than allowing writers to freely sell newly minted options on any exchange in any currency. The protocol did not allow sellers to get out of their positions before expiry. Further, it did not allow for arbitrary collateral types, preventing ETH, the most popular collateral asset in DeFi, from being used as collateral for synthetic USD-strike options (see section on Collateral Asset Differs from Strike Asset). The lack of arbitrary collateral types also prevented many assets from being used as strike assets due to their high interest rates. We address improvements that allow for the relaxation of these restrictions throughout the paper.

Maker, UMA, and Yield Protocol have made considerable strides in ETH-collateralized synthetics. As such, they are significant inspirations to the ideas put forth in this paper, especially in informing this paper's notions of vault collateralization, token fungibility, and liquidation. Our notions of series and reverse dutch auction token sales are strongly influenced by Yield Protocol [3].

2 Mechanism

In the following section, we will discuss a framework for generalized *put* options in DeFi, as protective puts are the first envisioned use case. Note that the framework can be trivially extended to call options for arbitrary cryptoassets as well (see Section 9).

As in all options markets, the two key actors in the protocol are those who want to sell options, and those who want to buy options. At a high level, sellers deposit collateral in smart contracts called *vaults*, allowing them to mint and sell fungible ERC20 options called *oTokens* and collect premiums. Buyers are free to purchase these ERC20 oTokens on exchanges that support ERC20s, as well as to exercise the oTokens if doing so is profitable.

Those who mint and sell oTokens are analogous to those who mint DAI in the Maker system, or those who mint yTokens in the Yield Protocol [3]. Those who buy and hold oTokens are analogous those who buy and hold DAI on exchanges.

2.1 Buyer motivation

Imagine that Bob holds a substantial amount of DAI. However, Bob is scared of what would happen to the value of his holdings if a black swan event causes DAI to break its peg with the

dollar. Therefore, Bob purchases from Alice protective puts (see section 3.1) on his DAI against a 1 USDC strike.

2.2 Seller Motivation

Since Bob pays an option premium to Alice in return for her protection, Alice is making a profit unless DAI crashes in price.

2.3 Selling Options

How does Alice sell options to Bob that she does not yet own? She can mint them from the protocol itself. Sellers, like Alice, who want to mint and sell options have to put down sufficient collateral in a smart contract that we will call a *vault*, which is analogous to a vault in Multi Collateral DAI, a CDP in Single Collateral DAI, or a repo in Yield Protocol [3].

Selling the option obligates Alice to give up some of her collateral in the vault (in exchange for the underlying asset - in this case DAI) if Bob wants to exercise his oToken. For example if Alice has USDC collateral in her vault, Alice may have to give up some amount of that USDC at (in a European option) or before (in an American option) the exercise date in exchange for Bob's DAI if and only if Bob exercises his oToken.

2.3.1 Seller Collateral Requirement

In the simplest case, the collateral in Alice's vault must equal the strike price times the number of options she wishes to mint. This keeps her fully collateralized, as that is the exact amount that she will be required to send to Bob upon exercise (in return for Bob's underlying asset).

Collateral requirements become more complex in section 7, when we consider the case where the collateral asset differs from the underlying asset. It would be ideal for Alice to be able to sell option contracts while being only partially collateralized; we will discuss this possibility and capital efficiency in greater depth in section 10.

2.4 Options Fungibility

After Alice mints these oTokens and sells them to Bob, Carol opens a new vault, posting collateral to it so she can mint options of the same series (i.e. options with the same specifications/parameters) as the ones that Alice has minted. Since they are of the same series, both Carol's and Alice's options are represented by the same ERC20 oToken, making them fungible with each other.

Carol subsequently sells the oTokens she has minted to Dan. As more and more sellers and buyers emerge, a marketplace begins to form around this series.

3 Use Cases

3.1 Financial Insurance through Protective Puts

In traditional finance, owners of an asset who want to be protected against some downside risk often protect their portfolios by buying put options where the underlying is an asset that they own. At a high level, should the need arise, the option allows them to easily dispose of their asset at a certain predetermined price, thereby capping the potential loss on said position. For example, if they buy a stock for $50 a share and want to cap their loss at $10, they can purchase a put option with a strike price of $40. This will give them the ability to sell the stock for $40 even if the stock price crashes to, say, $20. Since it is an option, they have no obligation to exercise if the price of the stock stays above $40 or even goes up in price. In this protective

position (where they own the stock and also own a put option with a strike at $40), they get to keep all their gains but are exposed to only a $10 maximum loss.

3.2 Key Use Case: Compound Deposit Insurance

When users deposit funds on the Compound Money Markets platform on Ethereum, they get a receipt, which is a interest bearing ERC20 asset called a cToken that represents their loan balance [8]. This allows them to later redeem their deposited funds.

Let's say Bob deposits 1 USDC on Compound and receives cUSDC for doing so. In the normal case, Bob can retrieve his 1 USDC plus interest from Compound whenever he so chooses. However, Bob fears that if an adverse event occurs on Compound (e.g. hack, flash crash in market value of collateral, depositor flight caused by liquidity crisis, etc.), his cUSDC will not be redeemable for the 1 USDC he deposited (plus interest). Essentially, the owner of cUSDC wants to be able to redeem their cUSDC for a certain number of USDC regardless of what happens to Compound.

In order to protect Bob against such risks, we create a put option similar to the one in the previous section, but one where the underlying asset is cUSDC rather than DAI. As before, Alice mints a oToken and sells it to Bob. Let's say that the strike of the oToken that Alice mints is 0.99 USDC.[3] Then, Bob's oToken gives him the right to exchange his cUSDC (which is currently worth $1) for 0.99 USDC before 11:59 PM on December 31, 2019 with Alice.

Then later (but still before the option's expiry on December 31st), imagine that there is a hack or liquidity crisis on Compound that causes the amount of USDC redeemable for Bob's cUSDC to fall drastically to 0 USDC. This is far below 0.99 USDC (i.e. the put is in the money). At that point, Bob will exercise his oToken to sell his cUSDC to Alice for 0.99 USDC, which is nearly his deposit size.

3.3 Key Use Case: DAI Price Hedge

Consider a put option series for 1 DAI, at a strike price of 0.99 USDC, which expires at 11:59 PM on December 31, 2019.

If Alice wants to mint and sell exactly one oToken of the above put series, she must put down exactly 0.99 USDC as collateral in a vault. After specifying the desired option series's attributes as parameters, a new put option oToken of that series is minted to her address. [4] She can subsequently sell this oToken wherever and to whomever she wants (e.g. on Uniswap or 0x), which is how she collects her option premium.

Imagine that Alice sells her oToken to Bob at the market rate of 0.10 USDC (Alice can choose any purchase currency). Since the oToken is an ERC20, the sale could happen on any ERC20-compliant DEX or exchange of Alice's choosing, and she can also collect the premium from Bob in the currency of her choosing. The premium that Bob pays Alice is immediate revenue for Alice. As long as Bob holds the oToken that he has purchased, it gives him the right to exchange 1 DAI for 0.99 USDC on (before) 11:59 PM on December 31, 2019.

Later (but still before December 31st), imagine that the price of 1 DAI falls drastically to 0.50 USDC, which is far below the option's strike price of 0.99 USDC (i.e. the put is in the money). If Bob were to try to sell his 1 DAI on any exchange, he would only get 0.50 USDC for it. Luckily for Bob, because he owns the put option, he can exercise it to sell his 1 DAI to Alice for her 0.99 USDC of collateral, which is removed from her vault. If Bob exercises his oToken, he limits his loss to one USDC cent (due to a strike price of 0.99 USDC, compared to the 1 USDC that he paid for the DAI). This is significantly better than the fifty USDC cents he would have lost otherwise.

[3] This option is slightly out of the money. In general, there are many benefits with using a strike slightly out of the money.

[4] Note that if Alice changes even a single attribute parameter, she will end up with an entirely new series.

3.3.1 Options Benefit over Mutuals

Nexus Mutual is a current attempt to address the issue of insurance in DeFi, but is unfortunately oversubscribed and thus cannot cover new buyers [12]. Therefore, while validating that users want insurance, the fact that their insurance contracts are oversubscribed underlies issues with their model. In the Nexus model, Nexus Mutual itself acts as a single underwriter of risk, leading to a severe limit on the amount of insurance offered. Further, Nexus requires human involvement for claim and fraud assessment, which can be extremely difficult to execute in subjective cases such as distinguishing between code bugs and hacks (e.g. in the 'Parity multisig hack'). In addition, Nexus Mutual is limited in scope as it only protects against hacks; its Compound insurance provides no recourse against liquidity crises on Compound, for example [9].

While mutuals are common in many forms of insurance, financial insurance is usually conducted using derivative instruments such as protective put options strategies (explained above in section 3.1). That is, buying put options is one of the most commonly used strategies for financial insurance in traditional finance for three main reasons. First, options marketplaces marketplace support arbitrarily many underwriters (options sellers). Second, such options incentivize options buyers to exercise only when it is profitable to them (i.e. when their options are truly in the money), practically eliminating insurance fraud and eliminating the need for subjective human claim and fraud assessment. Third, protective puts offer protection against exactly the instance for which protection is being sought, viz. a decrease in the financial value of the asset. The protection is offered regardless of what circumstances cause the decrease in the financial value.[5] In our above example on the DAI price hedge, the put option protects against both technical and financial risks, that is, a protective put on DAI would protect the user against DAI breaking its peg regardless of whether the cause is a hack or a flash crash in the value of collateral.

3.4 Key Use Case: Options as Oracles of Volatility and Risk

Options markets are also powerful oracles of volatility and market sentiment. In traditional finance, the VIX index, which is commonly referred to as Wall Street's 'fear gauge,' is computed using the prices of options . Using the Black-Scholes equation, one can work back from an option's price to derive the implied volatility (a proxy for the market's estimate of the future price variability) of the underlying asset. Further, we can use option prices to assess the market's estimate of the probability that an asset's price will reach certain strike prices in a specific time period.

The options outlined in this paper will similarly be important early warning signs in DeFi. Imagine, for example, that the price of a protective put on DAI starts to drastically increase. This may be a good early warning sign that a vulnerability has been found and that an attack may be imminent.

Options market will become on-chain oracles of volatility and risk; for example, they can be used to rate the risk of different types of collateral that are used in Multi-Collateral DAI.

4 Ensuring Liquidity

As important as options are, it is difficult to deliver even plain vanilla option markets in DeFi given that both the price volatility of most cryptoassets and the complexity of option contracts negatively affect liquidity. This means that additional work is required for options to be viable in DeFi.

[5] In typical mutual insurance, the circumstances that are insured against are specified, and non-specified circumstances are not covered.

As discussed earlier, when minting an option token, Alice needs to specify an option series. Remember that an option series is one where all the option parameters are the same, so selecting an option series effectively means selecting all the option parameters (such as underlying asset, strike asset, strike price, expiry time, whether American or European, etc.). When selecting an option series to mint, Alice will be incentivized to ensure the liquidity of the series. This is crucial, as a liquid market is necessary for the health of this options protocol. Liquidity allows users to buy and sell options on demand at a reasonable price.

Alice herself has a strong incentive to only mint oTokens that she believes will be highly liquid (or that are already highly liquid) for two main reasons. First, so that she can quickly find a buyer who will pay her a reasonable premium for her newly minted oToken. Second, so that after she sells her oTokens, if she wants to exit her position (in a process called unwinding which we discuss later), she will have to buy exactly as many oTokens as she sold, for which she will want a liquid market.

4.1 Choosing Appropriate Option Parameters

An option with each of the option parameters defined belongs to a particular option *series* (e.g. the option we described earlier, that gives Bob the right to sell 1 DAI for 1 USDC at 11:59 PM on December 31, 2019). If an option differs from another even on just one of the above parameters, it then belongs to a different series (e.g. the other option we described earlier, that gives Bob the right to sell 1 DAI for *0.99* USDC at 11:59 PM on December 31, 2019).

Crucially, oTokens of any particular series are fungible, but they are not fungible with oTokens of a different series. A major challenge preventing thriving options markets in DeFi is that there are many parameters to select when creating an options series. Thus, when one mints new options, they run the risk of creating a oToken that does not have very high liquidity or fungibility.

The important parameters:

- Parameter 1: Expiry time
- Parameter 2: European vs American
- Parameter 3: Underlying asset
- Parameter 4: Strike Price
- Parameter 5: Strike asset
- Parameter 6: Call or Put
- Parameter 7: Collateral / margin type
- Parameter 8: Collateral / margin requirement

If there are too many series of options trading for Bob to choose from, this would fragment liquidity, preventing a liquid market from forming around any particular series.

The key desired result here is to find a particular options contract or set of options contracts that will have significant user demand on both the sell and buy side. We can attempt to maximize liquidity by ensuring that the options we mint will not be too expensive, will have strike prices that are always desirable for buyers and sellers, and will not vary too much on the other above criteria.

We can limit the number of strike prices and expiry dates that valid options can have (thus limiting the number of different options series in circulation). For example, we can decide to have only one strike price and expiry date that trades at any time for every token pair.

This strategy encourages liquidity to develop around a few different puts, but presents the challenging task of predicting *a priori* which options series are likely to be most liquid.

4.1.1 Expiry Time

We limit option expiries to the end of the current quarter. Also, during the last month of the quarter, we allow trading in options expiring at the end of the following quarter; this one month of overlap between two successive option series will allow option owners and writers to 'roll' their oTokens (i.e. sell/buy oTokens from the current series and buy/sell oTokens from the next one.)

4.1.2 Strike Price

We should generally choose to encourage the adoption of series that are at the money or slightly out of the money, as these tend to be the most liquid in traditional finance [13].

By focusing on options on DAI and cUSDC, we are in the unique position of knowing what strike prices (denominated in USDC) should always be at the money or slightly out of the money. In addition, by focusing on DAI and cUSDC underlying, we solve problems relating to the following sections 4.2 and 4.3.

4.2 Price Volatility of Cryptocurrencies

According to the Black-Scholes model of options pricing, the expected (implied) volatility of prices of an underlying asset is one of the most important variables that determines the price of any given option. As the underlying asset's price volatility increases, all else being equal, the price of the option also increases. Since the vast majorities of cryptocurrencies are extremely volatile, most cryptocurrency options are prohibitively expensive to buy, preventing a liquid market for options from forming at a fair price.

In addition, the high volatility means that no strike price is able to collect a majority of liquidity because no strike price is consistently at the money; a strike price that was previously at the money may be seriously in or out of the money a few days later. Therefore, we must find cryptoassets with a low amount of volatility when we bootstrap our options marketplace.

4.3 An Approach to Liquid Options

The above sections suggest that, in order to bootstrap an initially liquid options marketplace in DeFi, one must first address the dual goals of reducing the volatility of the underlying asset and decreasing the complexity of the options.

One way we can try to fulfill our dual aims of reducing volatility and options complexity, while providing useful options for users, is to create puts on stablecoins, such as DAI, and on interest-bearing deposits, such as cryptoassets deposited on Compound. This helps in achieving our two aims as follows. First, since stablecoins and interest bearing deposits are, in expectation, extremely low in volatility relative to the dollar, these options contracts should not be prohibitively expensive to buy.[6] Second, we can specify strikes - at $0.99, for example - that will always be only slightly out of the money (except in the extreme cases that we're trying to protect users against), and thus are most likely to be liquid to trade.

In addition, since these put options solve pressing user pain points in DeFi (by protecting users against previously mentioned risks), we can expect sufficient buyer demand to bootstrap this two-sided marketplace.

[6] In theory, stablecoins such as DAI should always trade 1:1 with USD, and cUSDC should only be slowly increasing in value relative to USD.

5 Settlement

5.1 Physical Settlement and Cash Settlement

If Bob decides to exercise his option, he is doing so because it is profitable for him to do so, which implies that he would profit by exchanging his underlying asset for a certain amount (strike price) of the strike asset. There are two main ways in which settlement occurs (i.e. two ways in which the positive monetary value is transferred to Bob): *physical settlement* and *cash settlement*.

- In *physical settlement*, there is an actual (physical) exchange of the underlying asset and the strike asset. Upon Bob's exercise of his oToken, he supplies the underlying asset (which is given to sellers like Alice), and in return receives the strike asset (which is taken from sellers like Alice).
- In *cash settlement*, the exact difference in value between the strike asset and underlying asset, is transferred from Alice to Bob upon Bob's exercise.

For the following two examples, Let's consider the same options series as in section 3.3, where Bob has a put on 1 DAI struck at 0.99 USDC. Alice deposited 0.99 USDC of collateral in her vault when she minted the oTokens.

5.1.1 Example: Physical Settlement

Upon exercise, Bob sends his exercise transaction, along with 1 DAI, to Alice's vault, and in return, 0.99 USDC is transferred from Alice's vault to Bob.

5.1.2 Example: Cash Settlement

Upon Bob's exercise, Alice sends Bob the difference between the price of DAI and USDC. This requires a trusted price oracle to determine the intrinsic value of the option. Let's say that, at expiry, the price oracle says that 1 DAI is worth 0.65 USDC. Given that the strike price of Bob's option is 0.99 USDC, Bob's option is in the money by 0.34 USDC (0.99 - 0.65). When Bob exercises his option, 0.34 USDC is transferred from Alice's vault to Bob. Alice is left with the remaining 0.65 USDC in her vault.

5.1.3 Benefits of Physical Settlement over Cash Settlement

- Buyers ostensibly prefer physical settlement since they can get rid of their distressed asset through the put option rather than having to do so on the market. Cash settlement opens up buyers to risk after expiry since they will have to find another way to get their distressed asset off their hands, which may be very difficult to do if there is a liquidity crisis, for example.
- Physically-settled options, unlike cash-settled options, do not require an oracle to determine the exchange rate between the underlying and strike assets, which is needed to determine the payout of the option. Reliance on oracles opens the system to further vulnerabilities, such as oracle manipulation [11]. For example, in extreme cases such as a severe hack on Compound or global settlement in Maker, it is not clear that price oracles will be able to reliably price cTokens or DAI, respectively.

5.1.4 Benefits of Cash Settlement over Physical Settlement

- Buyers do not need to send the underlying asset to exercise, just an exercise transaction, meaning that market participants such as professional traders and market makers can trade these options without ever having to worry about obtaining the underlying asset.
- Cash-settled options are more capital efficient, since sellers only need to post the expected difference between the underlying asset and strike price as collateral, rather than the entirety of the strike price (see section 11 for further explanation). A more capital-efficient system, all else being equal, is more likely to develop liquidity as it is far more attractive to sellers.

Assuming there are multiple option sellers beyond Alice, there are two main ways that Bob can collect seller collateral in the event of exercise: First, the protocol itself can specify a vault to get closed out based on some logic. Perhaps vaults with the lowest collateralization ratio get liquidated first in order to keep the system as properly capitalized as possible (see section 7 for further discussion on collateralization ratios). Second, collateral can be removed from vaults proportionally based on the number of outstanding put oTokens that have been minted from each vault.

6 Exercise

Buyers like Bob can exercise their options in two ways, depending on the specifications of the oTokens that they hold.

6.1 Exercising American Options

In an option with American exercise, Bob can exercise whenever he wants to as long as his exercise transaction is included in the blockchain before the option expires. When he exercises, he sends his underlying asset (assuming physical settlement) and gets the appropriate amount of seller collateral.

Note that if Bob exercises before it is optimal to do so, he may lose some of the time value of his option. Theoretically speaking, the only case in which it makes sense to exercise an American option early is if it is sufficiently in-the-money and if the yield/interest rate you get from the strike asset you receive will be higher than the yield you lose from giving up the underlying asset you currently hold (i.e. the situation where the strike asset is sufficiently higher yielding than the underlying asset so that the yield differential between the two assets makes up for the lost time value of early exercise). In our protocol, for reasons discussed in section 7, it is unlikely for the strike asset to be higher yielding than the underlying asset. Say Bob has an option on DAI, and the price of DAI goes to 0.90 USDC. Then Bob's option is in the money and he can exercise his option to get 1 USDC. However, the yield on DAI is higher than that on USDC (from rates we have seen in DeFi to date), meaning that Bob will give up the higher yield on DAI and receive the lower yield on USDC were he to exercise his option early. In addition, he will also be be giving up an remaining time value on his option. This argues against early exercise.

However, waiting till the very last moment to exercise this American option will cause Bob other issues, similar to the ones Bob will face during the exercise of a European option, as described below.

6.2 Exercising European Options

European exercise means that Bob can only exercise at the exact time of expiry. This creates a complication due to the liveness properties of the blockchain. If expiry is approaching on a

specific block, there is no guarantee that Bob can get his exercise transaction included in the chain before that block. If we include some grace period after expiry to account for the liveness properties of the blockchain, it is equivalent to extending expiry to a later block, and so the same problem persists.

Imagine Bob's option is in the money and so he wishes to exercise, but there are 5 hours left until expiry. Bob fears that he is exercising too early; if the prices of the underlying and strike assets move against him in the next 5 hours, he may end up inadvertently exercising an out-of-the-money option come expiry and thus lose a substantial amount of money. However, he also fears submitting his exercise transaction later, since if his transaction does not show up in any block until after exercise, he will lose money too, assuming that the option actually ends up being in the money upon expiry.

There are two possible solutions that may make Bob feel more comfortable:

6.2.1 American at the End

The options contract becomes American just for the final d number of days before expiry (or final b number of blocks), meaning that Bob can exercise it at any time in that exercise period. This decreases Bob's stress because he knows he has a sufficiently long time period in which he can exercise. However, this is still not ideal because it means that Bob is getting short-changed again by early exercising, as we saw with American options above.

6.2.2 Using an Exercise Oracle

We can solve the aforementioned problem by utilizing a strategy used in exchange-traded options in traditional finance: using an *exercise oracle*. The exercise oracle looks at a price oracle at the time of expiry to determine if an option is in or out of the money.

Using an exercise oracle allows Bob to exercise exactly on expiry despite the liveness properties of the blockchain. Bob submits his 1 DAI, along with a request to conditionally exercise the option come expiry, to a pre-specified trusted exercise oracle. This request must be submitted sufficiently early to ensure that it is included in the chain before expiry. Upon expiry, the exercise oracle the relative value of the underlying asset to the strike price, and exercises for Bob only if the option is in the money.[7]

Of course, Bob can cancel his exercise transaction at any time before expiry. And, as described above, the exercise oracle can be used with American or European options.

6.3 Pros and Cons of American and European Options

American options give more optionality to the buyer and thus are never worth less that European options to the buyer. *Ceteris paribus*, it is easier for Bob as a buyer to exit his position for an in-the-money American options contract than a European one as Bob always has the option to exercise the former, rather than having to sell the options contract.[8]

European options are more likely to develop highly liquid markets. This is due to precisely the same property as above: buyers must sell their options if they want to exit their positions, which means more liquidity on exchanges for buyers trying to buy options.

[7] For the physically-settled option in our example, exercising means depositing Bob's 1 DAI into Alice's vault and taking 0.99 USDC from Alice's vault and depositing it into Bob's account.

[8] Exercising rather than selling the option may entail the loss of some time value; however, that may be needed in the absence of liquidity in the options market.

7 Strike Asset differs from Collateral Asset

Minting and selling an oToken obligates Alice to potentially give some amount of her USDC up later. If she sells her option to Bob (assuming Bob holds it until expiry), she's obligated to give some amount of her USDC in exchange for Bob's cUSDC or DAI if Bob exercises the option before some predetermined date.

For reasons of capital efficiency and risk, ideally, the strike asset is the same as collateral asset. That is how we have described the protocol thus far, where strike prices and Alice's collateral are both denominated in USDC, meaning that Alice must post her collateral to her vault in USDC and pay Bob in USDC as well upon exercise. In such a case, the protocol does not require Alice to post any more collateral than the strike price, because (in physically-settled options), she'll send exactly that amount to Bob if he exercises.

The above might work for insuring DAI:USDC, but it does not work for cUSDC:USDC options, as we must deal with a few financial constraints.

Note that Alice takes similar risk when putting her collateral on Convexity to sell options as compared with depositing it on Compound. That is, if Compound gets hacked and Alice has deposited money in Compound and sold cUSDC:USDC put options, she will lose money as both a depositor on Compound and as an options seller because Bob will exercise his option. Therefore, she should expect similar returns on both, or, if she provides USDC collateral to sell put options on cUSDC that expire in a month, she should expect a larger premium from that as the yield she would get by depositing her USDC on Compound, otherwise she would never enter into this agreement.

Note that Alice has to deposit collateral in a vault if she wants to mint and sell options. Let's say the option she is selling is a put option on cUSDC:USDC, which provides protection against Compound getting hacked. Imagine that she posts USDC as collateral. Let's compare the following two scenarios. Scenario 1: Alice deposits her USDC on Compound. Scenario 2: Alice deposits her USDC in a vault on Convexity and writes a put option on cUSDC:USDC.

In Scenario 1, Alice receives the yield on Compound (let's call it the cUSDC yield). In Scenario 2, she gets the option premium on her oTokens.

In Scenario 1, Alice is exposed to the risk that a hack or other black swan event causes her cUSDC to be worthless. In Scenario 2, Alice is exposed to the same risks as she will be forced give up her USDC collateral to Bob if Compound gets hacked or threatened. However, now she also faces risks that threaten the Convexity Protocol as well.

Thus, the oToken premium has to be larger than the cUSDC yield for Alice to consider writing the options.

Now, let's look at Bob. He is investing his USDC in Compound and earning the cUSDC yield. As explained above, the premium he would pay for the oToken would be larger than the yield on cUSDC he is earning. So, if he deposits money with Compound and then buys protection on Convexity, he has a negative yield. It would be better for him to keep his USDC in his wallet in this case rather than depositing in in Compound and buying insurance for it. [9]

The problem is that USDC is a high-yielding currency. If Alice uses USDC as her collateral, she has the opportunity cost of losing that high yield, which needs to be made up at least in full by the premium Bob pays her. This would make the option too expensive for Bob. The way this can be fixed is if Alice can use a low-yielding asset as collateral. Ether fits this profile.

Many potential sellers like Alice want to HODL ETH and put it to good use in the meantime, but there's very little to do with ETH in DeFi right now; one gets almost no interest from depositing ETH on Compound. So, if Alice puts down a ETH as collateral in her vault and sells the above put option, she will receive an option premium for doing so which far exceeds what she would get from depositing that ETH on Compound

[9] This does not necessarily apply if he is using Compound for leverage rather than savings).

7.1 Example: ETH as collateral

Let's look at an example where Alice has her collateral denominated in ETH. When we use an asset other than the strike asset as collateral, there is the risk that the collateral asset loses value relative to the strike asset. Therefore, Alice must over-collateralize, adding more ETH to her vault than the USDC value she would have to pay Bob upon expiry.

Imagine she starts by collateralizing with $2 of ETH. If the option is never exercised, Alice gets all of her ETH back. If the option is exercised, Alice gets 1 DAI from Bob, gives $0.99 of her ETH to Bob, and keeps any of her remaining ETH. If ETH falls in price, Alice can top up her vault to remain sufficiently collateralized; otherwise, she runs the risk of getting liquidated, which we discuss further in the following section.

7.2 Liquidations

Liquidations should only happen if the strike asset is not the same as the collateral asset. If the strike asset is different from the collateral asset, the protocol must keep Bob safe even if Alice's collateral decreases in value compared to the strike price. If Alice's collateral were to go below some minimum collateral ratio (as judged by an collateral:strike asset oracle), it is important that anyone in the system should be able to liquidate her.

Of course, to ensure that she remains properly collateralized, thereby preventing herself from getting liquidated, Alice can add collateral to her vault at any time.

7.2.1 Collateral Replacement

In this type of liquidation, a liquidator must replace Alice's collateral, which is not denominated in the strike asset, with collateral in the strike currency in an amount equal to the strike price times the number of options minted from her vault. The liquidator will then receive all of Alice's original collateral in return. Since Alice must be over-collateralized even at the minimum collateral ratio, the liquidator makes money from this liquidation. And since the vault, which now belongs to the liquidator, contains the correct amount of collateral in the strike currency, Bob will have access to his expected payoff if he decides to exercise his option.

7.2.2 Burning Options

In this type of liquidation, a liquidator must burn the exact number of oTokens that Alice's vault backs. Whoever liquidates this vault should get as much ETH as the strike price of those put oTokens plus a penalty, and the rest should go back to Alice.

Note that since all options in a series are fungible, the protocol contains liquidity from vaults other than Alice's, allowing Bob to exercise, so he will not be bothered by Alice getting liquidated.[10]

8 Early Unwinds

Even though options contracts have dates of expiry, that does not mean that Alice and Bob are locked into their positions until that expiry date, even when they are short or long European options.

At any time, Alice can completely exit her short position in a process called unwinding. To unwind her own vault, she can buy any of the oTokens of the series that the vault corresponds to, and then burn them to release collateral. If she burns as many oTokens as she has minted and sold, then she can completely exit her short put position (and thus unlock the entirety of

[10]Liquidating Alice by burning oTokens can only be done by someone who owns a sufficient number of oTokens; if Bob is the only one long oTokens, then he will be the only one who can liquidate her via this method.

her collateral). If she burns fewer oTokens than she has minted and sold, then she essentially has a smaller short put position than she did before, and she can take away some collateral (as much as she wants as long as she stays above the collateral requirement for her now smaller position size).

For Bob to unwind his position, he should just sell his oTokens on a DEX or another exchange. For example, if he has sold his DAI and thus does not want any DAI insurance any longer, he can sell his DAI oTokens on Uniswap or 0x. [11]

9 Extending the Protocol to Call Options

Though we have referred to these options as *puts* for the entirety of the paper, since they are FOREX options at their core, they are also already *call* options. For an exchange between different cryptocurrencies and tokens, it is unclear as to which asset is being "bought" and which is being "sold." That is, if Bob buys a put that gives him the right to sell 1 DAI for a strike price of 1 USDC, this is the same as a call option that gives him the right to buy 1 USDC for a strike price of 1 DAI. Therefore, this paper is a generalized options protocol that allows DeFi users to create call options as well as put options.

10 Future Work

10.1 Collateral Rehypothecation

In order to make Convexity more attractive to sellers like Alice, we might want to allow her to post her collateral in interest-bearing assets so that she doesn't have to give up the interest on assets she posts as collateral. One way to do this would be to have sellers post Yield Tokens as collateral that expire at the same time that the puts expire.

However, this introduces further risk to option buyers as they are exposed to new risks that threaten the platforms on which seller collateral is rehypothecated. As a result of this complexity, introducing collateral rehypothecation is an area of future work; it is not necessary for initial implementations of the protocol.

10.2 Dutch Auctions

In a Dutch auction, we offer up an asset for sale at some maximum price at which we think we could possibly sell the asset and periodically decrease the price offered until there is a buyer. Such an auction contract could be used for options sales in this protocol. This means that, after Alice mints an option, a Dutch Auction could be started whereby the protocol attempts to sell that option for Alice. This might be helpful for Alice, especially if she is the first seller of a new option series, because there might not a liquid market on any DEX around the series she minted yet.

In a Reverse Dutch Auction, we begin at some minimum price at which we think we could possibly buy a target amount of a target asset (e.g. the strike price for a put option) and offer to buy the target asset at that price, increasing the offer price until there is a seller. This could be extremely useful for the protocol, as, in the case that the collateral asset differs from the strike asset, if we want to deliver the strike asset to Bob, we could have the protocol offer to sell off increasing amounts of Alice's collateral for the desired quantity of the strike asset using a Reverse Dutch Auction.

The benefit of the aforementioned auction is that it is avoids the slippage and front-running that threaten taker sell orders for large amounts of the aforementioned assets on DEXes.

[11] Although Bob would be selling options, unlike Alice, he does not have a short options position because he is just selling the oTokens he previously bought; he is not selling options that he never previously owned.

10.3 Perpetual Options

Intuitively, if these options could be perpetual, they would both be able to always provide cover to whoever holds the tokenized long side, and they would also be significantly more fungible because all options would have the same expiry date (time infinity). Further, such options would not have to be continually renewed by buyers of insurance. Of course, these options would necessarily be American so they could be exercised at any time.

Using the Convexity protocol as outlined in the paper, it is already possible to create perpetual options by specifying an expiry date of 0, which means that the option will never expire. At first glance, we can see that the price of the option would be, at maximum, the strike price. More precisely, we could think of the price as the NPV of the expected payout of the option. Imagine that, given all possible prices of the underlying in the future and their probabilities, we determine that, in expectation, the option will be exercised in 5 years for a profit of $1.00 to the buyer. Then, the price of this option should be the (risk-adjusted) NPV of $1.00 received 5 years from now.

If we make the assumptions of Black-Scholes, we can also derive the price of a perpetual option by taking the limit of the equation as time to expiry approaches infinity.

The interesting thing about this option is that, unlike options which have finite expiries, out-of-the-money perpetual options do not decrease in value if the price of the underlying remains stable.

To improve the UX for the buyer, we could have the buyer pay for such a perpetual option periodically (e.g. per block). The writer of this paper is working on designs for perpetual American options in DeFi and for pricing perpetual options.

11 Capital Efficiency

Alice wants to put down as little collateral as possible because there is an opportunity cost to depositing collateral in the system. Therefore, it is a worthwhile goal to reduce the collateral requirement of sellers while maintaining Bob's safety.

Since the maximum payout of a put option is its strike price, the strike price is the maximum value of the option as a buyer could not make more from exercising the option than its strike price. Therefore, if the strike asset and collateral asset are the same, then the strike price should be the maximum value of the collateral requirement. However, for most options, the collateral requirements can be made lower by making some assumptions about the option.

In exchange traded options in traditional finance, the collateral requirement of an options contract is a function of volatility, the price of the underlying asset, and the time until expiry. That is to say, Alice must have as much collateral as the maximum value the option price could increase to in, say, 7 days. For a case like DAI:USDC puts, when physically-settled, need not be fully collateralized. However, estimating implied volatility is very difficult. It is a recursive problem, requiring the option to exist in the first place.

In such a scheme, under normal currencies, the capital efficiency of the protocol is higher for cash-settled than physically-settled options. This is because of the following: Imagine $1.00 strike and we expect DAI to go down to $.80 at worst in one week based on historical volatility. In a physical option, Alice sends maximum $.80 to Bob at expiry. In a cash option, Alice sends max $.20 to Bob at expiry. So, she requires less collateral.

The above undercollateralization could potentially work for DAI:USDC options, but not for cUSDC:USD options. This is because, for cUSDC:USD options, the value of the underlying (cTokens) in this case does not really take a "random walk" in the way that Black-Scholes implies: their value should be steadily increasing (cUSDC increasing in value compared to USDC), until a hack which should immediately decrease their value. Therefore, intuitively, the seller of the put needs to be fully collateralized.

As a result of this complexity, introducing collateral rehypothecation is an area of future work and not necessary for initial implementations of the protocol.

11.1 Insured Token Sets

For ease of use, one could create a token set, using Set Protocol, that couples a put option and its underlying together. For example, an at the money DAI put coupled with DAI could together form a set called "protected DAI." If it were perpetual like the options above, it wouldn't even decrease in value as time passed.

11.2 Multi-Collateral

Like Maker, our protocol would benefit from having multiple uncorrelated collateral assets. In addition, it is best if the collateral in Convexity vaults is uncorrelated with the collateral in systems that back the underlying assets of Convexity options.

11.3 Towards generalized CDP-style synthetics:

At the same time, frameworks like Maker and Yield Protocol provide for Synthetic Assets in a peer to contract manner. We can follow these models to build any one-side collateralized assets. Another large distinction between Yield and Convexity is that, compared to Yield, options contracts, in expectation, decrease in value over time, which should imply more sell-side demand.

Acknowledgments

This paper is heavily based on a number of conversations I had with Robert Leshner of Compound and Dan Robinson of Paradigm who remained helpful throughout the writing of the paper. I also really appreciate Nadir Akhtar, Arjun Balaji, Fred Ehrsam, Brock Elmore, Matt Huang, Apoo Koticha, Matteo Leibowitz, Allison Lu, Ashwin Ramachandran, Tom Schmidt, Roderik van der Graaf, Cyrus Younessi, and Tina Zhen for their thoughts and feedback on the ideas presented in the paper.

A special thanks to Aparna Krishnan and Alexis Gauba for heavy edits, feedback, and brainstorming help when writing this. The paper would not have been possible without them.

References

[1] Rangarajan K. Sundaram, and Sanjiv R. Das. Derivatives: Principles and Practice. McGraw-Hill Education, 2016.

[2] Juliano, Antonio. "dYdX: A Standard for Decentralized Margin Trading and Derivatives." (2017).

[3] Robinson, Dan. "The Yield Protocol: On-Chain Lending With Interest Rate Discovery." Paradigm Research: 2019.

[4] Maker DAO. "The DAI Stablecoin System." 2017.

[5] "UMA: A Decentralized Financial Contract System." 2018.

[6] "High-Yield Securities Disclosure" RBC Wealth Management, RBC Capital Markets, LLC: 2016.

[7] Evans, Alex. "DeFi Liquidity Models". Placeholder VC: 2019.

[8] Leshner, Robert. Hayes, Geoffrey "Compound: The Money Market Protocol." 2019.

[9] Karp, Hugh. Reinis, Melbardis "Nexus Mutual: A peer-to-peer discretionary mutual on the Ethereum blockchain."

[10] Morisander, "The biggest smart contract hacks in history." 2018.

[11] samczsun, "Taking undercollateralized loans for fun and for profit." 2019.

[12] Nexus Mutual Application, https://app.nexusmutual.io/#/SmartContractCover

[13] Urbi Garay, Roxana Justiniano, and Michele Lopez. "The Relationship between Options Moneyness and Liquidity: Evidence from Options on Futures on S&P 500 Index" Journal of Derivatives Use, Trading and Regulation, Vol. 8, No. 4, 2003